KABLOSUZ BİLGİSAYAR AĞLARINDA KULLANILAN WEP GÜVENLİK MEKANİZMASININ VERİ AKTARIM HIZI ÜZERİNDEKİ ETKİLERİ

Mesut ÖZEL

YÜKSEK LİSANS TEZİ
BİLGİSAYAR EĞİTİMİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

MAYIS 2007
ANKARA

Mesut ÖZEL tarafından hazırlanan KABLOSUZ BİLGİSAYAR AĞLARINDA KULLANILAN WEP GÜVENLİK MEKANİZMASININ VERİ AKTARIM HIZI ÜZERİNDEKİ ETKİLERİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Halil İbrahim BÜLBÜL
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Eğitimi Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan: : Prof. Dr. Ali Paşa AYDIN_____

Üye : Prof. Dr. İlhami ÇOLAK_____

Üye : Yrd. Doç. Dr. Halil İbrahim BÜLBÜL_____

Tarih : 22 Haziran 2007

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Mesut ÖZEL

KABLOSUZ BİLGİSAYAR AĞLARINDA KULLANILAN WEP GÜVENLİK MEKANİZMASININ VERİ AKTARIM HIZI ÜZERİNDEKİ ETKİLERİ
(Yüksek Lisans Tezi)

Mesut ÖZEL

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ
MAYIS 2007

ÖZET

Kablosuz Yerel Alan Ağları (WLAN) kullanıcılara sundukları bir çok avantaj nedeniyle tüm dünyada ve Türkiye'de son dönemlerde oldukça hızlı şekilde popülarite kazanmaktadır. Ancak, kablosuz ağlar, sundukları bu avantajlar yanında, sağlıklı şekilde kurulmadıkları, iyi konfigüre edilmedikleri ve yönetilmediklerinde, bazı güvenlik zafiyetlerini de beraberlerinde getirmektedirler. Bu zafiyetlerden en önemlisi güvenlik olup, halihazırda bu zafiyete yönelik olarak üç farklı yaklaşım (Kablolu Eşdeğer Güvenlik-WEP mekanizması, Wi-Fi Kablosuz Erişim Kontrolü-WPA ve Güvenliği Sıkılaştırılmış Ağ-RSN/WPA2 söz konusudur.

Günümüzde kablosuz ağlarda bu mekanizma ve protokollerin hepsi kullanılmakta olup, diğerlerine göre daha eski olan ve en çok kullanılan güvenlik mekanizması WEP'tir. WEP güvenlik mekanizması içerisinde şifresiz iletişim, 40 bit ve 104 bit şifreli iletişim özelliği isteğe bağlı olarak kullanılabilmektedir. Bazı kablosuz cihazlarda ise opsiyonel olarak 232 bit şifreleme de desteklenmektedir. Söz konusu bu şifreleleme işlemi, aralarında veri iletişimi yapılan cihazlara ait mikro işlemciler üzerinde ilave bir iş yükü (overhead) yaratmaktadır. Teorik olarak varlığı bilinen bu iş yükünün veri aktarım hızını etkilemesi, ya da en azından belirli bir dosya büyüklüğünden itibaren olumsuz etkilemesi beklenmektedir. Bu çalışmada; kablosuz ağlarda en

çok kullanılan güvenlik mekanizması olan WEP mekanizmasının içerisindeki şifreleme ve isteğe bağlı diğer özelliklerin teorik olarak öngörüldüğü şekilde veri aktarım hızını olumsuz olarak etkileyip-etkilemediği incelenmiştir.

Bu maksatla bir test ortamı tesis edilmiş, iki adet diz üstü bilgisayar ile tasarsız (ad-hoc / Peer-to-Peer) ağ yapısı oluşturulmuştur. Borland C/C++ programlama dili ile bir veri aktarma programı yazılmıştır. Windows XP işletim marifetiyle ateş duvarı (aktif iken / kapalı iken), şifreleme (Şifresiz / 64 bit şifreli / 128 bit şifreli), dosya boyutu (1 MB, 2 MB, 4 MB, 8 MB, 16 MB, 32 MB ve 64 MB), kimlik doğrulama protokolleri (açık kimlik doğrulama / paylaşımlı kimlik doğrulama) için sıradan bir büro ve elektromanyetik olarak temiz olduğu bilinen Faraday kafesi ortamında 16 800 kez veri aktarımı gerçekleştirilmiştir. Veri aktarım hızının tespiti maksadıyla her bir dosya 2 400 kez diğer bilgisayara aktarılmış ve aktarım süreleri kaydedilmiştir. Toplanan veriler varyans analizi ile istatiksel incelemeye tabi tutulmuş ve öncelikle şifresiz iletişim ile 64 bit şifreli iletişim, 64 bit şifreli iletişim ile 128 bit şifreli iletişim ve şifresiz iletişim ile 128 bit şifreli iletişim arasında fark olup-olmadığı incelenmiştir. İlave olarak ateş duvarı, kimlik doğrulama protokolü ve dosya boyutunun veri aktarım hızına etkileri de incelenmiş ve elde edilen tüm değerlendirmeler sonuç ve öneriler bölümünde ortaya konulmuştur.

Bilim Kodu : 702.3.006
Anahtar Kelimeler : Kablosuz Ağ Güvenliği, WLAN, WEP, WPA, RSN.
Sayfa Adedi : 123
Tez Yöneticisi : Yrd. Doç. Dr. Halil İbrahim BÜLBÜL

THE AFFECTS OF WEP (WIRED EQUIVALENT PRIVACY) SECURITY MECHANISM OVER DATA THROUGHPUT IN WIRELESS NETWORKS (M.Sc. Thesis)

Mesut OZEL

GAZI UNIVERSITY
INFORMATICS INSTITUTE
MAY 2007

ABSTRACT

Recently, Wireless Local Area Networks (WLANs) are gaining popularity worldwide and in Turkey due to the advantages offered for the users. On the other hand, WLANs bring some security drawbacks associated with them. Those security drawbacks occur mainly for the improper installations and configurations of WLANs. One of the most important drawbacks is security, where there are three different approaches for security needs in WLANs, namely WEP mechanism, WPA protocol and RSN protocol.

Where WEP, WPA and RSN/WPA2 security mechanism/protocols that are available in the market, of the three, the most preferred and widely used one is WEP Mechanism. In WEP, unencrypted, 40 bits encrypted and 104 bits encrypted communications are possible. In some wireless hardware produced by different firms the 232 bits of encryption is also embedded and supported optionally. This optional encryption process causes an overhead (encryption on the sender part and decryption on the receiver part) on the microprocessors of the computers that communicate with each other. It is anticipated that the theoritical overhead, that is definitely known to be present, affects the wireless data throughput due to the reciprocal encryption-decryption process. In this thesis, it is aimed to reach a conclusion if the encryption and other optional

parameters in WEP mechanism affect the data throughput as it is expected theoretically.

A test bed has been prepared to test the theoretical affects of the encryption process. Two notebook computers were connected to form an Ad Hoc (Peer-to-Peer) mode network. Then a Borland C/C++ code created to manage the data throughput. In order to understand the affects; with the help of Windows XP operating system, firewall status (Firewall on / Firewall Off), encryption status (No encryption / 64 bits key / 128 bits key), file size (1 MB, 2 MB, 4 MB, 8 MB, 16 MB, 32 MB, 64 MB) and authentication protocols (Open / Shared Authentication) were tested by running Borland C/C++ code 16 800 times. The data were collected in both a regular office and a Faraday Cage which is known to be clean electromagnetically. For the data throughput each file copied to the target computer 2 400 times and process times were recorded via the Borland C/C++ code. The data collected were then put through variance analysis (ANOVA – Analysis of Variances) test in order to understand if there was a difference of means for the affects of encryption status (No encryption vs. 64 bits key, 64 bits key vs. 128 bits key, No encryption vs. 128 bits key). Additionally, the affects of firewall status, authentication protocols and file size over data throughput were assessed and the overall results are listed in conclusions and recommendations part.

Science Code : **702.3.006**
Key Words : **Wireless Network Security, WLAN, WEP, WPA, RSN**
Page Number : **123**
Adviser : **Ass. Prof. Dr. Halil Ibrahim BULBUL**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, akademik açıdan her türlü desteği veren danışmanım ve hocam Sayın Yrd. Doç. Dr. Halil İbrahim BÜLBÜL'e, bilgi ve bilgisayar güvenliği konusunda desteğini hiç esirgemeyen Sayın Doç. Dr. Şeref SAĞIROĞLU'na, beni yetiştirip bu günlere getiren anne ve babama, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan sevgili eşim Funda ÖZEL'e ve yüksek lisans eğitimi ile tez çalışmalarım esnasında kendisine daha az vakit ayırmamdan hiç şikayetçi olmayan oğlum Kaan Ata ÖZEL'e teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER, KISALTMALAR VE TANIMLAR

Bu çalışmada kullanılmış bazı simgeler, kısaltmalar ve tanımlar açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
802.11	Wireless Networks Family Kablosuz Ağlar Ailesi
Bit	Bilişimde kullanılan en küçük bilgi birimi (0 veya 1).
ID	Identification Kimlik Bilgisi
K	Thousand Bin
KHz	Kilohertz (10^3 Hertz) Kiloherz
Mbps	Megabit (10^6 Bit) per second Mega bit bölü saniye
MHz	Megahertz (10^6 Hertz) Megaherz
s	Saniye
RC4	Rivest Şifreleme Algoritması
XOR	Girişlerden sadece birisi 1 ise, çıkışı 1 olan mantıksal işlem.

Kısaltmalar	**Açıklama**
AES	Advanced Encryption Standart Gelişmiş Şifreleme Standardı
AKD	Açık Kimlik Doğrulama
AP	Access Point Erişim Noktası
ARP	Address Resolution Protocol Adres Çözümleme Protokolü
CCK	Complementary Code Keying Tamamlayıcı Kod Anahtarlama
CRC	Cyclic Redundancy Check
DLL	Data Link Layer Veri Bağı Katmanı
DOS	Denial of Service Hizmet Reddetme
EAP	Extensible Authentication Protocol Genişletilebilir Kimlik Doğrulama Protokolü

IEEE	The Institute of Electrical and Electronic Engineers Elektrik ve Elektronik Mühendisleri Enstitüsü
ICV	Integrity Check Value Bütünlük Kontrol Değeri
IV	Initialization Vector Başlama Vektörü
KDC	Key Distribution Center Anahtar Dağıtım Merkezi
KEK	Key Encryption Key Anahtar Şifreleme Anahtarı
LAN	Local Area Network, Yerel Alan Ağı
LLC	Logical Link Control Mantıksal Bağ Kontrolü
MAC	Media Access Control Ortam Erişim Kontrolü
MAN	Metropolitan Area Network Metropol Alan Ağı
MIC	Message Integrity Code Mesaj Bütünlük Kodu
MIM	Man in the Middle Aradaki Adam
NIC	Network Interface Card Ağ Bağlantı Arabirimi/Kartı
OSI	Open System Interconnection Açık Sistem Mimarisi
PAN	Personal Area Network Kişisel Alan Ağı
PC	Personal Computer Kişisel Bilgisayar
PCI	Peripheral Component Interconnect Çevresel Birim Bağlantısı
PCMCIA	Personal Computer Memory Card Kişisel Bilgisayar Hafıza Kartı
PDA	Personal Digital Assistant, Cep Bilgisayarı veya Kişisel Sayısal Yardımcı
PHY	Physical Layer Fiziksel Katman
PMK	Pairwise Master Key Çiftli Ana Anahtar
PKD	Paylaşımlı Kimlik Doğrulama
PKE	Public Key Encryption Açık Anahtar Şifreleme
PKI	Public Key Infrastructure Açık Anahtar Alt Yapısı
PSK	Pre-Shared Key Önceden Paylaşılmış Anahtar

PTK	Pairwise Transient Key Çiftli Geçici Anahtar
P-WLAN	Public WLAN Kamuya/Halka Açık WLAN
RADIUS	Remote Authentication Dial-In User Service Uzak Bağlantı Kullanıcı Doğrulama Hizmeti
RC	Rivest Cipher Rivest Şifresi
RF	Radio Frequency Telsiz Frekansı
RSN	Robust Security Network Güvenliği Sıkılaştırılmış Ağ
SSL	Secure Sockets Layer Güvenli Soket Katmanı
TKIP	Temporal Key Integrity Protocol Geçici Anahtar Entegrasyon Protokolü
TSC	TSC - TKIP Sequence Counter TKIP Dizi Sayacı
VPN	Virtual Private Network Sanal Özel Ağ
WEP	Wired Equivalent Privacy Kablolu Eşdeğer Güvenlik
Wi-Fi	Wireless Fidelity Kablosuz Bağlılık
WLAN	Wireless Local Area Network Kablosuz Yerel Alan Ağı
WPA(2)	Wireless Protected Access-2 Kablosuz Erişim Kontrol Protokolü-2
WPAN	Kablosuz Kişisel Alan Ağı, Wireless Personal Area Network
WWAN	Wireless Wide Area Network Kablosuz Geniş Alan Ağı

Tanımlar	**Açıklama**
Altyapılı Ağ / Infrastructure Mode Network	Kablosuz ağların daha çok tercih edilen kullanım şekli olan altyapı çalışma modeli; kablolu ağa bağlı bir erişim noktası ve belirli sayıda kablosuz erişim özelliğine sahip cihaz ve bilgisayardan oluşan ağdır.
Bilgisayar Ağları	Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan bilgi sistemleri çalışma biçimine bilgisayar ağı (Computer Network) denilmektedir.

Elektromanyetik Dalga	Uzayda ya da maddesel bir ortamda yayılan elektrik alanı ve manyetik alan dalgalarının ortak adıdır. Kozmik, gama, x, morötesi, görünür bölge, kırmızı altı, mikrodalga, TV, radyo dalgaları elektromanyetik dalgalardır.
Erişim Noktası	Birden fazla bilgisayarı kablosuz olarak bir birine bağlayan veya İnternet bağlantılarını sağlayan, almış olduğu kablosuz ağ sinyalini tekrar güçlendirip yayınlayarak mesafeyi ve sinyal kalitesini artıran bir cihazdır.
İstemci Cihaz	Ağa bağlanmak isteyen ve kimlik doğrulama isteğinde bulunan kullanıcıdır.
Kablosuz Yerel Alan Ağları	Kablosuz yerel alan ağları iletişim için kablo yerine elektromanyetik radio frekans sinyallerini kullanan bir ağ şeklidir.
Kimlik Doğrulama Sunumcusu	RADIUS gibi asıllama hizmetleri için kurulmuş bir sunumcu cihazdır.
Kimlik Doğrulayıcı	İstemci cihaz ile kimlik doğrulama sunumcusu arasındaki erişim noktasıdır.
Tasarsız Ağ / Ad Hoc Ağ / Peer-to-Peer Ağ	İki ya da daha çok kablosuz iletişim özelliğine sahip bilgisayarın, bir sunumcu ve/veya erişim noktası cihazı olmadan birbirlerine bağlandığı kablosuz ağlardır.
Topoloji	Bilgisayarların birbirleri ile iletişiminin hangi hiyerarşik düzende olduğu mimari yapı (Topology) olarak ifade edilmektedir.

1. GİRİŞ

Kablosuz bilgisayar ağları, kablolu ağlara alternatif olarak tek başına veya kablolu ağların uzantısı olarak çalışabilen, kablolu ağlar tarafından sunulan tüm fonksiyonların sunulduğu, hareket gerektiren ve fiziksel alandan bağımsız olması istenilen uygulamalarda tercih edilen, kablolama alt yapısı için harcanan zaman ve maliyetten tasarruf sağlayan, kullanıcılara istenilen yer - zamanda ağa bağlanma ve ağ üzerindeki kaynakları ortak kullanma imkanı sunan, kullanıcı tanımlama, silme ve yer değiştirme işlemleri için ağ yöneticilerine esneklik sağlayan, kurulumu ve yönetimi daha kolay olan bir bilgi işlem ve veri iletişim ağıdır [1].

Modern kablosuz iletişim, 1800'lü yılların sonunda elektromanyetik dalgaların keşfedilmesiyle başlamış, ses kablosuz olarak ilk kez 1900 yılında taşınmış, 1920 yılında ise radyo telgraf ve radyo telefon teknolojilerine geçilmiş, 1940'lı yıllarda kısa dalga boyları üzerinden radyo mesajları taşınmış, 1950'li yıllara gelindiğinde kıtalar arasında ses ve telgraf mesaj alış-verişi gerçekleştirilmiştir. Kablosuz teknolojideki bu gelişmelere paralel olarak 1950'li yıllarda ilk kişisel bilgisayarın piyasaya sürülmesinin ardından bilgisayar ağlarının ilk uygulamaları da 1960'lı yılların sonlarında başlamış, yerel bilgisayar ağlarının yaygınlaşması ise 1980'li yıllarda gerçekleşmiştir.

Kablosuz teknoloji gelişimini, 1983 yılında hücresel teknoloji ve telefonların ortaya çıkması ile sürdürmüştür. Bu gelişmelere paralel olarak 1990'lı yıllardan itibaren IEEE tarafından kablosuz ağ standartlarının ortaya konulması ve kablosuz internet teknolojilerinin hızlı gelişimi, ağ tasarımcı ve üretici firmaları bilgisayar ağlarına yönelik kablosuz çözümler için cesaretlendirmiştir [2].

Bir bilgi sistem ağı, tek bir kişisel bilgisayarın işletim sisteminin yetenek ve özelliklerine oranla kullanıcılarına; programların ve dosyaların paylaşımı, ağ kaynaklarının paylaşımı, hata toleransı, disk önbelleği, elektronik posta, çalışma grubu, merkezi yönetim, kayıt koruma, güvenlik, uzaktan erişim, ekonomi, hafıza optimizasyonu gibi çok daha üstün özellikler ve yetenekler sunmaktadır.

Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan bilgi sistemleri çalışma biçimine bilgisayar ağı (Computer Network) denilmektedir. Bir bilgisayar ağında çok sayıda bilgisayar, yazıcı, tarayıcı vb. cihaz yer alabilmektedir. Klasik anlamdaki yerel alan bilgisayar ağları (Local Area Networks - LAN) üzerindeki cihazlar arasındaki bağlantı genellikle kablolar ile sağlanmaktadır. Kablo bağlantısının ekonomik, verimli ve mümkün olmadığı durumlarda radyo frekansı, mikro dalgalar ve uydular aracılığıyla da bilgi sistem ağı ağ içerisindeki cihazlar arasında bağlantı ve iletişim kurulabilmektedir.

Kablosuz yerel alan ağı (Wireless Local Area Networks - WLAN), iletişim için kablo yerine elektromanyetik RF sinyallerini kullanan ve avantajları nedeniyle kablolu ağların yerine kullanılan hatta bu ağlara göre daha üstün özellikleri bulunan bir ağ şeklidir. Bazı veri hızı kısıtlamaları dışında kablosuz ağ kullanılarak gerçekleştirilen veri iletişimi, geleneksel yerel alan ağları iletişim teknolojilerinin tüm özelliklerini kapsamakta hatta daha da fazla özellik içerebilmektedir.

Kablosuz bilgisayar ağlarının son dönemlerde yoğun olarak kullanılmaları ile ilgili olarak 2005 yılında yapılan araştırmalara göre kablosuz ağ kullanıcılarının tercih nedenleri yüzde olarak aşağıda sunulmuştur [3-4].

i. Kablolama Maliyeti : % 61
ii. Kampüs ve bina içi gezginlik : % 39
iii. Ağa cihaz ekleme ve çıkarma esnekliği : % 38
iv. Genel esneklik : % 30
v. Ağa cihaz ekleme ve çıkarma işgücü maliyeti : % 28
vi. Uygunluk (Bağlantı yapma ihtiyacı olmaması) : % 25
vii. Üretkenlik artışı : % 22
viii. Kolaylık maliyeti / ofis kullanımı : % 17
ix. İşbirliği ve koordinasyon kolaylığı : % 15
x. Zaman kazanımı (Etkinlik artışı) : % 14

Bu nedenlere ilave olarak kablosuz ağ teknolojisinin gelişmeye ve evrim geçirmeye devam ettiği ve kablosuz ürünlerin maliyetinin düşmekte olduğu da dikkatlerden kaçmaması gereken bir başka etkendir.

Bu bağlamda, internet üzerinde bulunan çeşitli araştırmalara göre 2010 yılında dünyadaki en zengin ilk 2000 (Fortune 2000) listesinde bulunacak şirketlerin büyük bir çoğunluğunun kablosuz ağ kuracağı tahmin edilmektedir.

Kablosuz ağlar için IEEE tarafından geliştirilen 802.11x standartlar ailesinde kablolu ağ düzeyinde fiziksel koruma sağlamak üzere geliştirilen ilk mekanizma Kablolu Eşdeğer Güvenlik (Wired Equivalent Privacy - WEP) mekanizmasıdır. WEP mekanizmasının güvenlik kapsamında istenilen başarıyı sağlayamaması nedeniyle, Kablosuz Korumalı Erişim (Wi-Fi Protected Access - WPA) güvenlik protokolü geliştirilmiş, ancak bu protokolde de bazı sakıncaların belirlenmesini müteakip kablosuz ağlardaki güvenlik zafiyetlerini gidermek maksadıyla daha güçlü bir güvenlik öngören IEEE 802.11i standardı geliştirilmiştir. 2004 yılında onaylanan ve IEEE tarafından geliştirilen 802.11i standardı kapsamında Güvenliği Sıkılaştırılmış Ağ (Robust Security Network - RSN/WPA2) olarak adlandırılan güvenlik protokolü literatür ve kablosuz ağ teknolojisindeki yerini almıştır.

Günümüzde kablosuz ağ donanım ve yazılımları kapsamında her üç güvenlik mekanizma ve protokolü de satın alınan ürünler ve mevcut teknoloji kapsamında desteklenmektedir. WEP mekanizması neredeyse piyasada mevcut tüm kablosuz cihazlar tarafından desteklenmekte olup, WPA ve RSN için ise ilave maliyet ödenmesi gerekmektedir. Bu kapsamda WEP mekanizması daha eski olmasına rağmen; daha ekonomik olması, daha çok ürün tarafından desteklenmesi ve hali hazırda daha geniş bir kullanıcı grubu tarafından kullanılması nedeniyle diğerlerine nazaran daha çok tercih edilen bir güvenlik mekanizması olarak varlığını sürdürmektedir.

2006 yılı itibariyle gelişmiş ülkelerde kablosuz ağların yaklaşık yarısında güvenlik mekanizma ve protokollerinin kullanılmadığı, güvenlik mekanizma ve protokollerini

kullanılan ağlarda; Londra (İngiltere)'da % 76'sının, Seattle'da (ABD) ise % 85'inin güvenlik için WEP mekanizmasını kullandığı [5], yine gelişmiş ülkelerden Almanya'da ise kablosuz ağlarda güvenlik mekanizma ve protokollerinin % 75-% 80 civarında kullanıldığı, bunlar içerisinde % 59,4 (2006 yılı için) ve % 46,3 (Mart 2007 için) oranında WEP güvenlik mekanizmasının kullanıldığı bilinmektedir [6].

Türkiye açısından konu ele alındığında kablosuz ağlarda ne oranda güvenlik mekanizma ve protokollerinin kullanıldığı, bunlar arasında WEP, WPA veya RSN (WPA2)'nin ne oranda kullanıldığı ile ilgili bir kaynak bulunmamaktadır. Gelişmiş ülkelerdeki durum dikkate alındığında Türkiye açısından kablosuz ağlarda güvenlik mekanizma ve protokollerinin kullanım oranının çok daha düşük olacağı ile kullananlarda da WEP kullanım oranının çok yüksek olacağı tahmin edilmektedir.

WEP güvenlik mekanizmasının kullanım oranının yüksek olması, herkes tarafından kolayca elde edilebilmesi ve maliyet açısından tercih edilmesi nedenleriyle WEP güvenlik mekanizması üzerinde detaylı bir inceleme yapılmıştır. Yapılan incelemede WEP içerisinde güvenlik sağlamak üzere bir takım ilave süreçler ve şifreleme işlemleri gerçekleştirildiği belirlenmiştir. Şifresiz iletişime oranla WEP güvenlik mekanizması tarafından yaratılan bu ilave iş yükünün kablosuz iletişimdeki veri aktarım hızına olumsuz etkisinin olup-olmadığının belirlenmesinin faydalı olacağı değerlendirilmiştir.

Bu çalışmada kablosuz ağlarda kullanılan ve kablolu ağlara eşdeğer bir güvenlik sağlamak üzere IEEE tarafından geliştirilen WEP güvenlik mekanizması içerisinde isteğe bağlı olarak kullanılan şifresiz iletişim, 40 bit şifreli iletişim ve 104 bit şifreli iletişim seçeneklerinin, veri aktarım hızına etkisinin olup-olmadığının belirlenmesi amaçlanmaktadır. WEP güvenlik mekanizması aktif iken, kablosuz olarak gönderilen ve alınan paketlerin tümünü özel bir takım süreçlerden geçirerek bir şifreleme algoritmasına tabi tutulmaktadır. Söz konusu bu özel süreç ile birlikte şifreleme işlemi nedeniyle, şifresiz iletişime nazaran, mikro işlemci üzerinde ilave bir iş yükünün (overhead) yaratıldığı teorik olarak bilinmektedir. Bu nedenle şifrelemenin veri aktarım hızını düşürmesi beklenmektedir.

2. KABLOSUZ AĞLAR VE GÜVENLİK

Kablosuz ağ kullanıcısı, pahalı ve zahmet gerektiren bir kablolama alt yapısı kurmak yerine, temel olarak içerisinde küçük bir RF (Radyo Frekansı) alma-gönderme birimi barındıran erişim noktaları (Access Point - AP) ile kablosuz iletişime uygun istemci cihazlar arasında veri alış-veriş ortamı sağlayabilmekte ve kolaylıkla kablosuz bir yerel alan ağı oluşturabilmektedir [7-8]. Bu kapsamda bu bölümde önce kablosuz ağların temel özellikleri, sonra kablosuz güvenlik konusu incelenmiştir.

2.1. Kablosuz Ağlarda Kullanılan Temel Donanımlar

Kablosuz ağlarda kullanılan temel donanımlar 3 başlık altında toplanmaktadır [9].

Kablosuz Ağ Kartları ve Adaptörler: Bu kart ve adaptörler (PCMCIA, PCI, Cardbus, USB vb.) kullanıcıların ağa, bir anten aracılığıyla ve kablosuz olarak erişmesi için gerekli fonksiyonları sunmaktadırlar.

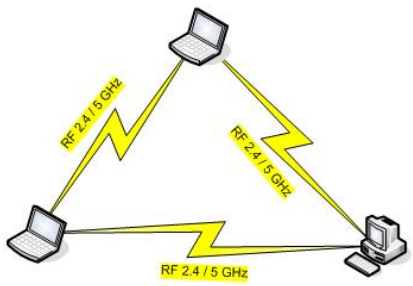
Erişim Noktaları (Access Points - AP): Temelde bir erişim noktası (Access Point - AP) konumundaki kablosuz bir cihaz, kablolu ortamda çalışan bir anahtar ve/veya hub cihazına karşılık gelmektedir.

Açık Alan Ağ Köprü Cihazları (Outdoor LAN Bridges): Açık alan köprü cihazları, birbirlerine yakın olan binalardaki mevcut ağ ve alt yapıyı birbirlerine kablosuz olarak bağlamak için kullanılmaktadır.

2.2. Kablosuz Ağların Mimari Yapıları

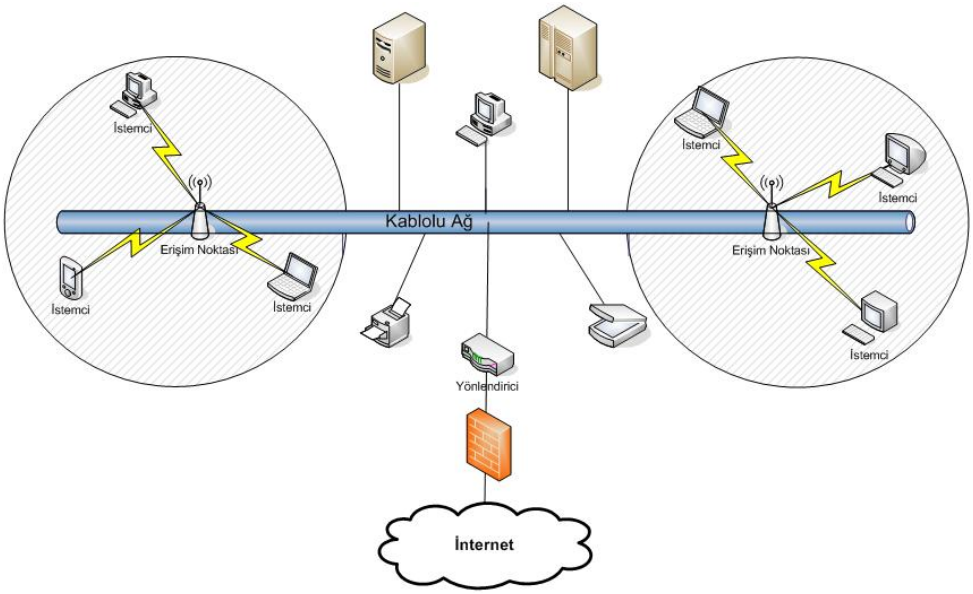
Bilgisayarların birbirleri ile iletişiminin hangi hiyerarşik düzende olduğu mimari yapı (Topoloji - Topology) olarak ifade edilmektedir. Kablosuz ağlarda cihazdan-cihaza (Peer-to-Peer / Ad Hoc Mode) ve altyapılı usta-çırak (Infrastructure - Client/Server) olmak üzere iki çeşit mimari yapı kullanılmaktadır [1-2, 7-8, 10-12].

Cihazdan - Cihaza Çalışma Modeli - Tasarsız Ağ (Peer-to-Peer / Ad Hoc Mode): Cihazdan-cihaza çalışma modeli; iki ya da daha çok kablosuz iletişim özelliğine sahip bilgisayarın, bir sunumcu ve/veya erişim noktası cihazı olmadan birbirlerine bağlandığı, tipik örneği Şekil 2.1.'de sunulan kablosuz ağlardır.



Şekil 2.1. Cihazdan - Cihaza çalışma modeli - Tasarsız ağ - Ad Hoc modu.

Altyapı çalışma modeli (Infrastructure Mode): Kablosuz ağların daha çok tercih edilen kullanım şekli olan altyapı çalışma modeli; kablolu ağa bağlı bir erişim noktası ve belirli sayıda kablosuz erişim özelliğine sahip cihaz ve bilgisayardan oluşmaktadır. Temel altyapı çalışma modeli Şekil 2.2.'de sunulmuştur.



Şekil 2.2. Altyapı çalışma modeli.

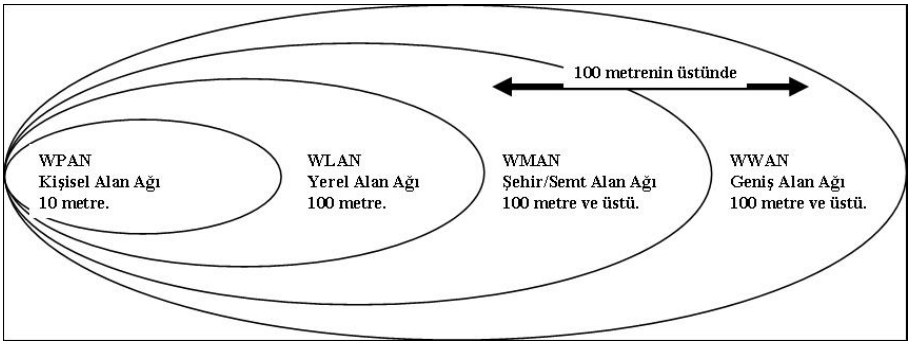
2.3. Kablosuz Ağların Kullanım Alanları

Kablosuz ağlar, eğitim, sağlık, lojistik ve benzeri sektörlerde faaliyet gösteren kamu kurum ve kuruluşlarının yanı sıra, küçük, orta ve büyük ölçekli işletmelerde, iş adamları, yöneticiler, çalışanlar, müşteriler, günlük kullanım için ev içi çoklu erişim kullanıcıları ve bireysel kullanıcılar gibi geniş bir yelpazede bulunan kullanıcılara, internete erişim ve/veya üyesi oldukları kurumsal ağa kablosuz olarak bağlanma imkanı sağlamaktadır.

Ayrıca toplu yaşantının sürdürüldüğü restoranlar, otobüs terminalleri, oteller, büyük alışveriş merkezleri, tren istasyonları, hava alanları, kalabalık cadde ve sokaklar gibi kamuya açık alanlarda oluşturulan ücretli veya ücretsiz (Erişim Alanları – Hot Spots) vasıtasıyla sunulan kablosuz internet erişim hizmetinin de hızla artmaya devam edeceği öngörülmektedir. İnternet üzerinde sürekli güncellenen http://jiwire.com/ sitesine göre 07 Kasım 2006 tarihi itibariyle dünya genelinde 130 ülkede ücretli ve ücretsiz olmak üzere toplam 129 187 adet, Türkiye'de ise başta büyük şehirlerimizde olmak üzere toplam 466 adet erişim alanı bulunmaktadır.

2.4. Kablosuz Ağların Gruplandırılması

Özel amaçlı, eğitim amaçlı, ulusal veya halka açık olarak kurulabilen kablosuz iletişim ağlarını, hizmet yapısı, çalışma prensipleri, büyüklük veya mimarisine (topoloji) göre olmak üzere farklı şekillerde gruplandırmak mümkündür.



Şekil 2.3. Kablosuz ağlarla ilgili mesafe bazında gruplandırma.

Kişisel ihtiyaçlar için ev veya işyeri içerisinde kurulacak 10 metre mesafeli kablosuz ağlardan, 100 metrenin çok daha üzerindeki semt, şehir veya daha büyük alanlardaki farklı ağ uygulamalarına kadar geniş bir yelpazede kablosuz ağ kurulumu mümkündür. Genellikle literatürde temel alınan kablosuz ağlarla ilgili mesafe bazında sınıflandırma Şekil 2.3.'de sunulmuştur [1-2, 7-8, 11-13].

2.5. Kablosuz Ağların Fayda ve Mahzurları

Geleneksel kablolu ağlara nazaran kablosuz ağlar genel hatları ile üretkenlik, hizmet etkinliği, hareketlilik, bağımsızlık ve maliyet açısından çeşitli faydalar sağlamaktadırlar [1, 4, 8, 11, 14-15]. WLAN'ların kullanıcılara sağladığı avantajlar ve geleneksel kablolu yerel alan ağlarına karşı belli başlı üstünlükleri ile ilgili tespitler aşağıda sunulmuştur.

i. Çalışma ortamından bağımsız olma ve hareketlilik imkanı sayesinde kullanıcılar, kendi organizasyonlarının kapsama alanı içerisinde her an gerçek zamanlı bilgiye erişebilmektedirler. Bu imkan, kablolu ağlarda bulunmayan hareketlilik, üretkenlik artışı sağlamakta ve bunlara bağlı hizmet kalitesini olumlu yönde etkilemektedir.

ii. Bina içerisinde duvarların, tavan veya tabanın delinmesini, çalışma odalarına sevk edilen hat uçlarının tespitini, montaj ve sonlandırma işlemleri gerektirmediğinden ve kabloların bir kanal ile bina içerisindeki taşınması zorunluluğu yaratmadığından kablosuz ağların kullanıma açılması kolay ve hızlı bir şekilde gerçekleştirilmektedir.

iii. Kablosuz ağların kurulma kolaylığı ve yeni erişim noktaları kullanılarak genişletilebilme imkanları ile kablolu ağların erişemeyecekleri yerlere erişme yetenekleri sayesinde sağladıkları esneklik büyük bir avantaj sağlamaktadır.

iv. Kurulum ve kullanım maliyetleri kapsamında, her ne kadar kablosuz ağların kurulumu için gerekli donanımların temel maliyetleri kablolu ağlara oranla yüksek görünse de, ömür boyu maliyet açısından ortaya çıkacak toplam maliyet daha düşük olmaktadır. Özellikle sık sık yer değiştirme, sürekli büyüme ve genişleme, kullanıcı ekleme ve çıkarma yapılan dinamik organizasyonlarda kullanılan kablolu ağlarda uzun dönemli maliyet etkinlik oranları çok daha yüksek olmaktadır.

v. Kablosuz ağlar çok farklı özel ihtiyaçlar ve uygulamalar kapsamında geniş bir topoloji yelpazesi içerisinde yapılandırılabilmektedirler. Konfigürasyon değişiklikleri kolayca gerçekleştirilebilmekte ve kablosuz ağ yapıları düşük sayıdaki kullanıcıların bir arada çalışmasına imkan sağlayan bire-bir (peer-to-peer mode) topolojiden, geniş bir alan içerisinde hareket imkanı tanıyan ve binlerce kullanıcının kullanabildiği tam alt yapılı (full-infrastructure mode) topolojiye kadar değişmektedir.

WLAN Sistemlerinin pek çok avantajının yanı sıra çeşitli dezavantajları da bulunmaktadır. Başlangıçta çok daha yoğun olan sorunlardan standartlaşma, ürün çeşitliliği, maliyet ve frekans tahsisi gibi konular günümüzde nispeten çözülmüş bulunmaktadır. Ancak halen aşağıda belirtilen sorunların, son kullanıcılar için birer dezavantaj olarak varlıklarını sürdürdükleri düşünülmektedir.

i. Pratikte, kablosuz bir ağ tek başına genellikle ilgili kurum veya kuruluşun tüm ihtiyacını karşılayamamakta, yüksek seviyeli geniş bant hizmetleri için ağ temel iskeleti olarak kablolu bir ağın alt yapısına ve daha önceden kurulmuş olmasına ihtiyaç duymaktadır.

ii. Erişim noktası ile istemci cihaz arasına girebilecek olası engellerden (duvar, cam, kapı, ofis malzemeleri vb.) etkilenmeyi azaltmak için ağın ilk kurulum ve tesis maliyetini artıran ilave erişim noktalarının tesis edilmesi gerekmektedir.

iii. Kablosuz ağı kullanan istemci cihaz sayısı arttıkça ve erişim noktalarından mesafe olarak uzaklaştıkça her bir cihaz başına düşen verim göreceli olarak azalmaktadır.

iv. Kablosuz ağlarla ilgili standartların sürekli değişmesi ve gelişmesi, kullanılan teknolojinin zaman içerisinde değiştirilmesi, yenilenmesi veya güncellenmesi gerekliliğini ortaya çıkarmaktadır. Günümüzde kablosuz ağ standartları, kablolu ağ standartlarına oranla daha hızlı şekilde geliştirilmektedir.

v. Kablosuz ağların genel kullanımı arttıkça, özellikle 2,4 GHz frekans bandında çalışan kablosuz ağlarda, karışıklık ve enterferans oluşma ihtimali artmaktadır.

vi. Kablosuz ağlarda güvenliğin garantili şekilde sağlanması oldukça zor, sürekli takip edilmesi gereken ve uğraş gerektiren bir işlemdir.

Kablosuz ağların avantajları ile dezavantajlarının incelenmesi neticesinde bu tür ağların sunduğu imkan ve kolaylıkların daha fazla olduğu değerlendirilmektedir. Ancak, kablosuz ağların kablolu ağlara nazaran tüm bu avantajlarına rağmen kötü niyetli saldırıları engellemek ve izinsiz kullanımları önlemek kapsamında güvenlik açısından ciddi dezavantajlar yaratmalarının da dikkate alınması gereken en önemli hususlardan birisi olduğu düşünülmektedir.

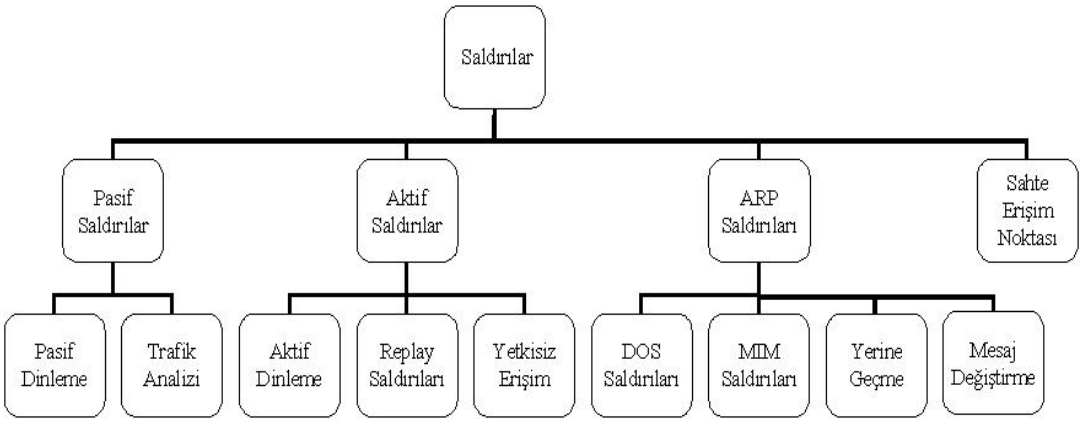
2.6. Kablosuz Ağ Güvenliği

Kablosuz ağ teknolojisinin ortaya çıktığı ilk dönemlerden itibaren güvenlikle ilgili zafiyetlerinin varlığı temel bir problem olarak görülmüştür. Güvenlikle ilgili olarak gerçekleştirilen tüm çalışmaların temelinde, bu teknolojinin kablolu ağların yerini alması maksadıyla gerekli güvenlik ihtiyaçlarının giderilmesi birinci öncelikli bir konu başlığı olmuştur.

Kablosuz ağların güvenliğinin sağlanması oldukça zor görünse de, bu zorlukların çoğunun makul güvenlik önlemleriyle aşılabileceği bilinmektedir. Makul önlemler ile aşılabileceği düşünülen ve literatürde kablosuz ağların dezavantajları olarak ortaya konulan güvenlikle ilgili riskler ve problemler ana başlıklar halinde sonraki sayfada sunulmuştur [7-8, 16-18].

i. Ağa kolay erişim imkanı bulunması,
ii. Yetkisiz hizmet kullanımı için hedef olması,
iii. MAC aldatma ve oturum ele geçirme saldırılarına maruz kalması,
iv. Trafik analizi ve dinlemeye maruz kalması,
v. Sahte erişim noktalarının kolayca kurulabilmesi,
vi. Diğer üst seviyeli saldırılara hedef olması.

Yukarıda kablosuz ağlarla ilgili olarak ortaya konulan güvenlik risk ve problemlerini destekler biçimde ve gerçekleştirilen saldırılar kapsamında kablosuz ağlarda dikkate alınması gereken toplam on farklı saldırı türü Şekil 2.4.'de sunulmuştur. Bunlar kabaca, pasif saldırılar, aktif saldırılar, ARP saldırıları ve sahte erişim noktası (Rouge Access Points) saldırıları olmak üzere dört ana başlıkta toplanmaktadır. *Pasif saldırılar;* pasif dinleme (Passive eavesdropping) ve trafik analizini (Traffic analysis), *aktif saldırılar;* aktif dinleme (Active eavesdropping), Replay saldırıları ve yetkisiz erişimi (Unauthorized Access), *ARP saldırıları ise;* DOS (Denial of Service), MIM (Man in the Middle), yerine geçme (Masquareding), oturum ele geçirme (Session Highjacking) ve mesaj değiştirmeyi (Message Forgery) kapsamaktadır. Bu saldırı türlerinden üçü (Trafik analizi, Pasif dinleme, Aktif dinleme) oturumun güvenlik ve gizliliğini, MIM saldırısı gizlilik ve doğruluğu, diğerleri ise ağ güvenliği, trafik ve verinin doğruluğunu ihlal etmektedir [18-20].



Şekil 2.4. WLAN saldırıları.

Söz konusu saldırı teknikleri kapsamında saldırganlar tarafından yapılacak girişimlerin önlenmesi maksadıyla güvenlikle ilgili tüm uzmanlar tarafından belirtildiği şekilde, bilgi sistemleri üzerinde bulunan bilgiye ait temel veri güvenliği bazı temel kriterler ile tanımlanmaktadır. Bu temel kriterlerin hepsi güvenli bir ağ ve bilgi güvenliği için sağlanması zorunlu kriterler olarak değerlendirilmekte olup, aşağıda sunulmuştur [16, 20-23].

i. Gizlilik (Secrecy - Confidentiality)
ii. Bütünlük (Integrity)
iii. Hazır olma (Availability)
iv. Kimlik doğrulama (Authentication)
v. İnkar edememezlik (Non-repudiation)

Kablosuz ağ uygulamalarında genel hatlarıyla yukarıda belirtilen saldırı teknikleri kapsamında belirlenen ve otoritelerce ortaya konulan beş temel güvenlik kriteri ile ilgili hassasiyetleri ortaya koymak amacını taşımaktadır. Bu bağlamda; WEP, WPA ve RSN güvenlik protokollerinin, tarihi süreçleri içerisinde sırasıyla incelenmesinin faydalı olacağı düşünülmektedir.

Söz konusu güvenlik protokolleri arasında, literatüre ilk giren kablosuz güvenlik mekanizması WEP olduğundan WPA ve RSN mekanizmalarından daha geniş bir şekilde ele alınacaktır. WPA ve RSN olarak anılan sonraki protokoller, WEP'in kullanılmaya başlanmasıyla ortaya çıkan zafiyetlerini gidermeye yönelik olarak geliştirildiklerinden, ve bu güvenlik protokollerinin evrimsel bir gelişim göstermeleri nedeniyle birbirlerinin devamı şeklinde düşünülmeleri bir hata olmayacaktır. Yine aynı çerçevede RSN güvenlik protokolü de WPA'nın zafiyetlerini gidermeye yönelik olarak ortaya atılmıştır ve IEEE 802.11i standardının öngörü özelliklerine sahiptir.

Kablosuz ağ güvenliğinin tam olarak anlaşılabilmesi için, temel protokol olarak görülen WEP'in amacı ve bu mekanizmada zaman içerisinde tespit edilen zayıflıkların bütünüyle ortaya konulması gerektiği düşünülmektedir. Bu kapsamda WEP mekanizmasının daha kapsamlı olarak ele alınmasında fayda görülmektedir.

2.7. Kablolu Eşdeğer Güvenlik (WEP) Mekanizması

Ortaya konulduğu ilk tarihte, kullanıcılara kablolu ağlardaki güvenliğe eşdeğer bir güvenlik ortamını kablosuz ağlarda sağlamayı amaçlayan kablosuz eşdeğer güvenlik (WEP) mekanizması, Eylül 1999'da onaylanan IEEE 802.11 standardının bir parçasıdır. Adından da anlaşılacağı üzere kablolu ağlara eşdeğer bir güvenlik alt yapısı sunmayı amaçlayan WEP mekanizması, aslında bu mekanizmayı geliştirenlerinde kabul ettiği biçimde tam bir güvenlik protokolü olmasa da, gizliliği sağlamak için RC4 (Rivest Cipher Stream Cipher) şifreleme ve bütünlük için ise CRC-32 (Checksum) algoritmasını kullanmaktadır.

IEEE tarafından ortaya konulan 802.11 standart dokümanında WEP protokolünün amacının kablolu ağlarda var olan güvenliğe eşdeğer bir güvenlik sağlamak, kullanıcıları rasgele dinleme ve kulak misafirliğinden korumak ve kablolu ağlarda yetkisiz girişleri önleyen fiziksel erişim kısıtlamalarının sağladığı fiziksel güvenlik özelliklerine eşdeğer bir fonksiyonelliği sağlamak olduğu ifade edilmektedir [24-27].

WEP mekanizmasının amacı kablolu ağlardan daha üstün veya daha yüksek bir güvenlik seviyesi sunmak değil, ancak en az ona denk bir güvenliği kablosuz ağlar için sağlamaktır. Ancak, gerçekte kablosuz ağlardaki WEP mekanizmasının sunduğu güvenlik seviyesinin, kablolu ağlarda fiziksel kısıtlamalar nedeniyle doğal olarak var olan güvenlik seviyesine eşdeğer olmadığı zaman içerisinde elde edilen tecrübeler göstermiştir.

802.11 standardı kablosuz ağlarda temel olarak iki farklı tip kimlik doğrulama mekanizması öngörmektedir. Bunlar; Açık Sistem Kimlik Doğrulama (Open System Authentication), ve Paylaşımlı Anahtar Kimlik Doğrulaması (Shared Key Authentication) mekanizmalarıdır. Bunlara ilave olarak MAC adresi ile kimlik doğrulama mekanizması da kullanılabilmektedir.

Açık sistem kimlik doğrulama: Bu yöntemde erişim noktası ağa bağlanmak isteyen tüm cihazların duyması maksadıyla kendisi ve parçası olduğu ağa ait davet yayınını

SSID (Service Set Identifier) yapmaktadır. Şekil 2.5.a.'da gösterildiği gibi bu daveti alan ve ağa bağlanmak isteyen istemci cihazlar tarafından gönderilen ID bilgileri marifetiyle kablosuz ağ ve ilgili erişim noktası kimlik doğrulama taleplerini ve ağa bağlantı isteklerini kabul etmektedirler. Erişim noktalarının SSID bilgilerini açık bir şekilde yayınlamaları isteğe bağlı olup ağ yönetimi tarafından bu davet yayını kapatılabilir, böylece sadece geçerli SSID değerini bilen istemci cihazlar ağa bağlanabilirler.

Şekil 2.5.a. Açık sistem kimlik doğrulama.

Paylaşımlı anahtar kimlik doğrulama: Paylaşımlı anahtar kimlik doğrulama mekanizması ise, paylaşımdaki WEP şifreleme anahtarı bilgisinin bir örneğinin şifrelenerek gönderilmesi ve gönderen tarafın legal bir kullanıcı olduğunun kanıtlanmasını içermektedir. WEP paylaşımlı anahtar kimlik doğrulama mekanizmasının kablosuz ağda kullanımı ve ağa bağlanma isteği yapan cihazın kimlik doğrulaması Şekil 2.5.b.'de görüldüğü gibi, aşağıdaki basamaklara göre gerçekleştirilmektedir.

i. İstemci cihaz tarafından erişim noktasına yapılan ağa bağlanma talebinin iletilmesi,

ii. Ağ erişim noktası tarafından rasgele üretilmiş 128 bitlik karşılama mesajı gönderilmesi,

iii. İstemci cihaz tarafından, erişim noktasının gönderdiği 128 bitlik karşılama mesajının WEP şifreleme anahtarı ile şifrelenerek geri gönderilmesi,

iv. Erişim noktası tarafından, istemci cihazdan gelen şifreli metnin çözülmesi ve geçerli WEP şifreleme anahtarının elde edilmesi sonrası istek yapan cihaza durum kodu (Status Code) bilgisi gönderilerek cihazın ağa kabul edilmesi.

Şekil 2.5.b. WEP paylaşımlı kimlik doğrulama.

İlk basamakta istemci cihaz ağa bağlantı isteğini göndermektedir. Erişim noktası bu isteğe bir karşılama mesajı ile cevap vermektedir. Bu basamaklarda eğer kablosuz ağ WEP mekanizması değil de, açık sistem güvenlik (Open System Security) mekanizması kullanıyor ise, istek yapan cihaz ile erişim noktası arasında sadece 1 ve 2 nci basamaklar gerçekleştirilerek istek yapan cihaz ağa kabul edilmektedir.

Ancak, kablosuz ağda eğer WEP mekanizması kullanılıyor ise, tüm basamaklar sırasıyla gerçekleştirilir. Dördüncü basamakta erişim noktası istek yapan cihaza bir durum kodu (Status Code) gönderir ve istemci cihaz ağa kabul edilir.

Burada iki ciddi sorun bulunmaktadır. Bunlardan birincisi; istek yapan cihazın, karşılama mesajını gönderen erişim noktası hakkında ve erişim noktasının geçerli WEP şifreleme anahtarının bilip bilmediği ile ilgili sağlıklı bilgisinin bulunmamasıdır. Çünkü, iletişim kurulan erişim noktası sadece rasgele 128 bitten oluşan bir karşılama mesajı göndermektedir.

Özetle, karşıdaki erişim noktası herhangi bir erişim noktası olabilir ve her isteğe karşılama mesajı ile birlikte doğru bir durum kodu ile cevap verebilir. Bu erişim noktası doğal olarak geçerli WEP simetrik şifreleme anahtarını bilmediği için daha

sonra gelen/gelecek paketleri açamayacağından işlevsel bir erişim noktası olmamaktadır. Bu noktada istemci cihaz ile erişim noktası arasında oluşturulmuş olan karşılıklı kimlik doğrulama (Mutual Authentication) kaybolmaktadır.

Buradaki ikinci ve önemli diğer bir sorun ise; bağlantıyı dinleyen (eavesdropping) bir saldırganın iki kritik bilgiyi elde etmesi durumudur. Bu kritik bilgilerden ilki, 2 nci adımda erişim noktası tarafından rasgele üretilen ve istek yapan cihaza gönderilen 128 bitlik karşılama mesajının açık olarak (Plaintext) elde edilmesidir. Aynı şekilde ikinci kritik bilgi ise 3 ncü adımda istemci cihaz tarafından erişim noktasına gönderilen ve açık olarak kendisine ulaştırılan mesajın şifrelenmiş (Cypertext) halinin ele geçirilmesidir. WEP mekanizmasında kullanılan RC4 tipi şifreleme simetrik bir şifreleme olduğundan, açık ve şifreli hali elde edilen bir şifreleme algoritmasının anahtarının elde edilmesi kripto analistler için iyi başlangıç noktası oluşturmaktadır.

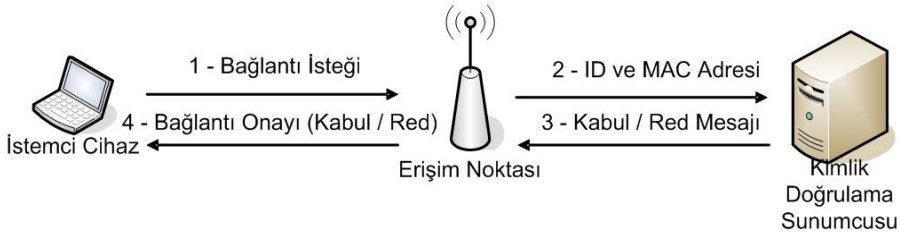
MAC adresi ile kimlik doğrulama (MAC address authentication): WEP'te kimlik doğrulama için kullanılabilecek bir başka mekanizma ise MAC adresi ile kimlik doğrulama mekanizmasıdır. Bu tür kimlik doğrulamada, ağda tanımlı bir erişim noktası üzerinden iletişim kuran istemci cihazların MAC (Media Access Control) adresleri bir sunumcuda RADIUS (Remote Authentication Dial-In User Service) tutulmaktadır. Sadece daha önceden belirlenmiş ve sunumcu üzerinde kayıtlı olan MAC adresine sahip kullanıcılar kimlik doğrulama işlemini gerçekleştirebilmektedirler. MAC adresi ile kimlik doğrulama Şekil 2.5.c'de gösterilmiş olup işlem basamakları aşağıya çıkarılmıştır.

i. İstemci cihaz, erişim noktasına kendi ID bilgisi ve MAC adresi ile birlikte kimlik doğrulama ve ağa bağlanma isteği gönderir.

ii. Erişim noktası, istemci cihazın MAC adresi ve ID bilgisini RADIUS sunumcusuna gönderir.

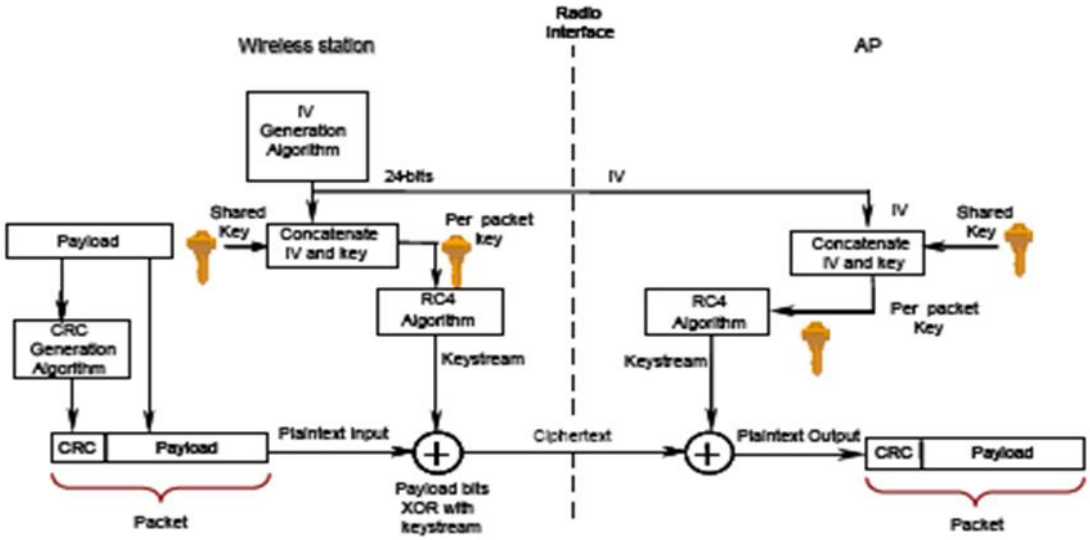
iii. Sunumcu ID bilgisi ile MAC adresi bilgisini karşılaştırır ve kabul ya da ret cevabını erişim noktasına gönderir.

iv. Sunumcudan gelen kabul cevabı doğrultusunda erişim noktası istemci cihazı ağa kabul veya red eder.



Şekil 2.5.c. MAC adresi ile kimlik doğrulama.

RC4 şifreleme algoritmasını kullanan WEP şifreleme mekanizmasının genel çalışma şekli Şekil 2.6.'dadır.



Şekil 2.6. RC4 şifreleme algoritmasını kullanan WEP mekanizması.

RC4 simetrik şifreleme algoritması, blok değil dizi (Stream) şifreleme yapmakta ve algoritma içerisinde XOR fonksiyonu kullanılmaktadır. XOR fonksiyonunun en önemli özelliği ise, bir veri setinin aynı anahtar ile iki kez XOR fonksiyonuna tabi

tutulması durumunda en baştaki orijinal veri setinin geri elde edilmesidir. Dolayısıyla şifrelenmiş bir metin ile aynı metnin açık halinin ele geçirilmiş olması durumunda kullanılan anahtar kolayca elde edilebilmektedir.

Bir başka ifade ile, WEP şifreleme mekanizmasında kullanılan RC4 algoritmasında 128 bitlik rasgele metin ve ilgili şifreleme anahtarı şu şekilde elde edilebilmektedir.

Açık Metin	(XOR)	RC4 Anahtarı	=	Şifreli Metin
Şifreli Metin	(XOR)	RC4 Anahtarı	=	Açık Metin

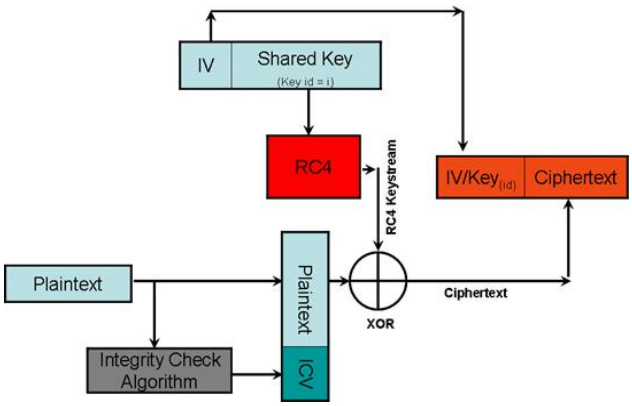
Buradan çıkartılan sonuç WEP mekanizması içerisinde kullanılan RC4 şifreleme anahtarının, zahmetsizce elde edilen ve erişim noktası tarafından istemci cihaza gönderilen karşılama mesajı (açık metin) ile istemci cihaz tarafından geri gönderilen karşılama mesajının şifrelenmiş halinin XOR işlemine tabi tutularak aşağıdaki şekilde elde edilmesidir.

RC4 Anahtarı	=	Şifreli Metin	(XOR)	Açık Metin

Bu şifreleme anahtarı elde edildikten sonra, erişim noktasına bağlantı isteği yaparak kolayca ağa bağlantı gerçekleştirilmektedir.

Şekil 2.7.'de gösterildiği gibi WEP mekanizması herhangi bir kablosuz ağda aktive edildiğinde, ağda gerçekleşen trafik içerisinde bulunan her bir 802.11 paketi ayrı ayrı olarak 64 bit uzunluğunda bir RC4 anahtarı ile şifrelenmektedir. Bu 64 bitlik standart RC4 anahtarı, 24 bitlik bir başlama vektörü (Initialization Vector - IV) ve 40 bit uzunluğundaki bir WEP anahtarından oluşmaktadır. Şifrelenmiş ve güvenli hale getirilmiş bir paket, RC4 anahtarı ve orijinal veri paketinin bit bit XOR'lanması ile elde edilmektedir. IV vektörü, paketi gönderen tarafından seçilerek periyodik olarak değiştirilmektedir. Böylece her paketin aynı IV değerine sahip anahtar ile şifrelenmesi durumunun önüne geçilmesi amaçlanmaktadır. IV vektörü her veri paketi içerisinde açık olarak gönderilmekte, pakete ilave olarak 4 bayt uzunluğunda olan bütünlük kontrol değeri (CRC - Integrity Check Value - ICV) orijinal paket

üzerinden hesaplanarak paketin sonuna eklenmektedir. Paketin sonuna eklenen bu ICV değeri de RC4 ile şifrelenerek gönderilmektedir [5-6, 28-29].



Şekil 2.7. WEP mekanizması şifreleme algoritması.

Ron RIVEST tarafından tasarlanan ve WEP mekanizması içerisinde gömülü olarak kullanılan RC4 şifreleme algoritmasının kriptografik olarak güçlü olduğuna inanılmaktadır. RC4'te kullanılan orijinal şifreleme anahtarı, 40 bit uzunluktadır. Ancak şifreleme algoritması kapsamında başlatma vektörü ile birlikte ortaya çıkan zafiyeti gidermek için daha sonradan çeşitli üreticiler tarafından 128 bite varan uzunluklarda uygulamalarda söz konusudur. Ancak, WEP mekanizmasında şifreleme işlemi sırasında kullanılan başlama vektörü (IV) yalnızca 24 bit uzunluğunda olduğundan, uzun zaman aralıklarında aynı IV değerinin tekrar kullanılması söz konusu olmakta ve bu nedenle güvenlik zafiyeti oluşmasına zemin hazırlanmaktadır.

Ayrıca, WEP mekanizmasında, şifreleme anahtarının yönetim imkanı sunulmamakta ve 802.11 standardında da paylaşılan gizli anahtarın nasıl yönetileceği ve dağıtılacağı ile ilgili bir açıklamada bulunmamaktadır. Bu durum herhangi bir kriptografik sistemdeki en büyük zafiyetlerden birisi olarak değerlendirilmekte ve bu nedenle sistem saldırılara açık hale gelmekte ve kolay bir hedef olmaktadır.

Bu tez çalışmasının temel konusu olan WEP mekanizmasının çalışma prensipleri ile ilgili daha detaylı bilgi üçüncü bölümde verilmektedir.

2.7.1. WEP Mekanizmasının Zafiyetleri ile İlgili Çalışmalar

WEP mekanizması, güvenli olduğuna inanılan RC4 şifreleme algoritmasını kullanmasına rağmen, hedeflediği güvenlik seviyesini sağlayamadığı ve sahip olduğu zafiyet ve açıklar nedeniyle hem pasif ve hem de aktif güvenlik saldırılarına karşı hassastır. WEP mekanizmasının bilgi sistemlerinde temel güvenlik kriterleri olarak bilinen, Kimlik Doğrulama (Authentication), Gizlilik (Secrecy) ve Bütünlük (Integrity) kriterlerinin sağlanmasında başarısız kabul edilmektedir [30].

Ayrıca, RC4 şifreleme algoritması tarafından üretilen ilk şifreli baytın, şifreleme anahtarının diğer baytları ile ilgili bilgi sızdırdığı ifade edilmektedir. Özellikle WEP mekanizması ile RC4 kullanılarak şifrelenmiş paketler üzerinde yeterince analiz yapılması neticesinde, WEP şifreleme anahtarlarının yeniden oluşturulabileceği ile WEP mekanizmasında kullanılan RC4 şifreleme algoritmasına karşı, pasif şifreli-metin (cipher-text-only) saldırısının nasıl gerçekleştirileceği ortaya konulmuştur [31]. Tekrar kullanıldığı belirlenen bir başlatma vektörünün ele geçirilmesi ve şifrelemede kullanılan anahtar içerisindeki bitlerin çok az bir kısmının bilinmesi sayesinde, yüksek bir olasılıkla, üretilen şifreli bitleri belirlemeye yetecek çok sayıda zayıf anahtar tespit edilebilmektedir.

WEP mekanizmasının kimlik doğrulama zafiyetlerine yönelik olarak ise basit bir dinleme (Eavesdropping) saldırısının kolayca gerçekleştirilebileceği [32] ve WEP mekanizması aktif olsa bile saldırı başarısının mümkün olduğu [30] bilinmektedir.

Pasif bir saldırı yöntemi kullanarak, WEP mekanizması aktive edilmiş kablosuz bir ağda kullanılan 128 bitlik gizli anahtarın elde edilebildiği, hatta yeterli sayıda paket toplaması ile şifreleme anahtarının 60 saniye gibi kısa bir sürede bulunabildiği, RC4 şifreleme algoritması ile birlikte kullanılan başlama vektörlerini (IV) düzgün kullanmadığı, WEP'in tamamen emniyetsiz olduğu, WEP'te bulunan zafiyet ve açıkların nedeni olarak da, RC4 gibi makul ve güvenli bir şifreleme algoritmasının, başlama vektörü gibi sakıncalara sahip bir uygulama ile birlikte kullanılması olduğu ortaya konulmuştur [5-6, 32-34].

Görüleceği üzere, buraya kadar ifade edilen çalışmalar, söz konusu WEP mekanizmasının bariz hassasiyetleri, daha net bir ifade ile zafiyet ve açıkları hakkında detaylı bilgi sunmaktadırlar. Tüm bu çalışmalarda, WEP tasarımcılarının, tam bir güvenlik sağlamak üzere kimlik doğrulama ve gizlilik sağlamanın gerekli olduğunun farkında olmalarına rağmen, ortaya koydukları mekanizmanın öngörülen ihtiyaçlara cevap vermediğini göstermektedir. Temel nokta WEP mekanizmasında kimlik doğrulama ve gizlilik sağlama için kullanılan algoritmanın kendisinin hassasiyetlerinin bulunmasıdır.

IEEE 802.11 standartlarına uygunluk onaylarını verme görevi olan bir organizasyon olan Kablosuz Ethernet Uyum Birliğinin (The Wireless Ethernet Compatibility Alliance - WECA) söz konusu çalışmalara cevaben yaptığı açıklama, kablosuz ağlarda zayıfta olsa bir güvenlik mekanizmasının varlığının, hiç bir güvenlik mekanizması olmamasından daha iyi olduğu ve WEP mekanizmasının amacının kablosuz ağlardaki tüm güvenlik ihtiyaçlarını karşılamak olmadığı yönündedir.

Bu açıklama ile en büyük güvenlik tehdidinin, WEP mekanizması dahil olmak üzere, imkanlar dahilindeki mevcut güvenlik mekanizmalarının hiç kullanılmaması veya doğru kullanılmaması olduğu net bir şekilde ortaya konulmaktadır.

Söz konusu eleştirilere yönelik olarak IEEE 802.11 Çalışma Grubu tarafından, WEP mekanizması ile ilgili bazı noktaları açıklığa kavuşturma amacıyla yazılı bir duyuru yapılmıştır. Bu kapsamda, WEP mekanizmasının güvenlik açıklarının kapalı bir standardizasyon sürecinden kaynaklandığı yönündeki eleştirileri reddedilmiş ve WEP mekanizmasının IEEE 802.11'in bir parçası olması nedeniyle diğer IEEE standartları gibi açık bir süreçte geliştirildiği belirtilmiştir. Aynı kapsamda, WEP mekanizmasının temel amacının kablolu ağlarla kıyaslanabilir seviyede bir güvenlik sağlamak olduğunu belirtilmiştir.

WEP mekanizması ile ilgili yukarıdaki tespitler kapsamında bu bölümde IEEE 802.1X Yerel ve Metropolitan Ağlar İçin, Port Tabanlı Ağ Erişim Kontrolü (Port - Based Network Access Control) standardından da bahsetmek gerekli görülmüştür.

2001 yılında ilk kez ortaya konulan IEEE 802.1X standardı, kimlik doğrulama altyapısının ihtiyaçlarını karşılamak için geliştirilmiştir. Hem kablolu ve hem de kablosuz ağlarda çalışması öngörülen 802.1X standardı kimlik doğrulama için ölçeklenebilir ve merkezi bir altyapı sağlamaktadır. Ancak, 802.1X yalnızca kimlik doğrulama ve anahtar yönetimi üzerine yoğunlaştığı için, güvenlik ihtiyaçlarını karşılamak maksadıyla kullanılan/üretilen şifreleme anahtarlarının ne zaman ve ne şekilde dağıtımının yapılacağı belirtilmemiştir.

IEEE 802.1X standardı sadece bir kimlik doğrulama metodundan ibaret değildir. 802.1X, daha çok kimlik doğrulama altyapısı olarak Genişletilebilir Kimlik Doğrulama Protokolünü (Extensible Authentication Protocol - EAP) kullanmaktadır. Yani 802.1X algoritması; kullanılan anahtar (switch) ve erişim noktaları, sertifika tabanlı kimlik doğrulama, akıllı kartlar, jeton (token) kartlar, tek-kullanımlık parolalar dahil olmak üzere geniş bir çerçevede farklı kimlik doğrulama metotlarını destekleyebilmektedir [35].

802.1X, her hangi bir kimlik doğrulama metodunun direkt olarak kullanılmasını zorunlu kılmamaktadır. Anahtar cihazları ve erişim noktaları EAP için geçiş noktaları olarak çalıştığından, anahtar ve erişim noktalarını güncelleme ihtiyacı olmadan, istemci ve kimlik doğrulama sunumcusuna ilave yazılım yüklenerek yeni kimlik doğrulama metotları kullanılabilmesine imkan tanımaktadır.

2.7.2. WEP Mekanizmasının Zafiyetleri

Şifreleme anahtarının direkt olarak kullanılması: Kriptografik açıdan güvenlik mekanizma ve protokollerinde ana şifreleme anahtarlarının direkt olarak kullanılması kesinlikle tavsiye edilmemekte, ana şifreleme anahtarlarının sadece geçici olarak kullanılan diğer anahtarların üretilmesinde kullanılması önerilmektedir. WEP

mekanizması ana şifreleme anahtarını direkt olarak kullandığı için bu bağlamda ciddi bir zafiyet sergilemektedir.

Kısa şifreleme anahtarı: WEP mekanizması, bir zafiyet olarak belirtilen ve 40 / 104 bit uzunluğunda olan bir anahtar öngörmektedir. 1997 yılında ilgili standart ve mekanizma ortaya ilk konulduğunda, 40 bitlik şifreleme anahtar uzunluğunun bazı uygulamalar için makul olacağı düşünülmüştür. Çünkü o dönemde amaç, rasgele dinleme ve kulak misafirliğine karşı güvenlik sağlamak olduğundan, 40 bitlik uzunluk yeterli kabul edilmiştir. Bu zafiyeti tespit eden bazı üretici firmalar ise zaman içerisinde 128 / 256 bit uzunluğu destekleyen şifreleme algoritmalarını içeren cihazları da piyasaya sürmüşlerdir. Şifreleme anahtar uzunluğunun değiştirilmesi belki bir seviyeye kadar güvenliği artırmış ancak, her iki durumda da yani 40 bit, veya 104 bitlik şifreleme anahtar uzunluğu kullanılması durumunda, RC4 algoritması ile şifreleme anahtarı ve 24 bit uzunluğundaki başlama vektörü (IV) ile ilgili zafiyetleri içermeye devam etmiştir. Ancak, 104 bit uzunluğundaki anahtarların kullanılması durumunda sistem özellikle brute-force saldırılarına karşı 40 bit uzunluğundaki anahtarlardan daha dayanıklı kılınmıştır.

Anahtar yönetim mekanizması eksikliği: WEP mekanizmasının en önemli zayıflıklarından birisi, herhangi bir anahtar yönetimi fonksiyonu öngörülmemiş olmasıdır. Çünkü anahtar yönetim mekanizması olmayan WEP'te kullanılan anahtarlar, ağ tarafından daha uzun sürelerle kullanılmaya ve dolayısıyla güvenlik açısından düşük kaliteli olmaya eğilimlidir. WEP mekanizması aktif edilmiş olan kablosuz ağların büyük bir çoğunluğu, ağdaki her istemci ve sunumcu cihaz tarafından paylaşılan tek ve ortak bir WEP şifreleme anahtarına sahiptir. WEP mekanizmasında erişim noktaları ve istemci cihazların tümü aynı WEP şifreleme anahtarı ile programlanmak zorundadır. Anahtar değişimini zaman programlı şekilde gerçekleştirmek ve senkronize hale getirmek çok zahmetli ve zor olduğu için sistem yöneticilerinin sorumluluğunda bulunan anahtar değişim işlemi nadiren gerçekleştirilmektedir.

RC4 şifreleme algoritmasının uygun kullanılmaması: WEP mekanizmasında kullanılan RC4 şifreleme algoritmasının, uygulanma şekli nedeniyle zayıf anahtarlara sahip olduğu bilinmektedir. WEP'te kullanılan anahtar ve bu anahtar ile üretilen şifreli paketler arasında normalde olması gerektiğinden daha fazla ilişki ve korelasyon vardır. Bu kapsamda güvenlik mekanizmasını kırmak için ilk etapta zayıf anahtarlarla şifrelenmiş paketler olarak adlandırılan paketlerin ele geçirilmesine ihtiyaç duyulmaktadır. WEP'te hangi paketlerin zayıf anahtarlarla şifrelendiğini belirlemek oldukça kolaydır, çünkü şifreli paketlerin ilk üç baytı, şifrelenmeden gönderilen ve her pakette bulunan başlama vektöründen (IV) alınmaktadır.

Zayıf IV değerleri olarak literatürde yer alan ve çeşitli istatistiki değerlendirmeler ve ilgili kaynak kodları ile tespit edilen bazı değerler bir fikir oluşturması açısından aşağıda sunulmuştur. Bu IV değerlerinin kullanılması durumunda ağdaki şifreleme anahtarının tespit edilmesi göreceli olarak kolaylaşmaktadır.

IV Değeri			Bit Dizilimi		
00	00	00	00000000	00000000	00000000
00	00	01	00000000	00000000	00000001
00	01	01	00000000	00000001	00000001
. . .					
FF	FF	FF	11001100	11001100	11001100

24 bitten oluşan başlama vektöründen toplamda üretilebilecek 16 milyon faklı paket değeri içerisinde, istatistiki olarak 9 000 kadarında zayıf anahtar kullanılması söz konusudur. Pasif dinleme ile ağ trafiğine erişim sağlamış bir saldırgan, her paketteki başlama vektörlerini filitreleyerek, zayıf anahtar barındırdığı bilinen paketleri kolayca ele geçirmektedir. Yeterli sayıda bu tip paket toplayan veya ele geçiren saldırgan, bunları analiz ederek, elde ettiği anahtarlar ile çok az sayıda deneme yaparak ağa kolaylıkla erişim sağlamaktadır. Tüm orijinal IP paketleri bilinen bir sayı değeri ile başladığı için, ne zaman doğru anahtara sahip olunduğunu anlamak oldukça kolaylaşmaktadır. 104 bitlik bir WEP anahtarını bulmak için, 2 000 ile 4 000

arası zayıf anahtar barındıran paket toplamak yeterli olmaktadır. Günlük 1 milyon paketin yaratıldığı yoğun bir ağda, bir günde birkaç yüz bu tip paket toplanabilmektedir. Bu da çok kısa bir toplama süreci sonunda doğru anahtarın elde edilebileceğinin en somut göstergesidir [5-6, 36-37].

Bir çok üretici, zayıf anahtarla şifrelenmiş paket üretmeyen başlama vektörü (IV) seçerek kullanmayan yeni yeni algoritmalar üretmeye çalışmaktadırlar. Çünkü bu tip saldırılara karşı en iyi savunmanın zayıf anahtarla şifrelenmiş IV değerlerinin kullanılmasının önüne geçmektir. Ancak, eğer ağdaki bir istasyon bile gerekli önlemler alınmadan ağda aktif olarak bulunuyor ve zayıf bir anahtarla şifrelenmiş bir paket üretiyorsa saldırıların başarıya ulaşma şansı olmaktadır.

Tekrar kullanılan - kısa başlama vektörü (IV): WEP'in 24 bit olan kısa başlama vektörü (IV) uzunluğu, WEP şifreleme anahtarının boyutundan bağımsız olarak, şifrelenen anahtar için en fazla 16 777 216 farklı RC4 şifre seti üretmektedir. Trafiği yeterince yoğun bir ağda, başlama vektörü değerleri kısa sürede kullanılıp tükeneceğinden bu sayıya kısa bir sürede erişilebilmekte ve dolayısıyla birbirlerini tekrarlayan başlama vektörü (IV) değerleri tekraren kullanılmaya başlanabilmektedir. Daha uzun sürelerde ise ağdaki trafik yoğunluğu nedeniyle başlama vektörleri (IV) değerlerinin tekrar kullanımı kaçınılmaz hale gelmektedir. RC4 şifre anahtarının orijinal paketle XOR'lanarak gönderildiği ve IV değerinin de her bir paketle birlikte açık olarak gönderildiği bilinmektedir. Eğer elde edilen bir IV değeri için RC4 şifre anahtarı bulunursa, saldırgan, aynı IV ile şifrelenmiş takip eden paketleri kolayca deşifre edebilmekte veya bu paketleri değiştirebilmekte ya da taklit edebilmektedir.

Bazı uygulamalarda IV değeri sıfırdan başlatılmakta ve aşamalı olarak her pakette arttırılmakta, 16 milyon paket gönderildikten sonra tekrar sıfırdan başlanmaktadır. Diğer bazı uygulamalarda ise IV değeri rasgele olarak seçilmektedir. Her ne kadar bu düzenleme iyi bir fikir gibi görünse de, gerçekte rasgele seçilmiş bir IV değeri ile gönderilen bir paketten sonra, takip eden ilk 5 000 paket içerisinde aynı IV değerinin kullanılması olasılığı % 50 olarak belirlenmiştir [36].

ICV bütünlük kontrol algoritmasının zafiyetleri: WEP'te kullanılan ve veri bütünlüğü ile hata kontrolünü sağlayan mekanizma olan bütünlük kontrol değeri (Integrity Check Value - ICV), gürültü, parazit ve genel hataları yakalama amaçlı bir algoritma olan (Cyclic Redundancy Check - CRC) CRC-32 tabanı üzerine oturmaktadır. Bu nedenle, dolaylı olarak CRC-32'nin sahip olduğu dezavantajlara sahiptir.

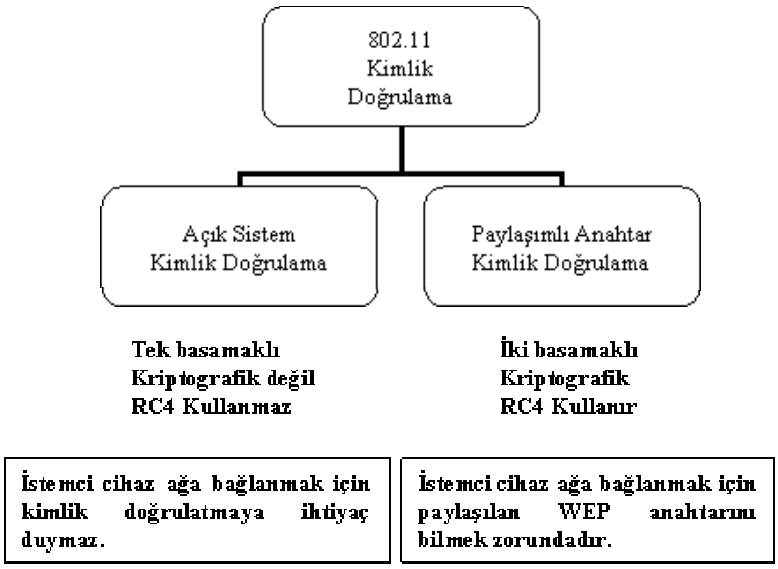
CRC-32 tabanlı ICV değeri, orijinal mesajın doğrusal bir fonksiyonudur ve bu nedenle herhangi bir saldırgan, şifrelenmiş bir mesajı ele geçirmeyi müteakip, değiştirebilme yeteneğine sahiptir. Saldırgan yaptığı bu değişiklikten sonra ICV'yi kolayca tekrar düzenleyebilme ve mesajı tekrar ağa gönderme yeteneğine sahip olmakta, böylece mesaj alıcı tarafında orijinal olarak algılanmaktadır. Bu sayede, saldırgan, hedef olarak seçtiği kurbanın kablosuz erişim noktasının kendisi için paketleri deşifre etmesini kolay bir şekilde sağlayabilmektedir.

CRC-32, hataları belirlemek ve bütünlüğün kontrolünü sağlamak maksadıyla geliştirilmiş bir mekanizma olmasına rağmen kriptografik özetleme fonksiyonları için ve özellikle güvenlik sağlamada kullanılması durumunda iyi bir çözüm olmadığı değerlendirilmektedir.

Kimlik doğrulama mesajlarının kolayca taklit edilmesi: Önceki bölümlerde ifade edildiği şekilde 802.11 standardında kablosuz ağlarda temel olarak iki farklı tip kimlik doğrulama mekanizması Açık Sistem Kimlik Doğrulama (Open System Authentication), ikincisi ise Paylaşımlı Anahtar Kimlik Doğrulaması (Shared Key Authentication) kullanılmakta olup detayları Şekil 2.8.'de sunulmuştur.

Teorik bilgiler, bir ağ üzerinde aktive edilmiş bir kimlik doğrulaması mekanizması varlığının, hiç bir kimlik doğrulama mekanizması kullanılmamasından daha iyi olduğu düşüncesine dayanmaktadır. Çünkü ağda bulunan herhangi bir istemci cihaz ya da erişim noktası, ağda bulunan tüm taraflar tarafından paylaşılan WEP şifreleme anahtarı bilgisine sahip olduğunu kanıtlamak zorundadır. Ancak, pratikte bunun doğru olmadığı, ağ üzerinde kimlik doğrulama işlemini faal hale getirmenin, aslında genel ağ güvenliğini azaltarak, WEP şifreleme anahtarının davetsiz misafir ve

saldırganlar için tahmin ve elde edilmesini daha kolay hale getirdiğini savunan kaynaklarda bulunmaktadır.



Şekil 2.8. 802.11 Kimlik doğrulama.

Paylaşımlı anahtar kimlik doğrulama mekanizması, paylaşımdaki WEP şifreleme anahtarı bilgisinin bir örneğinin şifrelenerek gönderilmesi ve gönderen tarafın legal bir kullanıcı olduğunun kanıtlanmasını içermektedir. Ancak, buradaki temel problem, ağı dinleyen veya gözlemleyen bir saldırganın, gönderilen şifreleme anahtarı bilgisi örneği ve bunun karşılığı olan şifrelenmiş cevabı ele geçirebilmesi riskidir.

Bu bilgileri elde eden bir saldırgan, ağda kullanılan RC4 şifreleme anahtarını tespit edebilmekte ve bu anahtarı daha sonra ağ elemanlarına kendisini doğrulatmak için kolayca kullanabilmektedir. Bu kapsamda, paylaşımlı anahtar kimlik doğrulama mekanizması, saldırganın (yanlış WEP anahtarı ile şifrelenmiş) çöp paketlerini ağa göndererek "denial-of-service" saldırıları gerçekleştirme yeteneğini azaltmaktadır [36].

Ancak, kendine has zafiyetlerine rağmen açık sistem kimlik doğrulamanın paylaşımlı kimlik doğrulamaya nazaran daha iyi bir ağ güvenliği sağladığı, bu nedenle ağ yöneticilerinin, açık veya paylaşımlı anahtar kimlik doğrulaması mekanizması yerine

802.1X gibi diğer bir tip kimlik doğrulama protokolünü kullanmayı tercih etmelerinin daha iyi olacağını dile getirilen kaynaklar da bulunmaktadır.

2.7.3. WEP Mekanizmasının Değerlendirilmesi

Yukarıda ortaya konulan zafiyetler kapsamında, kablosuz ağlarda güvenlik sağlanmasında WEP mekanizmasının ideal bir güvenlik çözümünden uzak olmasına rağmen, pasif ve amatör ruhlu saldırganlara karşı caydırıcılık sağlaması açısından yine de kullanılabileceği değerlendirilmektedir. Kablosuz bir ağda kötü de olsa bir güvenlik mekanizmasının aktif olmasının, hiç bir güvenlik mekanizmasına sahip olmayan ağlardan daha güvenli olacağı açıktır. Her ne kadar çeşitli zafiyetleri belirlenmiş ve ortaya konulmuş olsa da, WEP'in profesyonel olmayan sıradan saldırganlara karşı caydırıcı bir güvenlik seviyesi sağladığı düşünülmektedir.

Ancak, kararlı ve profesyonel bir saldırganın, yeterli bir zaman dilimi içerisinde, yeterince sayıda zayıf IV değeri elde etmesini müteakip kablosuz ağlarda kullanılan WEP şifreleme anahtarını keşfedebileceği unutulmamalıdır.

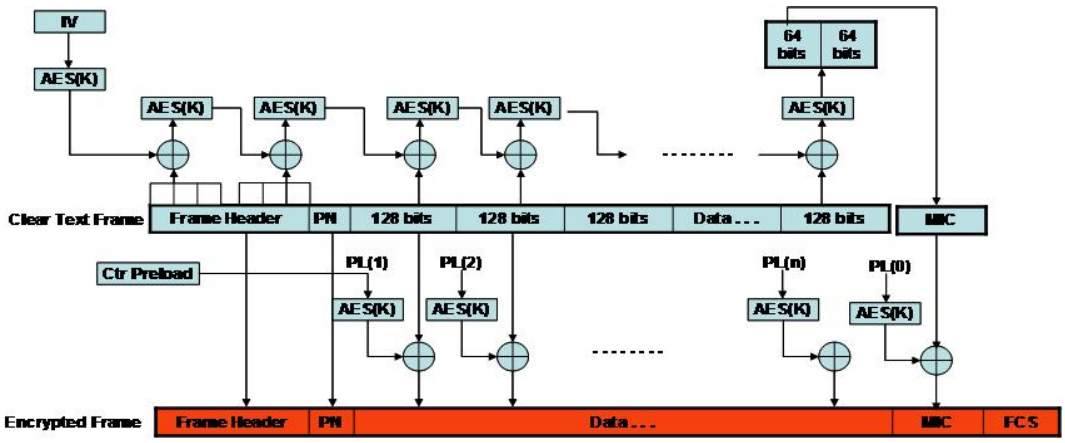
2.8. Korumalı Erişim Protokolü (Wi-Fi Protected Access Protocol - WPA)

802.11 tabanlı ilk kablosuz ağ güvenlik çözümü olan WEP mekanizması, içerisinde barındırdığı zafiyetler ve çeşitli teknik ve standardizasyon hatalarından dolayı bir çok eleştiriye maruz kalmıştır. Bu nedenle, standart geliştirme kuruluşları ile endüstriyel organizasyonlar, büyüyen kablosuz ağ güvenlik problemlerine çözüm bulmak amacıyla, bir sonraki jenerasyonda uygun çözümleri yaratmak için büyük para ve çaba sarf etmişlerdir.

Bir kablosuz ağ endüstrisi organizasyonu olan Wi-Fi Birliği (Wireless Fidelity Alliance), WEP mekanizmasının zafiyetleri ve tasarım hatalarını dikkate alarak, taslak 802.11i standardının bir alt kümesi olarak algılanan Wi-Fi Korumalı Erişim Protokolünü (WPA) yaratmıştır [38].

Wi-Fi Korumalı Erişim Protokolü'nün kısaltması olan WPA, WEP mekanizmasının güvenlik zafiyetlerinin giderilmesi ve mevcut mekanizmanın geliştirilmesi maksadıyla tasarlanmış bir protokoldür. Bu protokol, WEP mekanizması tabanlı olarak kullanılan mevcut Wi-Fi ürünleri üzerinde çalışması için tasarlanmasına rağmen, genel olarak WEP mekanizmasına ilave üç konuda daha güvenli çözümler sunmaktadır. Bunlar sırasıyla aşağıda ele alınmıştır.

i. Geçici Anahtar Entegrasyon Protokolü (Temporal Key Integrity Protocol – TKIP) vasıtasıyla geliştirilmiş veri şifreleme: TKIP, Şekil 2.9.'da verildiği gibi ağda kullanılan anahtarları bir özetleme algoritması kullanarak karıştırmakta ve bütünlük kontrol özelliği ekleyerek anahtarların değiştirilmesini önlemektedir.



Şekil 2.9. TKIP ve MIC.

TKIP bir geçici anahtar özetleme fonksiyonudur. Yeni donanım gerektirmeyen ve WEP mekanizmasının bütün güvenlik hassasiyetlerini ortadan kaldıran, alternatif bir protokoldür. WEP mekanizmasında olduğu gibi TKIP'te, şifreleme ve çözme için RC4 şifreleme algoritması kullanılmakta ve iletişime dahil olan tüm istasyonlar aynı gizli anahtarı paylaşmaktadırlar. Bu gizli anahtar 128 bit uzunluğunda olmakta ve geçici anahtar (Temporal Key - TK) olarak adlandırılmaktadır. TKIP aynı zamanda başlama vektörü IV olarak 48 bitlik bir vektör kullanmakta ve bu değeri ayrıca sayaç olarak ta kullanmaktadır.

TKIP mekanizmasında kullanılan geçici anahtar, tüm istasyonlar tarafından paylaşılmış olarak kullanılmasına rağmen, her bir istasyon tarafından bu ana anahtar kullanılarak farklı bir RC4 şifreleme anahtarı yaratılmaktadır. Geçici anahtar kullanılarak elde edilecek RC4 şifreleme anahtarını elde etmek için kullanılacak olan paket başına anahtar (Per-Packet Key – PPK), tüm istasyonlar tarafından 2 fazlı bir üretim aşaması sonrası elde edilmektedir.

ii. Kullanıcı Kimlik Doğrulaması: WEP mekanizmasında eksik olan bu özellik, genişletilebilir kimlik doğrulama protokolü (Extensible Authentication Protocol - EAP) ile sağlanmaktadır. WEP mekanizmasında kablosuz ağa giriş ve erişim, istemci cihazın donanımına özel olan MAC adresi ile düzenlenmektedir. Bu yöntemde, kullanılan MAC adreslerinin ele geçirilmesi ve çalınması nispeten kolay şekilde gerçekleştirilmektedir. EAP, yalnızca kimliği doğrulanmış istemci cihazların ağa erişimini sağlamak maksadıyla, daha güvenli olan açık anahtar şifreleme (Public Key Encryption - PKE) sistemi üzerine yapılandırılmıştır.

EAP, 802.1X kimlik doğrulama ve yetkilendirme isteklerini, genişletilebilir kimlik doğrulama Protokolünü (Extensible Authentication Protocol - EAP) kullanarak gerçekleştirmektedir. EAP, noktadan-noktaya protokol (Point-to-Point Protocol - PPP) bağlantıları ile kimlik doğrulama işleminde, istemci cihazlar için daha esnek bir altyapı sağlanması amacıyla geliştirilmiştir. EAP, belirli bir kimlik doğrulama mekanizması belirtmek yerine, üreticilerin kendi kimlik doğrulama mekanizmalarını yapılandırmaları için genişletilebilir bir platform sağlamaktadır [39-40].

iii. Bütünlük ve güvenlik kontrolü için yeni bir mekanizma kullanımı: TKIP için mesaj bütünlük kodu (Message Integrity Code) onu yaratan araştırmacının adıyla anılan “Michael” adlı yeni bir algoritma ile hesaplanmaktadır.

Şekil 2.10.’da sunulan Mesaj Bütünlük Kodu (Message Integrity Code - MIC), transfer hataları ya da kasıtlı değiştirmelerden kaynaklanan veri içeriğindeki değişiklik ve hataları yakalayarak güvenliği pekiştirmek maksadıyla kullanılmaktadır. TKIP için yeni bir düzenleme olan “MIC” Nels Ferguson

tarafından ortaya atılan “Michael” adlı yeni bir algoritma ile hesaplanmaktadır. Bu işlem 64 bitlik MIC kodunun, veri ve ICV değerleri üzerinde gerçekleştirilmektedir. Buradaki ICV değeri, veri ve MIC kodunun CRC değeridir.

Şekil 2.10. MIC - Mesaj bütünlük kodu.

2.8.1. WEP ile WPA’nın Karşılaştırılması

i. Ana (master) anahtar kullanımı: Ana anahtar, WEP mekanizmasındaki düzenlemenin aksine WPA protokolünde hiçbir zaman şifreleme işlemi için doğrudan kullanılmamaktadır. Ana anahtardan elde edilerek ortaya çıkarılan bir hiyerarşik anahtarlar serisi kullanılmaktadır. Kriptografik açıdan bu çok daha güvenli bir yöntemdir.

ii. Anahtar yönetimi ve güncelleme: Güvenli anahtar yönetimi WPA protokolünün içerisine direkt olarak gömülü halde bulunmaktadır, bu nedenle WPA protokolünde anahtar yönetimi, ele alınması gerekli bir zafiyet veya sorun olarak görülmemektedir.

iii. IV değerlerinin tekrar kullanımı ve uzunluğu: Başlama vektörü (IV)’nün uzunluğu, WEP mekanizmasında 24 bitten oluşmasına rağmen WPA protokolünde 48 bite çıkarılmıştır. Bu sayede, sayacın çok çabuk şekilde tekrar başa dönmesi ihtimali önlenmiş ve tekrar aynı IV anahtarının kullanılması ihtimali göreceli olarak azaltılmış olmaktadır.

Bunun yanı sıra, WEP mekanizmasının zafiyetlerinden birisi olan “replay saldırılarına” karşı, IV değerlerinin geçici anahtar entegrasyon protokolü (TKIP) dizi sayacı (TKIP Sequence Counter) olarak kullanılmaları sayesinde ilave güvenlik sağlanmaktadır.

iv. Zayıf IV değerleri: WPA protokolü, kolay tespit edilebilen zayıf IV değerlerinin kullanılmasını engelleyen bir düzenlemeye sahiptir. WPA' da her bir paket için farklı bir gizli anahtar kullanılmakta ve şifreleme algoritması ile anahtarın karıştırılması daha karmaşık bir şekilde gerçekleştirilmektedir.

iv. Mesaj bütünlük kontrolü: WEP mekanizmasının mesaj bütünlüğü ve güvenliğin sağlanması için kullandığı işlemlerin etkin ve güvenilir olmadığı bilinmektedir. WPA protokolünde ise, "Michael" adıyla anılan bir mesaj bütünlük kontrol mekanizması kullanmaktadır. Teorik olarak, milyonda bir ihtimalle doğru MIC değerini tahmin etmenin mümkün olacağı değerlendirilmektedir. Pratikte ise, her değiştirilmiş paket yapısı önce TSC (TSC - TKIP Sequence Counter)'den geçerek, Michael kodlama mekanizmasının işleme girdiği noktaya erişmek üzere doğru paket şifreleme anahtarına sahip olunması gereklidir. İleri seviyede bir güvenlik için, Michael mekanizmasının sunduğu diğer bir imkan ise, yapılan saldırıları fark etme ve yeni saldırıları bloke etmek için karşı tedbir getirebilmesidir.

2.8.2. WPA ile İlgili Dezavantaj

WPA ve 802.11i, 802.1X tabanlı anahtar kurulum ve kullanımına alternatif olarak, önceden paylaştırılmış anahtar (Pre-Shared Key - PSK) imkanı sağlamaktadır. PSK, 256 bit uzunluğunda olan bir sayı ya da 8 - 63 bayt uzunluğunda olan bir parola (passphrase)'dır. Ağda bulunan her istasyon kendi MAC adresine bağlı PSK değerine sahip olabilmektedir.

802.1X'in yerine PSK kullanıldığı durumlarda, çiftli ana anahtar (Pairwise Master Key - PMK) ve 4 yollu el sıkışmayı (4-way handshake) ve tüm çiftli geçici anahtar (Pairwise Transient Key - PTK) anahtarlama hiyerarşik hale gelmektedir. PSK parolasını (passphrase), PMK için gerekli olan 256 bitlik sayıya çevirmek için oldukça basit olan bir yöntem kullanılmaktadır.

Parola tabanlı (passphrase based) PSK'yı bilmeyen bir istasyon, ancak çevrim dışı bir saldırı yapabilmektedir. Ağda bir tek PSK olması durumunda dışarıdan yapılacak

bir saldırı, içeride birbirinden farklı birden çok PSK'lar olması durumunda da içeriden saldırı gerçekleştirmek daha kolay olmaktadır.

Sözlük saldırısına hedef olabilecek olan kısa parolalarla (passphrase) oluşturan anahtarların düşük seviyede bir güvenlik sağladığı, anahtar özetleme (hash) yalnızca daha güçlü bir formda kimlik doğrulama mekanizması uygulanabilir olmadığında tavsiye edildiği, 20 karakterden daha kısa bir parola ile oluşturulan bir anahtarın saldırılara karşı caydırıcı olması pek mümkün olmadığı belirlenmiştir [37, 41].

Kullanıcının seçebileceği her hangi bir 8 karakterlik dizinin, sözlükte kolayca bulunabileceği ihtimali dikkate alınmalıdır. İlgili standartta belirtildiği üzere, en az 20 karakterden uzun parolalar (passphrase) bu saldırılara karşı caydırıcı olmaya başlamak için gerekli görülmektedir. Bu uzunluk, genellikle bir çok insanın kullanmak isteyeceğinden daha fazladır ancak, 20 karakter uzunluğunun altında belirlenecek bir anahtar kullanılan ağa karşı çevrimdışı saldırı yapmak WEP saldırılarından daha kolay olabilmektedir .

2.8.3. WPA Protokolünün Değerlendirilmesi

WPA protokolü, WEP mekanizmasının bütün güvenlik zafiyet ve açıklarını gidermesi, eski donanımlarla da uyumlu olması ve güncellenebilir olması nedeniyle WEP mekanizmasından çok daha güçlü bir güvenlik sağlayan yeni bir çözüm gibi görünmektedir. Ancak, WPA protokolü ile ilişkili muhtemel bir zafiyet dikkati çekmektedir. Bu da bir çok insanın kullanmayı isteyeceğinden çok daha uzun olarak kullanılması tavsiye edilen en az 20 karakterlik parola bloğunun kullanılması gerekliliğidir.

WPA protokolünde eğer zayıf bir parola bloğu (passphrase) kullanılıyor ise, çevrim dışı bir sözlük saldırısı ile PSK kolayca tahmin edilebilmektedir. Genellikle uygulanan ve kabul gören kullanım şekli ağda tek bir PSK kullanılması olduğundan, PSK bir kez saldırganlar tarafından ele geçirildiği ve öğrenildiği zaman, saldırgan çok rahat bir şekilde ağın bir üyesi haline gelebilmektedir.

2.9. Sıkı Güvenlik Ağları – (Robust Security Networks – RSN/WPA2)

802.11i standardı, son haliyle 2004 yılında IEEE tarafından onaylanarak RSN Konsepti kapsamında tekrar ortaya konulmuştur. Kablosuz ağlarda kullanılan ağ elemanlarının ilave birtakım özellikleri desteklemesini gerektiren bu standart, sıkılaştırılmış güvenlik ağları RSN/WPA2 olarak bilinmektedir.

IEEE 802.11i standardı ile;

i. Kimlik doğrulama (Authentication)
ii. Şifreleme (Encryption)
iii. Yetkilendirme (Authorization)
iv. Anahtar Yönetimi (Key Management)

fonksiyonlarının gerçeklenmesi hedeflenmiştir.

WEP mekanizmasının zafiyetleri ışığında geliştirilen WPA, mevcut durum itibariyle RC4 şifreleme algoritmasına ve Geçici Anahtar Bütünlük Protokolüne (Temporary Key Integrity Protocol - TKIP) dayanmaktadır. Pek mümkün görünmese de, ileride parola bloğu zafiyetine ilave olarak bu protokolde yeni zafiyetlerin tespit edilmesi imkanı göz ardı edilmemektedir.

Bu kapsamda, IEEE 802.11i çalışma grubu hali hazırdaki 802.11'in güvenliğini daha da geliştirmek için Robust Security Network (RSN) adıyla yeni bir güvenlik mimarisini ortaya koymuştur. Bu yeni mimari, erişim kontrolü için IEEE 802.1X standardını ve şifreleme için de, WPA protokolünde kullanılan RC4 şifreleme algoritması yerine, gelişmiş şifreleme standardını (Advanced Encryption Standard - AES) kullanmaktadır. RSN, 802.1.X karşılıklı kimlik doğrulama ve anahtar yönetim süreci için, ikili anahtar değiştirme ve dört yollu el sıkışma protokolünü kullanmaktadır [39-42].

802.11i standardı farklı ağ yapılandırma uygulamalarına olanak sağlamakta ve TKIP kullanmaktadır. İlave olarak RSN, daha güçlü ve daha kapsamlı bir güvenlik çözümü sağlayan, AES ve CCMP (Counter Mode CBC MAC Protocol) kullanmaktadır.

İlave bir bilgi olarak piyasada mevcut olan ve/veya kullanılmakta olan WEP tabanlı ağ elemanları, RSN ile uyumlu olmadığı için, RSN'nin uygulanabilmesi için yeni donanım ve yazılım gerektiği hatırdan çıkarılmamalıdır.

RSN'de, bir blok şifreleme algoritması olan ve 128 bitlik veri blokları üzerinde çalışan Advanced Encryption Standard (AES) kullanılmaktadır. Bu mekanizma, WPA protokolünde kullanılan RC4 algoritması ile eşdeğerdir, fakat RSN protokolünde gerçekleştirilen şifreleme algoritması çok daha karmaşık bir yapı üzerinde çalışmaktadır.

CCMP ise, AES tarafından kullanılan ve WPA'daki TKIP'e eşdeğer bir ilave güvenlik işlemidir. CCMP, bilinen ve kanıtlanmış Cipher Block Chaining Message Authentication Code (CBC-MAC) metodunu kullanarak mesaj bütünlük kontrolü (Message Integrity Check - MIC) değerini hesaplamaktadır. Burada, orijinal mesajda olması muhtemel bir bitlik bir değişiklik bile, özetleme fonksiyonlarında olduğu şekilde, tamamen farklı bir sonuç üretilmesine neden olduğundan önemli bir farklılıktır.

Önceki bölümlerde ifade edildiği gibi, WEP mekanizmasının en kötü yanlarından birisi de, şifreleme anahtarlarının yönetimi ile ilgilidir. Pek çok ağ yöneticisi, geniş kablosuz ağlarda şifreleme anahtarlarının sık sık değiştirilmesi ve yönetilmesini pek pratik bulmamaktadır. Bu bakış açısı, WEP mekanizmasındaki şifreleme anahtarlarının çoğu zaman hiç değiştirilmemesi ve böylece saldırganların işlerinin kolaylaşmasına neden olmaktadır.

RSN, TKIP'e benzer şekilde sınırlı ömürleri olan şifreleme anahtarlar hiyerarşisi oluşturmaktadır. Fakat, AES/CCMP bütün ağda kullanılan tüm anahtarları

yönetebilmek için 512 bite ihtiyaç duyarken TKIP Çizelge 2.1.'de verildiği şekilde 768 bite ihtiyaç duymaktadır.

Çizelge 2.1. TKIP (WPA) ile AES-CCMP (RSN) toplam anahtar boyutları.

<table>
<tr><th>TKIP (WPA)</th><th>AES-CCMP (RSN)</th></tr>
<tr><td colspan="2">Geçici Anahtarlar</td></tr>
<tr><td>Veri Şifreleme Anahtarı (128 bit)</td><td rowspan="2">Veri Şifreleme ve Bütünlük Anahtarı (128 bit)</td></tr>
<tr><td>Veri Bütünlük Kontrol Anahtarı (128 bit)</td></tr>
<tr><td>EAPOL Şifreleme Anahtarı (128 bit)</td><td>EAPOL Anahtar Şifreleme Anahtarı (128 bit)</td></tr>
<tr><td>EAPOL Bütünlük Kontrol Anahtarı (128 bit)</td><td>EAPOL Bütünlük Kontrol Anahtarı (128 bit)</td></tr>
<tr><td colspan="2">Grup Anahtarları</td></tr>
<tr><td>Grup Şifreleme Anahtarı (128 bit)</td><td rowspan="2">Grup Şifreleme ve Bütünlük Anahtarı (128 bit)</td></tr>
<tr><td>Grup Bütünlük Anahtarı (128 bit)</td></tr>
<tr><td colspan="2">Toplam Anahtar Boyutu</td></tr>
<tr><td>768 bit</td><td>512 bit</td></tr>
</table>

802.11i'de tanımlanmış iki şifreleme standardı olan TKIP ve AES-CCMP için anahtar yönetimi ve üretimi süreci aynı şekilde gerçekleşmektedir. İkisi arasındaki tek fark ihtiyaç duyulan anahtar adedinin farklılığıdır. Bunun sebebi AES-CCMP'nin bütünlük kontrolü ve şifreleme algoritması süreçlerini birleştirmesidir.

AES-CCMP'de, ana anahtarlar TKIP'teki gibi doğrudan kullanılmamakta, fakat diğer anahtarları üretmek için kullanılmaktadır. Ağ yöneticisinin ağa, yalnızca tek bir ana anahtar sunması gerekmektedir. Mesajlar, 128 bitlik gizli bir şifreleme anahtarı ile 128 bitlik veri blokları halinde şifrelenmektedir. Şifreleme süreci yine karmaşık bir süreçtir, ancak ağ yöneticisi bu karmaşık hesaplamaların bütün detay ve inceliklerini bilmek zorunda değildir. Nihai sonuç olarak bu şifreleme algoritması, kırılması WPA'dan çok daha zor olan bir şifreleme algoritmasıdır.

RSN istemci cihazlar ve erişim noktaları arasında, kimlik doğrulama ve şifreleme algoritmalarının dinamik olarak uzlaştırılması mantığını kullanmaktadır. Standarttaki kimlik doğrulama mekanizmaları, 802.1X ve genişletilebilir kimlik doğrulama protokolü (Extensible Authentication Protocol - EAP) temeline dayanmaktadır. Şifreleme algoritması olarak ise ileri şifreleme standardı (AES) kullanılmaktadır.

Şifreleme algoritmalarının ve kimlik doğrulama mekanizmalarının dinamik olarak uzlaştırılması yetenekleri, RSN protokolünde, yeni tehditleri algılamak, yeni algoritma eklemek ve kablosuz ağlar üzerinde taşınan veriyi korumak için gerekli olan güvenlik tedbirlerinin, mükemmel seviyede evrimleştirilmesine olanak sağlamıştır.

Dinamik uzlaştırma mekanizması kullanması, 802.1X temelli olması, EAP ve AES kullanması nedeniyle, RSN, WEP ve WPA'dan bariz şekilde daha güçlü bir protokoldür. Günümüzün kablosuz ağ yapılarından beklenen güvenlik performansı, sadece 2004 yılında onaylanan 802.11i standardından sonraki dönemlerde üretilen RSN özellikli kablosuz ağ elemanları, yani istemci cihaz ve erişim noktaları tarafından kullanılmaktadır.

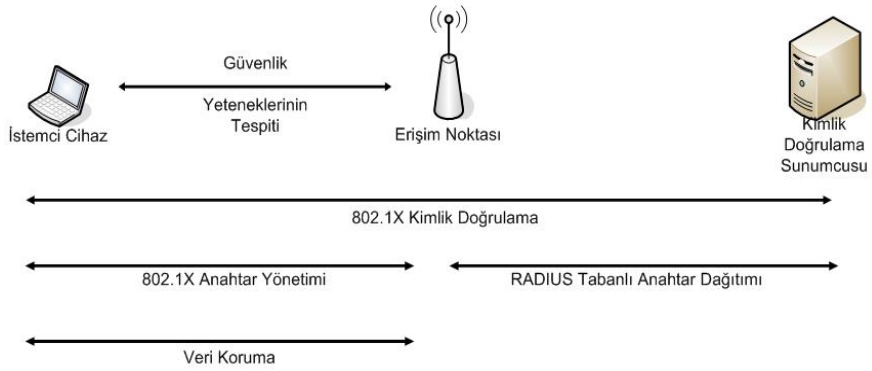
IEEE 802.11i standardı aşağıdaki fonksiyonları sağlamaktadır.

i. Korunmamış bilgilerin gönderilmemesi/alınmaması,
ii. Mesaj kaynağının asıllanması (Taklidi önleme),
iii. Mesajlara sıra numarası verilmesi (Replay saldırı tespiti),
iv. Tekrar anahtarlamayı önlemek için mesajlara sıra numarası (48 bit) verilmesi,
v. Her paket için şifreleme yapılmaması (gereksiz şifrelemeyi engelleme),
vi. Kaynak ve varış adreslerinin korunması,
vii. Gizlilik ve mesaj bütünlüğü için bir güçlü şifreleme algoritması kullanılması,
viii. Hizmet kalitesi gelişmelerine uyum sağlama.

2.9.1. RSN Ağların Çalışma Şekli

IEEE 802.11i standardı, veri güvenliği için yeni bir şifreleme algoritması kullanmakta, yetkisiz kullanıcıların ağa erişimini engellemek için kimlik doğrulama sunumcusu ile doğrulama yapmakta ve anahtar yönetimini de dinamik bir şekilde yapmaktadır. IEEE 802.11i standardı, iki katmandan oluşmaktadır. Alt katmanda, gelişmiş kriptolama algoritmaları (TKIP ve CCMP) bulunmakta, üst katmanda ise kimlik doğrulama ve anahtar dağıtımı için 802.1X protokolü bulunmaktadır [24-27].

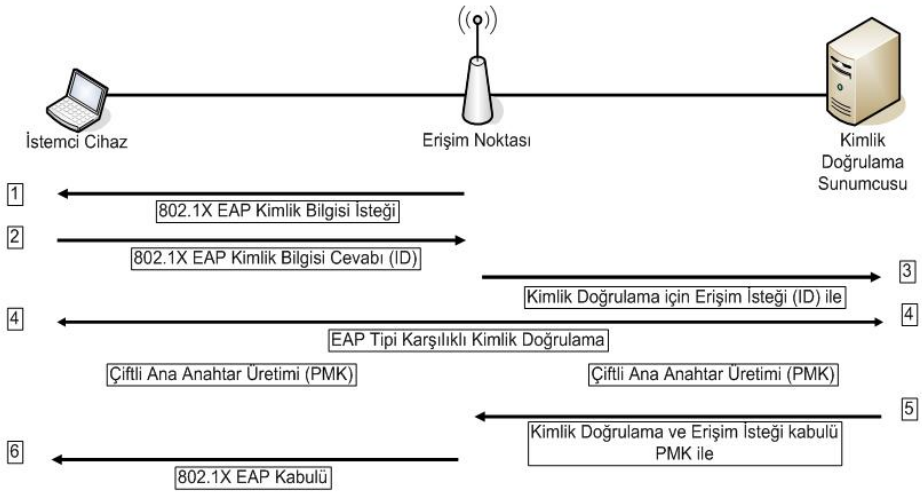
İstemci cihazlar ağ kaynaklarına erişmeden önce doğrulanmakta, kimlik doğrulama işleminden sonra üretilen oturum anahtarları Şekil 2.11'de gösterildiği gibi dağıtılmakta ve bu anahtarlar kullanılarak üretilecek yeni anahtarlar ile güvenli veri transferi yapılmaktadır.



Şekil 2.11. RSN kullanıcı kimlik doğrulama, anahtar yönetimi, veri transfer aşamaları.

Kimlik doğrulama: IEEE 802.11i standardı, karşılıklı kimlik doğrulama için 802.1X EAP tabanlı kimlik doğrulamayı öngörmektedir. 802.1X kablolu ağlar için geliştirilmesine karşın kablosuz ağlar için de kullanılmaktadır. Bu standart, istemci ile erişim noktası arasında bir kimlik doğrulama sunumcusu (authentication server) ve port-tabanlı erişim kontrolü sağlamaktadır [25-26].

802.1X standardı istemci cihaz kimlik doğrulayıcı ve kimlik doğrulama sunumcusu olmak üzere üç elemandan oluşmaktadır. Bu kapsamda asıllama ve kimlik doğrulama Şekil 2.12.'de gösterildiği şekilde aşağıdaki basamaklara göre gerçekleştirilmektedir.



Şekil 2.12. RSN Kimlik doğrulama.

i. İstemci cihaz, erişim noktasına bağlantı talebinde bulunur. Erişim noktası, bağlantı talebini alınca, tüm portları kapalı tutar fakat istemci cihaz ile arasında bir port açar.

ii. Erişim noktası, istemci cihazdan kimlik bilgisini (Identity - ID) ister.

iii. İstemci cihaz kimlik bilgisini gönderir ve bunu alan erişim noktası da bu kimlik bilgisini kimlik doğrulama sunumcusuna gönderir.

iv. Kimlik doğrulama sunumcusu, istemci cihazın kimliğini doğrular. Kimliği doğrulanan istemci cihaza gönderilmek üzere erişim noktasına bir kabul (Accept) mesajı gönderir. Erişim noktası, istemci cihazın portunu yetkilendirilmiş duruma getirir.

v. İstemci cihaz, kimlik doğrulama sunumcusundan, sunumcunun kimlik bilgisini (ID) ister. Kimlik doğrulama sunumcusu kimlik bilgisini istemci cihaza gönderir.

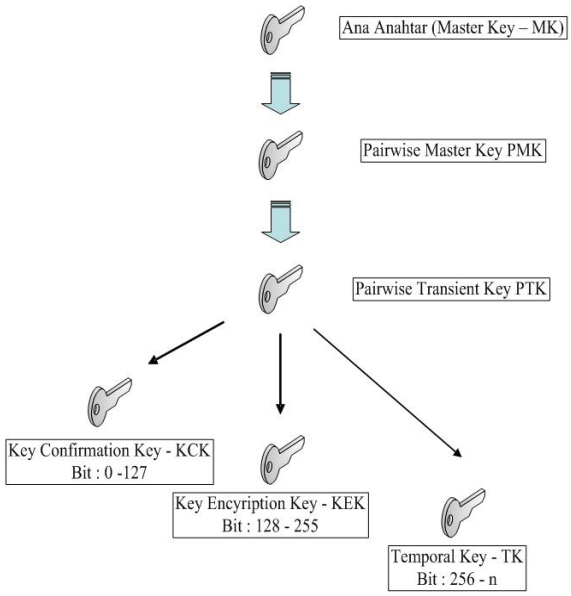
vi. İstemci cihaz, kimlik doğrulama sunumcusunun kimliğini doğruladığında, halka tamamlanır ve veri trafiğine başlanır.

Anahtar yönetimi: 802.1X kapsamında anahtar yönetim fonksiyonu da sunulmaktadır. İstemci cihaz ve kimlik doğrulama sunumcularının bir adet ana anahtarı (Master Key - MK) bulunmakta olup, bu anahtar kullanılarak, grup anahtar kümesi ve oturum anahtar kümesi olmak üzere iki farklı anahtar kümesi üretilmektedir. Grup anahtar kümesi, erişim noktası ve ona erişen istemci cihazlar arasında çoğullamada (multicast) kullanılmaktadır. Oturum anahtarları ise erişim noktası ile istemci cihazlar arasındaki bağlantı sırasında oluşturulmaktadır. Kimlik doğrulama işlemi sonunda, hem istemci cihaz tarafından hem de kimlik doğrulama sunumcusu tarafından MK'lerden, PMK (Pairwise Master Key) üretilmektedir. PMK, alt seviyede şifrelemede kullanılacak anahtarları üretmek maksadıyla kullanılmaktadır. Kimlik doğrulama işleminden sonra, kimlik doğrulama sunumcusu ürettiği PMK'yı kimlik doğrulayıcı olan erişim noktasına göndermektedir. Böylece hem istemci cihaz ve hem de erişim noktası PMK'dan alt seviyede gerekli şifreleri üretebilmektedirler [24-27, 35].

Kimlik doğrulama sunumcusunun olmadığı durumlarda, yani ev kullanıcıları veya küçük işyerlerinde, yukarıdaki işlemler, kimlik doğrulama sunumcusu olmadan yapılmaktadır. PMK, istemci cihaz ve erişim noktası üzerinden manuel olarak elle girilmektedir. Böylece alt seviyede kullanılacak diğer anahtarlar üretilmekte ve kimlik doğrulama sunumcusu kullanılmadan gerçekleştirilen bu işlemde tek fark önceden dağıtılan anahtarların kullanılması durumudur.

Şekil 2.13.'de görüldüğü gibi, 802.1X'de anahtar yönetimi hiyerarşik bir şekilde yapılmaktadır. İstemci cihaz tarafında, kimlik doğrulama sonrasında MK'dan üretilen PMK bulunmakta, sunumcu tarafında ise MK'dan üretilen PMK, erişim

noktasına iletilmektedir. Bu sayede istemci cihaz ve erişim noktası, bu anahtarlardan alt seviyede kullanılacak olan diğer anahtarları üretmektedirler. Bu anahtarlardan, sadece geçici anahtardan (Temporal Key - TK) elde edilen geçici ve tek kullanımlık anahtarlar üretilmektedir [26-27, 35, 38].

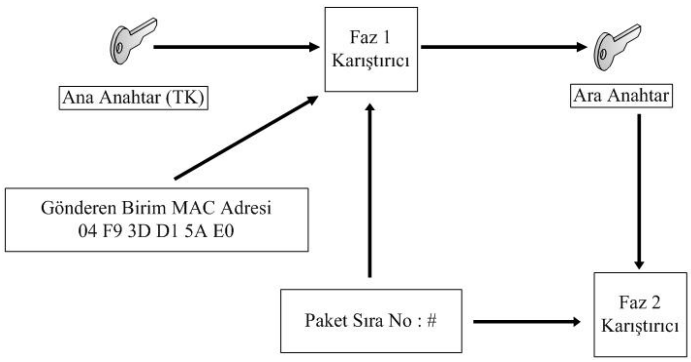


Şekil 2.13. 802.1x Anahtar üretim ve kullanımı.

Şifreleme: Anahtar yönetim mekanizması ile üretilen anahtarların dağıtımı tamamlandıktan sonra güvenli veri transferi işlemleri başlamaktadır. 802.11i standardında üst katman kimlik doğrulama ve anahtar dağıtımını, alt katman ise kriptografik şifrelemeyi sağlamaktadır. Şifreleme için IEEE 802.11i standardında ileri şifreleme standardı olan AES şifreleme algoritması kullanılmaktadır. Bu algoritmayı kullanan şifreleme protokolü CCMP (Counter-Mode/CBC-MAC Protocol) olarak adlandırılmaktadır. CCMP protokolü, AES şifreleme algoritmasını kullanabilmesi için ek donanıma ihtiyaç duymaktadır. IEEE 802.11i standardı kapsamındaki şifreleme protokolünde, piyasada bulunan ürünlerin mevcut donanımında değişikliğe gerek duyulmadan, sadece yazılım değişikliği ile bu katmanda ikinci bir şifreleme protokolü TKIP (Temporal Key Integrity Protocol) kullanılmaktadır [24-27, 35, 38, 40, 44].

TKIP (Temporal Key Integrity Protocol): TKIP protokolü, mevcut ürünlerin donanımında herhangi bir değişiklik yapmadan, sadece yazılım değişikliği yapılarak güvenli veri transferini sağlamak maksadıyla geliştirilmiştir. Bu nedenle, alt katmanda WEP mekanizmasını kullanmaktadır. TKIP'te; WEP mekanizmasının açıklarını ve zayıflıklarını yok edecek şekilde güvenli veri transferini gerçekleştirmek için bir dizi önlemler alınmıştır. WEP mekanizmasının etrafında bir kabuk görevi gören TKIP hakkında, CCMP protokolüne göre daha fazla işlem içerdiğinden, güvenlik sağlamaktan ziyade kullanıcılara zorluk çıkardığı görüşü hakimdir [35, 38, 40, 44]

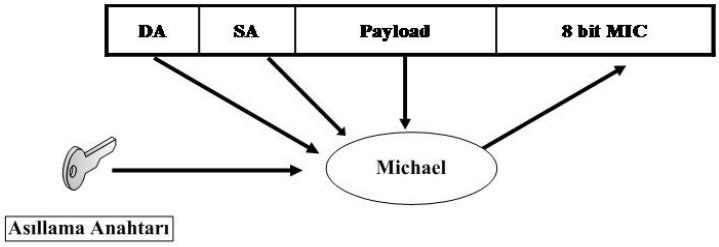
TKIP'de başlama vektörü (IV) 48 bite çıkarılmış olup, hem paketlere sıra numarası vermek, ve hem de her paket için tek kullanımlık anahtar üretmek için kullanılmaktadır. Paketlere sıra numarası verilmesi, "replay" saldırılarını önlemek için uygun bir yöntem olup, sıra numarası olmadan ve sırasız gelen paketlerde alıcı birim tarafından dikkate alınmamaktadır. 48 bit uzunluğundaki IV kullanımı ve aynı TK ile üretilecek tek kullanımlık anahtarlar çok sürelerde bir tekrarlanmaktadır. Bu nedenle, WEP mekanizmasındaki IV çatışmasından kaynaklanan saldırılar bu sayede önlenmektedir. TKIP'te tek kullanımlık anahtar üretimi Şekil 2.14.'de gösterilmiş olup, her paket için kullanılan IV değerleri TKIP'de değişmektedir. Bu yaklaşım ise, zayıf anahtar üretiminden faydalanan saldırıları önlemektedir [25-27, 35, 38, 40, 44].



Şekil 2.14. TKIP Tek kullanımlık anahtar üretimi.

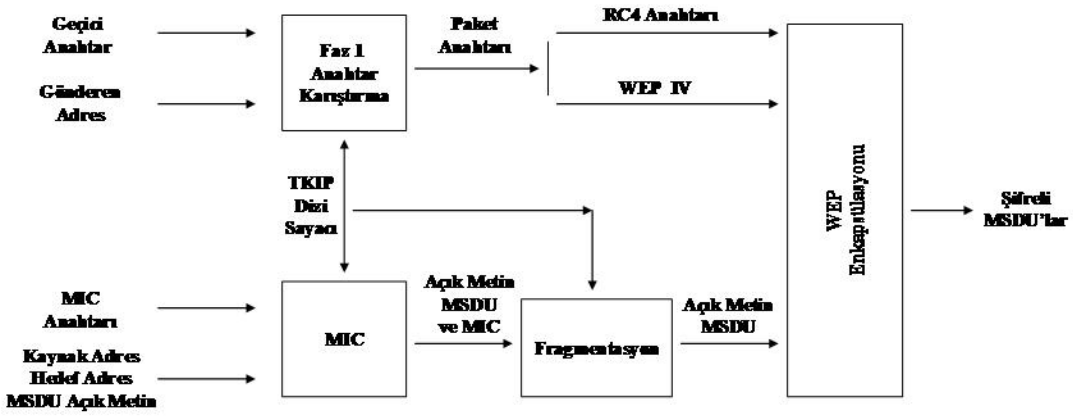
TKIP'de veri bütünlüğünü sağlamak için özellikleri daha önce sunulan "Michael" algoritması kullanılmaktadır. Michael - Mesaj Bütünlük Kodu (Message Integrity

Code – MIC), kaynak ve varış MAC adreslerini ve veriyi alarak bir sağlama bitleri toplamı (checksum) oluşturmaktadır. Bu sağlama bitleri, verinin sonuna şifrelenerek eklenmektedir. Bu yöntem, mesaj içeriğinin değiştirilmesini önlemekte olup, ayrıca WEP mekanizmasının tersine, alıcı ve göndericinin adresleri açık bir şekilde gönderilmemektedir. Michael algoritması Şekil 2.15.'de sunulmuştur [38, 40, 44].



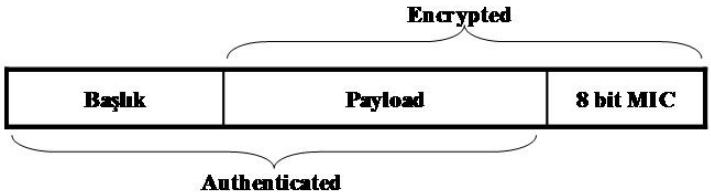
Şekil 2.15. Michael algoritması.

CCMP (Counter-Mode / CBC-MAC Protocol): CCMP, IEEE 802.11i protokolünün yeni şifreleme yöntemidir. Gelişmiş ve güçlü bir şifreleme algoritması olan AES (Advanced Encryption Standard)'i kullanmaktadır. Şekil 2.16.'da aşamaları sunulan AES şifreleme birçok farklı modda kullanılabilmekte olup, IEEE 802.11i standardı, AES'i CBC-MAC ile sayaç (counter) metodunu kullanır. Anahtar uzunluğu 128 bit olup, IEEE 802.11i standardında CCMP protokolünü kullanmak zorunludur [40, 44].



Şekil 2.16. TKIP'de Veri şifreleme aşamaları.

CCMP'de de IV kullanılmaktadır ve uzunluğu 48 bittir. IV, paketlere sıra numarası vermek için kullanılmaktadır. Bu paket numarası daha sonra, diğer bilgilerle beraber hem mesaj bütünlük kodu (MIC) oluşturmak, hem de paketi şifrelemek için AES şifreleme algoritmasında parametre olarak kullanılmaktadır. Şekil 2.17.'de CCMP ile oluşan paket görülmektedir.



Şekil 2.17. CCMP ile oluşan paket.

2.9.2. RSN Ağların Değerlendirilmesi

WPA protokolü, eski nesil cihazlardaki güvenliği, daha önce bahsedilen bir istisna dışında (20 karakterden az olmayan bir parola "passphrase" kullanımı) kabul edilebilir bir seviyeye çıkarmıştır. Buna mukabil, RSN protokolü ise, 802.11 serisi için kablosuz iletişim güvenliğinin son noktası olarak görülmektedir [8, 24, 34, 39].

i. IEEE 802.11i standardı, WEP mekanizmasında bulunmayan bir özellik olan anahtar yönetim fonksiyonunu hiyerarşik bir şekilde sunmaktadır.

ii. İstemci cihazlar, bir kimlik doğrulama sunumcusu tarafından doğrulanmakta, aynı zamanda istemci cihazlar da sunumcuyu (karşılıklı doğrulama - Mutual Authentication) doğrulamaktadırlar. Kimlik doğrulama, IEEE 802.11i standardı ve RSN'de zorunlu bir işlemdir.

iii. Kimlik doğrulama için kullanılan IEEE 802.1X protokolü, üst katman doğrulama protokollerini de desteklemektedir. Kimlik doğrulama sunumcusu olarak en yaygın kullanılan sunumcu RADIUS sunumcudur.

iv. Güçlü bir şifreleme algoritması olan AES'i kullanmaktadır. Böylece daha güvenilir şifreleme sağlanmaktadır.

v. Veri bütünlüğü, WEP'e göre daha güvenilir hale getirilmiş olup, RSN ayrıca dolaşımı (roaming) fonksiyonunu da desteklemektedir.

2.10. WEP, WPA ve RSN Güvenlik Protokollerinin Karşılaştırılması

WEP Mekanizması, WPA ve RSN güvenlik protokolleri ile ilgili özellikler kapsamında karşılaştırmalı tablo Çizelge 2.2.'de sunulmuştur.

Çizelge 2.2. WEP, WPA ve RSN protokollerinin karşılaştırılması.

Özellikler	**WEP**	**WPA**	**RSN**
Şifreleme Mekanizması	RC4 IV Kullanımı Sebebiyle Zayıf	RC4 / TKIP	AES / CCMP CCMP / TKIP
Şifreleme Anahtar Boyu	40 bit	128 bit	128 bit
Paket Başına Düşen Şifreleme Anahtarı	Birleştirilmiş	Karışık	İhtiyaç yok
Şifreleme Anahtar Yönetimi	Yok	802.1X	802.1X
Şifreleme Anahtar Değişimi	Yok	Her Paket İçin	İhtiyaç yok
IV Boyutu	24 bit	48 bit	48 bit
Kimlik Doğrulama	Zayıf	802.1X - EAP	802.1X - EAP
Veri Bütünlüğü	CRC 32 - ICV	MIC (Michael)	CCM
Başlık Bütünlüğü	Yok	MIC (Michael)	CCM
Replay Saldırılarının Önlenmesi	Yok	IV Dizisi	IV Dizisi

WEP mekanizmasında; üretici tanımlı bazı istisnalar hariç, 24 bitlik IV değeri ile 40 bitlik bir şifreleme anahtarı kullanılmaktadır. Bazı üreticiler ürünlerinde daha uzun (128/256 bit) anahtar boyutları kullanmaktadır. Ancak orijinal 802.11 en az 40 bitlik bir şifreleme anahtarı gerektirmektedir. Ağda paylaşılan ve tüm ağ elemanları tarafından kullanılan şifreleme anahtarı, yayınlanan paket başına IV değerleri ile

birleştirilmektedir. WEP mekanizması, sisteme gömülü olan herhangi bir anahtar yönetim mekanizmasına sahip değildir ve şifreleme anahtarı kullanılmadan da açık sistem kimlik doğrulama (Open system Authentication) çalışabilir. Mekanizmada otomatik veya periyodik olarak kullanılan anahtar yönetim ve değişim özelliği bulunmamaktadır. Bu kapsamda aynı IV değerinin tekrar kullanılmasına, saldırganlarca ağda kullanılan şifreleme anahtarının deşifre edilmesine ve zayıf IV'lerin yakalanmasına imkan tanınmaktadır. WEP mekanizmasının kimlik doğrulama mekanizması zayıftır ve veri bütünlük kontrolü, şifre korumalı olmayan CRC-32 ve ICV kullanılarak gerçekleştirilmektedir. Bir başka önemli zafiyet ise, WEP mekanizmasının "replay" saldırı önleme mekanizması ile başlık bütünlük kontrol mekanizmasına sahip olmamasıdır.

2003 yılında, WEP mekanizmasının zafiyet ve açıklarına karşı geçici bir çözüm olarak ortaya atılan WPA protokolü ve bu protokolü kullanan ürünler, Wi-Fi üreticiler birliği tarafından ilgili standardın onaylanmasını beklemeksizin piyasaya sürülmüştür. Söz konusu dönemde, kablosuz ağlar üzerine kurulu 802.11i standardının özelliklerinin bir alt kümesi olan WPA protokolünün, kablosuz iletişim alanında büyük bir güvenlik gelişmesi olduğu değerlendirilmiştir. WPA protokolü, piyasada mevcut ürünler gamı ile işletilmekte olan tüm kablosuz yerel alan ağ alt yapısını desteklemektedir. Kullanıcılar, mevcut kablosuz ağları üzerinde standart bir yazılım güncellemesi yaparak kolayca WPA protokolüne geçiş yapabilmektedir. WEP mekanizmasına yöneltilen sayısız eleştiriler ışığında, WPA protokolünün, bir çok alanda WEP mekanizmasından daha üstün özelliklere sahip olduğu bilinmektedir. Bu özellikler, RC4 - TKIP şifreleme mekanizması kullanımı, 128 bitlik anahtar boyu, gönderilen her paket başına karışık tipte şifreleme anahtarı kullanımı, 802.1X tipi dinamik şifreleme anahtarı yönetimi, 48 bitlik başlama vektörü (IV) boyu, kimlik doğrulama için 802.1X - EAP kullanımı, "replay" saldırılarını önlemek için veri ve başlık bütünlüğünü sağlamak üzere TKIP ve IV dizisine eklenen MIC şifreleme özellikleridir.

WAP protokolünün WEP mekanizmasına göre ilk ve en temel üstünlüğü bu protokolde TKIP mekanizmasının kullanılmasıdır. TKIP mekanizması; hem istemci

cihaz ve hem de erişim noktaları tarafından paylaşılan 128 bitlik geçici anahtar, istemci cihazın MAC adresi ve 48-bitlik paket dizi numarasını tanımlayan başlatma vektörü (IV) kullanmaktadır. Bu mekanizma, bir kimlik doğrulama sunumcusu üzerinden, ağdaki elemanlar arasında, port tabanlı erişim kontrolü ve karşılıklı kimlik doğrulama işleminin esas almaktadır. Kimlik doğrulama metodunun tam bir uygulaması olan genişletilebilir kimlik doğrulama protokolü (Extensible Authentication Protocol - EAP), 802.1X'in ortak kimlik doğrulamayı yönetmek için kullandığı protokoldür. Bu protokol, spesifik bir kimlik doğrulama mekanizması için, kablosuz ağlarda genel bir alt yapı sunmaktadır. Bu alt yapı üzerinde kullanılabilecek kimlik doğrulama metotları; parolalar, açık anahtar altyapısı (Public Key Infrastructure - PKI) sertifikaları veya diğer kimlik doğrulama jetonları olabilmektedir [35, 42].

Daha önce belirtildiği üzere, WPA protokolünde, en az 20 karakterden uzun parola bloklarının kullanılması, ağa yönelik saldırıları bertaraf etmek için gerekli görülmektedir. Bu şekilde bir parola bloğu seçimi bir çok ağ yöneticisinin veya kullanıcının tercih edeceğinden çok daha uzundur. Parolaların daha kısa olması durumunda, çevrim dışı bir saldırının, WEP mekanizmasına yapılan saldırılardan daha kolay hale geleceği düşünülmektedir.

RSN, 802.11i standardında belirtilen özelliklere sahip kablosuz ağlar için hali hazırdaki ve şu ana kadar geliştirilmiş olan en güçlü güvenlik sistemidir. WEP ve WPA' ya ithaf edilen bütün zafiyet ve kusurlar kapsamında, 802.11i standardı ve RSN'nin tam bir güvenlik sağladığı değerlendirilmektedir.

802.11i standardı, 2004 yılında onaylanmış ve takip eden dönemde RSN uyumlu ürün ve cihazlar piyasaya sürülmüştür. Kablosuz ağ güvenliğinde nihai çözüm olarak kabul edilen 802.11i standardının bu alanda tam bir güvenlik sağlaması beklenmektedir. RSN, WPA protokolünün sunduğu tüm avantajları sunmasının yanı sıra, AES şifreleme algoritması ve veri seti ile paket başlığının bütünlüğü için CCM kullanmaktadır.

WPA protokolü, eski nesil kablosuz ağ alt yapısını desteklediği için, hali hazırdaki WEP mekanizması kullanan ağ alt yapısı üzerine, basit bir yazılım güncellemesi aracılığıyla hem ucuz hem de zahmetsiz olarak gerçekleştirilebilmektedir. RSN güvenlik protokolü için ise böyle bir durum söz konusu değildir. Çünkü RSN protokolünde AES şifreleme algoritması kullanılabilmesi için ekstra donanım ile ilgili yazılımların güncellemesine ihtiyaç vardır.

Kablosuz güvenlik protokolleri, ileri seviye kripto analistlerin danışmanlığında, geniş öngörüler kapsamında hazırlanmalarına rağmen, her zaman istenen güvenlik seviyesinin elde edilmesi mümkün olmamaktadır. Bu nedenle, kablosuz ağların tüm güvenlik ihtiyaçlarını karşılayacak nihai güvenlik çözümüne ulaşılacak şekilde, güvenlik standart ve protokolleri sürekli olarak güncellenmekte ve yeniden tasarlanmaktadır [43]. Ancak, saldırganların teknoloji takibi ile elde ettikleri, bilgi birikimi ve tecrübelerinin kendi aralarında sürekli geliştiği ve paylaşıldığı günümüz güvenlik ortamında, kablosuz ağlara yönelik olarak bir çok açık kaynak ve ticari saldırı araç, saldırı analiz, yöntem ve yazılım seçenekleri internet üzerinden bile kolayca elde edilebilmektedir. Halihazırda piyasadan kolayca elde edilebilecek kablosuz ağ güvenlik tarama araç ve yazılımlarından bazılarına ait liste EK-1'de verilmiştir.

3. MATERYAL VE METOD

Bu bölümde, kablosuz ağlarda çok daha yaygın olarak ve daha çok kurumsal kullanıcılar dışında kalan kullanıcılar tarafından bireysel olarak kullanılan WEP güvenlik mekanizması içerisindeki isteğe bağlı özelliklerin veri aktarım hızına etkisini ölçmek üzere veri toplamak maksadıyla bir test ortamı oluşturulmuş, test düzeneği için aşağıdaki faaliyetler gerçekleştirilmiştir.

Donanım ve yazılım özellikleri aynı olan 2 adet HP Compaq nx5000 diz üstü bilgisayar kullanılmıştır. Bu bilgisayarların kablosuz ağları destekleme özellikleri incelenmiş ve her ikisinin de hem donanım ve hem de yazılım olarak kablosuz iletişimi destekledikleri görülmüştür. Test bilgisayarlarının donanım ve işletim sistemleri ile ilgili genel bilgiler aşağıda verilmiştir.

İşletim Sistemi	: Microsoft XP Professsional
Service Pack	: 2
Mikro işlemci	: Intel Centrino Mobile Technology
Mikro İşlemci Hızı	: 1.6 GHz
RAM	: 504 MB
Kablosuz Ağ Adaptörü	: Intel (R) Pro Wireless 2200BG

Yapılan incelemede oluşturulacak olan ağın hem donanım olarak ve hem de yazılım olarak gerçekleştirilebileceği belirlenmiş, her iki alternatif tasarsız (Peer-to-Peer / Ad Hoc) kablosuz ağ yapısı ile ilgili özellikleri ve test ortamında hangisinin kullanılmasının uygun olacağı açısından ayrı ayrı değerlendirilmiştir.

Öncelikle Windows XP işletim sisteminin sunduğu kablosuz ağ yapısı incelenmiş, bu yapının ad-hoc ağları desteklediği, ateş duvarı özelliğinin kablosuz ağlar için kullanılabildiği, güvenlik mekanizması olarak açık kimlik doğrulama, paylaşımlı kimlik doğrulama uygulamaları ile WEP ve WPA güvenlik protokollerini de desteklediği belirlenmiştir. Donanım olarak ise test bilgisayarlarında bulunan Intel (R) Pro Wireless 2200BG ağ adaptörünün de kablosuz ad-hoc yapıyı ayrıca

desteklediği, 802.11b ve 802.11g standartlarında 2.4 GHz frekans bandında toplam 13 kanal kullanılabildiği, ancak sadece açık kimlik doğrulama uygulaması ile WEP güvenlik protokolünün desteklendiği görülmüştür.

WPA ve RSN/WPA2 güvenlik protokolleri sahip olunan donanım ve yazılım tarafından desteklenmediği ve ad-hoc kablosuz ağ yapısını desteklemedikleri görülmüştür.

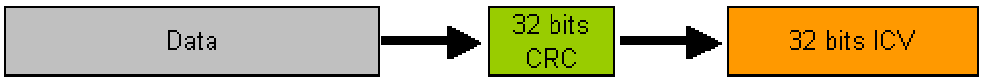
Bu kapsamda güvenlik mekanizmalarının veri aktarım hızı üzerindeki etkilerini belirlemek üzere test ortamında daha geniş bir perspektif sunması nedeniyle Windows XP işletim sistemi ile veri aktarım hızının daha sağlıklı olarak ölçülebilmesi ve erişim noktası üzerindeki gecikme etkilerinden kaçınmak maksadıyla ad-hoc kablosuz ağ uygulamalarının kullanılması tercih edilmiştir.

3.1. WEP Güvenlik Mekanizmasının Çalışma Prensipleri

WEP genellikle şifreleme için 40 veya 104 bit uzunluktaki anahtarları kullanmaktadır. Bazı üreticilerin 232 bit uzunluğuda destekleyen ürünleri piyasaya sürdükleri bilinmektedir. Bu anahtar uzunluğuna 24 bit uzunluğundaki Başlama Vektörü (Initialization Vector)'nün eklenmesiyle toplam anahtar uzunluğu 64, 128 ve destekleyen ürünlere sahip olunduğunda ise 256 bite kadar çıkmaktadır [24-29].

40 bit uzunluğundaki anahtar için 10 adet hexadecimal veya 5 adet alfa nümerik değer kullanılmaktadır. Bu anahtar istemci cihaz ve erişim noktaları tarafından ağa bağlanmak için sahip olunması gereken anahtardır. Diğer ifade ile WEP anahtarı tüm kullanıcılar tarafından bilinmesi ve cihazlara yüklenmesi gereken bir anahtardır.

WEP şifreleme mekanizmasında ilk önce açık veri üzerinden 32 bit uzunluktaki CRC (Cyclic Redundancy Code) değeri elde edilmektedir. Bu değer daha sonra Şekil 3.1.'de görüldüğü üzere bütünlük kontrol değeri (Integrity Check Value – ICV) olarak kullanılmaktadır [24-29, 43-44].

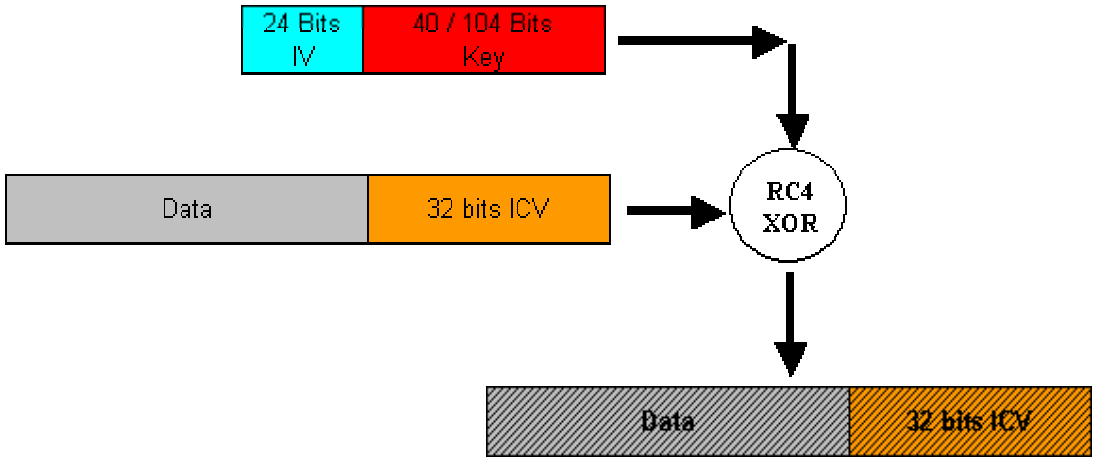


Şekil 3.1. ICV Değerinin elde edilmesi.

Daha sonra Şekil 3.2.'de gösterilen 40 bit uzunluktaki şifreleme anahtarı ve 24 bit uzunluktaki başlama vektörü (IV) değeri rasgele veya sıralı olarak belirlenmektedir.

Şekil 3.2. WEP anahtarı ve başlama vektörü.

24 bitlik başlama vektörü ile 40 bitlik şifreleme anahtarı birbirlerine eklenmekte ve şifreli veri elde edilmek üzere RC4 şifreleme algoritmasından geçirilmektedir. ICV değeri şifrelenecek açık metine eklenmekte RC4 şifreleme algoritmasından gelen grup ile XOR işlemine tabi tutulmaktadır. Sonuçta ortaya çıkan ve Şekil 3.3.'te görülen paket şifreli bir veri paketi haline gelmektedir [24-27, 29, 35, 43-44].



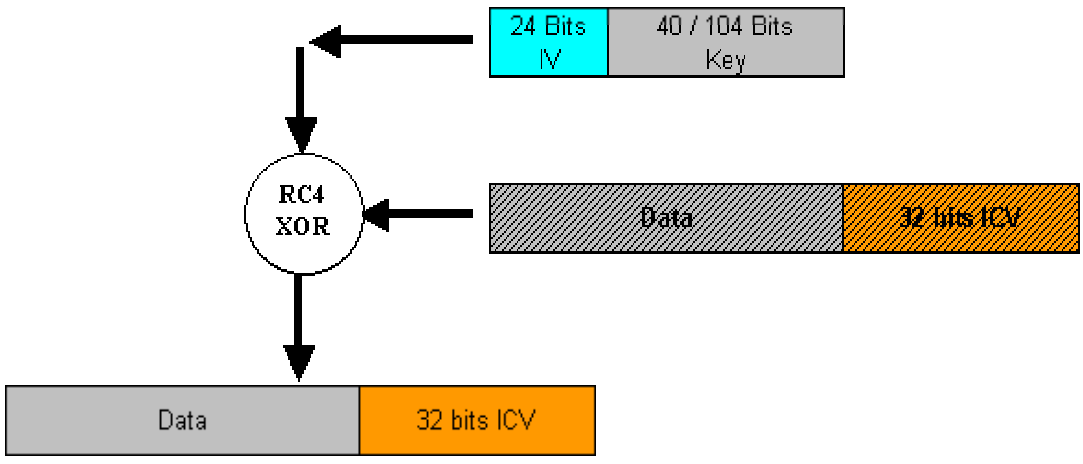
Şekil 3.3. Şifrelenmiş veri paketinin elde edilmesi.

Daha sonra Şekil 3.4.'de gösterildiği gibi 802.11 Başlık (Header) bilgisi ve 24 bit IV değeri bu pakete eklenmekte ve kablosuz ağ üzerinden gönderilmeye hazır veri paketi oluşturulmaktadır. Dikkat edilirse 802.11 başlık bilgisi ile 24 bitlik IV değeri paket içerisinde şifresiz olarak gönderilmektedir [24-29, 35].

Şekil 3.4. Şifrelenmiş veri paketinin gönderilmesi.

RC4 şifreleme, dizi tipi bir şifreleme algoritması olup, herhangi aynı bir şifreleme anahtarı tarafından üretilecek şifreli veri hep aynı olmaktadır. Ayrıca RC4 algoritmasında olduğu gibi bir açık veri grubunu XOR işlemine tabi tutmak her defasında aynı şifreli veri paketini vermektedir. Bu nedenle şifreli veri paketi üzerinde uygulanacak bir ters XOR işlemi de açık veri paketine erişilmesine imkan sağlamaktadır [29, 35, 43-44].

Alıcı tarafta ise Şekil 3.5.'te sunulan şekilde bu işlemlerin tersi gerçekleştirilerek açık veri paketi elde edilmektedir. Alıcı taraf şifreli paketle, açık olarak gelen 24 bitlik IV değeri ile kendisi tarafından bilinen 40 bitlik şifreleme anahtarını birbirlerine eklemekte ve şifreli olarak gelen veri paketinin veri ve ICV değerlerini RC4 şifreleme algoritmasından XOR işlemine tabi tutarak geçirmektedir. Böylece açık veri grubu ile 32 bitlik ICV değeri elde edilmektedir [24-29].

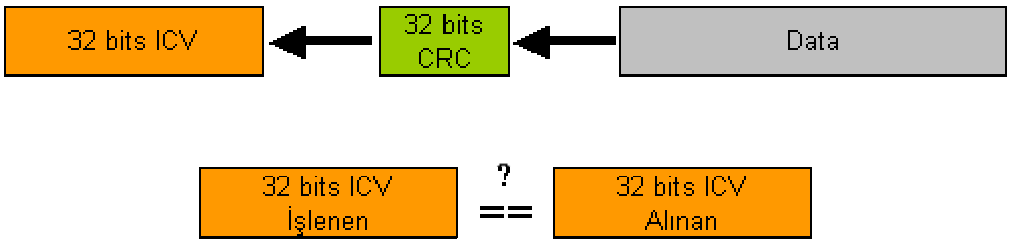


Şekil 3.5. Açık veri paketinin elde edilmesi.

Daha sonra alıcı taraf Şekil 3.6'daki gibi açık veri grubu üzerinden 32 bit uzunluktaki CRC (Cyclic Redundancy Code) değerini elde etmektedir.

Şekil 3.6. 32 bit CRC değerinin elde edilmesi.

Elde edilen değer Şekil 3.7.'de gösterildiği gibi şifreli veri paketi ile birlikte gelen ICV değerinin içeriği ile karşılaştırılmakta ve değerler birbirlerine eşit ise veri paketi kabul edilmekte farklı ise reddedilmektedir. Bu işlem kablosuz ağ üzerinden gönderilen ve veri yükü (payload) olarak adlandırılan büyüklükteki veriyi taşıyacak olan tüm paketler için aynı şekilde tekrarlanmaktadır [24-29].



Şekil 3.7. CRC ve ICV değerlerinin karşılaştırılması.

40 bit şifreleme anahtarı kullanılarak ortaya konulan bu çalışma prensipleri 104 bit şifreleme için de aynı şekilde gerçekleştirilmektedir.

Yukarıda ortaya konulan çalışma prensipleri kapsamında şifresiz olarak gerçekleştirilen bir kablosuz ağ iletişimine oranla şifreli iletişim doğal olarak mikro işlemci seviyesinde hem gönderen ve hem de alan tarafta belirli bir işlem zamanının harcanmasına neden olmaktadır. Bu çerçevede şifresiz iletişim ile şifreli iletişim arasında, ayrıca 64 bit şifreleme ile 128 bit şifreleme arasında mikro işlemci ve veri aktarım hızı açısından belirli seviyede bir fark olması beklenmektedir.

Bu çalışmada ortaya konulan test ortamı ve test topolojisi de söz konusu farkın var olup-olmadığı, var ise ne oranda bir fark olduğu ile bu farkın güvenlik riskleri açısından önemini tespit etmeye yönelik olarak kurulmuştur.

3.2. Test Ortamı

İşletim sisteminin sağladığı ad-hoc kablosuz ağ alt yapısı kullanılarak bir ağ oluşturulmuştur. Bu maksatla Windows desteği alınarak test bilgisayarlarının önce kablosuz olarak görüşmeleri için isteğe bağlı olarak otomatik veya manuel olarak çalışan Adhoc-İnternet isimli özel bir ağ tanımlanmıştır. Bu ağa ait temel özellikler aşağıda sunulmuştur.

Frekans Bandı	: 2.4 GHz
Kullanılan Kanal No	: 11
Kullanılan Frekans	: 2462 MHz
Desteklenen Kablosuz Ağ Standartları	: 802.11b ve 802.11g
Veri Hızı	: 54 Mbps (Teorik)
Kimlik Doğrulama	: Açık ve Paylaşımlı
Şifreleme	: Yok, WEP 64 bit ve WEP 128 bit
Mesafe	: 30 cm
Test Yapılan Yer	: Büro ortamı ve Faraday Kafesi
Test Zamanları	: Gündüz 10.00 – 16.00

Test ağına bağlı bilgisayarlar önce internet paylaşımı (İnternet Connection Sharing) için ve daha sonra ise dosya ve yazıcı paylaşımı (File and printer sharing) için konfigüre edilmişlerdir.

1 numaralı bilgisayar yerel alan ağı üzerinden internete bağlı bir makinedir ve 2 numaralı bilgisayar kablosuz ağ erişimi ile 1 nci bilgisayar üzerinden internete erişmektedir. Benzer şekilde 2 numaralı bilgisayar üzerinde paylaştırılmış bir klasör oluşturulmuş olup 1 numaralı bilgisayar da bu klasöre erişmekte okuma, yazma, silme ve güncelleme yapabilmektedir. 2 numaralı bilgisayar üzerinde oluşturulan paylaşımlı klasör 1 numaralı bilgisayar üzerinde (My Computer - Map Network Drive) ağ sürücüsü haritalama özelliği kullanılarak “Z” sürücüsü olarak tanıtılmıştır. Yazıcı kullanımı için ise 1 numaralı bilgisayar üzerinde tanımlı ve paylaştırılmış olan yazıcı kablosuz ağ üzerinden ortak olarak kullanılmaktadır.

Kablosuz ağ kurulum ve konfigürasyonu, internet hizmeti paylaşımı, dosya ve yazıcı paylaşımı için "Microsoft Windows XP Ad Hoc Internet Sharing with Microsoft Windows XP" [45] ve "Microsoft Windows XP File and Printer Sharing with Microsoft Windows" [46] destek dokümanlarından faydalanılmıştır.

Ölçümlerin elde edilmesinde olası dezavantajlarından kaçınmak maksadıyla kullanılan WEP 64 bit ve WEP 128 bitlik şifreler tüm uygulamalar için aynı karakter dizisi olarak seçilmiştir. Bu sayede farklı anahtarların işlem süresi üzerinde yaratması muhtemel iş yükünün etkileri bertaraf edilmiştir. Test; iyonizasyon etkilerinin bertaraf edilmesi açısından gündüz saatlerinde ve aynı yerde yapılmıştır.

3.3. Test Programı

Test bilgisayarları arasında gerekli olan kablosuz ağ oluşturulduktan sonra, 1 numaralı bilgisayar üzerinde bulunan Borland C/C++ derleyicisi kullanılarak bir program yazılmıştır. Bu program; 1MB, 2 MB, 4 MB, 8 MB, 16 MB, 32 MB ve 64 MB olmak üzere önceden hazırlanmış olan 7 farklı uzunluktaki metin dosyalarını 2 numaralı bilgisayar üzerindeki bulunan paylaştırılmış klasör yani "Z" sürücüsü içerisine aktarmakta ve işlem süresini ölçmektedir. Söz konusu programda işlem tekrar sayısı ölçümlerin istatiksel olarak sağlıklı olmasını sağlayacak şekilde 100 olarak belirlenmiştir. 1 numaralı bilgisayar üzerinde çalışan ve ilgili dosyayı 2 numaralı bilgisayar üzerindeki paylaştırılmış sürücüye saniyenin yüzde biri cinsinden ölçüm yaparak kopyalayan C/C++ programlama dili ile yazılmış olan bu program parçası Şekil 3.8.'de sunulmuştur.

Program içerisinde, zaman ölçümü için C/C++ programlama dili <*time.h*> kütüphanesinde tanımlı bulunan "time struct" kayıt yapısı, program içerisinde t1 ve t2 olarak adlandırılarak kullanılmıştır. Bu kayıt yapıları *ti_hour, ti_min, ti_sec ve ti_hund* alanlarından oluşmakta olup, bu alanlar sırasıyla saat, dakika, saniye ve saniyenin yüzde biri cinsinden zaman ölçümleri için kullanılmaktadır.

İstatistiki açıdan sağlıklı olması maksadıyla program işlem süresi ölçüm işlemini bir "for" döngüsü ile toplam 100 kez gerçekleştirmekte, her 25 işlem sonrası kullanıcıya verileri kaydetmesi için imkan tanımaktadır.

Program parçası sistem komutları kütüphanesinde <*dos.h*> bulunan "*system"* komutunu kullanarak *"dos"* kabuğuna çıkmakta ve veri aktarma işlemini gerçekleştirmektedir.

```
#include <stdio.h>
#include <time.h>
#include <dos.h>
#include <stdlib.h>
#include <conio.h>
#include <iostream.h>
#include <string.h>

int main ()
{
  struct  time t1,t2;
  int i=0;
  long int z1 = 0, z2 = 0, z3 = 0;

  clrscr ();
  for (i=1; i<101; i++)
  {
   gettime(&t1);
   system("copy 16MB.txt Z:16MB.txt");
   gettime(&t2);
   z1 =
(t1.ti_hour*60*60*100)+(t1.ti_min*60*100)+(t1.ti_sec*100)+t1.ti_hund;
   z2 =
(t2.ti_hour*60*60*100)+(t2.ti_min*60*100)+(t2.ti_sec*100)+t2.ti_hund;
   z3 = z2 - z1;
   printf("Olcum : %02i ",i);
   printf("  --> Islem Suresi : %d ", z3);
   if ((i % 25) == 0) getchar ();
   system("del Z:16MB.txt");
   z1 = 0;
   z2 = 0;
   z3 = 0;
  }
  printf("\nTESEKKURLER...");
  getchar();
  return 0;
}
```

Şekil 3.8. C/C++ programlama dili ile yazılmış olan veri aktarma - test programı.

Her bir kopyalama işlemi öncesinde program "gettime" komutunu kullanarak sistem zamanını *t1* kayıt yapısına kaydetmekte, dosya aktarma işlemini tamamlamasını müteakip aynı komut tekrar kullanılarak son sistem zamanını *t2* kayıt yapısına

kaydetmektedir. Dolayısıyla parametrik olarak programa sunulan her bir dosyanın aktarma işleminin süresi bu iki kayıt yapısı tarafından kaydedilen zaman ölçümlerinin farkı olarak hesaplanmaktadır. Programda saat, dakika, saniye cinsinden olan ölçümler saniyenin yüzde biri cinsine dönüştürülmektedir. Böylece her bir işlem süresi saniyenin yüzde biri cinsinden elde edilmekte ve sadece aktarma işlemi öncesi ve işlemin bitmesini müteakip hemen sonra sistem zaman değerleri alınmakta ve hesaplamalar için veya diğer işlemler için harcanan zamanın tutarlılık açısından etkisi minimum seviyeye indirilmektedir.

İşlem süresini *t1* ve *t2* kayıt yapılarının farkını alarak saniyenin yüzde biri cinsinden hesaplayan ve *z3* değişkenine atayan program, bu değeri ekrana yazmakta ve bir sonraki aktarma işlemine geçmeden önce 2 numaralı bilgisayar üzerinde paylaştırılmış "Z" klasörüne aktardığı dosyayı silerek üstüne yazma (overwrite) işleminin bir sonraki veri aktarma hızını etkilemesi ihtimalini ortadan kaldırmaktadır.

3.4. Aktarılan Dosyalar

1MB, 2 MB, 4 MB, 8 MB, 16 MB, 32 MB ve 64 MB olmak üzere, metin dosyaları şeklinde oluşturulan dosyalar sırasıyla, 1 024 KB bit, 2 048 KB, 4 096 KB, 8 192 KB, 16 384 KB, 32 768 KB ve 65 536 KB uzunluklarında olacak şekilde ve

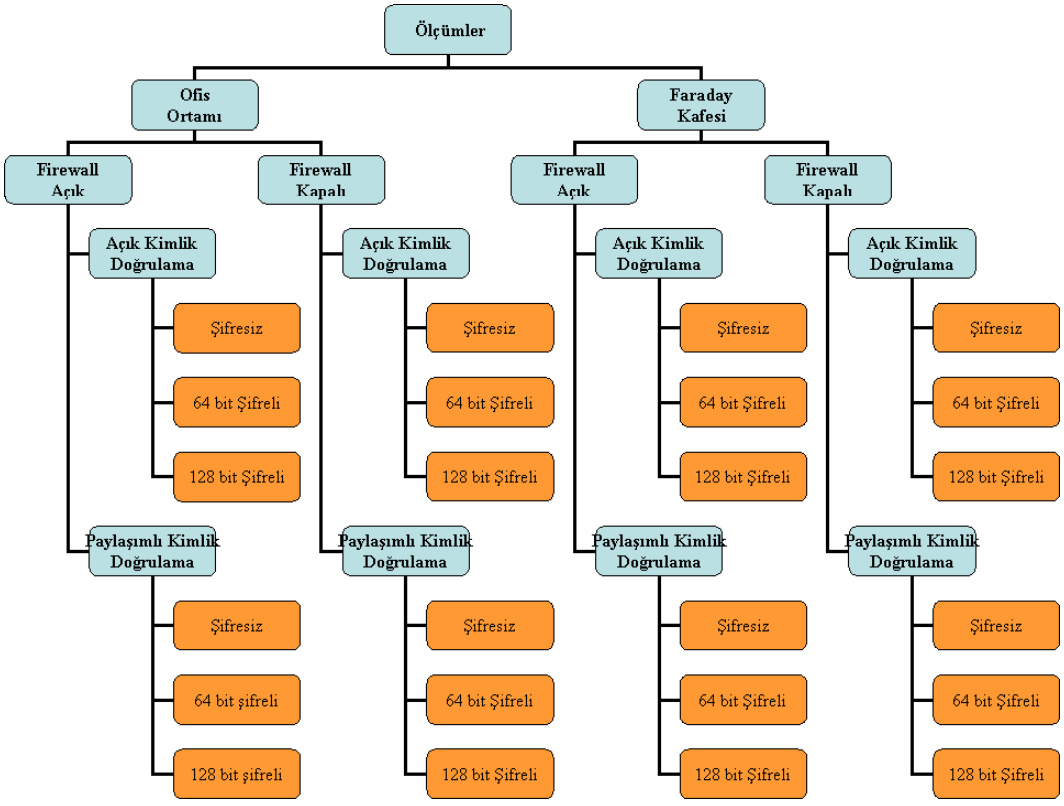
"abcdefghijklmnopqrstabcdefghijklmnopqrst"

metin bloğunun tekrarları ile oluşturulmuştur. Aşağıda test ortamında kullanılan metin dosyalarının tam uzunlukları bayt olarak sunulmuştur.

1 MB	:	1 048 576 bayt
2 MB	:	2 097 152 bayt
4 MB	:	4 194 304 bayt
8 MB	:	8 388 608 bayt
16 MB	:	16 777 216 bayt
32 MB	:	33 554 432 bayt
64 MB	:	76 108 864 bayt

3.5. Test Topolojisi

Ölçümler; önce büro ortamında, Windows XP işletim sisteminin ateş duvarı (Firewall) açık iken tüm dosya türleri için ve açık kimlik doğrulama (Open Authentication) için şifreleme yapılmadan, 64 bit ile şifreleme yapılarak ve 128 bit şifreleme yapılarak, daha sonra paylaşımlı kimlik doğrulama (Shared Authentication) için şifreleme yapılmadan, 64 bit ile şifreleme yapılarak ve 128 bit ile şifreleme yapılarak gerçekleştirilmiş daha aynı ölçümler ateş duvarı (firewall) kapalı iken tekrar yapılmıştır. Şekil 3.9.'da tek bir veri dosyası için test ve ölçüm ile ilgili genel topoloji sunulmuştur.



Şekil 3.9. Tek veri dosyası için test topolojisi (2400 ölçüm).

Büro ortamında olası diğer elektromanyetik alanlardan etkilenmenin söz konusu olabileceği düşünülerek aynı test ve ölçümler ayrıca elektromanyetik olarak korunmuş özelliklere sahip Faraday Kafesi olarak bilinen kapalı ve özel bir test ortamında yinelenmiştir. Bu sayede büro ortamında yapılan ölçümlerin enterferansa

maruz kalıp-kalmadığı ile büro ortamı ve Faraday kafesi arasında veri aktarım hızı açısından bir fark olup-olmadığının belirlenmesi amaçlanmıştır.

Faraday kafesinin kullanılması sayesinde diğer elektromanyetik alan enterferans kaynakları ile Windows XP işletim sisteminin ateş duvarının da (Firewall) veri aktarma işlemi üzerinde etkili olup-olmadığı ile ilgili bir takım sonuçlar ve değerlendirmelerin de yapılabileceği düşünülmüştür. Bu kapsamda yapılan incelemede Faraday kafesi içerisindeki ölçümler ile büro ortamındaki ölçümlerin ortalamaları dikkate alındığında aralarında çok büyük bir fark olmadığı, dolayısıyla büro ortamında kablosuz veri iletişimini etkileyen başkaca bir enterferans kaynağı olmadığı, testlerin diğer cihazların yaydığı olası elektromanyetik alanlardan etkilenmediği gözlemlenmiştir. Dolayısıyla büro ortamında yapılan testler enterferans etkilerine maruz kalmamıştır ve test enterferans açısından sağlıklı bir şekilde gerçekleştirilmiştir.

Farklı büyüklüklerdeki 7 veri paketi için her bir aktarma işleminin ortalama hızının farklı kimlik doğrulama ve farklı şifreleme özellikleri ile büro ve Faraday kafesi ortamında, ateş duvarı açık ve kapalı iken, açık ve paylaşımlı kimlik doğrulama için test edilerek belirlenmesi maksadıyla ortaya konulan test topolojisi ile toplam 2 400 X 7 = 16 800 adet veri toplanmıştır. Örnek olarak test ortamında toplanan ve büro ortamında, ateş duvarı açık iken, açık ve paylaşımlı kimlik doğrulamada, şifresiz, 64 bit ve 128 bit şifreli veri aktarma hızlarına ait değerler EK-2, diğer değerler ise tez CD'si içerisinde EK-3'te verilmiştir. Örnek olarak 1 MB uzunluğundaki dosyanın ortalama aktarım hızını ölçmek üzere şifresiz, 64 bit şifreli ve 128 bit şifreli olmak üzere toplam 100 X 3 X 2 X 4 = 2 400 adet veri toplanmıştır.

Farklı dosya boyutlarında elde edilen veri aktarım hızlarının kaba bir değerlendirmesinin yapmak üzere genel istatistikleri ve dağılımları ile görsel karakteristikleri aşağıda Çizelge 3.1.(a, b, c, d) ve Şekil 3.10.(a, b, c, d, e, f, g)'de sunulmuştur. Bu çizelge ve grafiklerin incelenmesi neticesinde şifreli iletişimin veri aktarım hızına olumsuz bir etkisinin bulunduğuna dair açıkça görülebilen tutarlı bir bilgi elde edilememektedir. Değerlerin birbirleri ile yakınlığı ise ortalamalar arasında

bir fark olmadığı düşüncesini daha çok destekler niteliktedir. Bu nedenle ortaya konulacak tespitlerin sağlıklı, tutarlı ve bilimsel olması maksadıyla istatistik biliminden yararlanma ihtiyacı kaçınılmaz görülmektedir.

Çizelge 3.1.a. Tüm dosyalar için veri aktarım hızları istatistikleri.

BÜRO_XP_Win_FW On						
	Open Authentication			Shared Authentication		
Dosya / İstatistik	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	21,90	22,73	22,51	22,13	22,88	22,67
Standart Sapma	1,69	3,27	2,85	3,66	2,67	3,11
Varyans	2,83	10,60	8,03	13,27	7,07	9,56
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	28	33	33	39	33	38
Minimum	11	11	11	16	16	16
Mod	22	22	22	22	22	22
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	28,45	28,07	28,73	27,89	27,63	27,57
Standart Sapma	4,02	3,10	3,75	2,56	3,06	3,84
Varyans	16,03	9,49	13,92	6,50	9,25	14,63
Medyan	28,00	28,00	28,00	27,50	28,00	27,00
Maximum	49	39	39	38	38	55
Minimum	11	16	16	22	16	16
Mod	27	27	28	27	27	27
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	38,55	38,55	38,22	38,32	38,77	38,16
Standart Sapma	4,06	6,37	4,75	5,79	6,00	4,26
Varyans	16,33	40,23	22,29	33,18	35,70	17,95
Medyan	38,00	38,00	38,00	38,00	38,00	38,00
Maximum	55	66	50	66	66	55
Minimum	27	22	17	27	22	22
Mod	38	38	38	38	38	38
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	58,35	58,87	60,09	60,46	59,37	59,98
Standart Sapma	9,48	9,44	10,65	12,15	10,60	9,18
Varyans	88,95	88,31	112,34	146,07	111,23	83,46
Medyan	55,00	55,00	55,00	55,00	55,00	55,00
Maximum	88	87	93	116	110	105
Minimum	28	27	28	44	27	49
Mod	55	55	55	55	55	55
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	106,28	125,39	123,08	112,67	127,82	121,88
Standart Sapma	31,95	46,82	48,64	41,51	57,45	45,42
Varyans	1010,40	2170,30	2341,79	1705,46	3266,97	2042,55
Medyan	94,00	99,00	99,00	99,00	98,50	99,00
Maximum	237	253	258	269	275	269
Minimum	44	61	82	61	55	77
Mod	93	93	93	88	88	99
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	683,21	679,05	662,61	676,71	670,60	717,89
Standart Sapma	95,29	84,81	72,73	75,43	85,17	166,57
Varyans	8989,19	7120,05	5237,16	5632,25	7182,14	27468,62
Medyan	645,50	648,00	642,00	648,00	637,00	640,00
Maximum	917	961	867	961	944	1352
Minimum	252	335	434	549	308	451
Mod	637	632	637	643	626	632
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	2261,57	2243,10	2241,24	2253,41	2220,82	2235,60
Standart Sapma	249,25	234,36	174,26	135,69	179,29	180,97
Varyans	61503,17	54377,19	30063,00	18227,64	31824,75	32421,26
Medyan	2274,00	2257,00	2247,00	2260,50	2258,00	2246,00
Maximum	2757	2713	2626	2532	2581	2790
Minimum	1318	1253	1268	1703	1296	1340
Mod	2274	2252	2153	2252	2263	2263

Çizelge 3.1.b. Tüm dosyalar için veri aktarım hızları istatistikleri.

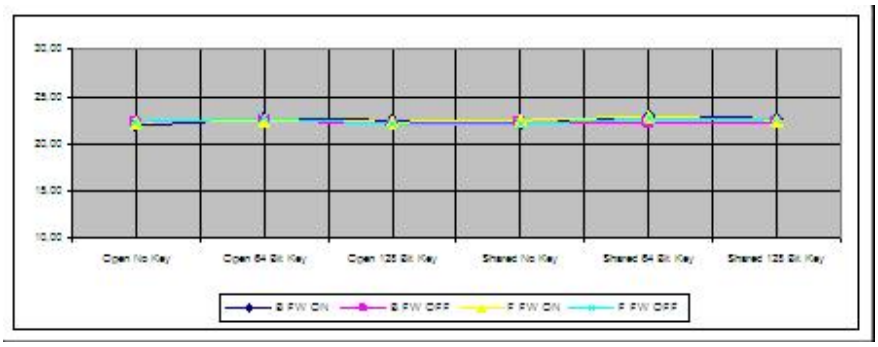
BÜRO_XP_Win_FW Off						
	Open Authentication			Shared Authentication		
Dosya / İstatistik	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	22,25	22,50	22,03	22,21	22,23	22,30
Standart Sapma	2,87	2,96	1,69	3,38	2,03	3,02
Varyans	8,13	8,67	2,83	11,33	4,10	9,05
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	33	28	38	33	33
Minimum	11	11	11	16	16	11
Mod	22	22	22	22	22	22
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	27,64	27,74	28,17	27,74	27,62	27,68
Standart Sapma	4,45	2,90	3,14	3,69	2,67	3,53
Varyans	19,59	8,33	9,74	13,47	7,08	12,36
Medyan	27,00	27,00	28,00	28,00	27,50	27,00
Maximum	44	39	39	39	38	44
Minimum	16	11	16	16	16	16
Mod	27	27	27	27	27	27
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	38,22	37,55	38,68	38,84	38,34	39,72
Standart Sapma	6,64	4,61	5,36	8,56	5,93	5,84
Varyans	43,63	21,05	28,46	72,47	34,86	33,80
Medyan	38,00	38,00	38,00	38,00	38,00	39,00
Maximum	72	50	61	93	61	77
Minimum	22	22	27	27	22	27
Mod	38	38	38	38	38	38
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	59,76	59,28	59,07	61,09	62,34	63,29
Standart Sapma	10,89	10,50	11,08	12,95	12,61	14,40
Varyans	117,36	109,10	121,51	165,94	157,34	205,39
Medyan	55,00	55,00	55,00	55,00	57,50	60,00
Maximum	93	110	93	116	105	137
Minimum	27	33	38	44	33	28
Mod	55	55	55	55	55	55
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	113,94	125,95	113,75	121,24	117,53	128,20
Standart Sapma	42,64	43,21	43,47	45,50	37,82	51,43
Varyans	1799,82	1848,29	1870,87	2049,14	1416,31	2618,98
Medyan	94,00	105,00	99,00	101,50	104,00	105,00
Maximum	231	242	274	258	242	313
Minimum	61	55	71	71	66	71
Mod	88	99	77	93	99	93
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	652,20	702,75	715,43	677,29	699,10	724,82
Standart Sapma	78,77	152,69	146,56	78,22	88,09	139,59
Varyans	6143,32	23080,67	21265,29	6056,45	7682,13	19291,75
Medyan	626,00	640,00	651,00	643,00	654,00	659,00
Maximum	1076	1390	1313	961	956	1263
Minimum	450	423	582	516	445	440
Mod	621	626	648	648	637	648
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	2220,70	2273,66	2380,77	2238,29	2275,24	2301,36
Standart Sapma	204,53	248,66	231,63	187,86	147,95	200,28
Varyans	41412,37	61211,02	53117,74	34936,91	21669,58	39710,19
Medyan	2252,00	2258,00	2402,50	2254,50	2285,00	2287,50
Maximum	2593	2823	3114	2647	2592	2669
Minimum	1275	1264	1687	1268	1499	1549
Mod	2263	2241	2208	2219	2285	2296

Çizelge 3.1.c. Tüm dosyalar için veri aktarım hızları istatistikleri.

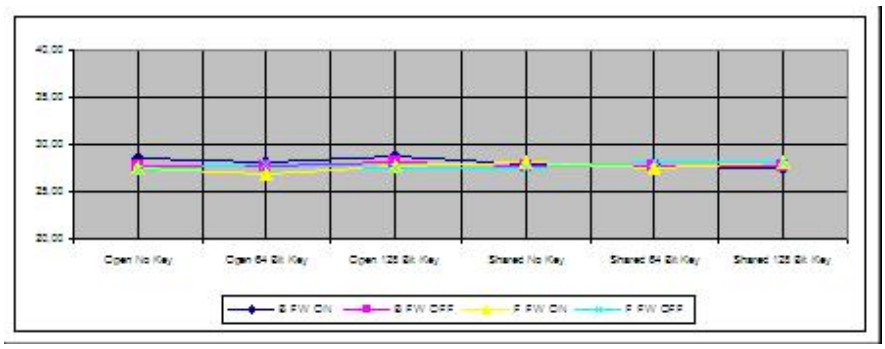
FARADAY_XP_Win_FW On						
	Open Authentication			Shared Authentication		
Dosya / İstatistik	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	22,18	22,39	22,25	22,44	22,80	22,52
Standart Sapma	1,78	2,74	2,21	2,45	3,36	2,11
Varyans	3,15	7,44	4,85	5,95	11,18	4,41
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	33	38	28	33	33
Minimum	16	11	16	11	11	17
Mod	22	22	22	22	22	22
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	27,47	26,91	27,70	28,19	27,47	28,11
Standart Sapma	2,24	2,84	3,08	3,54	3,53	2,66
Varyans	4,97	7,96	9,37	12,41	12,33	7,00
Medyan	27,00	27,00	27,00	28,00	27,00	28,00
Maximum	38	33	50	49	39	33
Minimum	16	16	17	16	11	16
Mod	27	27	27	27	27	27
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	37,74	38,29	38,77	38,19	39,15	39,60
Standart Sapma	5,95	5,08	4,08	5,41	7,00	5,40
Varyans	35,05	25,59	16,48	28,99	48,51	28,88
Medyan	38,00	38,00	38,00	38,00	38,00	39,00
Maximum	61	61	55	60	77	71
Minimum	22	22	22	22	16	27
Mod	33	38	38	38	38	38
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	59,30	64,53	61,41	59,87	59,11	61,25
Standart Sapma	7,10	12,01	13,17	10,99	10,60	10,59
Varyans	49,97	142,83	171,62	119,49	111,28	110,93
Medyan	55,00	60,00	55,00	55,00	55,00	57,50
Maximum	88	105	99	99	93	99
Minimum	49	39	33	38	33	38
Mod	55	55	55	55	55	55
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	131,83	132,43	134,31	125,19	128,31	128,52
Standart Sapma	53,72	48,84	55,08	46,37	49,25	52,95
Varyans	2857,46	2361,03	3003,43	2128,23	2401,59	2775,49
Medyan	105,00	105,00	109,50	110,00	101,50	99,00
Maximum	264	253	269	313	258	269
Minimum	60	60	71	83	71	82
Mod	93	99	93	93	99	99
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	685,80	692,21	695,09	681,16	664,93	673,88
Standart Sapma	77,67	108,09	113,50	90,12	94,55	98,32
Varyans	5973,06	11567,63	12753,88	8039,81	8849,89	9570,41
Medyan	651,00	654,00	648,00	643,00	643,00	643,00
Maximum	918	1126	1165	983	1209	1143
Minimum	593	423	516	440	286	362
Mod	643	637	637	637	643	643
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	2214,68	2261,73	2297,29	2291,60	2251,52	2215,93
Standart Sapma	213,49	187,09	250,64	209,61	188,38	198,04
Varyans	45122,44	34653,48	62192,91	43498,32	35133,81	38828,43
Medyan	2263,00	2268,00	2257,50	2274,00	2274,00	2263,00
Maximum	2571	2664	2939	2823	2559	2543
Minimum	1323	1632	1197	1318	1280	1335
Mod	2285	2241	2252	2279	2268	2268

Çizelge 3.1.d. Tüm dosyalar için veri aktarım hızları istatistikleri.

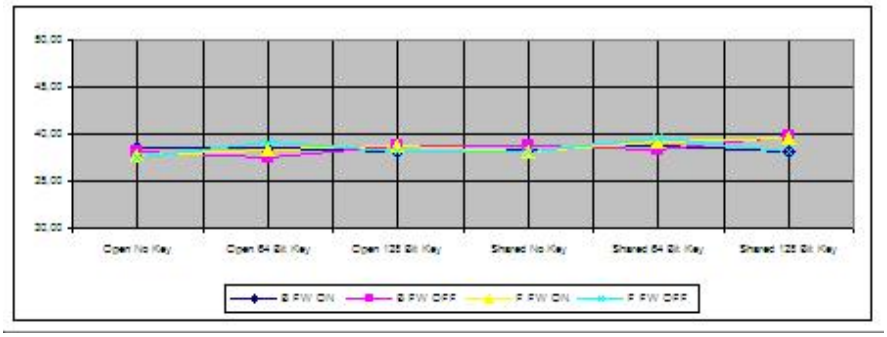
FARADAY_XP_Win_FW Off						
	Open Authentication			Shared Authentication		
Dosya / İstatistik	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	22,26	22,68	22,07	22,08	22,67	22,68
Standart Sapma	2,52	2,70	2,68	1,57	2,67	3,04
Varyans	6,27	7,22	7,13	2,45	7,04	9,16
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	39	33	33	33	33
Minimum	16	16	11	16	16	16
Mod	22	22	22	22	22	22
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	27,35	27,91	27,46	27,47	28,20	28,11
Standart Sapma	3,57	2,59	5,11	3,82	4,21	2,97
Varyans	12,63	6,62	25,87	14,41	17,58	8,76
Medyan	27,00	27,00	27,00	27,00	28,00	28,00
Maximum	44	39	55	49	44	39
Minimum	16	22	16	16	11	16
Mod	27	27	27	27	27	27
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	37,51	39,11	38,22	38,18	39,66	38,18
Standart Sapma	5,68	5,08	4,67	5,25	7,19	5,07
Varyans	31,91	25,58	21,59	27,25	51,12	25,43
Medyan	38,00	38,00	38,00	38,00	38,50	38,00
Maximum	72	55	55	66	77	55
Minimum	27	27	22	22	22	16
Mod	38	38	38	38	38	38
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	60,91	58,43	59,59	58,06	61,64	59,49
Standart Sapma	13,32	9,39	9,71	10,76	12,31	10,89
Varyans	175,68	87,27	93,40	114,54	150,11	117,45
Medyan	55,00	55,00	55,00	55,00	55,00	55,00
Maximum	126	99	99	88	115	104
Minimum	43	38	38	38	33	28
Mod	55	55	55	55	55	55
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	126,51	111,87	131,11	117,64	117,17	107,05
Standart Sapma	43,61	25,90	57,10	42,33	47,10	23,40
Varyans	1882,47	663,91	3227,94	1773,95	2195,84	541,93
Medyan	110,00	99,00	110,00	99,00	94,00	99,00
Maximum	247	187	346	269	258	170
Minimum	93	50	49	60	71	49
Mod	93	93	88	88	88	88
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	674,67	669,98	687,10	676,75	676,54	677,16
Standart Sapma	90,72	84,00	93,54	101,35	95,82	107,29
Varyans	8147,60	6985,32	8662,89	10169,53	9089,83	11396,35
Medyan	637,00	637,00	648,00	642,00	643,00	643,00
Maximum	896	1060	1032	1162	1112	1104
Minimum	258	500	516	335	538	451
Mod	637	632	637	637	621	648
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Ortalama	2221,18	2240,36	2262,49	2272,39	2254,58	2259,33
Standart Sapma	229,94	217,18	207,89	201,36	199,16	197,51
Varyans	52342,19	46695,51	42787,57	40141,70	39267,18	38619,42
Medyan	2219,00	2274,00	2257,00	2268,00	2254,50	2269,00
Maximum	2691	2548	2840	2823	2626	2653
Minimum	1230	1164	1318	1395	1631	1296
Mod	2219	2279	2274	2241	2373	2274



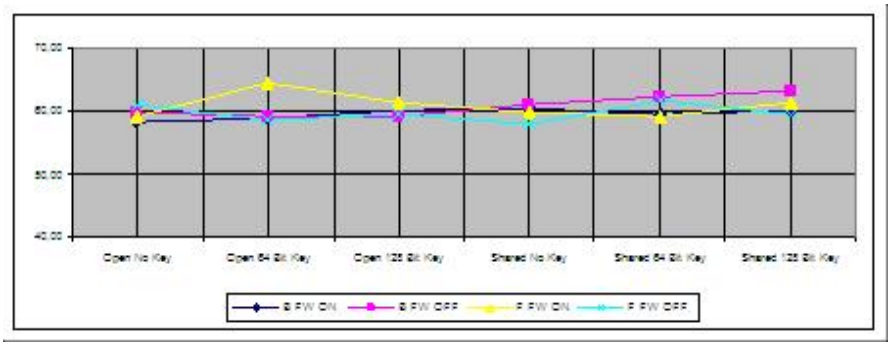
Şekil 3.10.a. Veri aktarım hızları görsel karakteristikleri (1 MB).



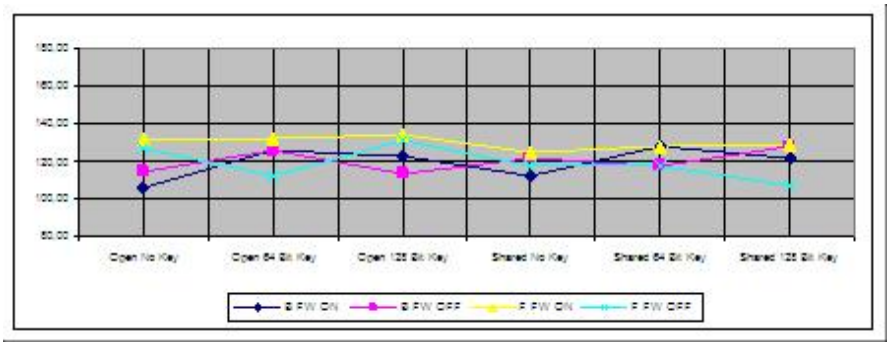
Şekil 3.10.b. Veri aktarım hızları görsel karakteristikleri (2 MB).



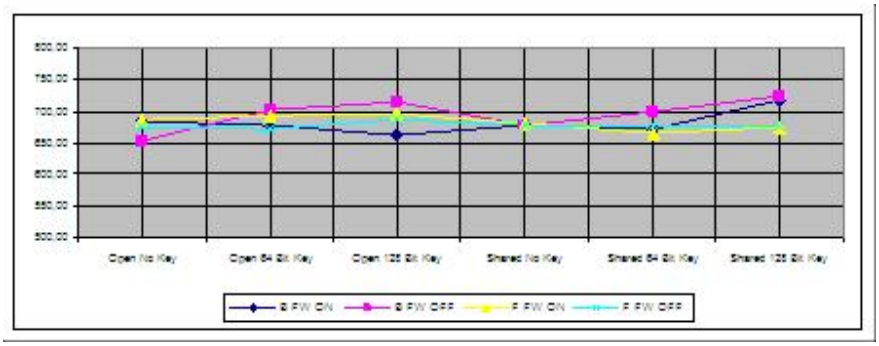
Şekil 3.10.c. Veri aktarım hızları görsel karakteristikleri (4 MB).



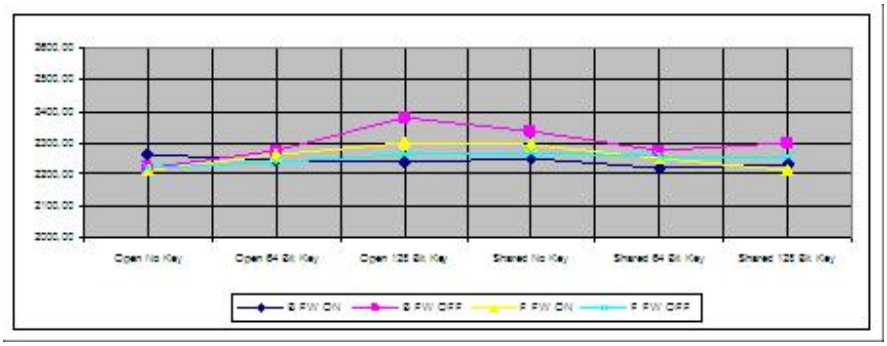
Şekil 3.10.d. Veri aktarım hızları görsel karakteristikleri (8 MB).



Şekil 3.10.e. Veri aktarım hızları görsel karakteristikleri (16 MB).



Şekil 3.10.f. Veri aktarım hızları görsel karakteristikleri (32 MB).



Şekil 3.10.g. Veri aktarım hızları görsel karakteristikleri (64 MB).

3.6. İstatiksel İnceleme

N ve M birimlik bağımsız iki veri grubu örneği, σ_1^2 ve σ_2^2 olarak tanımlanan varyanslara sahip şekilde ve grupların ortalamaları μ_1 ve μ_2 olarak ele alındığında test ortamında toplanan veriler, iki farklı iletişim özelliği çerçevesinde şifreli ve şifresiz iletişimin karşılaştırılmasında kullanılabilmektedir.

Örnek uzayından elde edilen belirli sayıdaki veri üzerinden σ_1^2 ve σ_2^2 değerleri kolayca elde edilebilmektedir. Test değeri olarak adlandırılan "Z" değerinin hesaplanması için ise aşağıdaki formül kullanılmaktadır.

$$Z = \frac{\overline{x_1} - \overline{x_2} - (\mu_1 - \mu_2)}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}} \tag{3.1}$$

$H_0 : \mu_1 = \mu_2$
$H_a : \mu_1 \neq \mu_2$ hipotezleri test edildiğinde (3.2)

$$Z \begin{cases} > Z_{1-\frac{a}{2}} \\ < Z_{1-\frac{a}{2}} \end{cases} \text{ ise } H_0 \text{ reddedilir.} \tag{3.3}$$

$H_0 : \mu_1 = \mu_2$
$H_a : \mu_1 > \mu_2$ hipotezleri test edildiğinde, $Z > Z_{1-\alpha}$ ise H_0 reddedilir.

$H_0 : \mu_1 = \mu_2$
$H_a : \mu_1 < \mu_2$ hipotezleri test edildiğinde, $Z <- Z_{1-\alpha}$ ise H_0 reddedilir.

Çizelge 3.2. Hipotez ve karar kuralları.

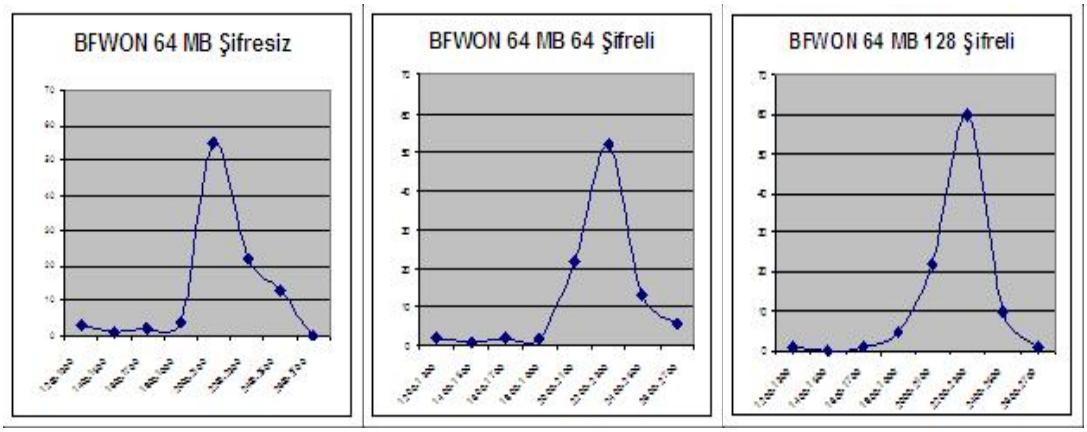
HİPOTEZ	KARŞI HİPOTEZ	TEST İSTATİSTİĞİ	RED BÖLGESİ	
$H_0 : \mu_1 = \mu_2$	$H_a : \mu_1 \neq \mu_2$	$Z = \frac{\overline{x_1} - \overline{x_2} - (\mu_1 - \mu_2)}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}}$	$Z > Z_{1-\frac{a}{2}}$	$Z < -Z_{1-\frac{a}{2}}$
$H_0 : \mu_1 \leq \mu_2$	$H_a : \mu_1 > \mu_2$		$Z > Z_{1-\alpha}$	
$H_0 : \mu_1 \geq \mu_2$	$H_a : \mu_1 < \mu_2$		$Z < -Z_{1-\alpha}$	

3.7. Varyans Analizi

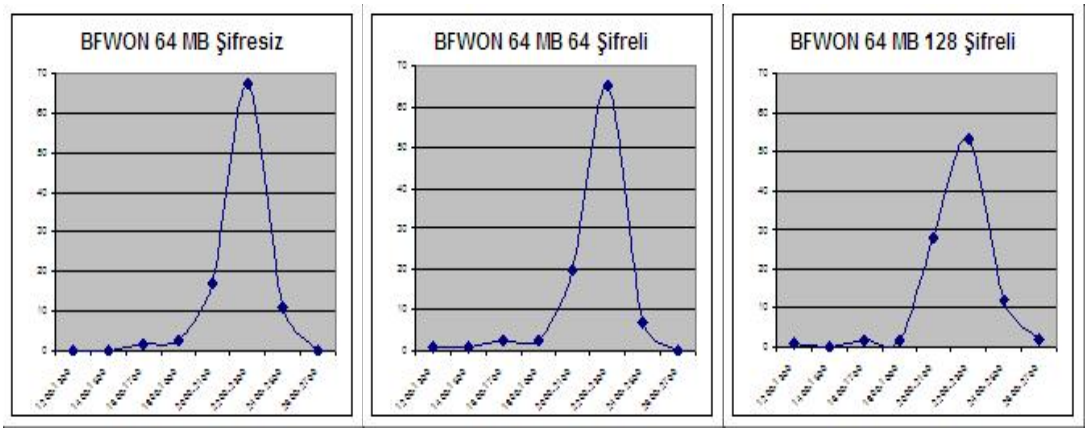
Test ortamında elde edilen verilerin kontrol edilmesi ve istatiksel açıdan aynı popülasyondan gelip-gelmediği bilinmeyen veri gruplarının analizi için ANOVA (Analysis of Variances) testlerinin de kullanılabildiği bilinmektedir. Varyans analizi testlerinde bilimsel araştırmalar için genellikle % 95 güven aralığında fark olup-olmadığı analiz edilmektedir.

Deneysel yöntemlerle toplanan bir veri paketi üzerinde varyans analizi yapılabilmesi için öncelikle iki temel şartın sağlanması gerekmektedir. Bunlardan ilki söz konusu veri gruplarının normal dağılıma sahip olmaları gerekliliği, ikincisi ise homojen bir varyans dağılımına sahip olmaları gerekliliğidir.

Veri gruplarının normal dağılıma sahip olup-olmadıklarının belirlenmesi için tüm veri grupları kendi içlerinde tekrar sayıları dikkate alınarak kümülatif normal dağılım için düzenlenmiştir. Bu düzenleme sonucunda görülmüştür ki, tüm veri grupları için bu şart sağlanmaktadır. Örnek olarak 64 MB boyutundaki dosya için; büro ortamında ateş duvarı aktif iken açık kimlik doğrulama (AKD) ve paylaşımlı kimlik doğrulamada (PKD) şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarım hızlarının normal dağılıma sahip oldukları Şekil 3.11.a ve 3.11.b'de görülmektedir.



Şekil 3.11.a. Normal dağılım grafikleri (AKD).



Şekil 3.11.b. Normal dağılım grafikleri (PKD).

Veri gruplarının homojen bir varyans dağılımına sahip olması şartı için ise SPSS istatistik programı kullanılarak yapılan *Levene Testi* sonuçları doğrultusunda elde edilen varyans hataları, düzeltmeye tabi tutulmuştur. Bu işlem sonrasında elde edilen homojen varyans dağılımına sahip veriler analiz edilmiştir. Bu kapsamda varyans analizi için gerekli olan söz konusu her iki şart sağlanmış olmaktadır.

Bu kapsamda varyans analizinde; şifresiz iletişim ile 64 bit şifreli iletişim, 64 bit şifreli iletişim ile 128 bit şifreli iletişim ve şifresiz iletişim ile 128 bit şifreli iletişim arasında, şifreleme işlemi için harcanan mikro işlemci zamanı nedeniyle olumsuz yönde bir fark olması gerektiği öngörüsü analiz edilmiştir. Varyans analizinde kullanılan ve şifrelemenin veri aktarım hızına etkisinin olup-olmadığının değerlendirilmesi ile ilgili hipotez ve karşıt hipotez aşağıdaki şekilde oluşturulmuştur.

$H_0 : \mu = \mu_0$ Ortalamalar arasında fark yoktur.

$H_a : \mu \neq \mu_0$ Ortalamalar arasında fark vardır.

Bu kapsamda SPSS İstatiksel Analiz programı kullanılarak her bir dosya boyutu için yapılan varyans analiz sonuçları 16 MB dosya boyu ile ilgili olarak EK-4'de diğer analiz sonuçları ise tez CD'si içerisinde EK-5'te sunulmuş olup, bu sonuçlarla ilgili değerlendirme ve tespitler aşağıda verilmiştir.

Her bir dosya boyutu ile ilgili olarak şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için 552, açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için 56, ateş duvarı aktif ve kapalı konum için 12 olmak üzere toplam 620 karşılaştırma yapılmış ve % 95 güven aralığında elde edilen veri grupları üzerinden bir fark olup-olmadığı analiz edilmiştir.

4. BULGULAR

Kablosuz ağlarda kullanılan WEP güvenlik mekanizmasında, şifreleme seçeneği aktif iken, gönderilen ve alınan paketlerin tümü özel bir takım süreçlerden ve RC4 şifreleme algoritmasından geçirilmektedir. Söz konusu bu süreçler ve şifreleme nedeniyle, mikro işlemci üzerinde ilave bir iş yükünün (overhead) yaratıldığı teorik olarak bilinmektedir. Bu nedenle şifrelemenin veri aktarım hızını düşürmesi beklenmektedir.

Test ortamında elde edilen veriler üzerinden ulaşılan bulgular, bu öngörü kapsamında incelemeye tabi tutulmuştur.

Bu kapsamda önce Büro ortamı ile Faraday Kafesi ortamı arasında fark olup-olmadığı, daha sonra her bir dosya boyutu için ateş duvarı aktif ve kapalı olmasının etkileri, açık kimlik doğrulama ve paylaşımlı kimlik doğrulama mekanizmalarının etkileri ile şifresiz, 64 bit şifreli ve 128 bit şifreli veri aktarma işlemleri arasındaki farklar değerlendirilmiştir.

Önce, büro ortamı ile Faraday kafesi ortamı arasında fark olup-olmadığı ile ilgili analiz her bir dosya boyutu için "Bölüm 3.6 İstatiksel İnceleme" kapsamında ortalamaların farkı hipotez testi ile yapılmış ve Çizelge 4.1'de verildiği şekilde her bir dosya boyutu için aralarında % 95 güven aralığında (Z<=1.58) hiç bir fark olmadığı belirlenmiştir.

Çizelge 4.1. Büro-Faraday kafesi ortalamaların farkı hipotez testi sonuçları.

1 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW ON	Ortalama	21,90	22,73	22,51	22,13	22,88	22,67	22,47	0,0255
	Varyans	2,83	10,60	8,03	13,27	7,07	9,56	8,56	
F FW ON	Ortalama	22,18	22,39	22,25	22,44	22,80	22,52	22,43	
	Varyans	3,15	7,44	4,85	5,95	11,18	4,41	6,16	
B FW OFF	Ortalama	22,25	22,50	22,03	22,21	22,23	22,30	22,25	0,1008
	Varyans	8,13	8,67	2,83	11,33	4,10	9,05	7,35	
F FW OFF	Ortalama	22,26	22,68	22,07	22,08	22,67	22,68	22,41	
	Varyans	6,27	7,22	7,13	2,45	7,04	9,16	6,54	

Çizelge 4.1. Devam Büro-Faraday kafesi ortalamaların farkı hipotez testi sonuçları.

2 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW	Ortalama	28,45	28,07	28,73	27,89	27,63	27,57	28,06	0,2237
ON	Varyans	16,03	9,49	13,92	6,50	9,25	14,63	11,63	
F FW	Ortalama	27,47	26,91	27,70	28,19	27,47	28,11	27,64	
ON	Varyans	4,97	7,96	9,37	12,41	12,33	7,00	9,01	
B FW	Ortalama	27,64	27,74	28,17	27,74	27,62	27,68	27,77	0,0072
OFF	Varyans	19,59	8,33	9,74	13,47	7,08	12,36	11,76	
F FW	Ortalama	27,35	27,91	27,46	27,47	28,20	28,11	27,75	
OFF	Varyans	12,63	6,62	25,87	14,41	17,58	8,76	14,31	
4 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW	Ortalama	38,55	38,55	38,22	38,32	38,77	38,16	38,43	0,0626
ON	Varyans	16,33	40,23	22,29	33,18	35,70	17,95	27,61	
F FW	Ortalama	37,74	38,29	38,77	38,19	39,15	39,60	38,62	
ON	Varyans	35,05	25,59	16,48	28,99	48,51	28,88	30,58	
B FW	Ortalama	38,22	37,55	38,68	38,84	38,34	39,72	38,56	0,0240
OFF	Varyans	43,63	21,05	28,46	72,47	34,86	33,80	39,05	
F FW	Ortalama	37,51	39,11	38,22	38,18	39,66	38,18	38,48	
OFF	Varyans	31,91	25,58	21,59	27,25	51,12	25,43	30,48	
8 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW	Ortalama	58,35	58,87	60,09	60,46	59,37	59,98	59,52	0,2284
ON	Varyans	88,95	88,31	112,34	146,07	111,23	83,46	105,06	
F FW	Ortalama	59,30	64,53	61,41	59,87	59,11	61,25	60,91	
ON	Varyans	49,97	142,83	171,62	119,49	111,28	110,93	117,69	
B FW	Ortalama	59,76	59,28	59,07	61,09	62,34	63,29	60,81	0,1670
OFF	Varyans	117,36	109,10	121,51	165,94	157,34	205,39	146,11	
F FW	Ortalama	60,91	58,43	59,59	58,06	61,64	59,49	59,69	
OFF	Varyans	175,68	87,27	93,40	114,54	150,11	117,45	123,07	
16 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW	Ortalama	106,28	125,39	123,08	112,67	127,82	121,88	119,52	0,3789
ON	Varyans	1010,40	2170,30	2341,79	1705,46	3266,97	2042,55	2089,58	
F FW	Ortalama	131,83	132,43	134,31	125,19	128,31	128,52	130,10	
ON	Varyans	2857,46	2361,03	3003,43	2128,23	2401,59	2775,49	2587,87	
B FW	Ortalama	113,95	125,95	113,75	121,24	117,53	128,20	120,10	0,0627
OFF	Varyans	1799,82	1848,29	1870,87	2049,14	1416,31	2618,98	1933,90	
F FW	Ortalama	126,51	111,87	131,11	117,64	117,17	107,05	118,56	
OFF	Varyans	1882,47	663,91	3227,94	1773,95	2195,84	541,93	1714,34	
32 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW	Ortalama	683,21	679,05	662,61	676,71	670,60	717,89	681,68	0,0087
ON	Varyans	8989,19	7120,05	5237,16	5632,25	7182,14	27468,62	10271,57	
F FW	Ortalama	685,80	692,21	695,09	681,16	664,93	673,88	682,18	
ON	Varyans	5973,06	11567,63	12753,88	8039,81	8849,89	9570,41	9459,11	
B FW	Ortalama	652,20	702,75	715,43	677,29	699,10	724,82	695,27	0,2945
OFF	Varyans	6143,32	23080,67	21265,29	6056,45	7682,13	19291,75	13919,93	
F FW	Ortalama	674,67	669,98	687,10	676,75	676,54	677,16	677,03	
OFF	Varyans	8147,60	6985,32	8662,89	10169,53	9089,83	11396,35	9075,25	

Çizelge 4.1. Devam Büro-Faraday kafesi ortalamaların farkı hipotez testi sonuçları.

64 MB	İstatistik	Open No Key	Open 64 Bit Key	Open 128 Bit Key	Shared No Key	Shared 64 Bit Key	Shared 128 Bit Key	Mean	Z<=1.58
B FW ON	Ortalama	2261,57	2243,10	2241,24	2253,41	2220,82	2235,60	2242,62	0,1103
	Varyans	61503,17	54377,19	30063,00	18227,64	31824,75	32421,26	38069,50	
F FW ON	Ortalama	2214,68	2261,73	2297,29	2291,60	2251,52	2215,93	2255,46	
	Varyans	45122,44	34653,48	62192,91	43498,32	35133,81	38828,43	43238,23	
B FW OFF	Ortalama	2220,70	2273,66	2380,77	2338,29	2275,24	2301,36	2298,34	0,3909
	Varyans	41412,37	61211,02	53117,74	34936,91	21669,58	39710,19	42009,64	
F FW OFF	Ortalama	2221,18	2240,36	2262,49	2272,39	2254,58	2259,33	2251,72	
	Varyans	52342,19	46695,51	42787,57	40141,70	39267,18	38619,42	43308,93	

Daha sonraki adımda ise, SPSS programı kullanılmış ve yapılan varyans analizi içerisinde 84 adedi ateş duvarı ile ilgili, 392 adedi kimlik doğrulama ile ilgili ve 3864 adedi de şifreleme ile ilgili olmak üzere toplam 4 340 adet karşılaştırma yapılmıştır.

Varyans analizi sonuçlarının detaylı incelenmesi neticesinde her bir dosya boyutu ile ilgili olarak elde edilen bulgular aşağıda verilmiştir.

1 MB dosya boyutu ile ilgili olarak : Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için 552, açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için 56, ateş duvarı aktif ve kapalı konum için 12 olmak üzere toplam 620 karşılaştırma yapılmış ve % 95 güven aralığında herhangi bir fark gözlenmemiştir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 100 desteklemektedir.

2 MB dosya boyutu ile ilgili olarak : Ateş duvarı aktif ve kapalı konum için yapılan 12 karşılaştırmada herhangi bir fark gözlenmemiştir.

Açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için yapılan 56 karşılaştırmadan 1 adedinde (büro ortamında ateş duvarı aktifken açık kimlik doğrulama ile Faraday kafesinde ateş duvarı aktifken açık kimlik doğrulama arasında) fark olduğu görülmüştür. Ancak bu farkın Faraday kafesi ortamındaki ölçümlerin daha tutarlı olması veya büro ortamındaki ölçümlerde ise kısmi de olsa

bir sinyal kirliliği veya enterferansa maruz kalınmasından kaynaklandığı değerlendirilmektedir.

Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için yapılan 552 karşılaştırmada herhangi bir fark gözlenmemiştir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 100 desteklemektedir.

4 MB dosya boyutu ile ilgili olarak : Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için 552, açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için 56, ateş duvarı aktif ve kapalı konum için 12 olmak üzere toplam 620 karşılaştırma yapılmış ve % 95 güven aralığında hiç bir fark gözlenmemiştir. Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 100 desteklemektedir.

8 MB dosya boyutu ile ilgili olarak : Ateş duvarı aktif ve kapalı konum için yapılan 12 karşılaştırmada herhangi bir fark gözlenmemiştir.

Açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için yapılan 56 karşılaştırmadan 1 adedinde (büro ortamında ateş duvarı aktifken açık kimlik doğrulama ile yine büro ortamında ateş duvarı kapalı iken paylaşımlı kimlik doğrulama arasında) fark olduğu görülmüştür. Ancak bu farkın kimlik doğrulama protokolleri arasındaki farklılıktan değil diğer nedenlerden kaynaklandığı değerlendirilmektedir. Her iki protokol arasında ağa bağlanma ve ağa kabul öncesi gerçekleştirilen işlemlerde farklılık vardır ancak bu işlemlerin veri aktarım hızını etkilemesinin mümkün olmadığı bilinmektedir.

Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için yapılan 552 karşılaştırmadan 3 adedinde fark bulunmuş olup, bunlardan 1 adedi hipotezi reddetmekte diğer 2 adedi ise reddetmemektedir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 99,82 oranında desteklemektedir.

16 MB dosya boyutu ile ilgili olarak : Ateş duvarı aktif ve kapalı konum için yapılan 12 karşılaştırmadan 3 adedinde (büro ortamında ateş duvarı aktif ile Faraday kafesinde ateş duvarı aktif arasında, büro ortamında ateş duvarı kapalı ile Faraday kafesinde ateş duvarı aktif arasında, Faraday kafesinde ateş duvarı aktif ile Faraday kafesinde ateş duvarı kapalı arasında) fark olduğu gözlenmiştir. Bu farkların diğer dosya boyutları ile ilgili veriler kapsamında tutarlı olarak desteklenmemesi kapsamında, ateş duvarının kullanılması nedeniyle değil diğer nedenlerden kaynaklandığı değerlendirilmektedir.

Açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için yapılan 56 karşılaştırmadan 4 adedinde (büro ortamında ateş duvarı aktifken açık kimlik doğrulama ile yine büro ortamında ateş duvarı aktifken açık kimlik doğrulama arasında, büro ortamında ateş duvarı kapalı iken açık kimlik doğrulama ile Faraday kafesinde ateş duvarı aktifken açık kimlik doğrulama arasında, Faraday kafesi ortamında ateş duvarı aktifken açık kimlik doğrulama ile Faraday kafesi ortamında ateş duvarı kapalı iken paylaşımlı kimlik doğrulama arasında, Faraday kafesi ortamında ateş duvarı aktifken paylaşımlı kimlik doğrulama ile Faraday kafesi ortamında ateş duvarı kapalı iken paylaşımlı kimlik doğrulama arasında) fark olduğu görülmüştür. Ancak bu farkın kimlik doğrulama protokolleri arasındaki farklılıktan değil diğer nedenlerden kaynaklandığı değerlendirilmektedir. Her iki protokol arasında ağa bağlanma ve ağa kabul öncesi gerçekleştirilen işlemlerde farklılık olduğu ve veri aktarım hızını etkilemesinin mümkün olmadığı bilinmektedir.

Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için yapılan 552 karşılaştırmadan 10 adedinde fark bulunmuş olup, bunlardan 2 adedi hipotezi reddetmekte diğer 8 adedi ise reddetmemektedir. Bu dosya boyutu ile ilgili olarak ortaya çıkan farklılıkların veri aktarım hızlarının büyük farklılıklar göstermesi ile standart sapma ve dolayısıyla varyans değerlerinin büyüklüğünden kaynaklandığı düşünülmektedir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 99,64 oranında desteklemektedir.

32 MB dosya boyutu ile ilgili olarak : Ateş duvarı aktif ve kapalı konum için yapılan 12 karşılaştırmadan 1 adedinde (büro ortamında ateş duvarı kapalı ile Faraday kafesinde ateş duvarı kapalı arasında) fark olduğu gözlenmiştir. Bu farkların diğer dosya boyutları ile ilgili veriler kapsamında tutarlı olarak desteklenmemesi kapsamında, ateş duvarının kullanılması nedeniyle değil diğer nedenlerden kaynaklandığı değerlendirilmektedir.

Açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için yapılan 56 karşılaştırmadan 2 adedinde (büro ortamında ateş duvarı aktifken açık kimlik doğrulama ile yine büro ortamında ateş duvarı kapalı iken paylaşımlı kimlik doğrulama arasında, büro ortamında ateş duvarı kapalı iken paylaşımlı kimlik doğrulama ile Faraday kafesinde ateş duvarı aktifken paylaşımlı kimlik doğrulama arasında) fark olduğu görülmüştür. Ancak bu farkın kimlik doğrulama protokolleri arasındaki farklılıktan değil diğer nedenlerden kaynaklandığı değerlendirilmektedir. Her iki protokol arasında ağa bağlanma ve ağa kabul öncesi gerçekleştirilen işlemlerde farklılık olduğu ve veri aktarım hızını etkilemesinin mümkün olmadığı bilinmektedir.

Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için yapılan 552 karşılaştırmadan 3 adedinde fark bulunmuş olup, bunlardan 2 adedi hipotezi reddetmekte diğer 1 adedi ise reddetmemektedir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 99,64 oranında desteklemektedir.

64 MB dosya boyutu ile ilgili olarak : Ateş duvarı aktif ve kapalı konum için yapılan 12 karşılaştırmadan 1 adedinde (büro ortamında ateş duvarı aktif ile büro ortamında ateş duvarı kapalı arasında) fark olduğu gözlenmiştir. Bu farkların diğer dosya

boyutları ile ilgili veriler kapsamında tutarlı olarak desteklenmemesi kapsamında, ateş duvarının kullanılması nedeniyle değil diğer nedenlerden kaynaklandığı değerlendirilmektedir.

Açık kimlik doğrulama ile paylaşımlı kimlik doğrulama için yapılan 56 karşılaştırmadan 1 adedinde (büro ortamında ateş duvarı aktifken paylaşımlı kimlik doğrulama ile yine büro ortamında ateş duvarı kapalı iken açık kimlik doğrulama arasında) fark olduğu görülmüştür. Ancak bu farkın kimlik doğrulama protokolleri arasındaki farklılıktan değil diğer nedenlerden kaynaklandığı değerlendirilmektedir. Her iki protokol arasında ağa bağlanma ve ağa kabul öncesi gerçekleştirilen işlemlerde farklılık olduğu ve veri aktarım hızını etkilemesinin mümkün olmadığı bilinmektedir.

Şifresiz, 64 bit şifreli ve 128 bit şifreli dosyaların aktarma hızları için yapılan 552 karşılaştırmadan 16 adedinde fark bulunmuş olup, bunlardan 12 adedi hipotezi reddetmekte diğer 4 adedi ise reddetmemektedir. Bu dosya boyutu ile ilgili olarak ortaya çıkan farklılıkların, veri toplama aşamasında yapılan bazı hatalardan kaynaklandığı, bu kapsamda aktarım hızlarının büyük farklılıklar göstermesi ile standart sapma ve dolayısıyla varyans değerlerinin büyük hesaplanmasının da etkili olduğu düşünülmektedir.

Bu dosya boyutu varyans analizi kapsamında % 95 güven aralığında hipotezi % 97,82 oranında desteklemektedir.

Çizelge 4.2. Varyans analizi karşılaştırma kod tablosu.

Ortam – Ateş Duvarı – Kimlik Doğrulama			Şifresiz	64 bit Şifreli	128 bit Şifreli
Büro Ortamı Kod = 1	Ateş Duvarı Aktif (FW On) Kod = 1	Açık Kimlik Doğrulama Kod = 1	Kod = 1	Kod = 2	Kod = 3
		Paylaşımlı Kimlik Doğrulama Kod = 2	Kod = 1	Kod = 2	Kod = 3
	Ateş Duvarı Kapalı (FW Off) Kod = 2	Açık Kimlik Doğrulama Kod = 1	Kod = 1	Kod = 2	Kod = 3
		Paylaşımlı Kimlik Doğrulama Kod = 2	Kod = 1	Kod = 2	Kod = 3

Çizelge 4.2. Devam Varyans analizi karşılaştırma kod tablosu.

Faraday Kafesi Ortamı Kod = 2	Ateş Duvarı Aktif (FW On) Kod = 1	Açık Kimlik Doğrulama Kod = 1	Kod = 1	Kod = 2	Kod = 3
		Paylaşımlı Kimlik Doğrulama Kod = 2	Kod = 1	Kod = 2	Kod = 3
	Ateş Duvarı Kapalı (FW Off) Kod = 2	Açık Kimlik Doğrulama Kod = 1	Kod = 1	Kod = 2	Kod = 3
		Paylaşımlı Kimlik Doğrulama Kod = 2	Kod = 1	Kod = 2	Kod = 3

Çizelge 4.2.'de verilen kod tablosuna göre SPSS istatistik programı kapsamında Faraday kafesi ortamı - Kod = 2, Ateş duvarı aktif - Kod = 1, Açık kimlik doğrulama - Kod =1 ve 128 bit şifreli iletişim - Kod =3 program çıktılarında "2113" şeklinde verilmektedir. Ya da bir örnek olarak "1222" kodu aşağıdaki şekilde ifade edilmektedir.

Büro Ortamı	Ateş Duvarı	Paylaşımlı Kimlik	64 bit
	Kapalı	Doğrulama	Şifreli
1	2	2	2

Çizelge 4.2.'de verilen varyans analizi karşılaştırma kod tablosu ve analiz sonuçlarının detaylı incelenmesi neticesinde her bir dosya boyutu ile ilgili olarak elde edilen sonuçlarla ilgili sonuçlar Çizelge 4.3.'de verilmiştir.

Çizelge 4.3. Varyans analizi sonuçlarının detaylı incelenmesi.

% 95 Güven Aralığında <u>Ateş Duvarı</u> Varyans Analiz Sonuçlarının Detaylı İncelenmesi								
Dosya Boyu	Fark Sayısı		Toplam	Grup Tanımları	Fark Nedeni		Hipotez Red / Toplam	Hipotez Destekleme Oranı
	Fark Var	Fark Yok		Farklı Gruplar	Aktif / Kapalı	Diğer		
1 MB	-	12	12	Yoktur			0/12	100,00
2 MB	-	12	12	Yoktur			0/12	100,00
4 MB	-	12	12	Yoktur			0/12	100,00
8 MB	-	12	12	Yoktur			0/12	100,00
16 MB	3	9	12	Vardır	2	1	2/12	83,34
32 MB	1	11	12	Vardır		1	0/12	100,00
64 MB	1	11	12	Vardır	1		1/12	91,67
Toplam	5	79	84				Ortalama	96,43

Çizelge 4.3. Devam Varyans analizi sonuçlarının detaylı incelenmesi.

% 95 Güven Aralığında Kimlik Doğrulama Varyans Analiz Sonuçlarının Detaylı İncelenmesi							
Dosya Boyu	Fark Sayısı		Toplam	Grup Tanımları	Fark Nedeni		Hipotez Red / Toplam	Hipotez Destekleme Oranı
	Fark Var	Fark Yok		Farklı Gruplar	AKD / PKD	Diğer		
1 MB	-	56	56	Yoktur			0/56	100,00
2 MB	1	55	56	Vardır		1	1/56	100,00
4 MB	-	56	56	Yoktur			0/56	100,00
8 MB	1	55	56	Vardır	1		1/56	98,21
16 MB	4	52	56	Vardır	1	3	1/56	98,21
32 MB	2	54	56	Vardır	1	1	1/56	98,21
64 MB	1	55	56	Vardır	1		1/56	98,21
Toplam	9	383	392				Ortalama	98,98

% 95 Güven Aralığında Şifreleme Varyans Analiz Sonuçlarının Detaylı İncelenmesi							
Dosya Boyu	Fark Sayısı		Toplam	Grup Tanımları	Fark Nedeni		Hipotez Red / Toplam	Hipotez Destekleme Oranı
	Fark Var	Fark Yok		Farklı Gruplar	Şifreleme	Diğer		
1 MB	-	552	552	Yoktur	-	-	0/552	100,00
2 MB	-	552	552	Yoktur	-	-	0/552	100,00
4 MB	-	552	552	Yoktur	-	-	0/552	100,00
8 MB	3	549	552	Vardır	1	2	1/552	99,82
16 MB	10	542	552	Vardır	2	8	2/552	99,64
32 MB	3	549	552	Vardır	2	1	2/552	99,64
64 MB	16	536	552	Vardır	12	4	12/552	97,82
Toplam	32	3832	3864				Ortalama	99,56

5. SONUÇ VE ÖNERİLER

Kablosuz ağlarda kullanılmakta olan WEP güvenlik mekanizması içerisinde şifresiz iletişim, 40 bit (64 bit) ve 104 bit (128 bit) şifreli iletişim özelliği isteğe bağlı olarak kullanılabilmektedir. Söz konusu bu şifreleleme işlemi, veri iletişimi yapan cihazlara ait mikro işlemciler üzerinde ilave bir iş yükü yaratmaktadır. Teorik olarak varlığı bilinen bu iş yükünün veri aktarım hızını etkilemesi, ya da en azından belirli bir dosya büyüklüğünden itibaren olumsuz etkilemesi beklenmektedir. Bu beklentiye ilave olarak ateş duvarının aktif ve kapalı olmasının, kullanılan kimlik doğrulama protokolünün ve aktarılan dosya boyutunun veri aktarım hızına etkileri de incelenmiş, istatistiksel hipotez testleri ve varyans analizi kullanılarak ulaşılan tespit ve sonuçlar aşağıda ortaya konulmuştur.

5.1. Sonuçlar

- Büro ortamı ile Faraday kafesi ortamında yapılan test ölçümleri arasında % 95 güven aralığında hiç bir fark olmadığı, büro ortamında diğer elektromanyetik sinyal üreticilerden kaynaklanan ve enterferans oluşturan farklı bir sinyal bulunmadığı,

- Büro / Faraday kafesi ortamında Windows XP işletim sistemine ait ateş duvarının açık veya kapalı olmasının % 95 güven aralığında kablosuz iletişim ve veri aktarım hızına % 96,43 oranda olumsuz bir etkisinin olmadığı,

- Büro / Faraday kafesi ortamında ateş duvarı aktif / kapalı iken teorik olarak beklenildiği şekilde açık kimlik doğrulama ile paylaşımlı kimlik doğrulama arasında % 95 güven aralığında ortalamaların farklı olduğuna dair % 98,98 oranda tutarlı ve tatminkar bir sonuç elde edilemediği,

- Açık / Paylaşımlı kimlik doğrulama altında normal dağılımlı iki kitlenin ortalamaları farkı için varyans analizi testleri sonucunda; % 95 güven aralığında

şifresiz iletişim ile 64 bit şifreli iletişim, 64 bit şifreli iletişim ile 128 bit şifreli iletişim, şifresiz iletişim ile 128 bit şifreli iletişim arasında teorik olarak olması öngörülen bir veri aktarım hızı kaybının % 99,56 oranda söz konusu olmadığı gözlemlenmiştir.

Üçüncü bölümde ortaya konulan hipotezler kapsamında gerçekleştirilen istatistiksel analiz yöntemi (Varyans Analizi) ile test ortamı olarak teşkil edilen ve özellikleri dördüncü bölümde verilen tasarsız (peer-to-peer / ad hoc) ağa ilişkin elde edilen sonuçlar aşağıda sunulmuştur.

- Kablosuz ağ kurulan ve kullanılan alanda enterferansa maruz kalınmadığı müddetçe, kablosuz ağın performansı ile Faraday kafesindeki performans arasında % 95 güven aralığında hiç bir fark bulunmamaktadır.

- Kablosuz veri iletişiminde ateş duvarı kullanılmasının, (iletişim ortamında gönderilen ve alınan verilerde sakıncalı bir durum olmadığı ve ateş duvarı tarafından iletişim engellenmediği veya bloke edilmediği sürece) % 95 güven aralığında ortalama % 96,43 oranında veri iletişim hızına olumsuz herhangi bir etkisi bulunmamaktadır.

- Kimlik doğrulama mekanizmaları açısından; açık kimlik doğrulama ile paylaşımlı kimlik doğrulama arasında % 95 güven aralığında ortalama % 98,98 oranında veri iletişim hızının olumsuz etkilenmesi kapsamında teorik olarak beklenen şekilde herhangi bir fark bulunmamaktadır.

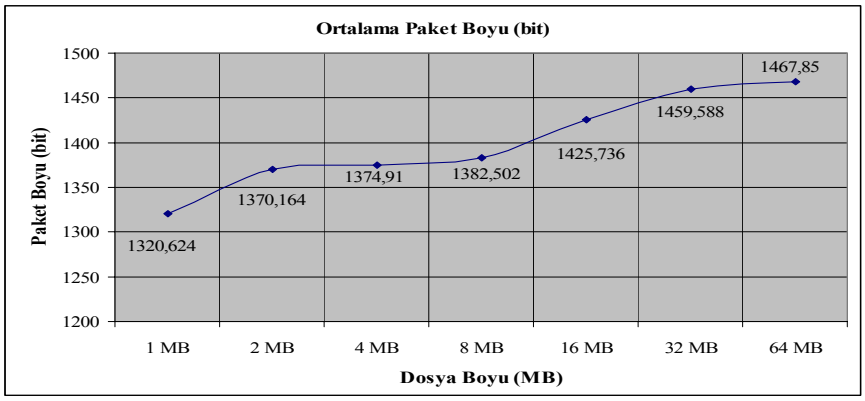
- WEP güvenlik mekanizması kapsamında Windows XP işletim sistemi ile gerçekleştirilen kablosuz iletişimde, şifresiz kullanım ile 64 bit (40 bit) şifreli kullanım, 64 bit (40 bit) şifreli kullanım ile 128 bit (104 bit) şifreli kullanım arasında ve ayrıca şifresiz kullanım ile 128 bit (104 bit) şifreli kullanım arasında veri aktarım hızı açısından % 95 güven aralığında ortalama % 99,56 oranında hiç bir fark bulunmamaktadır.

Test ortamı şartları ve bu ortamdan elde edilen veriler üzerinde yapılan diğer incelemelerde ayrıca belirlenen aşağıdaki tespit ve değerlendirmelerin de dikkate alınmasının faydalı olacağı düşünülmektedir.

- Aktarılan dosya boyutları büyüdükçe ortalamalar arasındaki farklılıklar göreceli olarak artması ve aktarılan paketlerin şifreleme ve çözümleme işlemlerinin mikro işlemci üzerinde ilave bir iş yükü oluşturması nedenleriyle, daha büyük dosya boyları için veri aktarım hızının daha fazla etkilenmesinin söz konusu olabileceği değerlendirilmektedir.

- Intel (R) Pro Wireless 2200BG kablosuz adaptör ve Intel Proset Wireless yazılımı üzerinde yapılan incelemede paket gönderme ve alma hatalarının oranının % 3 olduğu görülmüştür.

- Şekil 5.1.'den anlaşılacağı üzere test ortamında bilgisayarlar arasında aktarılan dosya boyutları büyüdükçe, kablosuz olarak aktarılan paket boylarının büyüdüğü (bit sayısının arttığı) görülmüştür.



Şekil 5.1. Dosya boyu - Paket boyu grafiği.

- Çizelge 5.1.'de sunulduğu gibi işletim sistemi, kablosuz adaptörü, ilgili yazılım veya donanım tarafından açıklanan teorik veri hızının test ortamında elde edilen veri hızına göre yüksek olduğu, bu nedenle üreticiler tarafından ortaya

konulan veya ifade edilen teorik hızların maksimum üst sınır olarak dikkate alınmasının uygun olacağı değerlendirilmektedir.

Çizelge 5.1. Teorik – Deneysel veri hızı verimlilik oranları [47].

Teorik Hız (Mbit/s)	Deneysel Hız (Mbit/s)	Verimlilik (%)
1	0.75	74.9
2	1,41	70.7
5,5	3,38	61.5
11	5,32	48.4

5.2. Öneriler

- WEP güvenlik mekanizması içerisinde şifreleme işlemleri nedeniyle mikro işlemci üzerinde oluşan iş yükünün 64 MB büyüklükten daha büyük uzunluktaki dosyalar üzerindeki veri aktarım hızını olumsuz yönde etkileyip-etkilemediği hakkında bir inceleme yapılması,

- Eldeki mevcut donanım ve yazılım imkanları nedeniyle yapılamayan, 256 bit (232 bit) şifreleme anahtarı kullanılması durumunda mikro işlemci üzerinde oluşan iş yükünün veri aktarım hızını olumsuz etkileyip-etkilemediği ile ilgili bir çalışma yapılması,

- Türkiye'de kablosuz ağlarda güvenlik mekanizma ve protokollerinin ne oranda kullanıldığı, güvenlik mekanizma ve protokolü kullanılan ağlarda hangilerinin kullanıldığı ile ilgili bir araştırma yapılması,

- İşletim sistemi, kablosuz ağ adaptörü, ilgili yazılım veya donanım tarafından açıklanan teorik veri hızının test ortamında elde edilen veri hızına göre yüksek olması nedeniyle özellikle 54 Mbps hız için verimlilik oranı ile ilgili bir çalışma yapılması,

- Bu çalışmada gerçekleştirilen veri aktarma işlemi sadece “text” dosyalar için gerçekleştirilmiş olup, dosya türünün değiştirilmesi (Ses, görüntü, resim vb dosyalar ile .doc, .ppt, .xls, .pdf vb. uzantılı) ve aynı uzunlukta, fakat farklı özellik ve yapılardaki dosyaların kablosuz olarak aktarılmaları durumunda veri hızının nasıl etkileneceği ile ilgili bir başka çalışma yapılması önerilmektedir.

KAYNAKLAR

1. Öztürk, E., "WLAN Kablosuz Yerel Alan Ağları (Wireless Local Area Networks) Teknolojisinin İncelenmesi, Mevcut Düzenlemelerin Değerlendirilmesi ve Ülkemize Yönelik Düzenleme Önerisi", Uzmanlık Tezi, ***Telekomünikasyon Kurumu***, Ankara, 1-11, 38-43 (2004).

2. Küçükünsal, J., "Metropol alanlar için kablosuz erişim (Wieless Metropolian Area Network / Kablosuz Metropol Alan Ağları–WMAN) Uygulamaları ve Düzenleme Önerileri", Uzmanlık Tezi, ***Telekomünikasyon Kurumu***, Ankara, 1-15 (2006).

3. Karnik, A., Passerini, K., "Wireless Network Security - A Discussion From a Business Perspective", ***IEEE Wireless Telecommunications Symposium***, California, 261-267 (2005).

4. NOP World Technology Group, "2003 Wireless LAN Benefits Study", Cisco Systems Inc., ***Conducted by NOP World Technology on Behalf of Cisco Systems***, ***California,*** 4-14 (2003).

5. Bittau, A., Handley, M., Lackey, J., "The Final Nail in WEP's Coffin", ***2007 IEEE Symposium on Security and Privacy***, IEEE Computer Society, California, 386-400 (2006).

6. Tews, E., Philipp, W. R., Pyshkin, A., Technical University of Darmstat, "Breaking 104 bit WEP in less than 60 seconds", ***Cryptology Report,*** 2007 (120): 1-12 (2007).

7. Briere, D., Walter, R., Hurley, P., "Part I : Wireless Networking Fundamentals Wireless Networking For Dummies", ***Wiley Publishing Incorporation***, New York, 7-18 (2003).

8. Gast, S. M., "Creating and Administering Wireless Networks, 802.11 Wireless Networks : The Definitive Guide", ***O'Reilly Inc.***, California, 299-313 (2002).

9. Esmailzadeh, R., Nakagawa, M., "TDD - CDMA for Wireless Communications", ***Artech House Publishers***, Norwood, 1-2 (2002).

10. Moioli, F., "Security in Public Access Wireless LAN Networks", M.Sc. Thesis, ***Royal Institute of Technology,*** Stockholm, 26-27 (2000).

11. Flikenger, R., "Building Wireless Community Networks", ***O'Reilly Inc.***, California, 17-28 (2002).

12. Wheat, J., Hiser, R., Tucker, J., Neely, A., Mc Cullough A., "Designing a Wireless Network", ***Syngress Publishing Inc.***, Rockland, 1-18, 115-206 (2001).

13. Stallings, W., "Data and Computer Communications", ***Prentice Hall,*** New Jersey, 1-63 (2003).

14. Khayat, M. M., "Wireless Local Area Network (WLAN), Advantages vs. Disadvantages", ***INNS 690 Professional Seminar,*** Heidelberg, 4-18 (2002).

15. Coleman, D. D., Westcott, D. A., "CWNA - Certified Wireless Network Administrator Official Study Guide", ***Wiley Publishing,*** Indiana, 3, 17-177 (2006).

16. Karygiannis, T., Owens, L., "Recommendations of the National Institute of Standards and Technology-NIST : Wireless Network Security, 802.11, Bluetooth and Handheld Devices", ***National Institute of Standards and Technology-NIST, Gaithersburgh***, 3: 13-36 (2002).

17. Cho, K., Jacquet, P., "Security Threats and Countermeasures in WLANs", ***AINTEC Springer-Verlag Magazine,*** 2005 (7): 168-182 (2005).

18. Hassinen, T., "Overwiev of WLAN Security", ***TKK T.110-5290 Seminar on Network Security***, Helsinki, 17-23 (2003).

19. Welch, J. D., Lathrop, S. D., "Wireless Security Threat Taxonomy", ***IEEE - Man and Cybernetics Society : IEEE Information Assurance Workshop***, New Jersey, 76-83 (2003).

20. Welch J. D., Lathrop S. D., "A Survey of 802.11a Wireless Security Threats and Security Mechanisms", ***Technical Report : United States Military Academy - West Point, New York,*** 1-28 (2003).

21. Talukder, A., Yavagal, R., "Mobile Computing, Security Issues in Mobile Computing", ***Mc Graw Hill,*** California, 591-599 (2006).

22. Beaver, K., Davis T. P., "Hacking Wireless Networks for Dummies", ***Wiley Publishing Inc.***, New Jersey, 9-18 (2005).

23. Boland, H., Mousavi, H., "Security issues of the IEEE 802.11b Wireless LAN", ***2004 Electrical and Computer Engineering Canadian Conference,*** Canada, 333-339 (2004).

24. IEEE LAN Standards Committee, "ANSI/IEEE Std 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Authentication and Privacy", ***IEEE Standart, IEEE LAN Standards Committee, New York,***21-63 (2003).

25. IEEE LAN Standards Committee, "IEEE Std. 802.11i, IEEE Standard for Information Technology, Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Networks, Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Medium Access Control (MAC) Security Enhancements, Wired equivalent privacy (WEP)", ***IEEE Standart, IEEE LAN Standards Committee, New York,*** 17-137 (2004).

26. National Institute of Standards and Technology, "802.11 Wireless Lan Security Framework", ***Technical Report : Department of Defense Information Systems Agency, Washington,*** 1-19 (2004).

27. Department of Defense, Defense Information Systems Agency, "Wireless Security Technical Implementation Guide", ***Technical Report : Department of Defense Information Systems Agency, Washington,*** 8-24 (2005).

28. Ferguson, N., "Michael:An Improved MIC for 802.11 WEP", ***The Norvegian Research Network 2002 Research Seminar,*** Trondheim, 45-68 (2002).

29. Housley, R., Whiting, D., Ferguson, N., "Wired Equivalent Protection - WEP", ***The Norvegian Research Network, 2001 Research Seminar,*** Trondheim, 19-33 (2001).

30. Borisov, N., Goldberg I., Wagner D., "Intercepting Mobile Communications : The Insecurity of 802.11", ***Seventh Annual International Conference on Mobile Computing And Networking,*** Rome, 16-21 (2001).

31. Fluhrer, S., Mantin, I., Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4", ***Lecture Notes on Computer Science Magazine,*** 2259 : 1-23 (2001).

32. Arbaugh, A. W., Shankar, N., Wan, J. Y.C., "Your 802.11 Wireless Network Has No Clothes", ***IEEE Wireless Communications Magazine,*** 9: 6-29 (2001).

33. Stubblefield, A., Ioannidis, J., Rubin, A. D., "Using the Fluhrer, Mantin, and Shamir Attack. to Break WEP", ***Technical Report : TD-4ZCPZZ AT&T Labs and Rice University, New Jersey,*** 1-13 (2001).

34. Stubblefield, A., Ioannidis, J., Rubin, D. A., "A Key Recovery Attack On The 802.11b Wired Equivalent Privacy Protocol (WEP)", ***ACM Transactions on Information and System Security Magazine,*** 7(2): 319-332 (2004).

35. IEEE LAN Standards Committee, "IEEE 802.1X-2004 IEEE Standards for Local and Metropolitan Area Networks - Port-Based Network Access Control", ***IEEE Standart, IEEE LAN Standards Committee, New York,*** 33-87 (2004).

36. Seys, S., "The insecurity of 802.11 - What's Wrong with WEP?", ***Computer Security and Industrial Cryptography Seminar,*** Leuven, 1-31 (2001).

37. Walker, J. R., "Unsafe At Any Key Size:An Analysis Of The WEP Encapsulation", ***Technical Report : IEEE Document - 802.11-00/362, New York,*** 2-16 (2000).

38. Potter, B., "Wireless Security's Future", ***IEEE Security & Privacy Magazine,*** 1 (4): 68-72 (2003).

39. Altunbaşak, H., Owen, H., **"**Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs", ***2004 IEEE Southeast Conference Proceedings,*** Florida, 77-83 (2004).

40. Frankel, S., Eydt, B., Owens, L., Scarfone, K., "Establishing Wireless Robust Security Networks : A Guide to IEEE 802.11i", ***Technical Report : National Institute of Standards and Technology, Washington,*** 1-61 (2007).

41. Moen, W., Raddum, H., Hole, J.K., "Weaknesses in the Temporal Key Hash of WPA", ***ACM SIGMOBILE : Mobile Computing and Communications Review,*** 8 (2) : 76-83 (2004).

42. Falk, M., "Fast and Secure Roaming in WLAN", M.Sc. Thesis, ***Linkoping University Database and Information Institute,*** Linkoping, 3-15 (2004).

43. İnternet : IEEE 802.11 Wireless Local Area Networks Group - The Working Group For WLAN Standards, "IEEE 802 Standards For Free Download". http://www.ieee802.org/11/ (2007).

44. Mishra, A., Arbaugh, W. A., "An Initial Security Analysis of the IEEE 802.11X Standart", ***University of Maryland Institute for Advanced Computer Studies Technical Report, California***, 1-12 (2002).

45. İnternet : Microsoft, "Ad Hoc Internet Sharing with Microsoft Windows". http://www.microsoft.com/downloads/details.aspx?FamilyID=fac8708e-3762-4e78-b372-8404eeb7f41a&DisplayLang=en (2007).

46. İnternet : Microsoft, “File and Printer Sharing with Microsoft Windows”. http://www.microsoft.com/downloads/details.aspx?familyid=87c0a6db-aef8-4bef-925e-7ac9be791028&displaylang=en (2007).

47. İnternet : The Norwegian Research Network, “Throughput”. http://forskningsnett.uninett.no/wlan/throughput.html (2007).

E K L E R

Kablosuz Ağ Güvenlik Tarama Araç ve Yazılımları

1. Airmagnet

http;://www.airmagnet.com : A commercial product, Airmagnet is a full-featured WLAN site-survey tool that runs on a Compaq iPaq.

2. Boingo

http://www.boingo.com : Boingo is free software that can be downloaded from the Internet; it searches all available networks, and lets you know when you are in the range of a high-speed service signal (or tells you where to find the closest one).

3. Netstumbler

http://www.netstumbler.org/ : Very popular and well known, Netstumbler is free software that can be downloaded from the Internet; it detects WLAN access points and displays information about them.

4. Sniffer

http://www.sniffer.com : This professional wireless analyzer could possibly be used to help look for rogue APaccess points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known APaccess point vendors.

5. Wildpackets

http://www.wildpackets.com/products/airopeek : This professional wireless analyzer could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.

6. Observer

http://www.networkinstruments.com/ : This tool could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.

7. Finisar Surveyor

http://www.gofinisar.com/products/protocol/wireless/surveyor_w.html : This tool could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.

8. Wellenreiter

http://www.remote-exploit.org/ : Similar to Netstumbler but less popular and not as well known, Wellenreiter detects WLAN access points and displays information about them.

9. Kismet

http://www.kismetwireless.net/ : Kismet is an open source wireless sniffer that could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs.

10. dachb0den

http://www.dachb0den.com/projects/bsd-airtools.html : This tool, which is not well known, seems to be a combination of Netstumbler and Airsnort functionality.

11. Hornet

http://www.bvsystems.com/Products/WLAN/Hornet/hornet.htm : This dedicated hardware looks for a list of access point MAC addresses that have been configured and downloaded from a PC. It does not seem to do anything that a WLAN sniffer cannot do.

12. IBM Distributed Wireless Security Auditor

http://www.research.ibm.com/gsal/dwsa/ : This tool is a prototype only; it is not for sale. It uses client software on enterprise NICs to detect and report on all detected access points and their security system; a back-end system compares the list of detected access points with a list of authorized access points and alerts on unknown access points. This tool might produce false positives.

13. IBM TP General—IBM Access Connections for Windows 2000/XP

http://www.pc.ibm.com/qtechinfo/MIGR-4ZLNJB.html : Access Connections is a connectivity assistant program for your ThinkPad computer. It enables you to quickly switch the network settings and Internet settings by selecting a location profile. You can define the network settings and Internet settings in the Location Profile for modem or /wired LAN or /wireless LAN network devices, and then restore that profile whenever you need it. By switching the location profile, you can connect to the network instantly without reconfiguring your settings when you move from office to home or go on the road.

Büro XP_Win FW On												
	Open Authentication			Shared Authentication				Open Authentication			Shared Authentication	
	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128		Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**2 MB**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	11	11	11	27	17	22	Deneme01	28	16	16	33	17	28
Deneme02	22	22	22	22	22	22	Deneme02	27	27	28	27	27	27
Deneme03	22	22	22	28	22	22	Deneme03	27	28	27	28	33	28
Deneme04	21	22	22	27	22	27	Deneme04	28	27	28	27	28	27
Deneme05	22	22	22	22	22	27	Deneme05	27	28	27	28	27	27
Deneme06	22	27	22	22	22	22	Deneme06	28	27	27	27	27	28
Deneme07	22	22	22	22	22	22	Deneme07	27	28	28	28	28	27
Deneme08	22	28	22	22	22	22	Deneme08	28	27	27	27	16	28
Deneme09	22	32	22	22	22	22	Deneme09	27	28	28	28	28	27
Deneme10	22	22	22	22	22	22	Deneme10	28	27	27	27	27	28
Deneme11	22	28	27	22	22	22	Deneme11	27	28	28	28	28	27
Deneme12	22	22	22	28	22	22	Deneme12	28	38	33	27	27	28
Deneme13	22	22	22	22	22	22	Deneme13	27	28	27	28	28	33
Deneme14	22	22	22	21	22	22	Deneme14	28	27	28	32	27	27
Deneme15	22	22	22	22	22	22	Deneme15	27	27	27	28	28	28
Deneme16	22	22	22	22	21	22	Deneme16	33	28	28	27	27	27
Deneme17	22	22	22	22	22	22	Deneme17	27	27	27	28	28	28
Deneme18	22	22	22	22	22	22	Deneme18	28	33	27	27	27	27
Deneme19	22	22	22	22	22	22	Deneme19	27	28	28	28	27	27
Deneme20	22	22	22	22	22	21	Deneme20	28	27	27	27	28	28
Deneme21	22	22	22	22	22	33	Deneme21	27	28	28	28	27	27
Deneme22	22	22	22	22	22	22	Deneme22	33	27	27	27	28	28
Deneme23	22	22	22	22	22	22	Deneme23	28	28	28	28	27	27
Deneme24	22	22	22	22	22	17	Deneme24	27	27	27	27	28	28
Deneme25	22	21	22	17	22	22	Deneme25	28	28	28	28	27	27
Deneme26	17	11	16	22	22	16	Deneme26	11	16	16	22	22	33
Deneme27	22	22	22	16	22	22	Deneme27	28	28	28	22	28	27
Deneme28	22	22	22	22	27	22	Deneme28	27	27	33	22	22	27
Deneme29	22	33	22	17	22	22	Deneme29	27	28	27	27	38	28
Deneme30	22	22	22	16	21	22	Deneme30	28	27	28	27	27	33
Deneme31	22	22	22	17	22	22	Deneme31	27	28	33	33	28	27
Deneme32	22	22	22	16	22	22	Deneme32	28	33	27	28	27	55
Deneme33	22	22	22	22	22	22	Deneme33	27	33	28	27	28	22
Deneme34	22	22	22	17	22	22	Deneme34	28	27	27	27	27	17
Deneme35	22	22	22	16	22	22	Deneme35	27	27	33	33	28	33
Deneme36	22	22	27	22	22	22	Deneme36	33	28	27	28	27	27
Deneme37	22	22	28	28	22	22	Deneme37	28	27	28	27	28	28
Deneme38	22	22	27	21	22	22	Deneme38	27	33	33	28	27	27
Deneme39	22	27	22	22	22	22	Deneme39	28	28	27	27	28	28
Deneme40	22	22	22	39	22	22	Deneme40	27	27	28	28	27	27
Deneme41	22	28	22	22	33	22	Deneme41	27	28	38	27	28	27
Deneme42	22	27	22	16	22	22	Deneme42	28	27	28	28	27	28
Deneme43	22	22	22	17	22	22	Deneme43	27	28	33	27	27	27
Deneme44	22	22	22	22	22	22	Deneme44	28	27	27	27	28	28
Deneme45	22	22	22	22	22	22	Deneme45	27	28	33	28	27	27
Deneme46	22	22	22	27	27	22	Deneme46	28	27	28	27	28	28
Deneme47	22	22	22	22	28	22	Deneme47	27	27	32	28	27	27
Deneme48	22	22	22	22	27	21	Deneme48	44	28	28	27	28	28
Deneme49	21	22	22	22	22	22	Deneme49	33	33	33	28	27	27
Deneme50	22	22	27	22	22	22	Deneme50	33	27	33	27	28	28
Deneme51	22	27	22	22	16	16	Deneme51	22	22	22	22	22	22
Deneme52	22	22	22	22	22	22	Deneme52	27	28	33	27	33	28
Deneme53	22	22	22	39	22	22	Deneme53	27	27	38	28	27	33
Deneme54	22	22	22	22	27	22	Deneme54	28	28	28	27	28	27
Deneme55	22	22	28	22	33	22	Deneme55	27	27	27	33	32	28
Deneme56	22	22	27	21	22	22	Deneme56	39	28	33	28	28	27
Deneme57	21	22	22	22	22	22	Deneme57	27	27	28	27	27	27
Deneme58	22	28	22	22	22	22	Deneme58	28	28	27	27	28	28
Deneme59	28	27	22	22	22	22	Deneme59	27	27	27	28	27	33
Deneme60	22	22	22	22	22	22	Deneme60	28	27	28	27	28	27
Deneme61	27	22	22	22	27	22	Deneme61	27	33	27	33	27	28
Deneme62	22	22	22	22	22	28	Deneme62	28	28	28	28	33	27
Deneme63	22	22	22	22	22	22	Deneme63	27	27	27	27	28	28
Deneme64	22	22	33	22	22	27	Deneme64	28	28	28	28	27	27
Deneme65	22	22	22	22	22	22	Deneme65	27	33	33	27	28	28
Deneme66	28	27	22	22	22	22	Deneme66	33	27	27	28	27	27
Deneme67	22	22	22	22	22	22	Deneme67	27	39	28	27	28	28
Deneme68	22	22	22	17	22	22	Deneme68	33	33	27	28	32	27
Deneme69	22	22	22	22	27	27	Deneme69	28	33	28	27	28	28
Deneme70	22	22	27	22	22	28	Deneme70	27	27	33	27	33	27
Deneme71	22	22	22	22	22	22	Deneme71	28	28	32	28	27	27
Deneme72	22	22	22	22	28	22	Deneme72	33	27	28	33	33	28
Deneme73	21	28	22	21	22	22	Deneme73	27	33	33	28	28	27
Deneme74	22	22	22	22	22	22	Deneme74	28	27	27	27	27	28
Deneme75	22	11	22	22	22	22	Deneme75	27	28	28	28	33	27
Deneme76	16	27	11	16	22	16	Deneme76	22	22	16	22	22	22
Deneme77	22	22	22	22	27	28	Deneme77	28	28	39	22	28	33
Deneme78	22	22	27	17	33	22	Deneme78	27	27	33	38	33	22
Deneme79	22	22	33	22	22	22	Deneme79	28	28	27	28	33	16
Deneme80	22	22	22	22	22	27	Deneme80	27	33	28	27	22	28
Deneme81	22	22	22	22	27	22	Deneme81	22	27	27	28	22	27
Deneme82	22	22	22	22	28	28	Deneme82	33	28	28	27	27	28
Deneme83	22	17	22	22	22	27	Deneme83	28	27	38	27	27	27
Deneme84	22	22	22	22	22	22	Deneme84	27	28	28	28	22	17
Deneme85	22	27	22	21	27	22	Deneme85	28	27	33	27	28	27
Deneme86	22	28	22	22	22	22	Deneme86	33	27	27	27	27	28
Deneme87	22	27	22	22	22	22	Deneme87	33	28	28	33	28	27
Deneme88	22	22	22	22	22	28	Deneme88	32	27	32	28	27	27
Deneme89	22	28	22	22	22	21	Deneme89	28	28	28	27	33	28
Deneme90	22	22	22	28	22	28	Deneme90	27	33	27	33	28	27
Deneme91	22	22	27	27	22	38	Deneme91	28	27	28	28	27	28
Deneme92	22	21	22	22	22	22	Deneme92	27	28	27	27	28	27
Deneme93	22	22	22	17	22	22	Deneme93	28	27	28	28	27	28
Deneme94	22	27	22	22	22	22	Deneme94	49	28	27	33	28	27
Deneme95	22	22	28	22	22	22	Deneme95	28	33	33	27	27	28
Deneme96	22	22	22	27	27	22	Deneme96	33	27	28	33	27	27
Deneme97	22	22	22	28	22	28	Deneme97	33	28	33	28	33	28
Deneme98	22	22	22	22	22	27	Deneme98	27	27	27	27	28	27
Deneme99	22	22	22	22	22	17	Deneme99	33	27	33	33	27	28
Deneme100	21	22	21	27	22	16	Deneme100	27	28	28	27	28	27
Ortalama	21,90	22,73	22,51	22,13	22,88	22,67	Ortalama	28,45	28,07	28,73	27,89	27,63	27,57
Standart Sapma	1,69	3,27	2,85	3,66	2,67	3,11	Standart Sapma	4,02	3,10	3,75	2,56	3,06	3,84
Varyans	2,83	10,60	8,03	13,27	7,07	9,56	Varyans	16,03	9,49	13,92	6,50	9,25	14,63
Medyan	22,00	22,00	22,00	22,00	22,00	22,00	Medyan	28,00	28,00	28,00	27,50	28,00	27,00
Maximum	28	33	33	39	33	38	Maximum	49	39	39	38	38	55
Minimum	11	11	11	16	16	16	Minimum	11	16	16	22	16	16
Mod	22	22	22	22	22	22	Mod	27	27	28	27	27	27

XP_Win FW On															
				Disabled									Disabled		
4 MB	Süre	4 MB	4 MB	4 MB	4 MB	4 MB	8 MB	Süre	Süre	8 MB	8 MB	8 MB	8 MB	8 MB	8 MB
Deneme01	**44**	**22**	**17**	**27**	**22**	**38**	**Deneme01**	**28**	**28**	**61**	**49**	**27**	**66**		
Deneme02	38	38	38	39	38	38	Deneme02	76	60	60	55	61	55		
Deneme03	39	66	39	38	44	39	Deneme03	61	61	61	55	60	61		
Deneme04	38	39	32	39	33	38	Deneme04	55	60	82	55	55	60		
Deneme05	39	38	39	38	38	39	Deneme05	55	61	61	88	66	55		
Deneme06	38	50	38	39	39	38	Deneme06	55	71	60	83	55	55		
Deneme07	55	38	39	38	38	39	Deneme07	55	60	60	54	55	55		
Deneme08	38	38	38	39	39	38	Deneme08	54	55	55	55	55	60		
Deneme09	39	39	39	38	38	39	Deneme09	77	55	55	55	55	55		
Deneme10	38	38	38	38	39	38	Deneme10	61	55	55	99	55	72		
Deneme11	39	44	33	28	38	38	Deneme11	60	55	55	49	55	71		
Deneme12	38	39	39	49	39	44	Deneme12	55	60	55	55	66	66		
Deneme13	39	38	43	39	38	39	Deneme13	61	66	88	55	60	82		
Deneme14	38	39	39	38	38	38	Deneme14	60	55	55	55	55	105		
Deneme15	39	38	38	33	39	39	Deneme15	77	55	60	55	55	60		
Deneme16	38	38	39	39	33	38	Deneme16	60	55	55	82	55	77		
Deneme17	38	39	38	38	38	39	Deneme17	55	55	55	55	55	55		
Deneme18	39	38	39	38	39	44	Deneme18	55	49	55	55	55	55		
Deneme19	38	66	44	33	38	38	Deneme19	55	55	55	55	54	60		
Deneme20	39	39	38	55	39	38	Deneme20	55	55	55	55	72	55		
Deneme21	38	38	39	44	33	39	Deneme21	55	55	55	77	55	83		
Deneme22	39	39	38	39	66	38	Deneme22	71	55	55	60	55	55		
Deneme23	38	38	38	38	38	33	Deneme23	72	55	55	66	55	54		
Deneme24	39	39	39	39	38	39	Deneme24	55	55	88	50	55	55		
Deneme25	38	43	38	38	39	38	Deneme25	55	60	54	54	55	55		
Deneme26	27	28	28	27	27	27	Deneme26	33	27	28	116	110	49		
Deneme27	39	49	38	38	39	38	Deneme27	55	72	54	93	49	55		
Deneme28	38	38	38	39	38	39	Deneme28	55	60	72	72	55	55		
Deneme29	39	39	39	38	38	33	Deneme29	60	55	66	54	82	88		
Deneme30	38	44	38	44	33	49	Deneme30	50	55	55	55	61	55		
Deneme31	39	38	44	39	39	39	Deneme31	49	82	55	55	55	60		
Deneme32	49	55	39	38	44	33	Deneme32	55	55	60	55	55	55		
Deneme33	39	39	38	39	38	38	Deneme33	77	55	60	55	55	55		
Deneme34	38	38	39	38	39	33	Deneme34	71	77	55	55	55	55		
Deneme35	38	39	38	39	38	39	Deneme35	55	55	83	55	76	77		
Deneme36	39	38	39	27	39	32	Deneme36	55	71	60	55	66	55		
Deneme37	38	38	38	27	38	55	Deneme37	55	55	61	55	55	60		
Deneme38	33	39	38	39	38	38	Deneme38	55	55	55	55	61	55		
Deneme39	39	33	39	33	55	33	Deneme39	55	55	54	71	55	61		
Deneme40	49	44	38	33	39	39	Deneme40	55	77	55	66	60	77		
Deneme41	39	38	39	38	38	38	Deneme41	55	60	55	55	55	60		
Deneme42	33	28	33	39	39	39	Deneme42	55	61	88	49	60	55		
Deneme43	38	38	38	38	38	38	Deneme43	55	55	55	55	55	66		
Deneme44	38	39	44	39	39	39	Deneme44	77	55	66	55	83	55		
Deneme45	39	38	44	44	44	38	Deneme45	87	60	55	55	55	55		
Deneme46	38	44	39	27	38	38	Deneme46	72	55	82	55	55	55		
Deneme47	39	38	38	38	33	44	Deneme47	55	77	50	55	60	54		
Deneme48	38	39	38	39	44	39	Deneme48	55	60	60	55	60	55		
Deneme49	33	38	39	38	27	33	Deneme49	55	55	61	55	77	66		
Deneme50	44	50	38	33	39	33	Deneme50	55	55	60	55	55	55		
Deneme51	28	44	22	27	27	22	Deneme51	39	49	39	44	33	61		
Deneme52	38	38	39	38	33	38	Deneme52	60	55	60	60	54	55		
Deneme53	38	39	44	39	38	39	Deneme53	50	55	61	55	88	55		
Deneme54	39	38	44	38	44	38	Deneme54	55	55	54	55	66	54		
Deneme55	38	39	38	39	39	39	Deneme55	55	77	55	55	61	77		
Deneme56	44	38	38	55	38	38	Deneme56	55	55	55	60	55	66		
Deneme57	39	44	39	38	39	39	Deneme57	55	60	77	72	55	55		
Deneme58	38	38	38	39	38	38	Deneme58	55	55	72	55	60	55		
Deneme59	39	39	39	27	39	39	Deneme59	65	61	55	55	71	72		
Deneme60	38	33	49	49	44	38	Deneme60	66	87	54	55	83	54		
Deneme61	39	38	39	38	38	49	Deneme61	55	55	55	55	60	55		
Deneme62	49	33	38	50	44	28	Deneme62	55	61	55	54	55	55		
Deneme63	38	39	39	38	38	38	Deneme63	61	55	77	55	82	66		
Deneme64	39	33	38	39	39	50	Deneme64	55	60	55	61	55	50		
Deneme65	33	38	39	38	38	38	Deneme65	55	55	88	55	55	60		
Deneme66	38	33	38	39	39	39	Deneme66	54	60	66	71	55	55		
Deneme67	39	33	38	33	44	33	Deneme67	55	55	55	61	55	55		
Deneme68	38	33	39	38	55	38	Deneme68	55	55	55	54	55	55		
Deneme69	39	33	44	33	38	39	Deneme69	55	66	55	55	55	55		
Deneme70	38	38	33	38	39	32	Deneme70	83	55	55	55	55	77		
Deneme71	39	55	38	39	38	39	Deneme71	71	55	60	55	82	60		
Deneme72	38	33	39	38	38	38	Deneme72	55	55	55	83	72	55		
Deneme73	38	33	33	44	39	33	Deneme73	55	55	82	55	55	55		
Deneme74	39	33	38	39	44	39	Deneme74	55	60	55	82	55	60		
Deneme75	38	33	33	38	55	38	Deneme75	55	55	55	71	60	61		
Deneme76	27	27	27	28	28	33	Deneme76	44	49	44	44	49	60		
Deneme77	50	33	44	38	43	38	Deneme77	55	83	55	55	61	55		
Deneme78	38	33	38	39	39	39	Deneme78	55	55	55	77	55	55		
Deneme79	39	39	33	38	44	38	Deneme79	66	55	88	55	55	49		
Deneme80	38	38	50	38	38	39	Deneme80	61	55	55	55	54	61		
Deneme81	33	39	38	39	39	38	Deneme81	54	55	55	55	55	55		
Deneme82	38	38	33	38	49	39	Deneme82	55	87	60	76	55	77		
Deneme83	39	39	33	39	39	38	Deneme83	55	66	61	55	55	54		
Deneme84	49	38	38	38	44	33	Deneme84	55	55	65	55	72	55		
Deneme85	39	38	39	44	33	38	Deneme85	55	55	66	55	60	61		
Deneme86	38	39	49	39	38	39	Deneme86	77	55	55	55	55	55		
Deneme87	39	38	38	44	38	38	Deneme87	66	55	55	55	77	55		
Deneme88	33	39	33	38	33	39	Deneme88	60	71	55	55	49	55		
Deneme89	38	38	50	33	38	49	Deneme89	55	55	61	88	55	54		
Deneme90	39	33	33	44	33	39	Deneme90	55	55	93	66	55	72		
Deneme91	38	39	38	66	38	38	Deneme91	55	55	55	55	55	55		
Deneme92	33	38	44	38	33	39	Deneme92	55	61	55	82	55	55		
Deneme93	38	50	39	39	39	38	Deneme93	55	55	55	55	60	55		
Deneme94	39	32	38	33	33	38	Deneme94	55	76	55	55	55	66		
Deneme95	38	33	33	39	33	39	Deneme95	55	55	60	55	72	71		
Deneme96	39	39	44	38	49	44	Deneme96	55	55	55	55	55	55		
Deneme97	33	33	44	39	28	38	Deneme97	55	55	60	55	55	55		
Deneme98	44	38	38	43	38	39	Deneme98	55	55	55	60	60	55		
Deneme99	38	33	33	39	33	38	Deneme99	88	83	61	83	55	55		
Deneme100	33	33	39	38	50	39	Deneme100	76	60	60	65	55	55		
Ortalama	38,55	38,55	38,22	38,32	38,77	38,16	Ortalama	58,35	58,87	60,09	60,46	59,37	59,98		
Standart Sapma	4,06	6,37	4,75	5,79	6,00	4,26	Standart Sapma	9,48	9,44	10,65	12,15	10,60	9,18		
Varyans	16,33	40,23	22,29	33,18	35,70	17,95	Varyans	88,95	88,31	112,34	146,07	111,23	83,46		
Medyan	38,00	38,00	38,00	38,00	38,00	38,00	Medyan	55,00	55,00	55,00	55,00	55,00	55,00		
Maximum	55,00	66,00	50,00	66,00	66,00	55,00	Maximum	88,00	87,00	93,00	116,00	110,00	105,00		
Minimum	27	22	17	27	22	22	Minimum	28	27	28	44	27	49		
Mod	38	38	38	38	38	38	Mod	55	55	55	55	55	55		

XP_Win FW On														
				Disabled								Disabled		
16 MB	Süre	16 MB	16 MB	16 MB	16 MB	16 MB	32 MB	Süre	32 MB	32 MB	32 MB	32 MB	32 MB	
Deneme01	**44**	**93**	**121**	**137**	**71**	**187**	**Deneme01**	**780**	**582**	**434**	**780**	**944**	**643**	
Deneme02	143	99	110	104	99	99	Deneme02	637	631	665	648	643	725	
Deneme03	132	99	99	105	99	170	Deneme03	604	665	664	637	742	632	
Deneme04	126	93	110	99	99	148	Deneme04	638	895	642	626	834	637	
Deneme05	93	99	98	98	219	187	Deneme05	747	692	632	632	675	846	
Deneme06	94	126	94	83	149	93	Deneme06	747	819	643	615	621	615	
Deneme07	93	127	93	99	82	105	Deneme07	642	648	637	632	758	615	
Deneme08	93	148	99	93	93	208	Deneme08	863	648	648	719	632	637	
Deneme09	94	99	99	99	94	132	Deneme09	631	632	637	638	818	824	
Deneme10	93	93	99	99	93	132	Deneme10	626	961	610	615	621	621	
Deneme11	83	220	93	99	93	132	Deneme11	621	642	642	643	620	1065	
Deneme12	93	225	94	94	94	126	Deneme12	730	643	648	648	638	626	
Deneme13	110	121	93	104	93	99	Deneme13	698	654	605	654	856	637	
Deneme14	208	93	93	99	94	93	Deneme14	642	631	648	637	632	1022	
Deneme15	237	94	94	88	76	143	Deneme15	665	621	626	632	643	1274	
Deneme16	142	170	93	93	94	105	Deneme16	769	599	840	714	637	736	
Deneme17	116	137	93	269	93	82	Deneme17	642	780	830	697	664	890	
Deneme18	93	220	94	121	94	121	Deneme18	797	648	653	687	632	626	
Deneme19	94	225	93	115	93	92	Deneme19	648	637	637	648	582	637	
Deneme20	214	93	94	231	93	99	Deneme20	610	626	643	829	846	627	
Deneme21	99	209	93	77	94	99	Deneme21	856	632	637	753	626	631	
Deneme22	93	121	93	93	225	110	Deneme22	616	615	643	653	643	703	
Deneme23	93	93	94	94	253	225	Deneme23	609	632	637	742	626	648	
Deneme24	94	93	104	93	263	137	Deneme24	637	719	659	802	626	649	
Deneme25	93	94	104	93	214	132	Deneme25	769	638	621	637	648	1191	
Deneme26	66	193	214	182	242	99	Deneme26	654	615	599	643	566	785	
Deneme27	104	110	121	93	231	99	Deneme27	632	643	670	632	643	451	
Deneme28	104	93	220	126	252	137	Deneme28	686	648	626	643	835	637	
Deneme29	94	104	219	116	105	247	Deneme29	605	654	627	637	631	637	
Deneme30	82	105	105	104	104	93	Deneme30	780	637	725	918	637	615	
Deneme31	99	98	115	99	99	94	Deneme31	889	632	637	654	632	632	
Deneme32	93	94	94	99	99	126	Deneme32	626	714	637	604	752	631	
Deneme33	94	126	98	93	93	132	Deneme33	753	697	649	714	797	649	
Deneme34	93	99	116	94	94	148	Deneme34	747	687	867	786	620	648	
Deneme35	94	99	82	93	263	121	Deneme35	616	648	681	653	632	769	
Deneme36	93	93	93	104	99	159	Deneme36	631	829	627	753	802	626	
Deneme37	99	94	94	94	93	94	Deneme37	758	753	604	615	637	620	
Deneme38	93	93	99	93	94	93	Deneme38	610	653	796	698	813	676	
Deneme39	94	99	93	93	93	93	Deneme39	637	742	615	626	676	615	
Deneme40	148	99	99	110	94	99	Deneme40	747	802	648	664	725	631	
Deneme41	99	93	93	264	98	83	Deneme41	890	637	769	643	637	583	
Deneme42	93	242	99	231	182	99	Deneme42	610	643	818	648	610	620	
Deneme43	94	132	99	98	121	104	Deneme43	632	653	637	884	626	643	
Deneme44	93	181	93	105	274	237	Deneme44	813	731	632	692	786	648	
Deneme45	93	121	94	93	203	153	Deneme45	637	615	736	676	626	632	
Deneme46	99	99	209	94	138	215	Deneme46	637	747	642	670	643	1054	
Deneme47	99	98	93	98	126	93	Deneme47	604	697	637	648	829	637	
Deneme48	93	94	159	105	104	93	Deneme48	467	627	637	643	643	621	
Deneme49	94	99	94	99	99	94	Deneme49	917	637	604	631	631	637	
Deneme50	104	219	98	94	275	99	Deneme50	659	802	653	643	698	632	
Deneme51	104	61	236	61	55	115	Deneme51	895	818	582	654	582	615	
Deneme52	105	93	121	99	137	115	Deneme52	649	654	643	631	654	648	
Deneme53	115	137	99	109	209	99	Deneme53	834	730	615	638	637	632	
Deneme54	110	132	104	88	132	99	Deneme54	725	632	626	867	620	648	
Deneme55	93	126	99	88	93	264	Deneme55	808	653	621	637	791	835	
Deneme56	88	94	104	88	143	93	Deneme56	615	648	736	763	626	621	
Deneme57	94	93	105	88	88	269	Deneme57	632	681	692	846	632	697	
Deneme58	88	231	93	88	93	88	Deneme58	653	648	615	736	835	632	
Deneme59	93	236	93	93	94	88	Deneme59	857	901	857	653	637	632	
Deneme60	104	132	171	88	88	159	Deneme60	648	670	824	648	593	703	
Deneme61	99	99	236	236	88	182	Deneme61	764	599	626	632	626	615	
Deneme62	99	99	88	99	87	98	Deneme62	670	719	610	609	670	1352	
Deneme63	104	120	88	104	105	88	Deneme63	719	852	664	643	698	642	
Deneme64	99	99	159	88	110	88	Deneme64	632	774	626	714	698	632	
Deneme65	99	253	88	88	142	88	Deneme65	851	703	643	676	643	730	
Deneme66	93	126	127	88	88	93	Deneme66	714	648	681	549	631	1088	
Deneme67	99	94	109	88	88	94	Deneme67	637	604	621	599	637	637	
Deneme68	94	93	94	148	88	93	Deneme68	665	610	620	637	660	626	
Deneme69	88	93	88	93	88	99	Deneme69	648	632	692	609	598	626	
Deneme70	87	94	99	116	88	88	Deneme70	599	840	824	775	626	632	
Deneme71	121	159	87	181	126	115	Deneme71	252	643	632	610	632	1010	
Deneme72	121	231	94	258	88	105	Deneme72	649	637	632	736	610	654	
Deneme73	104	126	99	88	88	110	Deneme73	681	714	637	604	857	1192	
Deneme74	105	132	88	137	88	98	Deneme74	615	763	675	626	631	631	
Deneme75	165	104	87	83	99	94	Deneme75	653	698	605	736	610	670	
Deneme76	116	214	82	110	105	176	Deneme76	609	747	560	593	747	846	
Deneme77	104	115	99	132	230	94	Deneme77	802	637	643	692	637	648	
Deneme78	93	94	99	126	138	115	Deneme78	643	599	637	621	703	632	
Deneme79	182	98	258	121	115	77	Deneme79	642	730	654	829	637	692	
Deneme80	104	226	226	99	93	252	Deneme80	632	654	824	615	637	648	
Deneme81	93	115	219	88	209	176	Deneme81	731	637	659	961	626	621	
Deneme82	94	93	220	88	94	99	Deneme82	736	807	648	714	764	867	
Deneme83	110	209	236	203	131	203	Deneme83	823	648	835	676	780	638	
Deneme84	87	121	220	132	149	88	Deneme84	786	643	676	649	621	829	
Deneme85	94	99	187	126	225	88	Deneme85	632	626	626	631	626	604	
Deneme86	93	99	219	127	220	104	Deneme86	626	626	643	643	626	703	
Deneme87	88	104	143	98	87	99	Deneme87	642	627	642	643	308	599	
Deneme88	87	93	192	94	248	88	Deneme88	725	626	637	851	626	813	
Deneme89	94	99	231	88	87	88	Deneme89	637	758	851	643	742	637	
Deneme90	110	94	148	99	88	93	Deneme90	643	631	632	637	631	637	
Deneme91	93	93	204	87	94	99	Deneme91	637	632	670	610	637	665	
Deneme92	93	93	93	88	93	94	Deneme92	631	873	791	637	632	643	
Deneme93	105	94	104	88	88	208	Deneme93	632	632	631	615	681	631	
Deneme94	99	126	99	99	88	110	Deneme94	637	626	566	736	648	1071	
Deneme95	99	93	94	170	88	116	Deneme95	687	637	670	637	615	1017	
Deneme96	98	94	93	176	88	87	Deneme96	642	335	637	637	775	741	
Deneme97	94	93	137	94	104	88	Deneme97	736	637	610	643	670	632	
Deneme98	93	94	214	120	198	88	Deneme98	643	632	626	670	627	1065	
Deneme99	220	164	99	88	170	88	Deneme99	632	769	708	648	626	687	
Deneme100	236	204	99	88	220	88	Deneme100	609	632	632	676	670	737	
Ortalama	106,28	125,39	123,08	112,67	127,82	121,88	Ortalama	683,21	679,05	662,61	676,71	670,6	717,89	
Standart Sapma	31,95	46,82	48,64	41,51	57,45	45,42	Standart Sapma	95,29	84,81	72,73	75,43	85,17	166,57	
Varyans	1010,40	2170,30	2341,79	1705,46	3266,97	2042,55	Varyans	8989,19	7120,05	5237,16	5632,25	7182,14	27468,62	
Medyan	94,00	99,00	99,00	99,00	98,50	99,00	Medyan	645,50	648,00	642,00	648,00	637,00	640,00	
Maximum	237,00	253,00	258,00	269,00	275,00	269,00	Maximum	917,00	961,00	867,00	961,00	944,00	1352,00	
Minimum	44	61	82	61	55	77	Minimum	252	335	434	549	308	451	
Mod	93	93	93	88	88	99	Mod	637	632	637	643	626	632	

EK-2 Devam

	XP_Win FW On					
	Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	2368	2251	2153	2279	2384	2351
Deneme02	2345	2280	2038	2197	2230	2236
Deneme03	2290	2477	2192	2532	2449	2263
Deneme04	2153	2186	2362	2296	2395	2235
Deneme05	1895	2246	2153	1923	2252	2280
Deneme06	2126	1253	2274	2252	1791	2093
Deneme07	2246	2301	2587	2257	2290	1993
Deneme08	2554	2081	2274	2345	2516	2197
Deneme09	2428	2329	2357	2258	2252	2269
Deneme10	2120	2285	2279	2279	2295	2159
Deneme11	2236	2170	1268	2422	2126	2241
Deneme12	2186	2213	2219	2406	2252	2439
Deneme13	2340	2082	2252	2274	2246	2548
Deneme14	2532	2268	2230	2104	2258	2247
Deneme15	1318	2258	2368	2361	1955	2268
Deneme16	2384	2515	2181	2192	2219	2274
Deneme17	2219	2252	2306	2285	2263	2263
Deneme18	2757	2312	2202	2280	2137	2318
Deneme19	2494	2153	2269	2279	2246	2230
Deneme20	2235	2494	1983	2302	2263	2323
Deneme21	2274	2609	2252	2273	2082	2263
Deneme22	2290	2279	2081	2500	2186	2280
Deneme23	2236	2197	1928	2279	2153	2120
Deneme24	2208	2422	2543	2126	2191	2532
Deneme25	2263	2115	2247	2257	2258	2170
Deneme26	2493	2565	2197	2186	1955	2274
Deneme27	2219	2258	2346	2219	2296	2455
Deneme28	2274	2257	2257	2302	2357	2263
Deneme29	2340	2263	2257	2362	2208	2131
Deneme30	2543	2296	2269	2350	2109	2263
Deneme31	2258	2263	2219	1747	2224	2159
Deneme32	2164	2604	2345	2252	2340	2527
Deneme33	2598	2010	2065	2301	2285	2169
Deneme34	1604	1664	2246	2263	2494	2098
Deneme35	2642	2181	2258	2257	1592	2230
Deneme36	2165	2230	2219	2147	2208	2257
Deneme37	2235	2378	2153	2121	2225	2192
Deneme38	2538	2587	2279	2268	2258	2246
Deneme39	2317	2362	1763	2230	2252	2258
Deneme40	2296	2208	2219	2274	2142	2411
Deneme41	2268	2526	2192	2252	2263	2483
Deneme42	2170	2175	2257	2466	2285	1735
Deneme43	1428	1313	2357	2114	2285	2203
Deneme44	2323	2203	2268	2225	2351	2246
Deneme45	2505	2295	2246	2241	2263	2241
Deneme46	2164	2044	2329	2411	2280	2120
Deneme47	2257	2037	2274	2230	2581	2137
Deneme48	2225	2313	1923	2356	2230	2406
Deneme49	2268	2208	2241	2274	2372	2274
Deneme50	2236	2252	2257	2373	2088	2208
Deneme51	2428	1500	2241	2235	2137	2148
Deneme52	2290	2345	2131	2285	2147	2285
Deneme53	2428	2400	2258	2499	2181	2246
Deneme54	2016	2274	2032	2290	2241	2087
Deneme55	2235	2466	1966	2258	2186	2109
Deneme56	2263	2324	2510	2301	2263	2324
Deneme57	2346	2565	2346	2307	2169	2169
Deneme58	2290	2614	2317	2356	2318	2131
Deneme59	2274	2313	2241	2268	2219	2169
Deneme60	2527	2202	2219	2263	2274	1978
Deneme61	2411	2170	2291	2115	1296	2158
Deneme62	2241	2636	2279	2428	2269	2302
Deneme63	2296	2098	2225	1993	2070	2230
Deneme64	1367	2252	1999	2213	2263	2356
Deneme65	2505	2713	2142	2252	2208	2790
Deneme66	2416	2099	2400	2373	2532	2280
Deneme67	2280	2285	2318	2147	2269	2114
Deneme68	2269	2543	2307	2291	2263	2318
Deneme69	2252	2290	2137	2235	2153	1763
Deneme70	2290	1719	2268	1703	1900	2219
Deneme71	2510	2258	2153	2268	2274	2263
Deneme72	2180	2290	2516	2368	2428	2120
Deneme73	2059	2642	2521	2132	2323	2175
Deneme74	2274	2257	2208	2202	2258	2170
Deneme75	2279	2225	2301	1813	2268	2334
Deneme76	2230	2192	2378	2263	2351	2274
Deneme77	2279	2252	2290	2394	2159	2268
Deneme78	2235	2202	2181	2170	2444	1703
Deneme79	2477	2236	2230	2087	2180	2604
Deneme80	2005	2147	2505	2235	2225	2257
Deneme81	2362	2131	2236	2258	2274	2131
Deneme82	2263	2252	2240	2252	2153	2258
Deneme83	2307	2269	2038	2312	2389	2186
Deneme84	2471	2219	2175	2241	2219	2263
Deneme85	2296	2147	2247	2230	2230	2153
Deneme86	2582	2257	2153	2197	2126	2328
Deneme87	2274	2428	2526	2230	2273	2110
Deneme88	2280	1950	2186	2280	2230	2317
Deneme89	2252	2235	2302	2488	1698	2576
Deneme90	1318	2401	2224	2323	2274	2439
Deneme91	2329	2257	2246	2241	2257	2499
Deneme92	2115	2247	2549	2159	2274	2247
Deneme93	2269	2186	2570	2246	2340	2241
Deneme94	2268	2246	2626	2175	2312	2224
Deneme95	2450	2290	2180	2417	2269	2422
Deneme96	2274	2126	2258	2246	2268	2258
Deneme97	2378	1906	2158	2252	2318	1340
Deneme98	2642	2285	2324	2499	1735	2219
Deneme99	1785	2257	2312	2071	2269	2246
Deneme100	2263	2192	2230	2301	2274	2181
Ortalama	2261,57	2243,10	2241,24	2253,41	2220,82	2235,60
Standart Sapma	249,25	234,36	174,26	135,69	179,29	180,97
Varyans	61503,17	54377,19	30063,00	18227,64	31824,75	32421,26
Medyan	2274,00	2257,00	2247,00	2260,50	2258,00	2246,00
Maximum	2757	2713	2626	2532	2581	2790
Minimum	1318	1253	1268	1703	1296	1340
Mod	2274	2252	2153	2252	2263	2263

Büro XP Win FW On						
	Open Authentication			Shared Authentication		
	Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
1 MB	Süre	Süre	Süre	Süre	Süre	Süre
Deneme01	11	11	11	27	17	22
Deneme02	22	22	22	22	22	22
Deneme03	22	22	22	28	22	22
Deneme04	21	22	22	27	22	27
Deneme05	22	22	22	22	22	27
Deneme06	22	27	22	22	22	22
Deneme07	22	22	22	22	22	22
Deneme08	22	28	22	22	22	22
Deneme09	22	32	22	22	22	22
Deneme10	22	22	22	22	22	22
Deneme11	22	28	27	22	22	22
Deneme12	22	22	22	28	22	22
Deneme13	22	22	22	22	22	22
Deneme14	22	22	22	21	22	22
Deneme15	22	22	22	22	22	22
Deneme16	22	22	22	22	21	22
Deneme17	22	22	22	22	22	22
Deneme18	22	22	22	22	22	22
Deneme19	22	22	22	22	22	22
Deneme20	22	22	22	22	22	21
Deneme21	22	22	22	22	22	33
Deneme22	22	22	22	22	22	22
Deneme23	22	22	22	22	22	22
Deneme24	22	22	22	22	22	17
Deneme25	22	21	22	17	22	22
Deneme26	17	11	16	22	22	16
Deneme27	22	22	22	16	22	22
Deneme28	22	22	22	22	27	22
Deneme29	22	33	22	17	22	22
Deneme30	22	22	22	16	21	22
Deneme31	22	22	22	17	22	22
Deneme32	22	22	22	16	22	22
Deneme33	22	22	22	22	22	22
Deneme34	22	22	22	17	22	22
Deneme35	22	22	22	16	22	22
Deneme36	22	22	27	22	22	22
Deneme37	22	22	28	28	22	22
Deneme38	22	22	27	21	22	22
Deneme39	22	27	22	22	22	22
Deneme40	22	22	22	39	22	22
Deneme41	22	28	22	22	33	22
Deneme42	22	27	22	16	22	22
Deneme43	22	22	22	17	22	22
Deneme44	22	22	22	22	22	22
Deneme45	22	22	22	22	22	22
Deneme46	22	22	22	27	27	22
Deneme47	22	22	22	22	28	22
Deneme48	22	22	22	22	27	21
Deneme49	21	22	22	22	22	22
Deneme50	22	22	27	22	22	22
Deneme51	22	27	22	22	16	16
Deneme52	22	22	22	22	22	22
Deneme53	22	22	22	39	22	22
Deneme54	22	22	22	22	27	22
Deneme55	22	22	28	22	33	22
Deneme56	22	22	27	21	22	22
Deneme57	21	22	22	22	22	22
Deneme58	22	28	22	22	22	22
Deneme59	28	27	22	22	22	22
Deneme60	22	22	22	22	22	22
Deneme61	27	22	22	22	27	22
Deneme62	22	22	22	22	22	28
Deneme63	22	22	22	22	22	22
Deneme64	22	22	33	22	22	27
Deneme65	22	22	22	22	22	22
Deneme66	28	27	22	22	22	22
Deneme67	22	22	22	22	22	22
Deneme68	22	22	22	17	22	22
Deneme69	22	22	22	22	27	27
Deneme70	22	22	27	22	22	28
Deneme71	22	22	22	22	22	22
Deneme72	22	22	22	22	28	22
Deneme73	21	28	22	21	22	22
Deneme74	22	22	22	22	22	22
Deneme75	22	11	22	22	22	22
Deneme76	16	27	11	16	22	16
Deneme77	22	22	22	22	27	28
Deneme78	22	22	27	17	33	22
Deneme79	22	22	33	22	22	22
Deneme80	22	22	22	22	22	27
Deneme81	22	22	22	22	27	22
Deneme82	22	22	22	22	28	28
Deneme83	22	17	22	22	22	27
Deneme84	22	22	22	22	22	22
Deneme85	22	27	22	21	27	22
Deneme86	22	28	22	22	22	22
Deneme87	22	27	22	22	22	22
Deneme88	22	22	22	22	22	28
Deneme89	22	28	22	22	22	21
Deneme90	22	22	22	28	22	28
Deneme91	22	22	27	27	22	38
Deneme92	22	21	22	22	22	22
Deneme93	22	22	22	17	22	22
Deneme94	22	27	22	22	22	22
Deneme95	22	22	28	22	22	22
Deneme96	22	22	22	27	27	22
Deneme97	22	22	22	28	22	28
Deneme98	22	22	22	22	22	27
Deneme99	22	22	22	22	22	17
Deneme100	21	22	21	27	22	16
Ortalama	21,90	22,73	22,51	22,13	22,88	22,67
Standart Sapma	1,69	3,27	2,85	3,66	2,67	3,11
Varyans	2,83	10,60	8,03	13,27	7,07	9,56
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	28	33	33	39	33	38
Minimum	11	11	11	16	16	16
Mod	22	22	22	22	22	22

Büro XP Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
1 MB	Süre	Süre	Süre	Süre	Süre	Süre
Deneme01	11	17	21	33	16	22
Deneme02	22	22	22	17	22	28
Deneme03	22	33	22	16	22	21
Deneme04	22	22	22	22	22	22
Deneme05	22	22	22	17	28	22
Deneme06	22	22	22	21	22	22
Deneme07	22	22	22	22	22	22
Deneme08	28	22	22	17	21	22
Deneme09	22	22	22	22	22	28
Deneme10	21	22	22	22	22	22
Deneme11	28	22	22	16	22	22
Deneme12	27	21	22	17	22	22
Deneme13	22	22	22	22	27	22
Deneme14	22	22	22	16	22	22
Deneme15	22	22	22	22	22	22
Deneme16	28	28	22	22	22	22
Deneme17	22	22	22	22	22	22
Deneme18	22	27	22	22	22	22
Deneme19	27	22	22	22	22	21
Deneme20	22	22	22	22	22	22
Deneme21	27	22	22	17	22	22
Deneme22	22	22	22	17	22	22
Deneme23	33	22	22	16	22	22
Deneme24	16	22	22	22	22	22
Deneme25	27	22	22	22	22	22
Deneme26	17	11	22	17	16	11
Deneme27	22	22	22	22	22	22
Deneme28	22	27	22	27	22	22
Deneme29	22	22	28	22	22	22
Deneme30	22	22	22	22	22	22
Deneme31	22	22	21	22	22	22
Deneme32	22	22	22	22	22	22
Deneme33	22	22	22	22	22	22
Deneme34	22	22	22	22	28	22
Deneme35	22	22	22	22	21	22
Deneme36	22	22	22	22	28	22
Deneme37	22	27	22	27	22	22
Deneme38	22	33	22	28	22	22
Deneme39	22	22	22	22	22	22
Deneme40	22	22	22	27	22	22
Deneme41	22	22	22	22	22	22
Deneme42	22	22	22	22	22	22
Deneme43	22	22	22	22	22	33
Deneme44	22	22	22	22	22	16
Deneme45	22	22	22	22	22	22
Deneme46	28	22	22	22	22	28
Deneme47	27	22	22	22	22	16
Deneme48	22	21	22	22	22	22
Deneme49	22	22	22	22	22	22
Deneme50	28	22	22	22	22	22
Deneme51	22	16	17	22	22	17
Deneme52	22	27	22	28	22	22
Deneme53	21	22	22	16	27	22
Deneme54	22	22	22	22	22	22
Deneme55	22	22	22	22	22	22
Deneme56	22	22	22	28	22	22
Deneme57	22	22	22	22	22	22
Deneme58	22	22	22	22	22	22
Deneme59	22	22	22	22	22	22
Deneme60	22	27	22	22	22	22
Deneme61	22	22	21	22	22	22
Deneme62	22	17	28	27	22	27
Deneme63	22	16	22	22	22	22
Deneme64	22	22	22	22	22	22
Deneme65	22	22	22	22	22	22
Deneme66	22	22	22	22	22	22
Deneme67	22	22	22	38	22	22
Deneme68	22	22	22	22	22	27
Deneme69	22	22	22	22	22	22
Deneme70	22	22	22	22	22	22
Deneme71	22	22	22	22	21	22
Deneme72	22	22	22	28	22	22
Deneme73	22	22	22	22	22	28
Deneme74	22	22	22	22	22	22
Deneme75	22	22	22	22	22	22
Deneme76	17	16	11	17	16	11
Deneme77	16	28	22	21	22	22
Deneme78	17	27	22	28	22	22
Deneme79	16	22	22	22	22	17
Deneme80	22	22	22	22	22	22
Deneme81	22	22	22	22	22	22
Deneme82	28	22	22	22	22	21
Deneme83	27	22	22	22	22	22
Deneme84	22	22	22	22	22	22
Deneme85	22	22	22	22	22	28
Deneme86	22	27	22	27	22	22
Deneme87	22	28	22	22	22	22
Deneme88	22	22	27	28	22	22
Deneme89	22	22	22	22	22	22
Deneme90	22	22	22	22	22	27
Deneme91	22	22	22	22	22	22
Deneme92	22	22	22	22	22	33
Deneme93	17	27	28	21	22	27
Deneme94	21	22	22	22	27	22
Deneme95	22	28	22	22	22	22
Deneme96	22	22	22	22	33	22
Deneme97	22	22	22	22	22	22
Deneme98	22	22	22	28	22	22
Deneme99	22	22	22	22	22	22
Deneme100	22	27	21	22	22	27
Ortalama	22,25	22,50	22,03	22,21	22,23	22,30
Standart Sapma	2,87	2,96	1,69	3,38	2,03	3,02
Varyans	8,13	8,67	2,83	11,33	4,10	9,05
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	33	28	38	33	33
Minimum	11	11	11	16	16	11
Mod	22	22	22	22	22	22

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	22	11	22	22	16	22
Deneme02	22	27	22	16	33	22
Deneme03	22	22	22	22	22	22
Deneme04	22	22	22	22	22	22
Deneme05	22	22	22	21	22	22
Deneme06	22	22	22	22	22	22
Deneme07	22	22	22	22	22	22
Deneme08	22	22	22	22	22	22
Deneme09	22	22	22	22	28	22
Deneme10	21	22	22	22	22	22
Deneme11	22	22	22	22	22	21
Deneme12	22	28	22	22	22	22
Deneme13	22	27	22	22	27	22
Deneme14	22	33	22	22	22	22
Deneme15	22	22	22	22	22	22
Deneme16	22	22	22	22	27	22
Deneme17	22	27	22	22	22	22
Deneme18	22	22	22	22	28	22
Deneme19	22	22	22	22	22	22
Deneme20	22	27	22	27	27	22
Deneme21	22	22	22	16	33	22
Deneme22	22	22	22	22	28	22
Deneme23	22	22	22	22	22	22
Deneme24	22	22	22	22	22	22
Deneme25	22	22	22	22	22	22
Deneme26	16	16	17	22	11	17
Deneme27	22	22	22	22	22	27
Deneme28	22	22	22	28	22	22
Deneme29	28	33	22	22	27	22
Deneme30	27	22	22	22	22	22
Deneme31	22	22	22	22	22	22
Deneme32	28	27	22	22	22	22
Deneme33	22	22	22	22	22	22
Deneme34	21	22	22	27	22	22
Deneme35	22	22	22	22	27	22
Deneme36	22	22	21	22	22	22
Deneme37	22	27	22	22	22	22
Deneme38	22	22	22	22	22	27
Deneme39	22	27	22	22	22	28
Deneme40	22	28	22	22	22	22
Deneme41	22	22	22	11	22	22
Deneme42	22	22	22	22	22	22
Deneme43	22	27	22	22	16	22
Deneme44	22	22	22	22	22	27
Deneme45	22	22	22	22	22	22
Deneme46	22	22	22	22	22	22
Deneme47	22	22	22	22	22	22
Deneme48	22	22	22	22	22	22
Deneme49	22	22	22	22	22	22
Deneme50	22	22	22	22	22	22
Deneme51	22	16	16	22	17	17
Deneme52	22	22	22	22	22	22
Deneme53	22	22	22	27	22	22
Deneme54	22	22	22	22	22	22
Deneme55	22	22	28	22	22	22
Deneme56	22	22	22	22	22	22
Deneme57	22	22	22	27	22	22
Deneme58	22	17	27	22	27	27
Deneme59	22	22	22	22	22	22
Deneme60	22	22	22	22	28	28
Deneme61	22	22	22	22	22	22
Deneme62	22	22	22	22	22	22
Deneme63	22	22	22	22	22	22
Deneme64	22	21	22	17	22	21
Deneme65	22	22	22	22	22	22
Deneme66	22	22	22	27	21	22
Deneme67	22	22	22	28	22	22
Deneme68	33	22	22	27	22	22
Deneme69	27	22	22	22	22	22
Deneme70	22	22	22	28	22	22
Deneme71	22	22	22	22	22	22
Deneme72	22	22	22	22	17	22
Deneme73	22	22	22	21	22	22
Deneme74	22	22	22	22	22	22
Deneme75	22	22	22	27	22	22
Deneme76	16	17	17	22	11	33
Deneme77	22	22	22	22	22	21
Deneme78	22	22	22	22	27	22
Deneme79	21	22	22	22	22	22
Deneme80	22	22	22	22	22	22
Deneme81	22	22	22	22	28	22
Deneme82	22	22	21	22	27	22
Deneme83	22	22	22	22	22	22
Deneme84	22	22	38	22	28	28
Deneme85	22	22	22	27	21	22
Deneme86	22	21	22	22	22	22
Deneme87	22	22	28	27	28	22
Deneme88	22	22	22	28	22	22
Deneme89	22	22	22	22	22	22
Deneme90	22	22	22	22	28	22
Deneme91	22	22	22	27	27	27
Deneme92	22	22	22	22	22	22
Deneme93	22	22	22	22	28	27
Deneme94	22	22	27	22	22	22
Deneme95	22	22	22	22	22	22
Deneme96	22	22	22	22	22	22
Deneme97	22	22	22	22	27	22
Deneme98	22	22	22	22	22	22
Deneme99	22	22	22	22	22	28
Deneme100	22	22	27	22	22	22
Ortalama	22,18	22,39	22,25	22,44	22,80	22,52
Standart Sapma	1,78	2,74	2,21	2,45	3,36	2,11
Varyans	3,15	7,44	4,85	5,95	11,18	4,41
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	33	38	28	33	33
Minimum	16	11	16	11	11	17
Mod	22	22	22	22	22	22

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
1 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	22	22	16	22	28	28
Deneme02	22	22	22	22	21	22
Deneme03	22	22	22	22	22	22
Deneme04	22	22	22	22	22	27
Deneme05	22	22	22	22	22	22
Deneme06	22	22	22	22	22	22
Deneme07	22	22	22	22	22	22
Deneme08	22	22	22	22	22	27
Deneme09	22	22	22	22	22	22
Deneme10	16	28	22	22	22	28
Deneme11	33	22	22	22	22	27
Deneme12	17	21	22	22	22	22
Deneme13	22	22	22	22	28	22
Deneme14	22	22	22	22	22	28
Deneme15	22	22	22	22	22	22
Deneme16	22	22	21	22	22	22
Deneme17	22	28	22	21	22	22
Deneme18	22	22	22	22	27	27
Deneme19	22	27	17	22	22	22
Deneme20	22	22	22	22	22	22
Deneme21	22	22	22	22	22	28
Deneme22	22	22	22	22	22	22
Deneme23	22	22	22	22	22	21
Deneme24	22	22	22	22	33	22
Deneme25	22	22	22	22	27	22
Deneme26	16	16	16	16	16	22
Deneme27	22	22	28	22	17	22
Deneme28	22	22	22	22	22	17
Deneme29	28	22	21	22	27	22
Deneme30	22	22	22	33	17	16
Deneme31	22	22	22	22	22	22
Deneme32	22	22	22	22	22	22
Deneme33	22	22	17	22	21	27
Deneme34	22	22	27	22	22	22
Deneme35	22	22	22	22	28	28
Deneme36	22	22	17	22	27	22
Deneme37	22	22	22	22	22	22
Deneme38	22	22	22	22	22	27
Deneme39	22	22	22	22	22	22
Deneme40	22	22	22	22	22	22
Deneme41	22	22	22	22	28	22
Deneme42	22	22	22	22	22	22
Deneme43	22	22	22	22	22	22
Deneme44	21	22	22	22	22	22
Deneme45	22	22	22	22	27	22
Deneme46	22	22	21	22	22	22
Deneme47	28	22	22	22	22	22
Deneme48	22	22	22	21	22	22
Deneme49	22	22	22	22	21	22
Deneme50	22	27	22	22	22	27
Deneme51	17	16	22	22	16	16
Deneme52	22	22	22	22	22	22
Deneme53	27	22	22	22	22	22
Deneme54	22	22	22	22	22	22
Deneme55	22	22	22	22	22	22
Deneme56	22	22	22	22	22	22
Deneme57	22	22	22	22	22	22
Deneme58	22	22	22	22	22	28
Deneme59	22	22	33	22	22	22
Deneme60	22	27	22	27	27	22
Deneme61	22	22	22	22	22	22
Deneme62	22	22	22	22	22	22
Deneme63	22	22	22	22	22	22
Deneme64	22	27	27	22	28	27
Deneme65	22	22	22	28	22	22
Deneme66	22	22	33	22	22	22
Deneme67	22	22	26	22	22	22
Deneme68	33	22	22	22	22	22
Deneme69	22	22	17	22	22	22
Deneme70	21	22	22	22	21	22
Deneme71	22	22	22	22	22	22
Deneme72	22	22	22	22	22	27
Deneme73	22	22	28	22	22	28
Deneme74	22	22	22	22	22	22
Deneme75	22	22	22	22	22	22
Deneme76	17	17	11	17	17	16
Deneme77	22	21	22	22	22	28
Deneme78	27	22	22	22	22	27
Deneme79	22	22	22	22	22	22
Deneme80	22	22	22	22	27	22
Deneme81	22	22	22	22	22	22
Deneme82	33	28	22	22	22	22
Deneme83	22	27	22	22	22	22
Deneme84	22	28	22	22	22	22
Deneme85	22	27	21	22	22	22
Deneme86	22	22	22	22	27	22
Deneme87	22	28	28	22	22	22
Deneme88	22	22	22	22	22	22
Deneme89	22	22	22	22	22	28
Deneme90	22	27	22	22	28	22
Deneme91	22	22	22	21	22	22
Deneme92	22	27	22	22	22	22
Deneme93	22	22	22	22	22	33
Deneme94	22	39	22	22	22	16
Deneme95	22	22	22	22	22	16
Deneme96	22	22	22	22	22	22
Deneme97	22	22	22	22	22	22
Deneme98	22	22	22	22	22	17
Deneme99	22	22	22	22	28	16
Deneme100	22	22	22	22	27	22
Ortalama	22,26	22,68	22,07	22,08	22,67	22,68
Standart Sapma	2,52	2,70	2,68	1,57	2,67	3,04
Varyans	6,27	7,22	7,13	2,45	7,04	9,16
Medyan	22,00	22,00	22,00	22,00	22,00	22,00
Maximum	33	39	33	33	33	33
Minimum	16	16	11	16	16	16
Mod	22	22	22	22	22	22

Büro XP Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	28	16	16	33	17	28
Deneme02	27	27	28	27	27	27
Deneme03	27	28	27	28	33	28
Deneme04	28	27	28	27	28	27
Deneme05	27	28	27	28	27	27
Deneme06	28	27	27	27	27	28
Deneme07	27	28	28	28	28	27
Deneme08	28	27	27	27	16	28
Deneme09	27	28	28	28	28	27
Deneme10	28	27	27	27	27	28
Deneme11	27	28	28	28	28	27
Deneme12	28	38	33	27	27	28
Deneme13	27	28	27	28	28	33
Deneme14	28	27	28	32	27	27
Deneme15	27	27	27	28	28	28
Deneme16	33	28	28	27	27	27
Deneme17	27	27	27	28	28	28
Deneme18	28	33	27	27	27	27
Deneme19	27	28	28	28	27	27
Deneme20	28	27	27	27	28	28
Deneme21	27	28	28	28	27	27
Deneme22	33	27	27	27	28	28
Deneme23	28	28	28	28	27	27
Deneme24	27	27	27	27	28	28
Deneme25	28	28	28	28	27	27
Deneme26	11	16	16	22	22	33
Deneme27	28	28	28	22	28	27
Deneme28	27	27	33	22	22	27
Deneme29	27	28	27	27	38	28
Deneme30	28	27	28	27	27	33
Deneme31	27	28	33	33	28	27
Deneme32	28	33	27	28	27	55
Deneme33	27	33	28	27	28	22
Deneme34	28	27	27	27	27	17
Deneme35	27	27	33	33	28	33
Deneme36	33	28	27	28	27	27
Deneme37	28	27	28	27	28	28
Deneme38	27	33	33	28	27	27
Deneme39	28	28	27	27	28	28
Deneme40	27	27	28	28	27	27
Deneme41	27	28	38	27	28	27
Deneme42	28	27	28	28	27	28
Deneme43	27	28	33	27	27	27
Deneme44	28	27	27	27	28	28
Deneme45	27	28	33	28	27	27
Deneme46	28	27	28	27	28	28
Deneme47	27	27	32	28	27	27
Deneme48	44	28	28	27	28	28
Deneme49	33	33	33	28	27	27
Deneme50	33	27	33	27	28	28
Deneme51	22	22	22	22	22	22
Deneme52	27	28	33	27	33	28
Deneme53	27	27	38	28	27	33
Deneme54	28	28	28	27	28	27
Deneme55	27	27	27	33	32	28
Deneme56	39	28	33	28	28	27
Deneme57	27	27	28	27	27	27
Deneme58	28	28	27	27	28	28
Deneme59	27	27	27	28	27	33
Deneme60	28	27	28	27	28	27
Deneme61	27	33	27	33	27	28
Deneme62	28	28	28	28	33	27
Deneme63	27	27	27	27	28	28
Deneme64	28	28	28	28	27	27
Deneme65	27	33	33	27	28	28
Deneme66	33	27	27	28	27	27
Deneme67	27	39	28	27	28	28
Deneme68	33	33	27	28	32	27
Deneme69	28	33	28	27	28	28
Deneme70	27	27	33	27	33	27
Deneme71	28	28	32	28	27	27
Deneme72	33	27	28	33	33	28
Deneme73	27	33	33	28	28	27
Deneme74	28	27	27	27	27	28
Deneme75	27	28	28	28	33	27
Deneme76	22	22	16	22	22	22
Deneme77	28	28	39	22	28	33
Deneme78	27	27	33	38	33	22
Deneme79	28	28	27	28	33	16
Deneme80	27	33	28	27	22	28
Deneme81	22	27	27	28	22	27
Deneme82	33	28	28	27	27	28
Deneme83	28	27	38	27	27	27
Deneme84	27	28	28	28	22	17
Deneme85	28	27	33	27	28	27
Deneme86	33	27	27	27	27	28
Deneme87	33	28	28	33	28	27
Deneme88	32	27	32	28	27	27
Deneme89	28	28	28	27	33	28
Deneme90	27	33	27	33	28	27
Deneme91	28	27	28	28	27	28
Deneme92	27	28	27	27	28	27
Deneme93	28	27	28	28	27	28
Deneme94	49	28	27	33	28	27
Deneme95	28	33	33	27	27	28
Deneme96	33	27	28	33	27	27
Deneme97	33	28	33	28	33	28
Deneme98	27	27	27	27	28	27
Deneme99	33	27	33	33	27	28
Deneme100	27	28	28	27	28	27
Ortalama	28,45	28,07	28,73	27,89	27,63	27,57
Standart Sapma	4,02	3,10	3,75	2,56	3,06	3,84
Varyans	16,03	9,49	13,92	6,50	9,25	14,63
Medyan	28,00	28,00	28,00	27,50	28,00	27,00
Maximum	49	39	39	38	38	55
Minimum	11	16	16	22	16	16
Mod	27	27	28	27	27	27

Büro XP Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	17	22	22	16	16	22
Deneme02	27	28	28	28	28	27
Deneme03	28	27	27	27	27	28
Deneme04	21	28	28	27	28	22
Deneme05	28	27	27	28	27	22
Deneme06	27	28	27	27	28	27
Deneme07	28	27	28	28	27	28
Deneme08	27	28	27	27	28	27
Deneme09	39	27	28	28	33	27
Deneme10	27	28	27	33	27	22
Deneme11	28	27	28	27	28	28
Deneme12	33	28	33	28	32	33
Deneme13	27	27	33	27	28	27
Deneme14	28	27	27	28	27	28
Deneme15	27	28	28	27	28	22
Deneme16	28	27	27	28	27	33
Deneme17	27	28	28	27	28	27
Deneme18	27	33	27	27	27	28
Deneme19	28	27	27	28	28	27
Deneme20	27	28	28	22	27	28
Deneme21	28	27	27	27	28	27
Deneme22	27	28	28	28	27	28
Deneme23	28	27	27	27	28	27
Deneme24	27	28	28	28	27	27
Deneme25	28	27	27	27	28	28
Deneme26	22	22	17	16	16	22
Deneme27	22	27	27	22	28	28
Deneme28	16	28	27	28	27	27
Deneme29	27	27	28	27	28	27
Deneme30	28	28	27	28	27	28
Deneme31	27	27	28	27	27	27
Deneme32	39	28	27	33	28	28
Deneme33	27	27	28	28	27	27
Deneme34	28	28	27	27	28	33
Deneme35	27	33	28	39	27	28
Deneme36	28	27	27	27	28	22
Deneme37	33	28	28	27	27	28
Deneme38	16	27	27	33	28	27
Deneme39	28	27	28	28	27	28
Deneme40	27	28	27	27	28	27
Deneme41	28	27	27	28	27	28
Deneme42	27	33	33	33	28	27
Deneme43	33	28	33	27	27	27
Deneme44	27	27	33	28	27	28
Deneme45	28	28	28	27	28	27
Deneme46	27	27	27	33	27	28
Deneme47	28	28	39	33	28	27
Deneme48	27	27	27	22	27	28
Deneme49	28	28	28	38	28	22
Deneme50	27	27	27	28	27	44
Deneme51	17	22	22	22	22	22
Deneme52	27	28	27	33	27	27
Deneme53	17	27	33	28	28	33
Deneme54	33	33	28	27	27	33
Deneme55	44	27	27	33	28	33
Deneme56	28	28	33	28	27	28
Deneme57	27	27	27	27	28	33
Deneme58	27	28	28	28	27	27
Deneme59	28	27	27	27	38	33
Deneme60	27	39	28	33	28	33
Deneme61	28	27	27	27	27	28
Deneme62	27	28	28	28	28	27
Deneme63	28	27	27	33	27	27
Deneme64	27	28	33	27	28	28
Deneme65	28	27	28	28	27	27
Deneme66	27	27	27	27	28	33
Deneme67	33	28	28	22	33	28
Deneme68	28	27	27	22	27	33
Deneme69	27	28	27	33	28	27
Deneme70	28	27	28	28	27	28
Deneme71	27	28	33	33	27	27
Deneme72	27	27	27	33	28	28
Deneme73	28	28	28	27	27	27
Deneme74	27	27	27	27	28	33
Deneme75	28	28	33	28	27	27
Deneme76	22	11	16	22	22	16
Deneme77	28	28	28	28	27	22
Deneme78	22	27	27	27	28	22
Deneme79	44	28	28	28	33	27
Deneme80	27	27	33	27	27	28
Deneme81	28	28	33	28	28	27
Deneme82	27	27	27	27	38	28
Deneme83	28	28	27	33	27	27
Deneme84	27	33	28	33	28	28
Deneme85	33	27	33	22	27	27
Deneme86	27	27	33	16	28	28
Deneme87	22	28	33	28	27	27
Deneme88	28	27	28	27	28	27
Deneme89	27	28	27	28	27	33
Deneme90	28	27	28	27	33	28
Deneme91	27	28	38	28	28	22
Deneme92	28	27	28	27	27	27
Deneme93	27	28	27	28	28	28
Deneme94	33	33	28	27	27	27
Deneme95	28	27	27	28	28	28
Deneme96	27	27	27	27	27	27
Deneme97	27	28	28	28	27	33
Deneme98	28	27	27	27	28	28
Deneme99	27	33	28	27	27	27
Deneme100	39	38	27	28	28	33
Ortalama	27,64	27,74	28,17	27,74	27,62	27,68
Standart Sapma	4,45	2,90	3,14	3,69	2,67	3,53
Varyans	19,59	8,33	9,74	13,47	7,08	12,36
Medyan	27,00	27,00	28,00	28,00	27,50	27,00
Maximum	44	39	39	39	38	44
Minimum	16	11	16	16	16	16
Mod	27	27	27	27	27	27

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	28	16	33	27	11	33
Deneme02	27	28	28	28	28	27
Deneme03	28	27	27	27	27	27
Deneme04	27	28	28	28	28	28
Deneme05	28	27	27	27	27	27
Deneme06	27	28	28	28	28	28
Deneme07	28	27	27	27	27	27
Deneme08	27	28	28	27	28	28
Deneme09	28	27	27	28	27	27
Deneme10	27	28	28	27	27	28
Deneme11	28	33	27	28	28	27
Deneme12	27	27	27	33	27	27
Deneme13	27	28	28	27	28	28
Deneme14	28	27	27	28	27	27
Deneme15	27	27	28	27	28	27
Deneme16	28	28	33	28	27	28
Deneme17	27	27	27	27	28	27
Deneme18	28	28	33	22	27	28
Deneme19	27	27	27	28	28	27
Deneme20	28	28	28	27	27	28
Deneme21	27	27	27	28	28	27
Deneme22	28	28	28	27	27	28
Deneme23	33	27	27	28	33	27
Deneme24	27	28	27	27	27	28
Deneme25	28	27	28	28	28	27
Deneme26	16	22	50	38	17	17
Deneme27	28	16	27	27	16	27
Deneme28	27	33	28	28	28	28
Deneme29	28	28	27	27	27	27
Deneme30	27	27	28	28	28	28
Deneme31	27	28	27	27	33	27
Deneme32	28	27	28	28	27	27
Deneme33	27	28	27	27	28	28
Deneme34	28	27	28	28	27	27
Deneme35	27	27	27	28	28	33
Deneme36	28	28	28	33	27	28
Deneme37	27	27	27	33	28	27
Deneme38	28	28	28	27	27	28
Deneme39	27	27	27	27	27	27
Deneme40	28	28	28	28	28	28
Deneme41	27	27	27	22	27	27
Deneme42	28	28	28	28	28	28
Deneme43	27	27	27	27	27	27
Deneme44	27	28	28	28	28	28
Deneme45	28	22	27	27	27	32
Deneme46	27	27	28	28	28	28
Deneme47	28	27	27	27	27	27
Deneme48	27	22	28	33	28	28
Deneme49	28	28	27	33	27	33
Deneme50	27	27	28	22	28	27
Deneme51	17	17	17	16	17	16
Deneme52	27	27	27	28	27	28
Deneme53	27	28	22	27	33	27
Deneme54	28	27	22	28	28	27
Deneme55	27	16	28	27	27	28
Deneme56	28	28	27	28	33	27
Deneme57	27	27	27	27	28	28
Deneme58	28	28	28	28	27	27
Deneme59	27	27	27	27	27	28
Deneme60	28	28	28	28	28	27
Deneme61	27	27	27	27	27	28
Deneme62	28	28	28	28	39	27
Deneme63	27	27	27	33	27	28
Deneme64	28	28	28	28	27	33
Deneme65	27	27	27	27	28	27
Deneme66	27	28	28	28	27	33
Deneme67	28	27	27	33	28	33
Deneme68	27	27	28	27	27	27
Deneme69	28	28	27	28	28	33
Deneme70	33	27	27	27	27	28
Deneme71	27	28	28	22	28	27
Deneme72	28	27	27	28	27	28
Deneme73	27	28	28	27	27	27
Deneme74	28	27	27	28	28	28
Deneme75	27	28	33	27	27	33
Deneme76	22	22	33	22	17	33
Deneme77	28	27	22	33	27	28
Deneme78	27	28	22	28	28	27
Deneme79	28	22	28	27	27	28
Deneme80	27	27	27	28	28	27
Deneme81	28	28	28	33	27	28
Deneme82	27	27	27	33	28	27
Deneme83	28	27	28	32	27	27
Deneme84	38	28	27	28	27	33
Deneme85	27	22	33	27	33	28
Deneme86	28	27	27	28	28	33
Deneme87	27	28	28	27	27	33
Deneme88	28	27	27	28	28	33
Deneme89	27	28	28	49	27	27
Deneme90	28	27	27	28	39	33
Deneme91	27	33	28	33	33	28
Deneme92	28	28	27	33	27	27
Deneme93	27	27	28	27	28	28
Deneme94	28	28	27	33	33	27
Deneme95	33	27	28	27	27	27
Deneme96	27	33	27	27	27	28
Deneme97	27	27	28	28	28	27
Deneme98	28	28	27	27	27	28
Deneme99	27	27	27	28	28	27
Deneme100	28	28	28	27	27	33
Ortalama	27,47	26,91	27,70	28,19	27,47	28,11
Standart Sapma	2,24	2,84	3,08	3,54	3,53	2,66
Varyans	4,97	7,96	9,37	12,41	12,33	7,00
Medyan	27,00	27,00	27,00	28,00	27,00	28,00
Maximum	38	33	50	49	39	33
Minimum	16	16	17	16	11	16
Mod	27	27	27	27	27	27

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
2 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	39	22	17	28	22	16
Deneme02	22	28	38	22	28	27
Deneme03	16	27	28	16	27	33
Deneme04	28	27	27	27	28	28
Deneme05	33	28	28	28	27	27
Deneme06	27	27	27	27	28	28
Deneme07	27	28	27	33	27	27
Deneme08	28	27	28	28	28	28
Deneme09	27	28	27	27	27	27
Deneme10	28	27	28	28	27	28
Deneme11	27	28	27	27	39	27
Deneme12	28	27	28	28	27	28
Deneme13	27	28	27	27	28	27
Deneme14	28	27	28	28	27	28
Deneme15	27	28	27	27	28	27
Deneme16	28	27	28	28	27	27
Deneme17	27	27	27	27	39	28
Deneme18	33	28	28	27	27	27
Deneme19	28	27	27	28	28	28
Deneme20	27	28	27	27	28	27
Deneme21	27	27	28	28	33	28
Deneme22	28	28	27	27	27	27
Deneme23	27	27	28	28	28	28
Deneme24	28	28	27	27	44	27
Deneme25	27	27	28	28	17	33
Deneme26	22	22	22	22	28	21
Deneme27	28	27	27	33	27	28
Deneme28	27	33	28	28	28	27
Deneme29	27	27	27	27	33	28
Deneme30	28	29	28	28	27	27
Deneme31	27	27	27	27	28	28
Deneme32	28	28	27	28	27	27
Deneme33	27	27	28	38	28	28
Deneme34	28	28	27	27	27	22
Deneme35	27	27	55	28	27	33
Deneme36	28	28	28	33	28	27
Deneme37	27	27	16	27	33	28
Deneme38	28	28	28	28	33	27
Deneme39	27	33	27	27	27	27
Deneme40	28	27	28	28	28	28
Deneme41	27	27	27	27	27	27
Deneme42	28	28	28	28	28	28
Deneme43	27	27	27	27	27	27
Deneme44	27	28	28	28	33	28
Deneme45	28	27	32	27	28	27
Deneme46	27	28	28	28	33	28
Deneme47	44	27	27	27	32	27
Deneme48	16	28	28	22	28	28
Deneme49	28	27	27	27	27	33
Deneme50	22	28	28	28	28	33
Deneme51	17	22	16	22	11	22
Deneme52	27	33	28	27	39	28
Deneme53	28	28	27	28	27	27
Deneme54	27	27	28	27	28	28
Deneme55	27	27	27	28	22	27
Deneme56	28	28	28	27	27	28
Deneme57	27	33	27	27	28	27
Deneme58	28	27	28	28	27	28
Deneme59	27	28	27	38	28	27
Deneme60	28	27	27	28	27	27
Deneme61	27	28	28	49	27	28
Deneme62	28	27	27	22	33	27
Deneme63	22	28	28	17	44	28
Deneme64	16	38	27	22	28	27
Deneme65	33	28	28	27	27	28
Deneme66	28	27	27	28	28	27
Deneme67	27	27	39	27	27	33
Deneme68	33	28	27	28	28	33
Deneme69	27	27	28	16	27	33
Deneme70	28	28	27	28	28	33
Deneme71	27	27	28	27	27	28
Deneme72	28	28	27	27	28	27
Deneme73	27	27	27	28	27	27
Deneme74	28	39	28	27	33	28
Deneme75	27	27	27	28	27	27
Deneme76	22	22	22	22	28	33
Deneme77	27	33	27	27	27	27
Deneme78	28	28	28	28	28	28
Deneme79	27	27	27	27	27	27
Deneme80	28	28	28	28	27	39
Deneme81	27	27	27	27	22	27
Deneme82	28	28	28	28	28	27
Deneme83	27	27	27	27	33	27
Deneme84	27	27	22	28	27	28
Deneme85	33	28	16	27	22	27
Deneme86	28	27	28	27	22	39
Deneme87	27	28	27	28	28	27
Deneme88	33	27	28	33	27	28
Deneme89	28	28	27	27	28	27
Deneme90	27	27	28	28	27	28
Deneme91	28	28	55	27	28	27
Deneme92	27	27	22	28	27	33
Deneme93	28	28	16	27	28	28
Deneme94	27	38	28	28	32	33
Deneme95	28	28	27	27	28	27
Deneme96	27	27	28	28	27	27
Deneme97	27	27	27	27	28	33
Deneme98	28	28	22	28	27	28
Deneme99	27	33	27	27	28	27
Deneme100	28	27	28	33	27	28
Ortalama	27,35	27,91	27,46	27,47	28,20	28,11
Standart Sapma	3,57	2,59	5,11	3,82	4,21	2,97
Varyans	12,63	6,62	25,87	14,41	17,58	8,76
Medyan	27,00	27,00	27,00	27,00	28,00	28,00
Maximum	44	39	55	49	44	39
Minimum	16	22	16	16	11	16
Mod	27	27	27	27	27	27

Büro XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
4 MB	Süre	Süre	Süre	Süre	Süre	Süre
Deneme01	44	22	17	27	22	38
Deneme02	38	38	38	39	38	38
Deneme03	39	66	39	38	44	39
Deneme04	38	39	32	39	33	38
Deneme05	39	38	39	38	38	39
Deneme06	38	50	38	39	39	38
Deneme07	55	38	39	38	38	39
Deneme08	38	38	38	39	39	38
Deneme09	39	39	39	38	38	39
Deneme10	38	38	38	38	39	38
Deneme11	39	44	33	28	38	38
Deneme12	38	39	39	49	39	44
Deneme13	39	38	43	39	38	39
Deneme14	38	39	39	38	38	38
Deneme15	39	38	38	33	39	39
Deneme16	38	38	39	39	33	38
Deneme17	38	39	38	38	38	39
Deneme18	39	38	39	38	39	44
Deneme19	38	66	44	33	38	38
Deneme20	39	39	38	55	39	38
Deneme21	38	38	39	44	33	39
Deneme22	39	39	38	39	66	38
Deneme23	38	38	38	38	38	33
Deneme24	39	39	39	39	38	39
Deneme25	38	43	38	38	39	38
Deneme26	27	28	28	27	27	27
Deneme27	39	49	38	38	39	38
Deneme28	38	38	38	39	38	39
Deneme29	39	39	39	38	38	33
Deneme30	38	44	38	44	33	49
Deneme31	39	38	44	39	39	39
Deneme32	49	55	39	38	44	33
Deneme33	39	39	38	39	38	38
Deneme34	38	38	39	38	39	33
Deneme35	38	39	38	39	38	39
Deneme36	39	38	39	27	39	32
Deneme37	38	38	38	27	38	55
Deneme38	33	39	38	39	38	38
Deneme39	39	33	39	33	55	33
Deneme40	49	44	38	33	39	39
Deneme41	39	38	39	38	38	38
Deneme42	33	28	33	39	39	39
Deneme43	38	38	38	38	38	38
Deneme44	38	39	44	39	39	39
Deneme45	39	38	44	44	44	38
Deneme46	38	44	39	27	38	38
Deneme47	39	38	38	38	33	44
Deneme48	38	39	38	39	44	39
Deneme49	33	38	39	38	27	33
Deneme50	44	50	38	33	39	33
Deneme51	28	44	22	27	27	22
Deneme52	38	38	39	38	33	38
Deneme53	38	39	44	39	38	39
Deneme54	39	38	44	38	44	38
Deneme55	38	39	38	39	39	39
Deneme56	44	38	38	55	38	38
Deneme57	39	44	39	38	39	39
Deneme58	38	38	38	39	38	38
Deneme59	39	39	39	27	39	39
Deneme60	38	33	49	49	44	38
Deneme61	39	38	39	38	38	49
Deneme62	49	33	38	50	44	28
Deneme63	38	39	39	38	38	38
Deneme64	39	33	38	39	39	50
Deneme65	33	38	39	38	38	38
Deneme66	38	33	38	39	39	39
Deneme67	39	33	38	33	44	33
Deneme68	38	33	39	38	55	38
Deneme69	39	33	44	33	38	39
Deneme70	38	38	33	38	39	32
Deneme71	39	55	38	39	38	39
Deneme72	38	33	39	38	38	38
Deneme73	38	33	33	44	39	33
Deneme74	39	33	38	39	44	39
Deneme75	38	33	33	38	55	38
Deneme76	27	27	27	28	28	33
Deneme77	50	33	44	38	43	38
Deneme78	38	33	38	39	39	39
Deneme79	39	39	33	38	44	38
Deneme80	38	38	50	38	38	39
Deneme81	33	39	38	39	39	38
Deneme82	38	38	33	38	49	39
Deneme83	39	39	33	39	39	38
Deneme84	49	38	38	38	44	33
Deneme85	39	38	39	44	33	38
Deneme86	38	39	49	39	38	39
Deneme87	39	38	38	44	38	38
Deneme88	33	39	33	38	33	39
Deneme89	38	38	50	33	38	49
Deneme90	39	33	33	44	33	39
Deneme91	38	39	38	66	38	38
Deneme92	33	38	44	38	33	39
Deneme93	38	50	39	39	39	38
Deneme94	39	32	38	33	33	38
Deneme95	38	33	33	39	33	39
Deneme96	39	39	44	38	49	44
Deneme97	33	33	44	39	28	38
Deneme98	44	38	38	43	38	39
Deneme99	38	33	33	39	33	38
Deneme100	33	33	39	38	50	39
Ortalama	38,55	38,55	38,22	38,32	38,77	38,16
Standart Sapma	4,06	6,37	4,75	5,79	6,00	4,26
Varyans	16,33	40,23	22,29	33,18	35,70	17,95
Medyan	38,00	38,00	38,00	38,00	38,00	38,00
Maximum	55,00	66,00	50,00	66,00	66,00	55,00
Minimum	27	22	17	27	22	22
Mod	38	38	38	38	38	38

Büro XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	27	22	33	33	22	33
Deneme02	39	49	39	38	38	39
Deneme03	38	39	43	44	39	38
Deneme04	28	38	39	38	38	39
Deneme05	38	39	44	28	33	38
Deneme06	38	38	38	49	38	38
Deneme07	39	50	44	39	39	39
Deneme08	38	38	39	38	38	38
Deneme09	50	39	38	39	55	39
Deneme10	38	38	39	38	39	49
Deneme11	39	39	44	38	38	39
Deneme12	38	38	38	39	39	38
Deneme13	39	39	44	38	38	39
Deneme14	33	33	38	39	38	44
Deneme15	38	38	39	38	55	38
Deneme16	38	39	38	39	38	38
Deneme17	50	38	44	38	39	39
Deneme18	33	33	39	39	38	38
Deneme19	33	38	38	49	39	39
Deneme20	38	38	33	33	38	38
Deneme21	33	39	38	93	61	39
Deneme22	39	38	44	27	38	38
Deneme23	38	33	44	33	44	39
Deneme24	39	39	39	39	38	38
Deneme25	32	33	49	55	33	38
Deneme26	33	22	28	44	28	27
Deneme27	39	44	44	33	38	39
Deneme28	38	33	38	39	33	38
Deneme29	28	38	33	38	39	39
Deneme30	38	44	39	38	49	38
Deneme31	39	38	44	28	44	39
Deneme32	38	39	38	33	33	38
Deneme33	39	49	39	27	38	39
Deneme34	38	38	38	33	39	38
Deneme35	38	39	33	38	33	55
Deneme36	39	38	50	39	38	38
Deneme37	38	39	33	33	33	39
Deneme38	50	44	38	38	33	38
Deneme39	38	38	33	55	44	39
Deneme40	39	39	49	39	33	38
Deneme41	38	44	33	38	39	39
Deneme42	39	38	39	28	38	38
Deneme43	38	38	38	38	33	39
Deneme44	39	39	44	33	38	32
Deneme45	38	33	39	33	33	39
Deneme46	50	38	38	44	55	44
Deneme47	38	33	39	49	39	38
Deneme48	71	33	38	39	38	39
Deneme49	39	39	44	38	39	38
Deneme50	38	33	38	39	33	39
Deneme51	22	27	27	28	22	28
Deneme52	39	38	50	27	33	38
Deneme53	38	38	38	39	39	39
Deneme54	38	39	39	38	44	38
Deneme55	39	38	39	44	38	39
Deneme56	38	44	38	39	39	38
Deneme57	44	39	38	33	38	39
Deneme58	39	33	39	44	38	44
Deneme59	38	33	38	44	50	38
Deneme60	39	38	39	43	38	44
Deneme61	38	44	33	44	39	38
Deneme62	39	33	38	39	38	39
Deneme63	38	38	38	33	39	38
Deneme64	38	39	39	38	38	55
Deneme65	50	38	38	44	39	39
Deneme66	38	33	38	38	38	38
Deneme67	39	39	39	39	33	39
Deneme68	38	38	33	60	55	49
Deneme69	39	39	38	38	38	38
Deneme70	33	38	39	39	39	39
Deneme71	38	39	33	33	38	38
Deneme72	33	38	61	38	39	50
Deneme73	38	38	44	39	38	49
Deneme74	72	33	33	44	39	28
Deneme75	44	33	38	44	38	38
Deneme76	27	22	33	28	27	27
Deneme77	33	44	33	38	39	44
Deneme78	33	44	39	39	33	39
Deneme79	39	38	33	38	38	49
Deneme80	38	39	38	39	39	39
Deneme81	33	38	38	44	49	38
Deneme82	38	39	33	33	39	39
Deneme83	39	38	33	33	38	38
Deneme84	38	39	39	32	39	38
Deneme85	39	38	38	33	38	39
Deneme86	33	44	33	33	44	49
Deneme87	33	38	33	44	33	39
Deneme88	38	39	39	44	38	38
Deneme89	33	38	44	33	39	39
Deneme90	49	33	33	28	38	38
Deneme91	33	39	33	33	39	44
Deneme92	33	33	38	55	38	39
Deneme93	33	38	60	33	33	38
Deneme94	39	33	33	32	39	38
Deneme95	33	38	33	33	32	39
Deneme96	38	38	44	39	33	38
Deneme97	39	39	33	38	39	77
Deneme98	38	38	39	39	38	44
Deneme99	33	33	38	38	39	39
Deneme100	38	33	39	61	33	44
Ortalama	38,22	37,55	38,68	38,84	38,34	39,72
Standart Sapma	6,64	4,61	5,36	8,56	5,93	5,84
Varyans	43,63	21,05	28,46	72,47	34,86	33,80
Medyan	38,00	38,00	38,00	38,00	38,00	39,00
Maximum	72	50	61	93	61	77
Minimum	22	22	27	27	22	27
Mod	38	38	38	38	38	38

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	33	22	33	39	16	60
Deneme02	38	39	44	38	39	39
Deneme03	39	38	38	39	44	38
Deneme04	39	44	39	38	38	39
Deneme05	38	38	43	60	39	38
Deneme06	39	39	39	22	38	39
Deneme07	38	38	55	33	38	44
Deneme08	39	39	44	38	39	38
Deneme09	49	38	38	39	38	39
Deneme10	38	39	39	38	39	38
Deneme11	39	38	38	39	38	38
Deneme12	38	39	39	38	39	44
Deneme13	60	38	38	39	38	44
Deneme14	39	38	39	38	44	33
Deneme15	38	50	38	39	39	39
Deneme16	39	44	38	38	38	38
Deneme17	38	38	39	55	38	39
Deneme18	39	44	38	38	39	38
Deneme19	38	39	39	39	38	38
Deneme20	38	38	38	38	39	39
Deneme21	39	39	33	39	38	38
Deneme22	38	38	39	44	39	39
Deneme23	39	38	44	38	38	38
Deneme24	38	39	38	39	39	39
Deneme25	39	38	38	54	76	44
Deneme26	27	39	27	33	27	33
Deneme27	39	38	38	39	39	38
Deneme28	38	39	39	44	38	39
Deneme29	33	38	38	39	39	71
Deneme30	39	39	39	33	49	44
Deneme31	43	38	38	33	39	39
Deneme32	33	38	39	38	38	38
Deneme33	39	38	38	44	39	38
Deneme34	38	39	39	33	38	39
Deneme35	39	44	38	38	38	33
Deneme36	38	39	39	39	50	49
Deneme37	39	33	38	38	38	39
Deneme38	44	55	38	33	39	38
Deneme39	33	38	39	39	38	39
Deneme40	33	39	38	38	39	38
Deneme41	32	32	39	39	38	39
Deneme42	39	39	27	38	44	38
Deneme43	38	38	39	39	38	38
Deneme44	33	39	38	38	39	44
Deneme45	33	38	44	38	38	39
Deneme46	33	33	38	33	39	33
Deneme47	33	39	39	33	38	38
Deneme48	39	38	38	22	39	39
Deneme49	44	39	33	44	38	38
Deneme50	33	49	22	44	39	44
Deneme51	22	33	49	38	16	27
Deneme52	39	33	38	39	39	38
Deneme53	38	33	39	38	38	39
Deneme54	38	39	38	39	33	38
Deneme55	39	38	39	38	50	39
Deneme56	33	39	44	39	38	38
Deneme57	49	38	39	55	39	39
Deneme58	39	38	38	33	38	38
Deneme59	38	39	39	33	39	39
Deneme60	39	38	38	33	38	38
Deneme61	38	39	39	33	38	44
Deneme62	44	44	38	27	39	38
Deneme63	38	38	33	33	38	44
Deneme64	39	39	38	33	39	39
Deneme65	38	38	39	39	38	38
Deneme66	39	38	38	38	39	39
Deneme67	55	39	39	39	44	38
Deneme68	38	38	44	38	38	39
Deneme69	39	39	38	39	39	55
Deneme70	38	38	39	38	38	38
Deneme71	39	39	38	38	77	38
Deneme72	43	33	38	39	44	39
Deneme73	39	33	50	38	38	38
Deneme74	33	38	38	39	39	39
Deneme75	38	33	39	38	38	44
Deneme76	28	28	33	33	27	28
Deneme77	33	44	33	39	39	38
Deneme78	38	38	38	38	38	38
Deneme79	33	55	39	50	38	39
Deneme80	44	33	38	39	44	38
Deneme81	33	33	44	38	39	39
Deneme82	33	61	39	33	38	38
Deneme83	38	32	38	38	39	44
Deneme84	33	33	38	39	38	39
Deneme85	33	33	39	49	33	33
Deneme86	33	33	38	39	44	38
Deneme87	33	44	44	38	39	38
Deneme88	33	33	44	39	38	39
Deneme89	33	33	39	33	38	44
Deneme90	38	33	38	38	39	38
Deneme91	61	33	39	39	38	39
Deneme92	33	33	38	38	44	38
Deneme93	33	38	38	33	39	39
Deneme94	33	39	39	38	33	55
Deneme95	33	38	38	39	38	38
Deneme96	33	39	39	38	39	38
Deneme97	33	38	38	39	38	39
Deneme98	60	39	39	33	38	38
Deneme99	33	44	49	39	39	33
Deneme100	33	38	39	38	38	44
Ortalama	37,74	38,29	38,77	38,19	39,15	39,60
Standart Sapma	5,95	5,08	4,08	5,41	7,00	5,40
Varyans	35,05	25,59	16,48	28,99	48,51	28,88
Medyan	38,00	38,00	38,00	38,00	38,00	39,00
Maximum	61	61	55	60	77	71
Minimum	22	22	22	22	16	27
Mod	33	38	38	38	38	38

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
4 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	39	50	22	66	33	16
Deneme02	38	38	38	39	39	44
Deneme03	39	39	39	38	38	39
Deneme04	38	38	38	38	50	38
Deneme05	38	39	39	39	38	33
Deneme06	39	38	38	38	38	39
Deneme07	44	39	44	39	39	38
Deneme08	38	44	38	38	38	38
Deneme09	39	49	39	39	39	39
Deneme10	38	39	38	38	38	38
Deneme11	39	38	39	39	39	39
Deneme12	38	39	33	38	38	38
Deneme13	33	38	38	38	39	33
Deneme14	33	39	39	44	38	39
Deneme15	38	33	38	39	39	44
Deneme16	39	38	38	38	38	44
Deneme17	38	44	39	39	33	38
Deneme18	39	38	38	38	38	38
Deneme19	27	39	39	39	39	39
Deneme20	39	38	55	38	38	49
Deneme21	33	39	38	50	44	39
Deneme22	38	38	33	38	44	38
Deneme23	39	39	39	38	28	39
Deneme24	38	38	38	39	38	38
Deneme25	33	39	38	38	33	39
Deneme26	27	27	28	27	28	28
Deneme27	39	33	38	39	49	38
Deneme28	33	33	39	38	39	39
Deneme29	38	55	49	38	38	33
Deneme30	38	38	38	33	39	38
Deneme31	33	39	39	39	38	39
Deneme32	72	33	38	38	49	38
Deneme33	33	33	39	39	39	55
Deneme34	38	33	33	38	38	38
Deneme35	33	33	38	39	39	39
Deneme36	39	38	39	38	38	38
Deneme37	38	39	38	33	39	39
Deneme38	39	32	39	49	38	38
Deneme39	38	55	33	39	39	33
Deneme40	33	39	38	38	43	39
Deneme41	33	38	38	39	39	32
Deneme42	38	39	39	38	38	28
Deneme43	39	38	38	33	39	38
Deneme44	38	39	39	39	44	39
Deneme45	33	38	38	38	77	27
Deneme46	28	39	33	39	38	33
Deneme47	38	38	39	38	33	33
Deneme48	39	38	44	38	39	39
Deneme49	38	33	38	55	38	38
Deneme50	38	33	33	39	55	39
Deneme51	28	27	27	22	22	22
Deneme52	38	39	39	39	38	38
Deneme53	39	38	43	38	39	44
Deneme54	38	38	39	38	55	39
Deneme55	38	39	38	39	38	38
Deneme56	39	38	39	38	39	50
Deneme57	38	39	38	39	38	38
Deneme58	39	44	39	38	38	39
Deneme59	38	55	44	33	50	38
Deneme60	39	38	38	39	27	39
Deneme61	38	39	39	38	39	38
Deneme62	39	38	38	39	38	44
Deneme63	38	38	38	38	39	38
Deneme64	39	39	39	38	38	39
Deneme65	38	38	38	39	39	38
Deneme66	60	39	44	44	38	39
Deneme67	39	38	28	33	33	38
Deneme68	38	39	38	27	60	39
Deneme69	39	38	39	33	39	33
Deneme70	27	55	27	50	38	38
Deneme71	33	39	39	38	39	38
Deneme72	39	38	38	39	38	39
Deneme73	38	55	38	38	39	38
Deneme74	33	38	39	38	38	44
Deneme75	38	39	38	28	60	39
Deneme76	27	33	27	39	22	38
Deneme77	44	38	55	38	33	38
Deneme78	39	39	39	39	38	39
Deneme79	38	49	38	38	39	33
Deneme80	39	39	39	33	38	38
Deneme81	38	38	38	33	39	39
Deneme82	39	38	39	33	38	55
Deneme83	38	39	38	49	39	38
Deneme84	33	38	38	39	38	39
Deneme85	38	44	33	38	39	38
Deneme86	39	39	39	39	38	38
Deneme87	38	38	38	33	55	39
Deneme88	33	39	39	38	38	44
Deneme89	39	38	49	39	39	38
Deneme90	33	38	33	33	38	39
Deneme91	38	39	39	32	39	38
Deneme92	39	38	38	39	44	39
Deneme93	33	39	49	33	38	33
Deneme94	38	38	39	33	39	33
Deneme95	38	39	38	38	54	38
Deneme96	55	38	39	39	33	44
Deneme97	39	50	38	38	39	38
Deneme98	33	38	39	44	38	44
Deneme99	33	39	38	39	39	39
Deneme100	33	38	39	33	44	38
Ortalama	37,51	39,11	38,22	38,18	39,66	38,18
Standart Sapma	5,68	5,08	4,67	5,25	7,19	5,07
Varyans	31,91	25,58	21,59	27,25	51,12	25,43
Medyan	38,00	38,00	38,00	38,00	38,50	38,00
Maximum	72	55	55	66	77	55
Minimum	27	27	22	22	22	16
Mod	38	38	38	38	38	38

Büro XP Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	28	28	61	49	27	66
Deneme02	76	60	60	55	61	55
Deneme03	61	61	61	55	60	61
Deneme04	55	60	82	55	55	60
Deneme05	55	61	61	88	66	55
Deneme06	55	71	60	83	55	55
Deneme07	55	60	60	54	55	55
Deneme08	54	55	55	55	55	60
Deneme09	77	55	55	55	55	55
Deneme10	61	55	55	99	55	72
Deneme11	60	55	55	49	55	71
Deneme12	55	60	55	55	66	66
Deneme13	61	66	88	55	60	82
Deneme14	60	55	55	55	55	105
Deneme15	77	55	60	55	55	60
Deneme16	60	55	55	82	55	77
Deneme17	55	55	55	55	55	55
Deneme18	55	49	55	55	55	55
Deneme19	55	55	55	55	54	60
Deneme20	55	55	55	55	72	55
Deneme21	55	55	55	77	55	83
Deneme22	71	55	55	60	55	55
Deneme23	72	55	55	66	55	54
Deneme24	55	55	88	50	55	55
Deneme25	55	60	54	54	55	55
Deneme26	33	27	28	116	110	49
Deneme27	55	72	54	93	49	55
Deneme28	55	60	72	72	55	55
Deneme29	60	55	66	54	82	88
Deneme30	50	55	55	55	61	55
Deneme31	49	82	55	55	55	60
Deneme32	55	55	60	55	55	55
Deneme33	77	55	60	55	55	55
Deneme34	71	77	55	55	55	55
Deneme35	55	55	83	55	76	77
Deneme36	55	71	60	55	66	55
Deneme37	55	55	61	55	55	60
Deneme38	55	55	55	55	61	55
Deneme39	55	55	54	71	55	61
Deneme40	55	77	55	66	60	77
Deneme41	55	60	55	55	55	60
Deneme42	55	61	88	49	60	55
Deneme43	55	55	55	55	55	66
Deneme44	77	55	66	55	83	55
Deneme45	87	60	55	55	55	55
Deneme46	72	55	82	55	55	55
Deneme47	55	77	50	55	60	54
Deneme48	55	60	60	55	60	55
Deneme49	55	55	61	55	77	66
Deneme50	55	55	60	55	55	55
Deneme51	39	49	39	44	33	61
Deneme52	60	55	60	60	54	55
Deneme53	50	55	61	55	88	55
Deneme54	55	55	54	55	66	54
Deneme55	55	77	55	55	61	77
Deneme56	55	55	55	60	55	66
Deneme57	55	60	77	72	55	55
Deneme58	55	55	72	55	60	55
Deneme59	65	61	55	55	71	72
Deneme60	66	87	54	55	83	54
Deneme61	55	55	55	55	60	55
Deneme62	55	61	55	54	55	55
Deneme63	61	55	77	55	82	66
Deneme64	55	60	55	61	55	50
Deneme65	55	55	88	55	55	60
Deneme66	54	60	66	71	55	55
Deneme67	55	55	55	61	55	55
Deneme68	55	55	55	54	55	55
Deneme69	55	66	55	55	55	55
Deneme70	83	55	55	55	55	77
Deneme71	71	55	60	55	82	60
Deneme72	55	55	55	83	72	55
Deneme73	55	55	82	55	55	55
Deneme74	55	60	55	82	55	60
Deneme75	55	55	55	71	60	61
Deneme76	44	49	44	44	49	60
Deneme77	55	83	55	55	61	55
Deneme78	55	55	55	77	55	55
Deneme79	66	55	88	55	55	49
Deneme80	61	55	55	55	54	61
Deneme81	54	55	55	55	55	55
Deneme82	55	87	60	76	55	77
Deneme83	55	66	61	55	55	54
Deneme84	55	55	65	55	72	55
Deneme85	55	55	66	55	60	61
Deneme86	77	55	55	55	55	55
Deneme87	66	55	55	55	77	55
Deneme88	60	71	55	55	49	55
Deneme89	55	55	61	88	55	54
Deneme90	55	55	93	66	55	72
Deneme91	55	55	55	55	55	55
Deneme92	55	61	55	82	55	55
Deneme93	55	55	55	55	60	55
Deneme94	55	76	55	55	55	66
Deneme95	55	55	60	55	72	71
Deneme96	55	55	55	55	55	55
Deneme97	55	55	60	55	55	55
Deneme98	55	55	55	60	60	55
Deneme99	88	83	61	83	55	55
Deneme100	76	60	60	65	55	55
Ortalama	58,35	58,87	60,09	60,46	59,37	59,98
Standart Sapma	9,48	9,44	10,65	12,15	10,60	9,18
Varyans	88,95	88,31	112,34	146,07	111,23	83,46
Medyan	55,00	55,00	55,00	55,00	55,00	55,00
Maximum	88	87	93	116	110	105
Minimum	28	27	28	44	27	49
Mod	55	55	55	55	55	55

Büro XP Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
8 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	27	50	77	87	49	55
Deneme02	77	55	55	77	55	61
Deneme03	61	55	55	88	105	60
Deneme04	60	82	55	72	65	61
Deneme05	55	60	55	49	99	82
Deneme06	55	55	82	55	61	88
Deneme07	55	55	60	55	60	61
Deneme08	82	72	55	71	55	55
Deneme09	72	60	66	66	71	60
Deneme10	54	55	55	66	61	88
Deneme11	55	55	61	55	55	77
Deneme12	55	55	55	55	55	60
Deneme13	55	60	55	55	55	61
Deneme14	55	55	54	55	55	66
Deneme15	55	55	55	116	55	60
Deneme16	55	55	77	55	54	88
Deneme17	55	55	55	55	83	55
Deneme18	55	55	55	54	93	60
Deneme19	55	55	55	72	72	55
Deneme20	55	55	55	71	55	55
Deneme21	55	60	55	55	54	61
Deneme22	87	55	55	55	55	76
Deneme23	72	55	82	55	77	72
Deneme24	66	55	77	55	88	82
Deneme25	49	55	55	66	55	61
Deneme26	50	66	44	50	49	44
Deneme27	55	60	55	54	83	55
Deneme28	60	55	55	55	60	60
Deneme29	55	88	55	66	60	55
Deneme30	66	60	66	66	55	71
Deneme31	71	55	50	55	55	55
Deneme32	61	61	55	55	83	55
Deneme33	55	55	55	55	55	55
Deneme34	55	82	82	55	55	55
Deneme35	54	55	77	55	54	82
Deneme36	55	55	55	55	55	61
Deneme37	55	55	55	71	83	54
Deneme38	50	55	55	60	55	55
Deneme39	60	88	60	55	55	50
Deneme40	72	55	55	49	61	55
Deneme41	54	54	61	55	54	55
Deneme42	55	61	55	50	55	66
Deneme43	44	55	55	110	55	82
Deneme44	55	71	71	99	61	60
Deneme45	55	55	55	76	60	55
Deneme46	55	55	55	55	61	55
Deneme47	83	66	60	55	60	72
Deneme48	76	55	55	55	60	60
Deneme49	61	55	83	55	61	61
Deneme50	55	55	54	61	93	60
Deneme51	33	33	82	55	33	28
Deneme52	55	55	83	94	83	66
Deneme53	93	55	54	54	55	60
Deneme54	82	61	83	55	66	83
Deneme55	61	71	55	55	55	60
Deneme56	60	55	55	55	54	60
Deneme57	55	55	55	61	61	77
Deneme58	88	60	55	55	77	55
Deneme59	55	55	65	55	60	55
Deneme60	60	50	55	54	61	55
Deneme61	55	82	61	72	60	50
Deneme62	55	55	82	55	66	54
Deneme63	55	55	66	60	55	55
Deneme64	50	60	55	55	55	61
Deneme65	82	55	55	55	55	55
Deneme66	66	55	55	60	60	55
Deneme67	55	55	55	44	61	60
Deneme68	55	55	55	55	54	66
Deneme69	55	49	55	55	55	88
Deneme70	55	66	55	55	55	55
Deneme71	55	55	82	55	55	71
Deneme72	54	55	55	55	83	55
Deneme73	72	55	55	55	55	61
Deneme74	55	55	55	55	54	60
Deneme75	55	77	55	55	55	55
Deneme76	82	44	44	88	44	33
Deneme77	60	55	55	83	88	55
Deneme78	77	55	83	66	55	83
Deneme79	61	55	93	44	82	54
Deneme80	71	55	55	55	55	61
Deneme81	55	55	55	54	61	66
Deneme82	55	55	55	72	54	60
Deneme83	60	82	49	55	55	77
Deneme84	55	55	50	66	55	60
Deneme85	61	55	77	55	94	55
Deneme86	71	55	38	77	55	61
Deneme87	72	66	55	54	60	66
Deneme88	55	55	55	55	77	82
Deneme89	60	60	50	55	60	83
Deneme90	50	55	44	61	61	137
Deneme91	49	88	44	55	60	55
Deneme92	50	55	71	55	72	55
Deneme93	55	55	50	49	65	44
Deneme94	55	55	44	55	55	88
Deneme95	82	55	44	55	61	60
Deneme96	60	71	55	55	77	55
Deneme97	55	110	55	55	55	60
Deneme98	55	55	55	55	55	110
Deneme99	55	55	44	71	54	66
Deneme100	55	77	55	88	61	55
Ortalama	59,76	59,28	59,07	61,09	62,34	63,29
Standart Sapma	10,89	10,50	11,08	12,95	12,61	14,40
Varyans	117,36	109,10	121,51	165,94	157,34	205,39
Medyan	55,00	55,00	55,00	55,00	57,50	60,00
Maximum	93	110	93	116	105	137
Minimum	27	33	38	44	33	28
Mod	55	55	55	55	55	55

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled		WEP_64	WEP_128	Disabled	WEP_64	WEP_128
8 MB		**Süre**	**Süre**		**Süre**	**Süre**
Deneme01	66	72	49	60	33	71
Deneme02	55	55	60	55	77	60
Deneme03	60	60	61	55	60	61
Deneme04	60	77	77	60	55	77
Deneme05	72	60	60	44	77	77
Deneme06	60	66	55	55	60	60
Deneme07	61	72	55	55	55	61
Deneme08	60	60	55	55	55	54
Deneme09	61	77	55	55	55	55
Deneme10	76	66	66	55	55	83
Deneme11	61	60	55	55	71	66
Deneme12	55	61	55	55	55	55
Deneme13	55	60	55	55	55	55
Deneme14	55	55	55	88	55	71
Deneme15	55	55	71	83	55	49
Deneme16	54	60	55	66	55	66
Deneme17	61	83	55	44	82	55
Deneme18	55	60	55	55	72	55
Deneme19	55	55	55	54	55	55
Deneme20	55	55	82	72	55	66
Deneme21	55	55	66	55	55	55
Deneme22	66	82	55	66	55	55
Deneme23	76	61	55	55	54	55
Deneme24	55	55	44	77	55	55
Deneme25	55	55	55	54	72	55
Deneme26	55	44	43	55	39	44
Deneme27	61	60	55	55	55	55
Deneme28	60	61	55	61	55	55
Deneme29	60	71	55	55	55	55
Deneme30	61	61	72	55	82	94
Deneme31	66	60	55	49	66	60
Deneme32	60	77	54	55	55	55
Deneme33	61	66	55	55	55	60
Deneme34	60	60	55	55	55	55
Deneme35	77	83	55	55	55	55
Deneme36	71	60	66	55	55	55
Deneme37	60	55	55	71	55	71
Deneme38	55	55	77	88	54	66
Deneme39	60	55	55	55	55	61
Deneme40	55	60	60	60	55	55
Deneme41	77	60	61	55	72	55
Deneme42	60	61	88	82	66	72
Deneme43	61	55	66	55	55	54
Deneme44	55	60	54	55	54	61
Deneme45	55	55	55	44	61	55
Deneme46	55	55	55	55	93	55
Deneme47	87	82	55	55	55	93
Deneme48	55	55	88	88	55	66
Deneme49	55	55	55	55	55	55
Deneme50	55	60	88	55	55	93
Deneme51	49	39	33	60	33	38
Deneme52	55	87	61	61	66	61
Deneme53	55	61	60	65	55	60
Deneme54	60	61	82	66	55	61
Deneme55	88	82	55	55	55	60
Deneme56	66	72	61	55	55	60
Deneme57	61	65	55	55	55	66
Deneme58	60	55	55	61	76	61
Deneme59	55	66	88	71	55	55
Deneme60	60	61	65	55	61	71
Deneme61	55	66	66	99	55	61
Deneme62	55	60	99	55	55	54
Deneme63	55	66	55	55	82	66
Deneme64	55	93	55	55	93	55
Deneme65	55	72	93	55	61	55
Deneme66	66	55	61	55	55	55
Deneme67	55	60	55	38	55	60
Deneme68	55	55	55	55	55	61
Deneme69	55	55	93	55	66	54
Deneme70	55	93	66	60	54	55
Deneme71	65	66	55	55	55	55
Deneme72	55	61	60	72	55	83
Deneme73	55	55	55	54	88	99
Deneme74	61	55	60	88	61	60
Deneme75	55	71	77	55	55	55
Deneme76	49	55	94	55	72	50
Deneme77	72	66	60	55	55	71
Deneme78	71	104	83	55	55	61
Deneme79	55	60	60	55	55	60
Deneme80	60	66	60	71	55	55
Deneme81	55	77	50	55	54	71
Deneme82	55	60	60	77	55	83
Deneme83	66	66	50	55	55	60
Deneme84	55	66	49	55	55	55
Deneme85	55	66	71	55	55	61
Deneme86	55	93	50	83	83	60
Deneme87	55	72	55	55	54	55
Deneme88	55	60	49	82	50	82
Deneme89	55	60	50	71	55	66
Deneme90	55	55	66	44	55	55
Deneme91	66	55	72	55	55	77
Deneme92	55	55	54	77	60	55
Deneme93	54	105	99	55	55	55
Deneme94	55	93	44	55	55	49
Deneme95	55	77	50	55	55	55
Deneme96	61	55	49	76	55	55
Deneme97	55	55	44	55	55	66
Deneme98	55	55	55	55	88	55
Deneme99	55	60	88	55	55	55
Deneme100	54	82	66	55	54	55
Ortalama	59,30	64,53	61,41	59,87	59,11	61,25
Standart Sapma	7,10	12,01	13,17	10,99	10,60	10,59
Varyans	49,97	142,83	171,62	119,49	111,28	110,93
Medyan	55,00	60,00	55,00	55,00	55,00	57,50
Maximum	88	105	99	99	93	99
Minimum	49	39	33	38	33	38
Mod	55	55	55	55	55	55

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled		WEP_64	WEP_128	Disabled	WEP_64	WEP_128
8 MB		**Süre**	**Süre**		**Süre**	**Süre**
Deneme01	105	49	55	55	61	28
Deneme02	54	55	55	77	55	55
Deneme03	55	55	55	61	55	60
Deneme04	60	55	55	55	54	55
Deneme05	55	55	55	77	83	104
Deneme06	55	93	66	66	71	60
Deneme07	55	55	55	55	55	55
Deneme08	55	55	55	49	55	61
Deneme09	60	55	55	55	55	55
Deneme10	83	61	82	39	55	55
Deneme11	71	60	55	49	71	55
Deneme12	83	55	55	44	99	82
Deneme13	60	55	71	49	72	55
Deneme14	55	55	55	50	55	49
Deneme15	55	55	99	88	60	55
Deneme16	55	55	60	66	55	55
Deneme17	55	55	55	60	71	77
Deneme18	55	55	55	55	55	60
Deneme19	66	55	55	55	55	55
Deneme20	54	55	55	55	55	55
Deneme21	55	60	55	77	55	55
Deneme22	55	55	71	49	88	72
Deneme23	55	55	61	61	55	71
Deneme24	55	55	55	55	55	60
Deneme25	83	55	88	54	55	55
Deneme26	65	44	60	66	61	39
Deneme27	44	66	61	60	55	54
Deneme28	61	55	55	55	55	55
Deneme29	55	60	55	49	55	55
Deneme30	55	55	55	55	54	61
Deneme31	55	55	82	55	55	60
Deneme32	55	60	55	83	55	55
Deneme33	54	55	55	55	55	55
Deneme34	83	55	55	55	66	49
Deneme35	71	55	55	49	55	55
Deneme36	61	55	71	49	55	77
Deneme37	55	60	55	55	55	55
Deneme38	55	66	60	55	55	55
Deneme39	43	77	55	44	55	55
Deneme40	44	82	61	66	115	55
Deneme41	55	83	55	61	77	60
Deneme42	55	60	44	54	77	55
Deneme43	55	71	77	55	55	55
Deneme44	55	55	82	61	72	55
Deneme45	55	99	77	82	77	72
Deneme46	60	55	55	66	77	82
Deneme47	61	55	55	55	54	77
Deneme48	55	55	55	55	72	55
Deneme49	55	55	55	55	82	55
Deneme50	55	55	65	60	55	55
Deneme51	71	38	38	44	33	50
Deneme52	60	55	66	55	55	76
Deneme53	88	55	55	88	55	55
Deneme54	55	60	55	55	54	55
Deneme55	55	55	55	55	55	55
Deneme56	55	72	55	54	55	72
Deneme57	77	54	55	61	88	55
Deneme58	126	88	76	66	61	71
Deneme59	55	55	66	49	55	82
Deneme60	55	55	55	83	93	61
Deneme61	72	55	55	55	60	55
Deneme62	55	55	55	49	55	55
Deneme63	76	55	61	38	55	55
Deneme64	50	71	49	55	55	87
Deneme65	55	55	55	55	72	66
Deneme66	60	77	55	55	54	50
Deneme67	61	55	66	55	55	55
Deneme68	76	55	55	66	66	55
Deneme69	61	55	55	77	55	55
Deneme70	115	55	54	55	55	54
Deneme71	55	55	66	55	55	50
Deneme72	55	55	61	55	55	55
Deneme73	55	55	55	55	55	60
Deneme74	55	55	55	49	82	61
Deneme75	55	82	55	77	55	55
Deneme76	71	44	60	72	55	83
Deneme77	50	66	66	55	55	66
Deneme78	55	55	60	49	77	55
Deneme79	66	61	83	55	72	54
Deneme80	60	54	55	55	60	55
Deneme81	55	55	55	49	55	55
Deneme82	55	55	55	83	55	72
Deneme83	60	55	54	77	55	60
Deneme84	55	55	61	60	55	72
Deneme85	61	55	49	55	88	82
Deneme86	82	55	55	49	82	55
Deneme87	55	55	55	55	60	55
Deneme88	60	55	55	50	55	55
Deneme89	55	66	55	55	55	55
Deneme90	55	66	55	55	55	71
Deneme91	44	55	88	50	55	38
Deneme92	55	55	60	38	77	55
Deneme93	55	54	55	49	66	55
Deneme94	55	55	55	50	60	77
Deneme95	60	55	60	55	55	55
Deneme96	77	55	55	66	55	55
Deneme97	72	55	55	49	55	55
Deneme98	44	55	77	55	55	49
Deneme99	60	55	55	82	55	55
Deneme100	55	54	55	66	55	55
Ortalama	60,91	58,43	59,59	58,06	61,64	59,49
Standart Sapma	13,32	9,39	9,71	10,76	12,31	10,89
Varyans	175,68	87,27	93,40	114,54	150,11	117,45
Medyan	55,00	55,00	55,00	55,00	55,00	55,00
Maximum	126	99	99	88	115	104
Minimum	43	38	38	38	33	28
Mod	55	55	55	55	55	55

Büro XP Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	44	93	121	137	71	187
Deneme02	143	99	110	104	99	99
Deneme03	132	99	99	105	99	170
Deneme04	126	93	110	99	99	148
Deneme05	93	99	98	98	219	187
Deneme06	94	126	94	83	149	93
Deneme07	93	127	93	99	82	105
Deneme08	93	148	99	93	93	208
Deneme09	94	99	99	99	94	132
Deneme10	93	93	99	99	93	132
Deneme11	83	220	93	99	93	132
Deneme12	93	225	94	94	94	126
Deneme13	110	121	93	104	93	99
Deneme14	208	93	93	99	94	93
Deneme15	237	94	94	88	76	143
Deneme16	142	170	93	93	94	105
Deneme17	116	137	93	269	93	82
Deneme18	93	220	94	121	94	121
Deneme19	94	225	93	115	93	92
Deneme20	214	93	94	231	93	99
Deneme21	99	209	93	77	94	99
Deneme22	93	121	93	93	225	110
Deneme23	93	93	94	94	253	225
Deneme24	94	93	104	93	263	137
Deneme25	93	94	104	93	214	132
Deneme26	66	193	214	182	242	99
Deneme27	104	110	121	93	231	99
Deneme28	104	93	220	126	252	137
Deneme29	94	104	219	116	105	247
Deneme30	82	105	105	104	104	93
Deneme31	99	98	115	99	99	94
Deneme32	93	94	94	99	99	126
Deneme33	94	126	98	93	93	132
Deneme34	93	99	116	94	94	148
Deneme35	94	99	82	93	263	121
Deneme36	93	93	93	104	99	159
Deneme37	99	94	94	94	93	94
Deneme38	93	93	99	93	94	93
Deneme39	94	99	93	93	93	93
Deneme40	148	99	99	110	94	99
Deneme41	99	93	93	264	98	83
Deneme42	93	242	99	231	182	99
Deneme43	94	132	99	98	121	104
Deneme44	93	181	93	105	274	237
Deneme45	93	121	94	93	203	153
Deneme46	99	99	209	94	138	215
Deneme47	99	98	93	98	126	93
Deneme48	93	94	159	105	104	93
Deneme49	94	99	94	99	99	94
Deneme50	104	219	98	94	275	99
Deneme51	104	61	236	61	55	115
Deneme52	105	93	121	99	137	115
Deneme53	115	137	99	109	209	99
Deneme54	110	132	104	88	132	99
Deneme55	93	126	99	88	93	264
Deneme56	88	94	104	88	143	93
Deneme57	94	93	105	88	88	269
Deneme58	88	231	93	88	93	88
Deneme59	93	236	93	93	94	88
Deneme60	104	132	171	88	88	159
Deneme61	99	99	236	236	88	182
Deneme62	99	99	88	99	87	98
Deneme63	104	120	88	104	105	88
Deneme64	99	99	159	88	110	88
Deneme65	99	253	88	88	142	88
Deneme66	93	126	127	88	88	93
Deneme67	99	94	109	88	88	94
Deneme68	94	93	94	148	88	93
Deneme69	88	93	88	93	88	99
Deneme70	87	94	99	116	88	88
Deneme71	121	159	87	181	126	115
Deneme72	121	231	94	258	88	105
Deneme73	104	126	99	88	88	110
Deneme74	105	132	88	137	88	98
Deneme75	165	104	87	83	99	94
Deneme76	116	214	82	110	105	176
Deneme77	104	115	99	132	230	94
Deneme78	93	94	99	126	138	115
Deneme79	182	98	258	121	115	77
Deneme80	104	226	226	99	93	252
Deneme81	93	115	219	88	209	176
Deneme82	94	93	220	88	94	99
Deneme83	110	209	236	203	131	203
Deneme84	87	121	220	132	149	88
Deneme85	94	99	187	126	225	88
Deneme86	93	99	219	127	220	104
Deneme87	88	104	143	98	87	99
Deneme88	87	93	192	94	248	88
Deneme89	94	99	231	88	87	88
Deneme90	110	94	148	99	88	93
Deneme91	93	93	204	87	94	99
Deneme92	93	93	93	88	93	94
Deneme93	105	94	104	88	88	208
Deneme94	99	126	99	99	88	110
Deneme95	99	93	94	170	88	116
Deneme96	98	94	93	176	88	87
Deneme97	94	93	137	94	104	88
Deneme98	93	94	214	120	198	88
Deneme99	220	164	99	88	170	88
Deneme100	236	204	99	88	220	88
Ortalama	106,28	125,39	123,08	112,67	127,82	121,88
Standart Sapma	31,95	46,82	48,64	41,51	57,45	45,42
Varyans	1010,40	2170,30	2341,79	1705,46	3266,97	2042,55
Medyan	94,00	99,00	99,00	99,00	98,50	99,00
Maximum	237,00	253,00	258,00	269,00	275,00	269,00
Minimum	44	61	82	61	55	77
Mod	93	93	93	88	88	99

Büro XP Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP 64	WEP 128	Disabled	WEP 64	WEP 128
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	88	55	159	116	66	209
Deneme02	104	104	181	137	99	181
Deneme03	99	110	170	126	99	132
Deneme04	93	176	116	132	109	104
Deneme05	94	104	104	126	105	99
Deneme06	88	137	94	105	132	176
Deneme07	99	127	98	93	115	225
Deneme08	93	104	94	121	93	225
Deneme09	83	137	99	115	99	93
Deneme10	99	132	93	116	242	193
Deneme11	121	104	93	94	110	258
Deneme12	104	110	94	98	93	115
Deneme13	93	220	99	116	99	116
Deneme14	88	137	131	115	110	98
Deneme15	93	99	121	137	88	198
Deneme16	220	94	138	116	93	203
Deneme17	154	98	82	110	231	231
Deneme18	225	165	77	104	99	225
Deneme19	231	225	71	121	93	132
Deneme20	220	121	171	93	93	121
Deneme21	109	154	181	94	116	93
Deneme22	110	104	137	93	186	154
Deneme23	99	94	126	93	116	176
Deneme24	88	93	82	94	99	99
Deneme25	99	99	88	93	131	93
Deneme26	187	154	77	104	225	115
Deneme27	93	110	110	105	116	116
Deneme28	99	93	77	93	115	121
Deneme29	94	93	82	110	99	104
Deneme30	88	94	126	231	214	104
Deneme31	87	181	77	219	88	171
Deneme32	171	214	77	226	115	192
Deneme33	88	99	77	225	160	209
Deneme34	88	220	77	252	131	98
Deneme35	76	126	88	176	99	106
Deneme36	88	105	132	88	116	93
Deneme37	88	93	76	231	115	99
Deneme38	99	94	77	258	154	248
Deneme39	99	99	77	93	219	115
Deneme40	88	93	104	94	138	220
Deneme41	88	99	77	93	99	88
Deneme42	77	93	77	93	98	93
Deneme43	87	220	187	94	137	93
Deneme44	88	132	88	77	105	88
Deneme45	94	110	104	99	214	88
Deneme46	99	120	132	93	99	88
Deneme47	87	105	88	93	88	93
Deneme48	215	99	98	94	93	116
Deneme49	77	219	99	93	93	88
Deneme50	104	132	94	93	143	104
Deneme51	61	192	154	132	182	71
Deneme52	93	127	104	94	98	99
Deneme53	94	104	88	142	99	93
Deneme54	88	242	99	143	160	94
Deneme55	94	148	99	104	126	121
Deneme56	203	99	99	137	93	98
Deneme57	88	99	88	198	99	105
Deneme58	132	98	93	115	99	93
Deneme59	137	220	83	132	93	88
Deneme60	115	121	131	132	160	93
Deneme61	110	104	127	209	93	94
Deneme62	93	105	88	258	93	88
Deneme63	88	230	219	93	105	93
Deneme64	88	94	99	121	88	93
Deneme65	88	104	181	93	115	127
Deneme66	93	143	83	94	110	126
Deneme67	88	99	88	93	88	104
Deneme68	88	170	99	88	104	105
Deneme69	94	126	197	93	110	104
Deneme70	93	94	258	88	88	110
Deneme71	93	93	137	94	88	99
Deneme72	94	83	138	93	88	165
Deneme73	121	98	115	77	120	94
Deneme74	93	94	215	94	110	87
Deneme75	88	208	274	88	94	126
Deneme76	198	83	83	170	82	77
Deneme77	93	214	104	99	105	88
Deneme78	99	214	99	93	93	94
Deneme79	171	132	82	99	110	98
Deneme80	104	110	121	104	99	226
Deneme81	93	99	94	94	93	137
Deneme82	94	98	88	93	104	110
Deneme83	208	110	109	94	88	110
Deneme84	121	116	88	76	208	109
Deneme85	127	94	88	88	99	286
Deneme86	230	104	143	132	99	131
Deneme87	99	104	104	132	143	215
Deneme88	110	116	83	116	192	126
Deneme89	115	142	110	115	110	126
Deneme90	99	138	93	132	93	116
Deneme91	93	126	116	93	88	115
Deneme92	94	115	104	99	94	104
Deneme93	93	99	83	225	99	313
Deneme94	121	94	252	220	87	88
Deneme95	115	93	83	132	94	94
Deneme96	214	93	170	88	154	93
Deneme97	231	94	77	88	203	93
Deneme98	121	93	214	88	104	94
Deneme99	203	93	77	71	105	93
Deneme100	88	226	77	193	115	115
Ortalama	113,94	125,95	113,75	121,24	117,53	128,20
Standart Sapma	42,64	43,21	43,47	45,50	37,82	51,43
Varyans	1799,82	1848,29	1870,87	2049,14	1416,31	2618,98
Medyan	94,00	105,00	99,00	101,50	104,00	105,00
Maximum	231	242	274	258	242	313
Minimum	61	55	71	71	66	71
Mod	88	99	77	93	99	93

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	104	60	159	149	71	192
Deneme02	127	105	149	148	99	88
Deneme03	197	137	143	148	171	99
Deneme04	110	137	110	215	98	143
Deneme05	105	110	93	269	99	98
Deneme06	241	99	104	126	99	99
Deneme07	105	99	99	104	99	99
Deneme08	99	98	94	83	99	220
Deneme09	104	99	94	93	93	99
Deneme10	253	220	148	93	94	99
Deneme11	220	253	209	116	93	93
Deneme12	208	175	225	110	121	99
Deneme13	220	127	115	120	214	93
Deneme14	88	93	88	121	93	94
Deneme15	93	104	104	94	94	98
Deneme16	99	94	99	121	99	105
Deneme17	99	93	99	142	93	104
Deneme18	110	94	93	116	93	93
Deneme19	104	214	88	115	99	204
Deneme20	99	99	88	148	143	93
Deneme21	93	93	94	99	94	93
Deneme22	121	99	87	93	164	94
Deneme23	121	132	143	99	242	225
Deneme24	116	99	176	132	220	132
Deneme25	109	214	269	99	258	126
Deneme26	132	203	99	214	77	82
Deneme27	121	104	115	203	99	236
Deneme28	93	165	132	104	159	264
Deneme29	94	121	88	165	105	225
Deneme30	241	99	88	121	98	209
Deneme31	248	99	88	99	110	126
Deneme32	219	110	93	99	94	110
Deneme33	94	104	99	110	230	99
Deneme34	93	99	104	209	182	99
Deneme35	170	104	259	121	99	214
Deneme36	138	154	109	99	98	126
Deneme37	93	220	264	99	220	127
Deneme38	93	230	231	104	214	110
Deneme39	94	121	126	93	121	99
Deneme40	99	94	121	99	209	98
Deneme41	175	164	115	94	209	99
Deneme42	259	226	94	93	115	247
Deneme43	225	142	93	93	104	231
Deneme44	247	99	104	94	99	181
Deneme45	220	94	226	126	99	94
Deneme46	219	98	219	93	99	99
Deneme47	231	187	231	94	104	98
Deneme48	99	192	231	93	99	94
Deneme49	93	209	71	94	93	99
Deneme50	94	94	93	164	94	93
Deneme51	60	60	137	148	71	88
Deneme52	225	105	204	93	99	99
Deneme53	127	126	98	116	99	269
Deneme54	109	126	99	181	99	209
Deneme55	264	138	99	258	98	137
Deneme56	231	104	171	88	209	94
Deneme57	148	171	236	137	214	93
Deneme58	126	99	121	83	105	220
Deneme59	99	241	143	110	93	263
Deneme60	193	154	99	132	110	237
Deneme61	93	132	88	126	214	126
Deneme62	93	115	93	121	214	115
Deneme63	231	105	93	99	127	127
Deneme64	93	214	88	88	247	137
Deneme65	94	104	94	88	225	121
Deneme66	115	99	208	203	209	104
Deneme67	93	99	121	132	154	94
Deneme68	94	99	131	126	126	98
Deneme69	121	93	94	127	126	99
Deneme70	137	99	93	98	110	99
Deneme71	121	93	105	94	126	104
Deneme72	121	94	225	88	110	132
Deneme73	104	93	214	99	94	258
Deneme74	115	94	110	87	93	203
Deneme75	99	93	132	88	99	132
Deneme76	77	99	77	88	203	83
Deneme77	99	148	94	99	203	93
Deneme78	93	231	93	226	94	93
Deneme79	94	121	93	137	93	88
Deneme80	93	104	77	110	115	99
Deneme81	99	104	127	110	105	231
Deneme82	99	99	98	109	110	99
Deneme83	99	99	132	286	98	99
Deneme84	126	99	264	131	110	93
Deneme85	93	99	231	215	203	110
Deneme86	94	115	225	126	94	99
Deneme87	93	110	181	126	93	93
Deneme88	94	110	253	116	105	93
Deneme89	104	209	126	115	98	99
Deneme90	93	203	93	104	105	99
Deneme91	94	104	99	313	99	99
Deneme92	93	93	132	88	132	93
Deneme93	198	138	121	94	120	94
Deneme94	110	93	126	93	94	93
Deneme95	186	192	121	93	93	94
Deneme96	105	220	104	94	104	87
Deneme97	115	137	88	154	99	160
Deneme98	99	220	88	165	99	181
Deneme99	93	231	187	93	99	93
Deneme100	105	236	242	94	220	88
Ortalama	131,83	132,43	134,31	125,19	128,31	128,52
Standart Sapma	53,72	48,84	55,08	46,37	49,25	52,95
Varyans	2857,46	2361,03	3003,43	2128,23	2401,59	2775,49
Medyan	105,00	105,00	109,50	110,00	101,50	99,00
Maximum	264	253	269	313	258	269
Minimum	60	60	71	83	71	82
Mod	93	99	93	93	99	99

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
16 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	247	142	49	66	156	49
Deneme02	94	116	99	192	148	105
Deneme03	99	99	99	170	131	98
Deneme04	99	170	99	121	121	88
Deneme05	93	93	263	126	110	88
Deneme06	99	94	149	121	99	143
Deneme07	237	98	93	105	93	88
Deneme08	93	99	115	98	99	99
Deneme09	93	99	231	88	203	159
Deneme10	132	105	99	159	94	170
Deneme11	214	137	93	143	126	127
Deneme12	138	137	165	93	242	104
Deneme13	109	143	126	88	121	93
Deneme14	149	121	138	88	230	88
Deneme15	143	93	148	88	138	88
Deneme16	214	132	93	99	93	99
Deneme17	137	143	99	88	88	88
Deneme18	126	154	94	88	88	88
Deneme19	110	104	93	87	225	126
Deneme20	99	104	220	94	225	88
Deneme21	99	99	88	110	116	88
Deneme22	93	99	93	82	126	88
Deneme23	127	98	143	88	115	88
Deneme24	170	99	209	187	127	93
Deneme25	165	99	120	88	219	115
Deneme26	126	88	182	88	71	121
Deneme27	132	104	99	104	94	82
Deneme28	126	99	219	88	214	143
Deneme29	132	99	121	77	99	88
Deneme30	126	98	93	88	93	87
Deneme31	110	99	138	77	93	149
Deneme32	110	99	110	87	94	104
Deneme33	99	105	131	143	99	88
Deneme34	203	153	94	192	93	88
Deneme35	176	94	165	198	88	88
Deneme36	198	93	126	94	165	143
Deneme37	214	137	99	175	88	137
Deneme38	93	143	126	127	88	126
Deneme39	94	110	132	214	104	88
Deneme40	93	104	302	258	258	104
Deneme41	93	105	225	198	209	88
Deneme42	94	126	138	116	88	132
Deneme43	93	165	93	87	88	94
Deneme44	93	115	231	88	120	87
Deneme45	94	94	186	138	99	99
Deneme46	99	120	138	137	88	143
Deneme47	99	94	104	99	88	104
Deneme48	93	93	115	110	93	88
Deneme49	94	94	220	82	242	88
Deneme50	93	93	231	115	203	94
Deneme51	171	50	66	60	94	66
Deneme52	247	148	247	94	121	105
Deneme53	165	148	116	93	98	99
Deneme54	236	94	236	209	88	87
Deneme55	242	93	94	247	77	88
Deneme56	120	93	88	88	88	88
Deneme57	105	154	148	88	88	99
Deneme58	126	94	220	87	88	104
Deneme59	110	98	115	88	137	116
Deneme60	231	105	88	88	94	126
Deneme61	219	110	93	72	82	137
Deneme62	110	148	88	87	88	127
Deneme63	93	93	88	132	88	104
Deneme64	94	116	93	132	88	143
Deneme65	99	153	93	126	87	88
Deneme66	93	105	88	121	88	110
Deneme67	126	93	225	99	193	93
Deneme68	116	94	231	88	88	121
Deneme69	93	148	121	99	72	88
Deneme70	110	93	104	99	88	93
Deneme71	99	94	99	88	88	93
Deneme72	93	104	126	93	88	99
Deneme73	94	93	346	93	87	121
Deneme74	93	94	88	149	198	88
Deneme75	93	104	88	148	225	132
Deneme76	94	77	77	148	71	138
Deneme77	181	93	94	215	214	99
Deneme78	115	94	186	269	116	87
Deneme79	110	93	138	126	88	116
Deneme80	121	93	88	104	131	104
Deneme81	121	94	77	83	110	126
Deneme82	104	93	87	93	110	99
Deneme83	99	99	132	93	94	88
Deneme84	99	187	110	116	98	132
Deneme85	198	99	88	110	94	88
Deneme86	170	170	88	120	88	88
Deneme87	93	165	77	121	93	110
Deneme88	94	98	121	94	88	120
Deneme89	93	154	230	121	88	138
Deneme90	93	154	94	142	88	110
Deneme91	99	132	88	116	88	93
Deneme92	110	82	87	115	87	132
Deneme93	94	154	132	148	88	88
Deneme94	126	165	83	121	88	154
Deneme95	121	93	126	94	94	137
Deneme96	121	94	121	131	104	88
Deneme97	126	93	93	99	115	159
Deneme98	121	99	88	94	88	165
Deneme99	121	93	88	93	94	132
Deneme100	93	99	93	93	87	98
Ortalama	126,51	111,87	131,11	117,64	117,17	107,05
Standart Sapma	43,61	25,90	57,10	42,33	47,10	23,40
Varyans	1882,47	663,91	3227,94	1773,95	2195,84	541,93
Medyan	110,00	99,00	110,00	99,00	94,00	99,00
Maximum	247	187	346	269	258	170
Minimum	93	50	49	60	71	49
Mod	93	93	88	88	88	88

Büro XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	780	582	434	780	944	643
Deneme02	637	631	665	648	643	725
Deneme03	604	665	664	637	742	632
Deneme04	638	895	642	626	834	637
Deneme05	747	692	632	632	675	846
Deneme06	747	819	643	615	621	615
Deneme07	642	648	637	632	758	615
Deneme08	863	648	648	719	632	637
Deneme09	631	632	637	638	818	824
Deneme10	626	961	610	615	621	621
Deneme11	621	642	642	643	620	1065
Deneme12	730	643	648	648	638	626
Deneme13	698	654	605	654	856	637
Deneme14	642	631	648	637	632	1022
Deneme15	665	621	626	632	643	1274
Deneme16	769	599	840	714	637	736
Deneme17	642	780	830	697	664	890
Deneme18	797	648	653	687	632	626
Deneme19	648	637	637	648	582	637
Deneme20	610	626	643	829	846	627
Deneme21	856	632	637	753	626	631
Deneme22	616	615	643	653	643	703
Deneme23	609	632	637	742	626	648
Deneme24	637	719	659	802	626	649
Deneme25	769	638	621	637	648	1191
Deneme26	654	615	599	643	566	785
Deneme27	632	643	670	632	643	451
Deneme28	686	648	626	643	835	637
Deneme29	605	654	627	637	631	637
Deneme30	780	637	725	918	637	615
Deneme31	889	632	637	654	632	632
Deneme32	626	714	637	604	752	631
Deneme33	753	697	649	714	797	649
Deneme34	747	687	867	786	620	648
Deneme35	616	648	681	653	632	769
Deneme36	631	829	627	753	802	626
Deneme37	758	753	604	615	637	620
Deneme38	610	653	796	698	813	676
Deneme39	637	742	615	626	676	615
Deneme40	747	802	648	664	725	631
Deneme41	890	637	769	643	637	583
Deneme42	610	643	818	648	610	620
Deneme43	632	653	637	884	626	643
Deneme44	813	731	632	692	786	648
Deneme45	637	615	736	676	626	632
Deneme46	637	747	642	670	643	1054
Deneme47	604	697	637	648	829	637
Deneme48	467	627	637	643	643	621
Deneme49	917	637	604	631	631	637
Deneme50	659	802	653	643	698	632
Deneme51	895	818	582	654	582	615
Deneme52	649	654	643	631	654	648
Deneme53	834	730	615	638	637	632
Deneme54	725	632	626	867	620	648
Deneme55	808	653	621	637	791	835
Deneme56	615	648	736	763	626	621
Deneme57	632	681	692	846	632	697
Deneme58	653	648	615	736	835	632
Deneme59	857	901	857	653	637	632
Deneme60	648	670	824	648	593	703
Deneme61	764	599	626	632	626	615
Deneme62	670	719	610	609	670	1352
Deneme63	719	852	664	643	698	642
Deneme64	632	774	626	714	698	632
Deneme65	851	703	643	676	643	730
Deneme66	714	648	681	549	631	1088
Deneme67	637	604	621	599	637	637
Deneme68	665	610	620	637	660	626
Deneme69	648	632	692	609	598	626
Deneme70	599	840	824	775	626	632
Deneme71	252	643	632	610	632	1010
Deneme72	649	637	632	736	610	654
Deneme73	681	714	637	604	857	1192
Deneme74	615	763	675	626	631	631
Deneme75	653	698	605	736	610	670
Deneme76	609	747	560	593	747	846
Deneme77	802	637	643	692	637	648
Deneme78	643	599	637	621	703	632
Deneme79	642	730	654	829	637	692
Deneme80	632	654	824	615	637	648
Deneme81	731	637	659	961	626	621
Deneme82	736	807	648	714	764	867
Deneme83	823	648	835	676	780	638
Deneme84	786	643	676	649	621	829
Deneme85	632	626	626	631	626	604
Deneme86	626	626	643	643	626	703
Deneme87	642	627	642	643	308	599
Deneme88	725	626	637	851	626	813
Deneme89	637	758	851	643	742	637
Deneme90	643	631	632	637	631	637
Deneme91	637	632	670	610	637	665
Deneme92	631	873	791	637	632	643
Deneme93	632	632	631	615	681	631
Deneme94	637	626	566	736	648	1071
Deneme95	687	637	670	637	615	1017
Deneme96	642	335	637	637	775	741
Deneme97	736	637	610	643	670	632
Deneme98	643	632	626	670	627	1065
Deneme99	632	769	708	648	626	687
Deneme100	609	632	632	676	670	737
Ortalama	683,21	679,05	662,61	676,71	670,60	717,89
Standart Sapma	95,29	84,81	72,73	75,43	85,17	166,57
Varyans	8989,19	7120,05	5237,16	5632,25	7182,14	27468,62
Medyan	645,50	648,00	642,00	648,00	637,00	640,00
Maximum	917	961	867	961	944	1352
Minimum	252	335	434	549	308	451
Mod	637	632	637	643	626	632

Büro XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	719	582	703	824	807	813
Deneme02	769	769	610	516	736	506
Deneme03	621	687	802	654	846	758
Deneme04	626	643	873	664	637	856
Deneme05	604	796	884	632	621	627
Deneme06	632	796	643	796	582	659
Deneme07	846	654	604	884	956	648
Deneme08	642	626	654	643	643	763
Deneme09	660	648	582	637	697	808
Deneme10	620	626	654	851	643	681
Deneme11	813	445	653	626	758	675
Deneme12	621	797	621	649	643	874
Deneme13	620	758	621	703	637	714
Deneme14	626	631	834	598	638	648
Deneme15	604	879	583	615	642	813
Deneme16	621	637	906	868	637	642
Deneme17	725	638	626	637	626	632
Deneme18	626	626	615	632	753	632
Deneme19	769	714	637	626	621	642
Deneme20	472	786	632	753	714	609
Deneme21	627	818	637	714	664	758
Deneme22	730	638	604	648	709	638
Deneme23	615	620	1154	642	807	648
Deneme24	626	698	664	918	566	774
Deneme25	627	741	1153	654	626	808
Deneme26	725	544	730	604	868	620
Deneme27	632	654	802	714	813	769
Deneme28	615	686	637	786	648	665
Deneme29	686	632	643	653	654	599
Deneme30	676	779	642	753	928	824
Deneme31	626	632	627	615	648	643
Deneme32	731	637	834	648	786	637
Deneme33	725	637	709	642	703	631
Deneme34	736	632	884	648	818	440
Deneme35	709	643	665	638	709	626
Deneme36	675	664	983	620	857	637
Deneme37	769	610	637	835	692	747
Deneme38	632	796	648	643	637	1137
Deneme39	604	637	1066	648	675	786
Deneme40	676	654	1153	802	643	642
Deneme41	609	692	907	708	648	851
Deneme42	703	626	642	681	637	731
Deneme43	610	632	648	835	819	659
Deneme44	626	423	703	643	807	654
Deneme45	637	582	631	621	610	1076
Deneme46	593	626	649	637	818	983
Deneme47	638	621	802	631	643	956
Deneme48	631	621	642	643	631	676
Deneme49	637	626	610	637	654	1032
Deneme50	605	961	653	703	643	775
Deneme51	582	588	582	637	824	742
Deneme52	549	642	736	643	818	659
Deneme53	599	687	835	736	780	824
Deneme54	637	632	780	609	725	692
Deneme55	609	648	637	632	769	659
Deneme56	775	637	654	763	763	643
Deneme57	610	643	648	648	632	626
Deneme58	736	642	648	648	714	966
Deneme59	604	703	1219	632	654	868
Deneme60	626	879	648	961	697	890
Deneme61	736	593	615	642	758	873
Deneme62	593	626	621	643	659	780
Deneme63	692	627	1313	654	626	648
Deneme64	621	593	637	631	874	638
Deneme65	829	686	632	621	648	653
Deneme66	615	604	659	599	642	621
Deneme67	643	890	697	780	764	626
Deneme68	626	620	648	648	824	522
Deneme69	621	786	654	637	785	626
Deneme70	637	1055	659	626	643	1263
Deneme71	450	835	659	632	648	1181
Deneme72	599	774	637	615	632	637
Deneme73	621	588	670	632	648	626
Deneme74	587	1197	648	719	741	649
Deneme75	621	577	643	638	670	664
Deneme76	824	593	857	615	703	632
Deneme77	627	615	670	643	741	807
Deneme78	774	638	648	648	626	638
Deneme79	615	620	676	654	709	823
Deneme80	621	714	796	637	445	654
Deneme81	626	1148	610	632	758	654
Deneme82	610	610	868	714	637	730
Deneme83	687	588	626	697	615	599
Deneme84	631	599	774	687	637	642
Deneme85	621	626	616	648	648	918
Deneme86	621	588	637	829	896	670
Deneme87	632	709	714	753	653	648
Deneme88	604	736	621	653	643	643
Deneme89	632	1088	609	742	670	857
Deneme90	620	912	648	802	615	670
Deneme91	621	983	813	637	626	648
Deneme92	632	1027	653	643	643	676
Deneme93	576	555	626	632	637	796
Deneme94	621	610	660	643	796	610
Deneme95	692	818	609	637	637	868
Deneme96	637	615	742	648	649	626
Deneme97	604	593	642	637	626	774
Deneme98	610	1390	835	610	615	616
Deneme99	621	796	692	642	730	637
Deneme100	1076	852	626	648	819	648
Ortalama	652,20	702,75	715,43	677,29	699,10	724,82
Standart Sapma	78,77	152,69	146,56	78,22	88,09	139,59
Varyans	6143,32	23080,67	21265,29	6056,45	7682,13	19291,75
Medyan	626,00	640,00	651,00	643,00	654,00	659,00
Maximum	1076	1390	1313	961	956	1263
Minimum	450	423	582	516	445	440
Mod	621	626	648	648	637	648

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	741	719	626	714	731	846
Deneme02	670	698	659	676	637	642
Deneme03	654	675	654	632	653	643
Deneme04	664	654	785	725	791	643
Deneme05	632	632	588	615	637	648
Deneme06	796	637	818	736	643	873
Deneme07	884	637	626	681	626	643
Deneme08	643	599	632	632	780	697
Deneme09	637	626	588	643	648	632
Deneme10	851	637	1040	615	648	697
Deneme11	626	621	890	626	637	500
Deneme12	649	670	686	648	616	725
Deneme13	703	637	626	648	642	835
Deneme14	598	642	698	593	642	769
Deneme15	615	818	598	665	643	670
Deneme16	868	708	731	769	599	665
Deneme17	637	780	824	901	642	873
Deneme18	632	879	516	664	632	654
Deneme19	626	681	961	753	324	626
Deneme20	753	664	714	714	632	758
Deneme21	714	659	676	604	653	620
Deneme22	648	665	649	643	648	648
Deneme23	642	654	631	631	638	610
Deneme24	918	620	643	626	758	648
Deneme25	654	621	643	786	626	637
Deneme26	604	753	851	890	609	632
Deneme27	714	593	643	802	643	648
Deneme28	786	637	637	637	632	928
Deneme29	653	752	610	643	648	648
Deneme30	753	653	637	642	642	632
Deneme31	615	885	615	627	648	643
Deneme32	698	659	736	834	638	653
Deneme33	626	670	637	709	620	643
Deneme34	664	730	637	884	835	654
Deneme35	643	423	643	665	643	626
Deneme36	648	654	775	983	648	741
Deneme37	884	626	642	637	802	643
Deneme38	692	643	658	648	708	632
Deneme39	676	653	879	615	681	791
Deneme40	670	1104	835	626	835	648
Deneme41	648	808	747	627	643	609
Deneme42	643	791	670	725	621	654
Deneme43	631	708	648	632	637	890
Deneme44	643	643	572	615	631	637
Deneme45	654	626	829	686	643	813
Deneme46	631	637	637	676	637	362
Deneme47	638	577	626	626	703	632
Deneme48	867	763	1165	731	637	753
Deneme49	637	626	626	725	643	642
Deneme50	763	632	577	736	736	654
Deneme51	846	698	616	709	609	725
Deneme52	736	742	631	675	632	648
Deneme53	653	675	637	769	763	643
Deneme54	648	588	598	632	286	659
Deneme55	632	708	720	604	736	637
Deneme56	609	638	621	676	643	632
Deneme57	643	637	631	609	648	571
Deneme58	714	637	615	703	626	763
Deneme59	676	637	638	610	714	533
Deneme60	632	956	631	626	824	643
Deneme61	725	631	615	637	648	626
Deneme62	615	758	862	593	643	637
Deneme63	736	588	654	638	631	643
Deneme64	681	632	764	631	621	615
Deneme65	632	620	862	637	642	631
Deneme66	643	594	615	605	643	775
Deneme67	615	1126	654	582	626	653
Deneme68	626	928	637	549	791	764
Deneme69	648	708	631	599	643	681
Deneme70	648	682	632	637	708	637
Deneme71	593	664	873	609	709	818
Deneme72	665	648	642	775	714	638
Deneme73	769	626	637	808	643	1143
Deneme74	901	868	714	620	823	626
Deneme75	664	643	742	769	638	632
Deneme76	753	698	648	665	615	494
Deneme77	714	643	698	599	715	621
Deneme78	604	961	659	824	642	868
Deneme79	643	654	653	643	1209	637
Deneme80	631	610	654	637	637	648
Deneme81	626	977	642	631	703	637
Deneme82	786	637	615	440	637	599
Deneme83	890	736	676	626	648	719
Deneme84	637	660	752	637	670	632
Deneme85	648	637	632	747	643	708
Deneme86	604	637	538	802	654	637
Deneme87	637	664	610	637	637	659
Deneme88	763	653	1109	643	626	648
Deneme89	769	709	593	642	604	637
Deneme90	742	889	659	627	615	643
Deneme91	719	637	632	834	643	615
Deneme92	654	649	785	709	659	676
Deneme93	653	620	797	884	643	642
Deneme94	637	637	725	665	631	643
Deneme95	649	637	598	983	791	637
Deneme96	648	742	813	637	621	587
Deneme97	643	692	802	648	653	637
Deneme98	654	670	692	632	819	890
Deneme99	753	648	797	670	637	648
Deneme100	637	813	824	791	648	643
Ortalama	685,80	692,21	695,09	681,16	664,93	673,88
Standart Sapma	77,67	108,09	113,50	90,12	94,55	98,32
Varyans	5973,06	11567,63	12753,88	8039,81	8849,89	9570,41
Medyan	651,00	654,00	648,00	643,00	643,00	643,00
Maximum	918	1126	1165	983	1209	1143
Minimum	593	423	516	440	286	362
Mod	643	637	637	637	643	643

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
32 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	840	818	588	769	703	615
Deneme02	649	637	1032	632	637	615
Deneme03	587	659	890	604	648	637
Deneme04	637	642	686	676	670	824
Deneme05	840	637	626	609	643	621
Deneme06	258	709	698	703	654	1065
Deneme07	638	626	598	610	637	626
Deneme08	813	769	731	626	626	637
Deneme09	637	648	824	637	604	1022
Deneme10	769	648	516	593	615	1104
Deneme11	659	835	654	638	643	736
Deneme12	621	632	664	631	659	719
Deneme13	840	632	632	637	643	632
Deneme14	632	637	796	605	631	708
Deneme15	763	626	884	582	791	637
Deneme16	643	632	643	549	621	659
Deneme17	632	638	637	599	653	648
Deneme18	609	681	851	637	819	637
Deneme19	879	637	626	609	637	643
Deneme20	621	615	649	775	648	615
Deneme21	637	769	703	610	698	676
Deneme22	747	643	598	736	659	654
Deneme23	802	632	615	604	653	730
Deneme24	609	648	868	626	654	599
Deneme25	632	648	637	736	642	642
Deneme26	649	631	632	593	615	918
Deneme27	642	643	626	692	676	637
Deneme28	830	632	753	621	752	928
Deneme29	697	632	714	829	632	643
Deneme30	725	626	648	615	538	1087
Deneme31	714	615	642	961	610	808
Deneme32	610	550	918	714	1112	637
Deneme33	615	752	654	676	615	785
Deneme34	637	626	604	649	637	451
Deneme35	626	637	714	631	648	637
Deneme36	637	610	786	643	896	637
Deneme37	638	653	653	643	653	615
Deneme38	823	632	753	851	643	632
Deneme39	627	648	615	643	670	631
Deneme40	626	632	648	637	615	649
Deneme41	692	626	566	610	626	648
Deneme42	631	637	643	637	643	769
Deneme43	627	626	835	615	637	626
Deneme44	637	1060	631	736	796	620
Deneme45	730	769	637	637	637	676
Deneme46	632	1044	632	637	649	621
Deneme47	631	631	752	643	626	637
Deneme48	676	638	797	775	615	632
Deneme49	626	664	620	642	730	615
Deneme50	826	571	632	658	819	648
Deneme51	577	582	802	879	1099	632
Deneme52	632	637	637	835	813	648
Deneme53	637	720	813	747	653	835
Deneme54	631	653	676	670	626	621
Deneme55	676	632	725	648	660	697
Deneme56	648	637	637	572	609	632
Deneme57	637	621	610	829	742	632
Deneme58	604	818	626	637	642	648
Deneme59	824	643	786	637	835	632
Deneme60	626	620	626	714	692	692
Deneme61	627	764	643	763	626	648
Deneme62	620	659	829	698	621	621
Deneme63	632	637	643	747	587	620
Deneme64	615	632	631	637	621	648
Deneme65	802	626	698	599	824	610
Deneme66	632	632	582	730	627	648
Deneme67	725	621	654	654	774	637
Deneme68	637	637	637	637	615	632
Deneme69	577	648	620	807	621	648
Deneme70	790	643	977	648	626	928
Deneme71	638	857	637	643	610	648
Deneme72	708	500	736	626	687	632
Deneme73	626	731	660	626	631	643
Deneme74	896	626	637	627	621	653
Deneme75	631	642	637	626	621	643
Deneme76	758	736	664	758	632	654
Deneme77	604	851	653	631	604	626
Deneme78	610	703	709	632	632	648
Deneme79	736	632	889	873	620	698
Deneme80	626	626	637	632	621	659
Deneme81	659	632	649	626	632	653
Deneme82	615	615	620	637	576	654
Deneme83	594	747	637	335	907	642
Deneme84	620	780	637	637	642	615
Deneme85	637	692	742	1162	648	676
Deneme86	621	620	692	907	703	752
Deneme87	676	626	670	642	631	632
Deneme88	790	627	648	648	649	538
Deneme89	627	725	813	703	802	610
Deneme90	856	697	544	631	642	659
Deneme91	621	769	654	649	610	648
Deneme92	648	643	686	802	653	835
Deneme93	753	796	632	642	582	676
Deneme94	780	670	779	610	736	626
Deneme95	802	626	632	653	835	643
Deneme96	609	643	637	582	780	642
Deneme97	621	747	637	736	879	637
Deneme98	637	632	632	752	681	615
Deneme99	829	620	643	653	664	653
Deneme100	692	642	664	885	632	609
Ortalama	674,67	669,98	687,10	676,75	676,54	677,16
Standart Sapma	90,72	84,00	93,54	101,35	95,82	107,29
Varyans	8147,60	6985,32	8662,89	10169,53	9089,83	11396,35
Medyan	637,00	637,00	648,00	642,00	643,00	643,00
Maximum	896	1060	1032	1162	1112	1104
Minimum	258	500	516	335	538	451
Mod	637	632	637	637	621	648

Büro XP Win FW On						
Open Authentication				Shared Authentication		
Disabled		WEP 64	WEP 128	Disabled	WEP 64	WEP 128
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	2368	2251	2153	2279	2384	2351
Deneme02	2345	2280	2038	2197	2230	2236
Deneme03	2290	2477	2192	2532	2449	2263
Deneme04	2153	2186	2362	2296	2395	2235
Deneme05	1895	2246	2153	1923	2252	2280
Deneme06	2126	1253	2274	2252	1791	2093
Deneme07	2246	2301	2587	2257	2290	1993
Deneme08	2554	2081	2274	2345	2516	2197
Deneme09	2428	2329	2357	2258	2252	2269
Deneme10	2120	2285	2279	2279	2295	2159
Deneme11	2236	2170	1268	2422	2126	2241
Deneme12	2186	2213	2219	2406	2252	2439
Deneme13	2340	2082	2252	2274	2246	2548
Deneme14	2532	2268	2230	2104	2258	2247
Deneme15	1318	2258	2368	2361	1955	2268
Deneme16	2384	2515	2181	2192	2219	2274
Deneme17	2219	2252	2306	2285	2263	2263
Deneme18	2757	2312	2202	2280	2137	2318
Deneme19	2494	2153	2269	2279	2246	2230
Deneme20	2235	2494	1983	2302	2263	2323
Deneme21	2274	2609	2252	2273	2082	2263
Deneme22	2290	2279	2081	2500	2186	2280
Deneme23	2236	2197	1928	2279	2153	2120
Deneme24	2208	2422	2543	2126	2191	2532
Deneme25	2263	2115	2247	2257	2258	2170
Deneme26	2493	2565	2197	2186	1955	2274
Deneme27	2219	2258	2346	2219	2296	2455
Deneme28	2274	2257	2257	2302	2357	2263
Deneme29	2340	2263	2257	2362	2208	2131
Deneme30	2543	2296	2269	2350	2109	2263
Deneme31	2258	2263	2219	1747	2224	2159
Deneme32	2164	2604	2345	2252	2340	2527
Deneme33	2598	2010	2065	2301	2285	2169
Deneme34	1604	1664	2246	2263	2494	2098
Deneme35	2642	2181	2258	2257	1592	2230
Deneme36	2165	2230	2219	2147	2208	2257
Deneme37	2235	2378	2153	2121	2225	2192
Deneme38	2538	2587	2279	2268	2258	2246
Deneme39	2317	2362	1763	2230	2252	2258
Deneme40	2296	2208	2219	2274	2142	2411
Deneme41	2268	2526	2192	2252	2263	2483
Deneme42	2170	2175	2257	2466	2285	1735
Deneme43	1428	1313	2357	2114	2285	2203
Deneme44	2323	2203	2268	2225	2351	2246
Deneme45	2505	2295	2246	2241	2263	2241
Deneme46	2164	2044	2329	2411	2280	2120
Deneme47	2257	2037	2274	2230	2581	2137
Deneme48	2225	2313	1923	2356	2230	2406
Deneme49	2268	2208	2241	2274	2372	2274
Deneme50	2236	2252	2257	2373	2088	2208
Deneme51	2428	1500	2241	2235	2137	2148
Deneme52	2290	2345	2131	2285	2147	2285
Deneme53	2428	2400	2258	2499	2181	2246
Deneme54	2016	2274	2032	2290	2241	2087
Deneme55	2235	2466	1966	2258	2186	2109
Deneme56	2263	2324	2510	2301	2263	2324
Deneme57	2346	2565	2346	2307	2169	2169
Deneme58	2290	2614	2317	2356	2318	2131
Deneme59	2274	2313	2241	2268	2219	2169
Deneme60	2527	2202	2219	2263	2274	1978
Deneme61	2411	2170	2291	2115	1296	2158
Deneme62	2241	2636	2279	2428	2269	2302
Deneme63	2296	2098	2225	1993	2070	2230
Deneme64	1367	2252	1999	2213	2263	2356
Deneme65	2505	2713	2142	2252	2208	2790
Deneme66	2416	2099	2400	2373	2532	2280
Deneme67	2280	2285	2318	2147	2269	2114
Deneme68	2269	2543	2307	2291	2263	2318
Deneme69	2252	2290	2137	2235	2153	1763
Deneme70	2290	1719	2268	1703	1900	2219
Deneme71	2510	2258	2153	2268	2274	2263
Deneme72	2180	2290	2516	2368	2428	2120
Deneme73	2059	2642	2521	2132	2323	2175
Deneme74	2274	2257	2208	2202	2258	2170
Deneme75	2279	2225	2301	1813	2268	2334
Deneme76	2230	2192	2378	2263	2351	2274
Deneme77	2279	2252	2290	2394	2159	2268
Deneme78	2235	2202	2181	2170	2444	1703
Deneme79	2477	2236	2230	2087	2180	2604
Deneme80	2005	2147	2505	2235	2225	2257
Deneme81	2362	2131	2236	2258	2274	2131
Deneme82	2263	2252	2240	2252	2153	2258
Deneme83	2307	2269	2038	2312	2389	2186
Deneme84	2471	2219	2175	2241	2219	2263
Deneme85	2296	2147	2247	2230	2230	2153
Deneme86	2582	2257	2153	2197	2126	2328
Deneme87	2274	2428	2526	2230	2273	2110
Deneme88	2280	1950	2186	2280	2230	2317
Deneme89	2252	2235	2302	2488	1698	2576
Deneme90	1318	2401	2224	2323	2274	2439
Deneme91	2329	2257	2246	2241	2257	2499
Deneme92	2115	2247	2549	2159	2274	2247
Deneme93	2269	2186	2570	2246	2340	2241
Deneme94	2268	2246	2626	2175	2312	2224
Deneme95	2450	2290	2180	2417	2269	2422
Deneme96	2274	2126	2258	2246	2268	2258
Deneme97	2378	1906	2158	2252	2318	1340
Deneme98	2642	2285	2324	2499	1735	2219
Deneme99	1785	2257	2312	2071	2269	2246
Deneme100	2263	2192	2230	2301	2274	2181
Ortalama	2261,57	2243,10	2241,24	2253,41	2220,82	2235,60
Standart Sapma	249,25	234,36	174,26	135,69	179,29	180,97
Varyans	61503,17	54377,19	30063,00	18227,64	31824,75	32421,26
Medyan	2274,00	2257,00	2247,00	2260,50	2258,00	2246,00
Maximum	2757	2713	2626	2532	2581	2790
Minimum	1318	1253	1268	1703	1296	1340
Mod	2274	2252	2153	2252	2263	2263

Büro XP Win FW Off						
Open Authentication				Shared Authentication		
Open - Disabled		WEP 64	WEP 128	Disabled	WEP 64	WEP 128
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	2208	2224	2143	2208	2395	1939
Deneme02	2247	2219	2356	2263	2312	2279
Deneme03	2372	2230	2208	2493	2401	2263
Deneme04	2296	2181	2433	2219	2312	2323
Deneme05	2126	2482	2390	2274	1890	1967
Deneme06	2274	2406	2340	2340	2142	2284
Deneme07	2356	1944	2405	2543	2323	2043
Deneme08	2257	2121	2548	2258	2400	2269
Deneme09	2110	2395	2257	2153	2263	2208
Deneme10	2175	2224	2169	2279	2109	2367
Deneme11	2175	2153	2169	1763	2423	2065
Deneme12	2461	2291	2434	2219	2405	2170
Deneme13	2109	2351	2252	2192	2247	2433
Deneme14	2251	2197	2323	2257	2279	2467
Deneme15	1275	2076	2466	2357	2131	2658
Deneme16	2356	2373	2240	2268	2263	1994
Deneme17	2268	1340	2208	2246	2285	2202
Deneme18	2389	2186	2285	2329	2137	2263
Deneme19	2263	2202	2208	2274	2235	2554
Deneme20	2285	2697	2488	1923	2477	2510
Deneme21	2350	2126	2110	2241	2269	2010
Deneme22	2258	2570	2301	2257	2224	2642
Deneme23	2526	2291	1933	2241	2274	2214
Deneme24	1533	2361	2033	2131	2318	2246
Deneme25	2257	2274	2383	2258	2521	1549
Deneme26	2202	1956	2488	2032	2246	2241
Deneme27	2346	1982	2362	1966	2279	2313
Deneme28	2350	2263	2016	2510	2269	2609
Deneme29	2285	2275	2246	2346	2082	2274
Deneme30	2406	2659	2411	2317	2284	2642
Deneme31	2197	2389	2751	2241	2181	2290
Deneme32	2329	2241	2477	2219	2290	2285
Deneme33	2158	2279	2499	2043	2456	2296
Deneme34	2186	2214	2208	2186	2279	2285
Deneme35	2269	2417	2477	2159	2340	2653
Deneme36	2065	2615	2093	2125	2296	2268
Deneme37	2236	1971	1687	2213	2252	2444
Deneme38	2186	2401	2461	2109	2197	2422
Deneme39	2273	2372	2417	2257	2285	2609
Deneme40	2236	2203	2504	1741	2510	2236
Deneme41	2527	1928	2718	2258	2235	2109
Deneme42	2219	2153	2461	2647	2515	2224
Deneme43	1444	2208	2280	2345	2373	2296
Deneme44	2076	1851	2131	2214	2384	2263
Deneme45	2280	2208	2356	2202	2247	2543
Deneme46	2515	2246	2159	2296	2367	2455
Deneme47	2148	2192	2257	2521	2241	2280
Deneme48	2268	2367	2191	2274	2412	2598
Deneme49	2263	2312	2088	2428	2285	2559
Deneme50	2280	2477	2571	2246	2136	2197
Deneme51	2224	2257	2521	2384	2258	2126
Deneme52	2252	1264	2417	2274	2307	2329
Deneme53	2241	2213	1763	2493	2515	2466
Deneme54	2219	2268	2460	2318	2131	1895
Deneme55	2296	2258	2713	2329	2285	2532
Deneme56	2406	2543	2477	2115	2302	2488
Deneme57	2263	2153	2609	2252	2317	2296
Deneme58	2252	2422	3021	1664	2291	2460
Deneme59	2301	2307	2400	2230	2592	2268
Deneme60	1362	2197	2543	2406	2357	2406
Deneme61	2593	2241	3059	2345	2329	2581
Deneme62	2169	2740	2686	2213	2208	2247
Deneme63	2252	2554	2488	2280	2268	2427
Deneme64	2225	2241	2790	2076	2291	2417
Deneme65	2312	2401	2511	2494	1499	2290
Deneme66	2263	2274	2582	2273	2219	2346
Deneme67	2274	2213	2505	2219	2406	2274
Deneme68	2494	2609	2411	2241	2279	2269
Deneme69	2032	2477	2400	2482	2236	1796
Deneme70	2296	2082	1790	2176	2373	2339
Deneme71	2153	2197	2493	2284	2219	2669
Deneme72	2219	2230	2416	2571	2482	2203
Deneme73	2247	2225	3114	2241	2285	2219
Deneme74	2197	2713	2504	2422	1895	2136
Deneme75	2252	2823	2439	2357	2296	2543
Deneme76	2132	2357	2395	2279	2224	2241
Deneme77	2202	2213	2334	1268	2197	2312
Deneme78	1813	2230	2302	2219	2280	2307
Deneme79	2263	2263	2142	2252	2383	2169
Deneme80	2394	2367	2269	2230	2285	2279
Deneme81	2170	2263	2241	2368	2181	2329
Deneme82	2087	2488	2384	2181	2202	2449
Deneme83	2235	2329	2434	2306	1868	2450
Deneme84	2258	2279	2648	2202	2384	2296
Deneme85	2252	1395	2554	2269	2389	2175
Deneme86	2312	2258	2548	1983	2043	2351
Deneme87	2241	2241	2372	2252	2175	2159
Deneme88	2230	2246	2521	2081	2417	2236
Deneme89	2197	2175	2472	1928	2246	2406
Deneme90	2230	2235	2460	2543	2252	2274
Deneme91	2280	2164	2428	2247	2499	2543
Deneme92	2488	2181	2653	2197	2071	2285
Deneme93	2323	2554	2417	2346	2301	2251
Deneme94	2241	2076	2427	2257	2302	1626
Deneme95	2159	2312	2252	2257	2268	2329
Deneme96	2246	2527	2258	2269	2335	2362
Deneme97	1889	2560	2230	2219	2339	2323
Deneme98	2154	2302	2175	2345	2346	2258
Deneme99	2257	2571	2346	2065	2131	2104
Deneme100	2302	2785	2312	2246	2290	2290
Ortalama	2220,70	2273,66	2380,77	2238,29	2275,24	2301,36
Standart Sapma	204,53	248,66	231,63	187,86	147,95	200,28
Varyans	41412,37	61211,02	53117,74	34936,91	21669,58	39710,19
Medyan	2252,00	2258,00	2402,50	2254,50	2285,00	2287,50
Maximum	2593	2823	3114	2647	2592	2669
Minimum	1275	1264	1687	1268	1499	1549
Mod	2263	2241	2208	2219	2285	2296

Faraday XP_Win FW On						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	1581	2411	2747	2279	2367	2263
Deneme02	2241	2241	2406	2120	2301	1900
Deneme03	2246	2011	2379	2323	2301	2455
Deneme04	2236	2246	2263	2252	2290	2285
Deneme05	2340	2428	2214	2191	2043	2307
Deneme06	2351	2285	2240	2219	2236	2279
Deneme07	2268	1955	2516	2472	2230	2175
Deneme08	2213	2241	1197	2274	2444	2263
Deneme09	2395	2461	2175	1626	2263	2230
Deneme10	1406	2257	2213	2357	2285	2285
Deneme11	2285	2181	2368	2548	2252	2247
Deneme12	2219	2247	2164	2263	2306	2274
Deneme13	2302	2213	2186	2334	2554	2290
Deneme14	2279	2109	2719	2279	1862	2131
Deneme15	2109	2257	2609	2197	2274	2373
Deneme16	2247	1741	2631	2532	2060	2312
Deneme17	2175	2258	2092	2296	2356	2241
Deneme18	2158	2647	2274	1923	2422	2340
Deneme19	1450	2345	2455	2252	2268	2241
Deneme20	2280	2214	2609	2257	2329	2285
Deneme21	2257	2202	2460	2345	2313	1444
Deneme22	2521	2296	2148	2258	2268	2274
Deneme23	2175	2521	2088	2279	2301	2110
Deneme24	2285	2274	2252	2422	2121	2169
Deneme25	2285	2428	2526	2406	2268	2268
Deneme26	2439	2246	2043	2274	2230	2274
Deneme27	2312	2384	2186	2104	2274	2033
Deneme28	1949	2274	2159	2361	2252	2350
Deneme29	2258	2493	2125	2192	2466	2208
Deneme30	2219	2318	2445	2285	2114	1604
Deneme31	2307	2329	2356	2280	2225	2269
Deneme32	2235	2115	2450	2279	2241	2279
Deneme33	2263	2252	2301	2302	2411	2329
Deneme34	2262	1664	2247	2241	2230	2268
Deneme35	2247	2230	1972	2401	2356	2263
Deneme36	2301	2406	2109	2274	2274	2252
Deneme37	2291	2345	2142	2213	2373	2263
Deneme38	2433	2213	2581	2609	2235	2087
Deneme39	2208	2280	2126	2477	2285	2236
Deneme40	2252	2076	2510	2082	2499	2340
Deneme41	2175	2494	2241	2197	2290	2252
Deneme42	2279	2273	2269	2230	2258	2405
Deneme43	2285	2219	2713	2225	2301	2280
Deneme44	2571	2241	2840	2713	2307	2301
Deneme45	2290	2482	2702	2823	2356	2543
Deneme46	2170	2176	2769	2357	2268	2285
Deneme47	1867	2284	2257	2213	2263	2329
Deneme48	2280	2571	2225	2230	2115	2268
Deneme49	2114	2241	2240	2263	2428	1335
Deneme50	2274	2422	2252	2367	1993	2384
Deneme51	2065	2329	1653	2263	2213	2269
Deneme52	2351	2208	2262	2488	2252	2296
Deneme53	2329	2033	2132	2329	2373	2488
Deneme54	2296	2257	2219	2279	2147	2148
Deneme55	2274	2563	2565	1395	2291	2526
Deneme56	2526	2279	2340	2258	2235	2302
Deneme57	2269	2274	2263	2241	1703	2230
Deneme58	2510	2378	2510	2246	2268	2087
Deneme59	2235	2411	2483	2175	2368	2164
Deneme60	1544	1906	1944	2235	2411	2236
Deneme61	2202	2467	2565	2164	2268	2296
Deneme62	2444	2301	2214	2181	2241	1758
Deneme63	2296	2313	2329	2554	2428	2263
Deneme64	2285	2433	2252	2235	2521	2379
Deneme65	2186	2395	2092	2477	2268	2235
Deneme66	2302	2274	2115	2005	1538	2208
Deneme67	2142	2230	2394	2362	2230	2203
Deneme68	2230	2224	2197	2263	2313	2279
Deneme69	1680	1664	1687	2307	2191	2295
Deneme70	2263	2285	2251	2471	2269	2126
Deneme71	2241	2186	2236	2296	2307	1736
Deneme72	2093	2175	2219	2582	2389	2279
Deneme73	2169	2153	2604	2274	2471	2290
Deneme74	2291	2186	2115	2280	2302	2268
Deneme75	2274	2537	2268	2252	1763	2230
Deneme76	2268	1900	2368	1318	2302	2136
Deneme77	2307	2384	1708	2329	2087	2258
Deneme78	2081	2296	2208	2115	2219	2246
Deneme79	2241	2214	2417	2269	2367	2252
Deneme80	2186	2241	2488	2268	2367	1500
Deneme81	2433	2340	2208	2450	2252	2081
Deneme82	2378	2285	2340	2274	2307	2219
Deneme83	2093	2373	2246	2378	2323	2219
Deneme84	2356	2291	2439	2642	2236	2379
Deneme85	2362	1632	2224	2548	1785	2274
Deneme86	2164	2263	2939	2372	2241	2268
Deneme87	2268	2093	2395	2521	2334	2455
Deneme88	2208	2335	2252	2472	2066	2274
Deneme89	2335	2372	2136	2460	2334	1879
Deneme90	2324	2131	2252	2428	2186	2262
Deneme91	2312	2186	2274	2653	2274	2192
Deneme92	2137	2477	2340	2417	2285	2093
Deneme93	2114	2148	2258	2427	2559	2224
Deneme94	2274	2504	2439	2252	1280	2318
Deneme95	2164	2153	1906	2258	2373	2373
Deneme96	2302	2175	2345	2246	2274	2252
Deneme97	1323	2088	2208	2175	2345	2247
Deneme98	2384	2175	2219	2235	2175	2268
Deneme99	2120	2493	2554	2164	2433	2137
Deneme100	2252	2664	2466	2181	2230	2318
Ortalama	2214,68	2261,73	2297,29	2291,60	2251,52	2215,93
Standart Sapma	213,49	187,09	250,64	209,61	188,38	198,04
Varyans	45122,44	34653,48	62192,91	43498,32	35133,81	38828,43
Medyan	2263,00	2268,00	2257,50	2274,00	2274,00	2263,00
Maximum	2571	2664	2939	2823	2559	2543
Minimum	1323	1632	1197	1318	1280	1335
Mod	2285	2241	2252	2279	2268	2268

Faraday XP_Win FW Off						
	Open Authentication			Shared Authentication		
	Open - Disabled	WEP_64	WEP_128	Disabled	WEP_64	WEP_128
64 MB	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**	**Süre**
Deneme01	2433	2208	2126	2554	2225	2504
Deneme02	1230	2258	2246	2241	2241	2439
Deneme03	2142	2422	2554	2401	2411	2395
Deneme04	2175	2252	2428	2274	2230	2334
Deneme05	2691	2395	2120	2213	2356	2302
Deneme06	2143	2236	2236	2609	2274	2142
Deneme07	2279	2455	2186	2477	2373	2269
Deneme08	2159	2235	2340	2082	2235	2241
Deneme09	2153	2461	2532	2197	2285	2384
Deneme10	2247	1401	1318	2230	2499	2434
Deneme11	1631	2279	2384	2225	2290	2648
Deneme12	2323	2120	2219	2713	2258	2554
Deneme13	2598	2323	2757	2823	2301	2548
Deneme14	2263	2252	2494	2357	2307	2372
Deneme15	2065	2191	2235	2213	2356	2521
Deneme16	2543	2219	2274	2230	2065	2472
Deneme17	2488	2472	2290	2263	2159	2460
Deneme18	2483	2274	2236	2367	2153	2428
Deneme19	2186	1626	2208	2263	2247	2653
Deneme20	1879	2357	2263	2488	1631	2417
Deneme21	2142	2548	2493	2329	2323	2427
Deneme22	2515	2263	2219	2279	2598	2252
Deneme23	2120	2334	2274	1395	2263	2258
Deneme24	2521	2279	2340	2258	2065	2230
Deneme25	2099	2197	2543	2241	2543	2175
Deneme26	2219	2532	2258	2246	2488	2346
Deneme27	2114	2296	2153	2175	2483	2312
Deneme28	2444	1923	2279	2235	2186	2230
Deneme29	2044	2252	1763	2164	1879	2285
Deneme30	1516	2257	2219	2181	2142	2247
Deneme31	2098	2345	2192	2554	2515	2274
Deneme32	2246	2258	2257	2076	2120	2290
Deneme33	2170	2279	2357	2312	2521	2131
Deneme34	2136	2422	2268	2527	2099	2373
Deneme35	2582	2406	2246	2560	2219	2312
Deneme36	2268	2274	2329	2274	2114	2241
Deneme37	2054	2104	2274	2493	2444	2340
Deneme38	2373	2361	1923	2318	2044	2241
Deneme39	2054	2192	2241	2329	2285	2285
Deneme40	2225	2285	2257	2115	2373	1444
Deneme41	2169	2280	2241	2252	2291	2274
Deneme42	2082	2279	2131	1664	1632	2110
Deneme43	2263	2302	2258	2230	2263	2169
Deneme44	2219	2273	2032	2406	2093	2268
Deneme45	2395	2500	1966	2345	2335	2274
Deneme46	2180	2279	2510	2213	2372	2033
Deneme47	2170	2126	2346	2280	2131	2350
Deneme48	2169	2257	2317	2076	2186	2208
Deneme49	2165	2186	2241	2494	2477	1604
Deneme50	2191	2219	2219	2273	2148	2269
Deneme51	2147	2302	2043	2219	2504	2279
Deneme52	2071	2362	2186	2241	2153	2088
Deneme53	2230	2350	2159	2482	2175	2137
Deneme54	2186	1747	2125	2176	2088	2147
Deneme55	2339	2252	2445	2284	2197	2181
Deneme56	2296	2301	2356	2571	1687	2241
Deneme57	2269	2263	2450	2241	2251	2186
Deneme58	2224	2257	2301	2422	2236	2263
Deneme59	2225	2147	2247	2329	2219	2169
Deneme60	2180	2285	1972	2208	2604	2318
Deneme61	2329	2302	2109	2033	2115	2219
Deneme62	2263	2280	2142	2257	2268	2274
Deneme63	2268	2488	2581	2565	2368	1296
Deneme64	2236	1164	2126	2279	1708	2269
Deneme65	1280	2236	2510	2274	2208	2070
Deneme66	2258	2202	2241	2378	2417	2263
Deneme67	2142	2257	2269	2411	2488	2208
Deneme68	2455	2522	2713	1906	2208	2532
Deneme69	2340	2367	2840	2340	2340	2269
Deneme70	2186	2252	2702	2285	2521	2263
Deneme71	2103	2202	2769	2494	2208	2153
Deneme72	2538	2274	2257	1592	2301	1900
Deneme73	2104	1747	2225	2208	2378	2274
Deneme74	2197	2202	2240	2225	2290	2428
Deneme75	2136	2362	2252	2258	2181	2323
Deneme76	2219	2258	2202	2252	2230	2258
Deneme77	2565	2224	1813	2142	2505	2268
Deneme78	2258	2291	2263	2263	2236	2351
Deneme79	2268	2279	2394	2285	2240	2159
Deneme80	2219	2137	2170	2285	2038	2444
Deneme81	2571	2262	2087	2351	2175	2280
Deneme82	2164	1346	2235	2263	2247	2383
Deneme83	1922	2263	2258	2280	2153	2285
Deneme84	2307	2164	2252	2581	2526	2181
Deneme85	2543	2274	2312	2230	2186	2202
Deneme86	2115	2258	2241	2372	2302	1868
Deneme87	2433	2356	2230	2088	2224	2384
Deneme88	2120	2428	2197	2137	2246	2389
Deneme89	2389	2284	2230	2147	2549	2043
Deneme90	2148	2269	2273	2307	2570	2175
Deneme91	2307	2109	2230	2323	2626	2417
Deneme92	2389	2422	1698	2236	2180	2246
Deneme93	1961	2395	2274	1785	2258	2291
Deneme94	2394	2290	2257	2241	2158	2274
Deneme95	2274	2313	2274	2334	2324	2268
Deneme96	2164	2230	2340	2066	2285	2307
Deneme97	2549	2285	2312	2334	2373	2081
Deneme98	2307	2279	2269	2186	2291	2241
Deneme99	2257	2252	2268	2274	1632	2186
Deneme100	2219	2301	2318	2285	2263	2433
Ortalama	2221,18	2240,36	2262,49	2272,39	2254,58	2259,33
Standart Sapma	229,94	217,18	207,89	201,36	199,16	197,51
Varyans	52342,19	46695,51	42787,57	40141,70	39267,18	38619,42
Medyan	2219,00	2274,00	2257,00	2268,00	2254,50	2269,00
Maximum	2691	2548	2840	2823	2626	2653
Minimum	1230	1164	1318	1395	1631	1296
Mod	2219	2279	2274	2241	2373	2274

Univariate Analysis of Variance

Warnings

Post hoc tests are not performed for OFFAR because there are fewer than three groups.

Between-Subjects Factors

		N
OFFAR	1,00	1200
	2,00	1200
FAFK	11	600
	12	600
	21	600
	22	600
AKPK	111	300
	112	300
	121	300
	122	300
	211	300
	212	300
	221	300
	222	300
O64128	1111	100
	1112	100
	1113	100
	1121	100
	1122	100
	1123	100
	1211	100
	1212	100
	1213	100
	1221	100
	1222	100
	1223	100
	2111	100
	2112	100
	2113	100
	2121	100
	2122	100
	2123	100
	2211	100
	2212	100
	2213	100
	2221	100
	2222	100
	2223	100

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
1,00	11	111	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			Total	118,2500	43,81507	300

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
1,00	11	112	1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	120,7900	48,83772	300
		Total	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	119,5200	46,37309	600
	12	121	1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			Total	117,8800	43,34152	300
		122	1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	122,3233	45,32719	300
		Total	1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	120,1017	44,36419	600
	Total	111	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			Total	118,2500	43,81507	300
		112	1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	120,7900	48,83772	300
		121	1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			Total	117,8800	43,34152	300
		122	1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	122,3233	45,32719	300
		Total	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	119,8108	45,36177	1200

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
2,00	21	211	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			Total	132,8567	52,44927	300
		212	2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	127,3400	49,45277	300
		Total	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	130,0983	51,00524	600
	22	221	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			Total	123,1633	44,70719	300
		222	2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	113,9533	39,15202	300
		Total	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	118,5583	42,23861	600
	Total	211	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			Total	132,8567	52,44927	300
		212	2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	127,3400	49,45277	300
		221	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			Total	123,1633	44,70719	300
		222	2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	113,9533	39,15202	300

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
2,00	Total	Total	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	124,3283	47,16258	1200
Total	11	111	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			Total	118,2500	43,81507	300
		112	1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	120,7900	48,83772	300
		Total	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	119,5200	46,37309	600
	12	121	1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			Total	117,8800	43,34152	300
		122	1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	122,3233	45,32719	300
		Total	1211	113,9400	42,63797	100
			1212	125,9500	43,20830	100
			1213	113,7500	43,47143	100
			1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	120,1017	44,36419	600
	21	211	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			Total	132,8567	52,44927	300
		212	2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	127,3400	49,45277	300

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
Total	21	Total	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	130,0983	51,00524	600
	22	221	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			Total	123,1633	44,70719	300
		222	2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	113,9533	39,15202	300
		Total	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	118,5583	42,23861	600
	Total	111	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			Total	118,2500	43,81507	300
		112	1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			Total	120,7900	48,83772	300
		121	1211	113,9400	42,63797	100
			1212	125,9600	43,20830	100
			1213	113,7500	43,47143	100
			Total	117,8800	43,34152	300
		122	1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			Total	122,3233	45,32719	300
		211	2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			Total	132,8567	52,44927	300
		212	2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			Total	127,3400	49,45277	300
		221	2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			Total	123,1633	44,70719	300
		222	2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	113,9533	39,15202	300

Descriptive Statistics

Dependent Variable: TIME

OFFAR	FAFK	AKPK	O64128	Mean	Std. Deviation	N
Total	Total	Total	1111	106,2800	31,94695	100
			1112	125,3900	46,82115	100
			1113	123,0800	48,63587	100
			1121	112,6700	41,50528	100
			1122	127,8200	57,44534	100
			1123	121,8800	45,42221	100
			1211	113,9400	42,63797	100
			1212	125,9600	43,20830	100
			1213	113,7500	43,47143	100
			1221	121,2400	45,49550	100
			1222	117,5300	37,82347	100
			1223	128,2000	51,43379	100
			2111	131,8300	53,72452	100
			2112	132,4300	48,83517	100
			2113	134,3100	55,07968	100
			2121	125,1900	46,36519	100
			2122	128,3100	49,25294	100
			2123	128,5200	52,94832	100
			2211	126,5100	43,60602	100
			2212	111,8700	25,89632	100
			2213	131,1100	57,10117	100
			2221	117,6400	42,33047	100
			2222	117,1700	47,09587	100
			2223	107,0500	23,39661	100
			Total	122,0696	46,31642	2400

Levene's Test of Equality of Error Variances[a]

Dependent Variable: TIME

F	df1	df2	Sig.
6,974	23	2376	,000

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept+OFFAR+FAFK+AKPK+O64128+OFFAR * FAFK+OFFAR * AKPK+FAFK * AKPK+OFFAR * FAFK * AKPK+OFFAR * O64128+FAFK * O64128+OFFAR * FAFK * O64128+AKPK * O64128+OFFAR * AKPK * O64128+FAFK * AKPK * O64128+OFFAR * FAFK * AKPK * O64128

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	150946,610[a]	23	6562,896	3,122	,000
Intercept	35762359,620	1	35762359,620	17009,872	,000
OFFAR	,000	0	.	.	.
FAFK	,000	0	.	.	.
AKPK	,000	0	.	.	.
O64128	77431,067	16	4839,442	2,302	,002
OFFAR * FAFK	,000	0	.	.	.
OFFAR * AKPK	,000	0	.	.	.
FAFK * AKPK	,000	0	.	.	.
OFFAR * FAFK * AKPK	,000	0	.	.	.
OFFAR * O64128	,000	0	.	.	.
FAFK * O64128	,000	0	.	.	.
OFFAR * FAFK * O64128	,000	0	.	.	.
AKPK * O64128	,000	0	.	.	.
OFFAR * AKPK * O64128	,000	0	.	.	.
FAFK * AKPK * O64128	,000	0	.	.	.
OFFAR * FAFK * AKPK * O64128	,000	0	.	.	.
Error	4995414,770	2376	2102,447		
Total	40908721,000	2400			
Corrected Total	5146361,380	2399			

a. R Squared = ,029 (Adjusted R Squared = ,020)

Estimated Marginal Means

OFFAR * FAFK * AKPK

Dependent Variable: TIME

OFFAR	FAFK	AKPK	Mean	Std. Error	95% Confidence Interval	
					Lower Bound	Upper Bound
1,00	11	111	118,250[a]	2,647	113,059	123,441
		112	120,790[a]	2,647	115,599	125,981
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.
	12	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	117,880[a]	2,647	112,689	123,071
		122	122,323[a]	2,647	117,132	127,515
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.

OFFAR * FAFK * AKPK

Dependent Variable: TIME

OFFAR	FAFK	AKPK	Mean	Std. Error	95% Confidence Interval	
					Lower Bound	Upper Bound
1,00	21	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.
	22	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.
2,00	11	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.
	12	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	.[b]	.	.	.
		222	.[b]	.	.	.
	21	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	132,857[a]	2,647	127,665	138,048
		212	127,340[a]	2,647	122,149	132,531
		221	.[b]	.	.	.
		222	.[b]	.	.	.
	22	111	.[b]	.	.	.
		112	.[b]	.	.	.
		121	.[b]	.	.	.
		122	.[b]	.	.	.
		211	.[b]	.	.	.
		212	.[b]	.	.	.
		221	123,163[a]	2,647	117,972	128,355
		222	113,953[a]	2,647	108,762	119,145

a. Based on modified population marginal mean.

b. This level combination of factors is not observed, thus the corresponding population marginal mean is not estimable.

Post Hoc Tests

FAFK

Multiple Comparisons

Dependent Variable: TIME
Dunnett T3

(I) FAFK	(J) FAFK	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
11	12	-,5817	2,62000	1,000	-7,4859	6,3226
	21	-10,5783*	2,81425	,001	-17,9946	-3,1621
	22	,9617	2,56078	,999	-5,7866	7,7100
12	11	,5817	2,62000	1,000	-6,3226	7,4859
	21	-9,9967*	2,75975	,002	-17,2694	-2,7239
	22	1,5433	2,50076	,990	-5,0467	8,1334
21	11	10,5783*	2,81425	,001	3,1621	17,9946
	12	9,9967*	2,75975	,002	2,7239	17,2694
	22	11,5400*	2,70359	,000	4,4151	18,6649
22	11	-,9617	2,56078	,999	-7,7100	5,7866
	12	-1,5433	2,50076	,990	-8,1334	5,0467
	21	-11,5400*	2,70359	,000	-18,6649	-4,4151

Based on observed means.
*. The mean difference is significant at the ,05 level.

AKPK

Multiple Comparisons

Dependent Variable: TIME
Dunnett T3

(I) AKPK	(J) AKPK	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
111	112	-2,5400	3,78809	1,000	-14,3965	9,3165
	121	,3700	3,55821	1,000	-10,7664	11,5064
	122	-4,0733	3,63974	1,000	-15,4650	7,3183
	211	-14,6067*	3,94575	,007	-26,9577	-2,2556
	212	-9,0900	3,81459	,387	-21,0296	2,8496
	221	-4,9133	3,61409	,995	-16,2247	6,3980
	222	4,2967	3,39246	,998	-6,3216	14,9149
112	111	2,5400	3,78809	1,000	-9,3165	14,3965
	121	2,9100	3,76989	1,000	-8,8896	14,7096
	122	-1,5333	3,84694	1,000	-13,5737	10,5070
	211	-12,0667	4,13765	,098	-25,0169	,8836
	212	-6,5500	4,01277	,950	-19,1091	6,0091
	221	-2,3733	3,82268	1,000	-14,3379	9,5912
	222	6,8367	3,61386	,814	-4,4762	18,1496
121	111	-,3700	3,55821	1,000	-11,5064	10,7664
	112	-2,9100	3,76989	1,000	-14,7096	8,8896
	122	-4,4433	3,62079	,999	-15,7757	6,8891
	211	-14,9767*	3,92828	,004	-27,2732	-2,6801
	212	-9,4600	3,79652	,305	-21,3432	2,4232
	221	-5,2833	3,59501	,985	-16,5350	5,9683
	222	3,9267	3,37212	1,000	-6,6278	14,4812

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME
Dunnett T3

(I) AKPK	(J) AKPK	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
122	111	4,0733	3,63974	1,000	-7,3183	15,4650
	112	1,5333	3,84694	1,000	-10,5070	13,5737
	121	4,4433	3,62079	,999	-6,8891	15,7757
	211	-10,5333	4,00228	,216	-23,0607	1,9941
	212	-5,0167	3,87304	,998	-17,1388	7,1055
	221	-,8400	3,67573	1,000	-12,3442	10,6642
	222	8,3700	3,45805	,358	-2,4539	19,1939
211	111	14,6067*	3,94575	,007	2,2556	26,9577
	112	12,0667	4,13765	,098	-,8836	25,0169
	121	14,9767*	3,92828	,004	2,6801	27,2732
	122	10,5333	4,00228	,216	-1,9941	23,0607
	212	5,5167	4,16193	,997	-7,5095	18,5428
	221	9,6933	3,97897	,345	-2,7613	22,1480
	222	18,9033*	3,77880	,000	7,0724	30,7342
212	111	9,0900	3,81459	,387	-2,8496	21,0296
	112	6,5500	4,01277	,950	-6,0091	19,1091
	121	9,4600	3,79652	,305	-2,4232	21,3432
	122	5,0167	3,87304	,998	-7,1055	17,1388
	211	-5,5167	4,16193	,997	-18,5428	7,5095
	221	4,1767	3,84894	1,000	-7,8702	16,2236
	222	13,3867*	3,64164	,007	1,9866	24,7868
221	111	4,9133	3,61409	,995	-6,3980	16,2247
	112	2,3733	3,82268	1,000	-9,5912	14,3379
	121	5,2833	3,59501	,985	-5,9683	16,5350
	122	,8400	3,67573	1,000	-10,6642	12,3442
	211	-9,6933	3,97897	,345	-22,1480	2,7613
	212	-4,1767	3,84894	1,000	-16,2236	7,8702
	222	9,2100	3,43104	,188	-1,5292	19,9492
222	111	-4,2967	3,39246	,998	-14,9149	6,3216
	112	-6,8367	3,61386	,814	-18,1496	4,4762
	121	-3,9267	3,37212	1,000	-14,4812	6,6278
	122	-8,3700	3,45805	,358	-19,1939	2,4539
	211	-18,9033*	3,77880	,000	-30,7342	-7,0724
	212	-13,3867*	3,64164	,007	-24,7868	-1,9866
	221	-9,2100	3,43104	,188	-19,9492	1,5292

Based on observed means.
*. The mean difference is significant at the ,05 level.

O64128

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O54128	(J) O54128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1111	1112	-19,1100	5,66818	,214	-40,7271	2,5071
	1113	-16,8000	5,81898	,656	-39,0019	5,4019
	1121	-6,3900	5,23765	1,000	-26,3413	13,5613
	1122	-21,5400	6,57311	,282	-46,6726	3,5926
	1123	-15,6000	5,55318	,736	-36,7715	5,5715
	1211	-7,6600	5,32786	1,000	-27,9597	12,6397
	1212	-19,6700	5,37361	,085	-40,1466	,8066
	1213	-7,4700	5,39479	1,000	-28,0285	13,0885
	1221	-14,9600	5,55918	,840	-36,1547	6,2347
	1222	-11,2500	4,95096	,996	-30,0968	7,5968
	1223	-21,9200	6,05478	,099	-45,0374	1,1974
	2111	-25,5500*	6,25055	,019	-49,4281	-1,6719
	2112	-26,1500*	5,83565	,004	-48,4166	-3,8834
	2113	-28,0300*	6,36740	,005	-52,3625	-3,6975
	2121	-18,9100	5,63058	,222	-40,3813	2,5613
	2122	-22,0300	5,87066	,063	-44,4324	,3724
	2123	-22,2400	6,18396	,108	-45,8593	1,3793
	2211	-20,2300	5,40564	,064	-40,8304	,3704
	2212	-5,5900	4,11245	1,000	-21,2489	10,0689
	2213	-24,8300	6,54305	,055	-49,8457	,1857
	2221	-11,3600	5,30328	,999	-31,5648	8,8448
	2222	-10,8900	5,69090	1,000	-32,5951	10,8151
	2223	-,7700	3,95981	1,000	-15,8606	14,3206
1112	1111	19,1100	5,66818	,214	-2,5071	40,7271
	1113	2,3100	6,75105	1,000	-23,3770	27,9970
	1121	12,7200	6,25692	1,000	-11,0924	36,5324
	1122	-2,4300	7,41093	1,000	-30,6474	25,7874
	1123	3,5100	6,52334	1,000	-21,3104	28,3304
	1211	11,4500	6,33263	1,000	-12,6481	35,5481
	1212	-,5600	6,37117	1,000	-24,8037	23,6837
	1213	11,6400	6,38904	1,000	-12,6714	35,9514
	1221	4,1500	6,52845	1,000	-20,6898	28,9898
	1222	7,8600	6,01900	1,000	-15,0590	30,7790
	1223	-2,8100	6,95532	1,000	-29,2777	23,6577
	2111	-6,4400	7,12639	1,000	-33,5634	20,6834
	2112	-7,0400	6,76542	1,000	-32,7818	18,7018
	2113	-8,9200	7,22910	1,000	-36,4379	18,5979
	2121	,2000	6,58935	1,000	-24,8712	25,2712
	2122	-2,9200	6,79564	1,000	-28,7772	22,9372
	2123	-3,1300	7,06806	1,000	-30,0296	23,7696
	2211	-1,1200	6,39821	1,000	-25,4660	23,2260
	2212	13,5200	5,35055	,938	-6,9396	33,9796
	2213	-5,7200	7,38428	1,000	-33,8348	22,3948
	2221	7,7500	6,31196	1,000	-16,2700	31,7700
	2222	8,2200	6,64096	1,000	-17,0476	33,4875
	2223	18,3400	5,23414	,148	-1,7020	38,3820

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O54128	(J) O54128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1113	1111	16,8000	5,81898	,656	-5,4019	39,0019
	1112	-2,3100	6,75105	1,000	-27,9970	23,3770
	1121	10,4100	6,39386	1,000	-13,9279	34,7479
	1122	-4,7400	7,52690	1,000	-33,3921	23,9121
	1123	1,2000	6,65479	1,000	-24,1222	26,5222
	1211	9,1400	6,46756	1,000	-15,4767	33,7567
	1212	-2,8700	6,50569	1,000	-27,6289	21,8889
	1213	9,3300	6,52320	1,000	-15,4949	34,1549
	1221	1,8400	6,65980	1,000	-23,5011	27,1811
	1222	5,5500	6,16122	1,000	-17,9174	29,0174
	1223	-5,1200	7,07876	1,000	-32,0547	21,8147
	2111	-8,7500	7,24691	1,000	-36,3278	18,8278
	2112	-9,3500	6,89226	1,000	-35,5736	16,8736
	2113	-11,2300	7,34784	1,000	-39,1950	16,7350
	2121	-2,1100	6,71951	1,000	-27,6774	23,4574
	2122	-5,2300	6,92192	1,000	-31,5666	21,1066
	2123	-5,4400	7,18956	1,000	-32,7983	21,9183
	2211	-3,4300	6,53218	1,000	-28,2888	21,4288
	2212	11,2100	5,51005	1,000	-9,8703	32,2903
	2213	-8,0300	7,50066	1,000	-36,5813	20,5213
	2221	5,4400	6,44773	1,000	-19,1005	29,9805
	2222	5,9100	6,77013	1,000	-19,8494	31,6694
	2223	16,0300	5,39708	,569	-4,6465	36,7065
1121	1111	6,3900	5,23765	1,000	-13,5613	26,3413
	1112	-12,7200	6,25692	1,000	-36,5324	11,0924
	1113	-10,4100	6,39386	1,000	-34,7479	13,9279
	1122	-15,1500	7,08707	,999	-42,1619	11,8619
	1123	-9,2100	6,15294	1,000	-32,6240	14,2040
	1211	-1,2700	5,95036	1,000	-23,9102	21,3702
	1212	-13,2800	5,99136	,998	-36,0766	9,5166
	1213	-1,0800	6,01037	1,000	-23,9491	21,7891
	1221	-8,5700	6,15835	1,000	-32,0047	14,8647
	1222	-4,8600	5,61543	1,000	-26,2288	16,5088
	1223	-15,5300	6,60918	,988	-40,6964	9,6364
	2111	-19,1600	6,78897	,723	-45,0198	6,6998
	2112	-19,7600	6,40903	,449	-44,1563	4,6363
	2113	-21,6400	6,89671	,397	-47,9159	4,6359
	2121	-12,5200	6,22288	1,000	-36,2019	11,1619
	2122	-15,6400	6,44092	,974	-40,1588	8,8788
	2123	-15,8500	6,72771	,987	-41,4734	9,7734
	2211	-13,8400	6,02011	,993	-36,7463	9,0663
	2212	,8000	4,89214	1,000	-17,8773	19,4773
	2213	-18,4400	7,05920	,896	-45,3441	8,4641
	2221	-4,9700	5,92837	1,000	-27,5264	17,5864
	2222	-4,5000	6,27751	1,000	-28,3913	19,3913
	2223	5,6200	4,76455	1,000	-12,5942	23,8342

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1122	1111	21,5400	6,57311	,282	-3,5926	46,6726
	1112	2,4300	7,41093	1,000	-25,7874	30,6474
	1113	4,7400	7,52690	1,000	-23,9121	33,3921
	1121	15,1500	7,08707	,999	-11,8619	42,1619
	1123	5,9400	7,32335	1,000	-21,9501	33,8301
	1211	13,8800	7,15399	1,000	-13,3799	41,1399
	1212	1,8700	7,18813	1,000	-25,5166	29,2566
	1213	14,0700	7,20398	1,000	-13,3755	41,5155
	1221	6,5800	7,32790	1,000	-21,3271	34,4871
	1222	10,2900	6,87792	1,000	-15,9515	36,5315
	1223	-,3800	7,71064	1,000	-29,7237	28,9637
	2111	-4,0100	7,86530	1,000	-33,9382	25,9182
	2112	-4,6100	7,53979	1,000	-33,3105	24,0905
	2113	-6,4900	7,95848	1,000	-36,7713	23,7913
	2121	2,6300	7,38221	1,000	-25,4799	30,7399
	2122	-,4900	7,56691	1,000	-29,2924	28,3124
	2123	-,7000	7,81248	1,000	-30,4284	29,0284
	2211	1,3100	7,21211	1,000	-26,1657	28,7857
	2212	15,9500	6,30126	,933	-8,2112	40,1112
	2213	-3,2900	8,09970	1,000	-34,1077	27,5277
	2221	10,1800	7,13671	1,000	-17,0121	37,3721
	2222	10,6500	7,42832	1,000	-17,6325	38,9325
	2223	20,7700	6,20272	,237	-3,0441	44,5841
1123	1111	15,6000	5,55318	,735	-5,5715	36,7715
	1112	-3,5100	6,52334	1,000	-28,3304	21,3104
	1113	-1,2000	6,65479	1,000	-26,5222	24,1222
	1121	9,2100	6,15294	1,000	-14,2040	32,6240
	1122	-5,9400	7,32335	1,000	-33,8301	21,9501
	1211	7,9400	6,22991	1,000	-15,7652	31,6452
	1212	-4,0700	6,26908	1,000	-27,9236	19,7836
	1213	8,1300	6,28724	1,000	-15,7925	32,0525
	1221	,6400	6,42886	1,000	-23,8205	25,1005
	1222	4,3500	5,91083	1,000	-18,1526	26,8526
	1223	-6,3200	6,86193	1,000	-32,4353	19,7953
	2111	-9,9500	7,03527	1,000	-36,7309	16,8309
	2112	-10,5500	6,66937	1,000	-35,9279	14,8279
	2113	-12,4300	7,13929	1,000	-39,6110	14,7510
	2121	-3,3100	6,49069	1,000	-28,0069	21,3869
	2122	-6,4300	6,70002	1,000	-31,9252	19,0652
	2123	-6,6400	6,97618	1,000	-33,1938	19,9138
	2211	-4,6300	6,29656	1,000	-28,5878	19,3278
	2212	10,0100	5,22857	1,000	-9,9751	29,9951
	2213	-9,2300	7,29638	1,000	-37,0161	18,5561
	2221	4,2400	6,20890	1,000	-19,3857	27,8657
	2222	4,7100	6,54309	1,000	-20,1857	29,6057
	2223	14,8300	5,10938	,639	-4,7262	34,3862

Based on observed means.

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1211	1111	7,6600	5,32786	1,000	-12,6397	27,9597
	1112	-11,4500	6,33263	1,000	-35,5481	12,6481
	1113	-9,1400	6,46796	1,000	-33,7567	15,4767
	1121	1,2700	5,95036	1,000	-21,3702	23,9102
	1122	-13,8800	7,15399	1,000	-41,1399	13,3799
	1123	-7,9400	6,22991	1,000	-31,6452	15,7652
	1212	-12,0100	6,07038	1,000	-35,1066	11,0866
	1213	,1900	6,08914	1,000	-22,9781	23,3581
	1221	-7,3000	6,23525	1,000	-31,0256	16,4256
	1222	-3,5900	5,69966	1,000	-25,2815	18,1015
	1223	-14,2600	6,68089	,999	-39,6949	11,1749
	2111	-17,8900	6,85881	,899	-44,0102	8,2302
	2112	-18,4900	6,48295	,693	-43,1643	6,1843
	2113	-20,3700	6,96546	,616	-46,9016	6,1616
	2121	-11,2500	6,29899	1,000	-35,2193	12,7193
	2122	-14,3700	6,51448	,998	-39,1653	10,4253
	2123	-14,5800	6,79818	,999	-40,4665	11,3065
	2211	-12,5700	6,09875	1,000	-35,7747	10,6347
	2212	2,0700	4,98860	1,000	-16,9821	21,1221
	2213	-17,1700	7,12639	,977	-44,3232	9,9832
	2221	-3,7000	6,00822	1,000	-26,5600	19,1600
	2222	-3,2300	6,35297	1,000	-27,4069	20,9459
	2223	6,8900	4,86354	1,000	-11,7093	25,4893
1212	1111	19,6700	5,37361	,085	-,8066	40,1466
	1112	,5600	6,37117	1,000	-23,6837	24,8037
	1113	2,8700	6,50569	1,000	-21,8889	27,6289
	1121	13,2800	5,99136	,998	-9,5166	36,0766
	1122	-1,8700	7,18813	1,000	-29,2566	25,5166
	1123	4,0700	6,26908	1,000	-19,7836	27,9236
	1211	12,0100	6,07038	1,000	-11,0866	35,1066
	1213	12,2000	6,12921	1,000	-11,1204	35,5204
	1221	4,7100	6,27439	1,000	-19,1639	28,5839
	1222	8,4200	5,74245	1,000	-13,4356	30,2756
	1223	-2,2500	6,71743	1,000	-27,8219	23,3219
	2111	-5,8800	6,89440	1,000	-32,1332	20,3732
	2112	-6,4800	6,52061	1,000	-31,2961	18,3361
	2113	-8,3600	7,00052	1,000	-35,0223	18,3023
	2121	,7600	6,33773	1,000	-23,3559	24,8759
	2122	-2,3600	6,55195	1,000	-27,2963	22,5763
	2123	-2,5700	6,83409	1,000	-28,5908	23,4508
	2211	-,5600	6,13876	1,000	-23,9168	22,7968
	2212	14,0800	5,03744	,748	-5,1619	33,3219
	2213	-5,1600	7,16066	1,000	-32,4405	22,1205
	2221	8,3100	6,04882	1,000	-14,7047	31,3247
	2222	8,7800	6,39138	1,000	-15,5411	33,1011
	2223	18,9000*	4,91361	,046	,1058	37,6942

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME
Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1213	1111	7,4700	5,39479	1,000	-13,0885	28,0285
	1112	-11,6400	6,38904	1,000	-35,9514	12,6714
	1113	-9,3300	6,52320	1,000	-34,1549	15,4949
	1121	1,0800	6,01037	1,000	-21,7891	23,9491
	1122	-14,0700	7,20398	1,000	-41,5155	13,3755
	1123	-8,1300	6,28724	1,000	-32,0625	15,7925
	1211	-,1900	6,08914	1,000	-23,3581	22,9781
	1212	-12,2000	6,12921	1,000	-35,5204	11,1204
	1221	-7,4900	6,29254	1,000	-31,4327	16,4527
	1222	-3,7800	5,76227	1,000	-25,7117	18,1517
	1223	-14,4500	6,73439	,999	-40,0856	11,1856
	2111	-18,0800	6,91093	,894	-44,3949	8,2349
	2112	-18,6800	6,53807	,688	-43,5619	6,2019
	2113	-20,5600	7,01679	,610	-47,2830	6,1630
	2121	-11,4400	6,35570	1,000	-35,6239	12,7439
	2122	-14,5600	6,56934	,998	-39,5618	10,4418
	2123	-14,7700	6,85076	,999	-40,8532	11,3132
	2211	-12,7600	6,15731	1,000	-36,1873	10,6673
	2212	1,8800	5,06002	1,000	-17,4497	21,2097
	2213	-17,3600	7,17656	,975	-44,6996	9,9796
	2221	-3,8900	6,06765	1,000	-26,9764	19,1964
	2222	-3,4200	6,40920	1,000	-27,8085	20,9685
	2223	6,7000	4,93677	1,000	-12,1843	25,5843
1221	1111	14,9600	5,55918	,840	-6,2347	36,1547
	1112	-4,1500	6,52845	1,000	-28,9898	20,6898
	1113	-1,8400	6,65980	1,000	-27,1811	23,5011
	1121	8,5700	6,15835	1,000	-14,8647	32,0047
	1122	-6,5800	7,32790	1,000	-34,4871	21,3271
	1123	-,6400	6,42886	1,000	-25,1005	23,8205
	1211	7,3000	6,23525	1,000	-16,4256	31,0256
	1212	-4,7100	6,27439	1,000	-28,5839	19,1639
	1213	7,4900	6,29254	1,000	-16,4527	31,4327
	1222	3,7100	5,91647	1,000	-18,8142	26,2342
	1223	-6,9600	6,86679	1,000	-33,0936	19,1736
	2111	-10,5900	7,04000	1,000	-37,3886	16,2086
	2112	-11,1900	6,67436	1,000	-36,5868	14,2068
	2113	-13,0700	7,14396	1,000	-40,2685	14,1285
	2121	-3,9500	6,49582	1,000	-28,6654	20,7654
	2122	-7,0700	6,70499	1,000	-32,5840	18,4440
	2123	-7,2800	6,98096	1,000	-33,8517	19,2917
	2211	-5,2700	6,30185	1,000	-29,2480	18,7080
	2212	9,3700	5,23494	1,000	-10,6398	29,3798
	2213	-9,8700	7,30096	1,000	-37,6732	17,9332
	2221	3,6000	6,21427	1,000	-20,0462	27,2462
	2222	4,0700	6,54818	1,000	-20,8460	28,9860
	2223	14,1900	5,11590	,766	-5,3916	33,7716

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME
Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1222	1111	11,2500	4,95098	,995	-7,5968	30,0968
	1112	-7,8600	6,01900	1,000	-30,7790	15,0590
	1113	-5,5500	6,16122	1,000	-29,0174	17,9174
	1121	4,8600	5,61543	1,000	-16,5088	26,2288
	1122	-10,2900	6,87792	1,000	-36,5315	15,9515
	1123	-4,3500	5,91083	1,000	-26,8526	18,1526
	1211	3,5900	5,69966	1,000	-18,1015	25,2815
	1212	-8,4200	5,74245	1,000	-30,2756	13,4356
	1213	3,7800	5,76227	1,000	-18,1517	25,7117
	1221	-3,7100	5,91647	1,000	-26,2342	18,8142
	1223	-10,6700	6,38439	1,000	-34,9995	13,6595
	2111	-14,3000	6,57034	,999	-39,3491	10,7491
	2112	-14,9000	6,17696	,977	-38,4281	8,6281
	2113	-16,7800	6,68161	,946	-42,2602	8,7002
	2121	-7,6600	5,98360	1,000	-30,4426	15,1226
	2122	-10,7800	6,21005	1,000	-34,4358	12,8758
	2123	-10,9900	6,50703	1,000	-35,7940	13,8140
	2211	-8,9800	5,77243	1,000	-30,9607	12,9907
	2212	5,6600	4,58392	1,000	-11,8213	23,1413
	2213	-13,5800	6,84920	1,000	-39,7100	12,5500
	2221	-,1100	5,67869	1,000	-21,7135	21,4935
	2222	,3600	6,04039	1,000	-22,6414	23,3614
	2223	10,4800	4,44749	,986	-6,5015	27,4615
1223	1111	21,9200	6,05478	,099	-1,1974	45,0374
	1112	2,8100	6,95532	1,000	-23,6577	29,2777
	1113	5,1200	7,07876	1,000	-21,8147	32,0547
	1121	15,5300	6,60918	,988	-9,6364	40,6964
	1122	,3800	7,71064	1,000	-28,9637	29,7237
	1123	6,3200	6,86193	1,000	-19,7953	32,4353
	1211	14,2600	6,68089	,999	-11,1749	39,6949
	1212	2,2500	6,71743	1,000	-23,3219	27,8219
	1213	14,4500	6,73439	,999	-11,1856	40,0856
	1221	6,9600	6,86679	1,000	-19,1736	33,0936
	1222	10,6700	6,38439	1,000	-13,6595	34,9995
	2111	-3,6300	7,43758	1,000	-31,9294	24,6694
	2112	-4,2300	7,09247	1,000	-31,2167	22,7567
	2113	-6,1100	7,53605	1,000	-34,7855	22,5655
	2121	3,0100	6,92471	1,000	-23,3421	29,3621
	2122	-,1100	7,12130	1,000	-27,2060	26,9860
	2123	-,3200	7,38171	1,000	-28,4063	27,7663
	2211	1,6900	6,74308	1,000	-23,9782	27,3582
	2212	16,3300	5,75852	,707	-5,7176	38,3776
	2213	-2,9100	7,68504	1,000	-32,1556	26,3356
	2221	10,5600	6,66131	1,000	-14,8015	35,9215
	2222	11,0300	6,97386	1,000	-15,5077	37,5677
	2223	21,1500	5,65052	,069	-,5135	42,8135

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2111	1111	25,5500*	6,25055	,019	1,6719	49,4281
	1112	6,4400	7,12639	1,000	-20,6834	33,5634
	1113	8,7500	7,24691	1,000	-18,8278	36,3278
	1121	19,1600	6,78897	,723	-6,6998	45,0198
	1122	4,0100	7,86530	1,000	-25,9182	33,9382
	1123	9,9500	7,03527	1,000	-16,8309	36,7309
	1211	17,8900	6,85881	,899	-8,2302	44,0102
	1212	5,8800	6,89440	1,000	-20,3732	32,1332
	1213	18,0800	6,91093	,894	-8,2349	44,3949
	1221	10,5900	7,04000	1,000	-16,2086	37,3886
	1222	14,3000	6,57034	,999	-10,7491	39,3491
	1223	3,6300	7,43758	1,000	-24,6694	31,9294
	2112	-,6000	7,26030	1,000	-28,2284	27,0284
	2113	-2,4800	7,69422	1,000	-31,7552	26,7952
	2121	6,6400	7,09652	1,000	-20,3710	33,6510
	2122	3,5200	7,28847	1,000	-24,2148	31,2548
	2123	3,3100	7,54311	1,000	-25,3901	32,0101
	2211	5,3200	6,91940	1,000	-21,0266	31,6666
	2212	19,9600	5,96401	,236	-2,8878	42,8078
	2213	,7200	7,84020	1,000	-29,1123	30,5523
	2221	14,1900	6,83973	1,000	-11,8590	40,2390
	2222	14,6600	7,14447	1,000	-12,5315	41,8515
	2223	24,7800*	5,85980	,012	2,3014	47,2586
2112	1111	26,1500*	5,83565	,004	3,8834	48,4166
	1112	7,0400	6,76542	1,000	-18,7018	32,7818
	1113	9,3500	6,89226	1,000	-16,8736	35,5736
	1121	19,7600	6,40903	,449	-4,6363	44,1563
	1122	4,6100	7,53979	1,000	-24,0905	33,3105
	1123	10,5500	6,66937	1,000	-14,8279	35,9279
	1211	18,4900	6,48295	,693	-6,1843	43,1643
	1212	6,4800	6,52061	1,000	-18,3361	31,2961
	1213	18,6800	6,53807	,688	-6,2019	43,5619
	1221	11,1900	6,67436	1,000	-14,2068	36,5868
	1222	14,9000	6,17696	,977	-8,6281	38,4281
	1223	4,2300	7,09247	1,000	-22,7567	31,2167
	2111	,6000	7,26030	1,000	-27,0284	28,2284
	2113	-1,8800	7,36114	1,000	-29,8948	26,1348
	2121	7,2400	6,73396	1,000	-18,3825	32,8625
	2122	4,1200	6,93594	1,000	-22,2699	30,5099
	2123	3,9100	7,20305	1,000	-23,4993	31,3193
	2211	5,9200	6,54703	1,000	-18,9957	30,8357
	2212	20,5600	5,52765	,072	-,5888	41,7088
	2213	1,3200	7,51360	1,000	-27,2799	29,9199
	2221	14,7900	6,46277	,994	-9,8083	39,3883
	2222	15,2600	6,78446	,996	-10,5541	41,0741
	2223	25,3800*	5,41505	,002	4,6335	46,1265

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2113	1111	28,0300*	6,36740	,005	3,6975	52,3625
	1112	8,9200	7,22910	1,000	-18,5979	36,4379
	1113	11,2300	7,34794	1,000	-16,7360	39,1960
	1121	21,6400	6,89671	,397	-4,6359	47,9159
	1122	6,4900	7,95848	1,000	-23,7913	36,7713
	1123	12,4300	7,13929	1,000	-14,7510	39,6110
	1211	20,3700	6,96546	,616	-6,1616	46,9016
	1212	8,3600	7,00052	1,000	-18,3023	35,0223
	1213	20,5600	7,01679	,610	-6,1630	47,2830
	1221	13,0700	7,14396	1,000	-14,1285	40,2685
	1222	16,7800	6,68161	,946	-8,7002	42,2602
	1223	6,1100	7,53605	1,000	-22,5655	34,7855
	2111	2,4800	7,69422	1,000	-26,7952	31,7552
	2112	1,8800	7,36114	1,000	-26,1348	29,8948
	2121	9,1200	7,19965	1,000	-18,2873	36,5273
	2122	6,0000	7,38893	1,000	-22,1195	34,1195
	2123	5,7900	7,64022	1,000	-23,2803	34,8603
	2211	7,8000	7,02514	1,000	-18,9541	34,5541
	2212	22,4400	6,08637	,082	-,8843	45,7643
	2213	3,2000	7,93367	1,000	-26,9867	33,3867
	2221	16,6700	6,94668	,980	-9,7917	43,1317
	2222	17,1400	7,24693	,986	-10,4448	44,7248
	2223	27,2600*	5,98429	,003	4,2966	50,2234
2121	1111	18,9100	5,63058	,222	-2,5613	40,3813
	1112	-,2000	6,58935	1,000	-25,2712	24,8712
	1113	2,1100	6,71951	1,000	-23,4574	27,6774
	1121	12,5200	6,22288	1,000	-11,1619	36,2019
	1122	-2,6300	7,38221	1,000	-30,7399	25,4799
	1123	3,3100	6,49069	1,000	-21,3859	28,0059
	1211	11,2500	6,29899	1,000	-12,7193	35,2193
	1212	-,7600	6,33773	1,000	-24,8759	23,3559
	1213	11,4400	6,35570	1,000	-12,7439	35,6239
	1221	3,9500	6,49582	1,000	-20,7654	28,6654
	1222	7,6600	5,98360	1,000	-15,1226	30,4426
	1223	-3,0100	6,92471	1,000	-29,3621	23,3421
	2111	-6,6400	7,09652	1,000	-33,6510	20,3710
	2112	-7,2400	6,73396	1,000	-32,8625	18,3825
	2113	-9,1200	7,19965	1,000	-36,5273	18,2873
	2122	-3,1200	6,76431	1,000	-28,8585	22,6185
	2123	-3,3300	7,03794	1,000	-30,1162	23,4562
	2211	-1,3200	6,36492	1,000	-25,5388	22,8988
	2212	13,3200	5,31070	,945	-6,9846	33,6246
	2213	-5,9200	7,35546	1,000	-33,9269	22,0869
	2221	7,5500	6,27822	1,000	-16,3408	31,4408
	2222	8,0200	6,60890	1,000	-17,1256	33,1656
	2223	18,1400	5,19339	,153	-1,7433	38,0233

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2122	1111	22,0300	5,87066	,063	-,3724	44,4324
	1112	2,9200	6,79564	1,000	-22,9372	28,7772
	1113	5,2300	6,92192	1,000	-21,1066	31,5666
	1121	15,6400	6,44092	,974	-8,8788	40,1588
	1122	,4900	7,56691	1,000	-28,3124	29,2924
	1123	6,4300	6,70002	1,000	-19,0652	31,9252
	1211	14,3700	6,51448	,998	-10,4253	39,1653
	1212	2,3600	6,55195	1,000	-22,5763	27,2963
	1213	14,5600	6,56934	,998	-10,4418	39,5618
	1221	7,0700	6,70499	1,000	-18,4440	32,5840
	1222	10,7800	6,21005	1,000	-12,8758	34,4358
	1223	,1100	7,12130	1,000	-26,9860	27,2060
	2111	-3,5200	7,28847	1,000	-31,2548	24,2148
	2112	-4,1200	6,93594	1,000	-30,5099	22,2699
	2113	-6,0000	7,38893	1,000	-34,1195	22,1195
	2121	3,1200	6,76431	1,000	-22,6185	28,8585
	2123	-,2100	7,23144	1,000	-27,7267	27,3067
	2211	1,8000	6,57825	1,000	-23,2354	26,8354
	2212	16,4400	5,56459	,586	-4,8526	37,7326
	2213	-2,8000	7,54082	1,000	-31,5022	25,9022
	2221	10,6700	6,49440	1,000	-14,0497	35,3897
	2222	11,1400	6,81460	1,000	-14,7891	37,0691
	2223	21,2600*	5,45276	,039	,3667	42,1533
2123	1111	22,2400	6,18396	,108	-1,3793	45,8593
	1112	3,1300	7,06806	1,000	-23,7696	30,0296
	1113	5,4400	7,18956	1,000	-21,9183	32,7983
	1121	15,8500	6,72771	,987	-9,7734	41,4734
	1122	,7000	7,81248	1,000	-29,0284	30,4284
	1123	6,6400	6,97618	1,000	-19,9138	33,1938
	1211	14,5800	6,79818	,999	-11,3065	40,4665
	1212	2,5700	6,83409	1,000	-23,4508	28,5908
	1213	14,7700	6,85076	,999	-11,3132	40,8532
	1221	7,2800	6,98096	1,000	-19,2917	33,8517
	1222	10,9900	6,50703	1,000	-13,8140	35,7940
	1223	,3200	7,38171	1,000	-27,7663	28,4063
	2111	-3,3100	7,54311	1,000	-32,0101	25,3901
	2112	-3,9100	7,20305	1,000	-31,3193	23,4993
	2113	-5,7900	7,64022	1,000	-34,8603	23,2803
	2121	3,3300	7,03794	1,000	-23,4562	30,1162
	2122	,2100	7,23144	1,000	-27,3067	27,7267
	2211	2,0100	6,85931	1,000	-24,1052	28,1252
	2212	16,6500	5,89419	,718	-5,9259	39,2259
	2213	-2,5900	7,78721	1,000	-32,2217	27,0417
	2221	10,8800	6,77893	1,000	-14,9346	36,6946
	2222	11,3500	7,08629	1,000	-15,6184	38,3184
	2223	21,4700	5,78872	,077	-,7317	43,6717

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2211	1111	20,2300	5,40564	,064	-,3704	40,8304
	1112	1,1200	6,39821	1,000	-23,2260	25,4660
	1113	3,4300	6,53218	1,000	-21,4288	28,2888
	1121	13,8400	6,02011	,993	-9,0663	36,7463
	1122	-1,3100	7,21211	1,000	-28,7857	26,1657
	1123	4,6300	6,29656	1,000	-19,3278	28,5878
	1211	12,5700	6,09875	1,000	-10,6347	35,7747
	1212	,5600	6,13876	1,000	-22,7968	23,9168
	1213	12,7600	6,15731	1,000	-10,6673	36,1873
	1221	5,2700	6,30185	1,000	-18,7080	29,2480
	1222	8,9800	5,77243	1,000	-12,9907	30,9507
	1223	-1,8800	6,74308	1,000	-27,3582	23,9782
	2111	-5,3200	6,91940	1,000	-31,6666	21,0266
	2112	-5,9200	6,54703	1,000	-30,8357	18,9957
	2113	-7,8000	7,02514	1,000	-34,5541	18,9541
	2121	1,3200	6,36492	1,000	-22,8988	25,5388
	2122	-1,8000	6,57825	1,000	-26,8354	23,2354
	2123	-2,0100	6,85931	1,000	-28,1252	24,1052
	2212	14,6400	5,07159	,656	-4,7346	34,0146
	2213	-4,6000	7,18473	1,000	-31,9700	22,7700
	2221	8,8700	6,07730	1,000	-14,2532	31,9932
	2222	9,3400	6,41834	1,000	-15,0830	33,7630
	2223	19,4600*	4,94862	,034	,5295	38,3905
2212	1111	5,5900	4,11245	1,000	-10,0689	21,2489
	1112	-13,5200	5,35055	,938	-33,9796	6,9396
	1113	-11,2100	5,51005	1,000	-32,2903	9,8703
	1121	-,8000	4,89214	1,000	-19,4773	17,8773
	1122	-15,9500	6,30126	,933	-40,1112	8,2112
	1123	-10,0100	5,22857	1,000	-29,9951	9,9751
	1211	-2,0700	4,98860	1,000	-21,1221	16,9821
	1212	-14,0800	5,03744	,748	-33,3219	5,1619
	1213	-1,8800	5,06002	1,000	-21,2097	17,4497
	1221	-9,3700	5,23484	1,000	-29,3798	10,6398
	1222	-5,6600	4,58392	1,000	-23,1413	11,8213
	1223	-16,3300	5,75852	,707	-38,3776	5,7176
	2111	-19,9600	5,96401	,236	-42,8078	2,8878
	2112	-20,5600	5,52765	,072	-41,7088	,5888
	2113	-22,4400	6,08637	,082	-45,7643	,8843
	2121	-13,3200	5,31070	,946	-33,6246	6,9846
	2122	-16,4400	5,56459	,586	-37,7326	4,8526
	2123	-16,6500	5,89419	,718	-39,2259	5,9259
	2211	-14,6400	5,07159	,656	-34,0146	4,7346
	2213	-19,2400	6,26990	,469	-43,2791	4,7991
	2221	-5,7700	4,96235	1,000	-24,7200	13,1800
	2222	-5,3000	5,37461	1,000	-25,8532	15,2532
	2223	4,8200	3,49002	1,000	-6,4612	16,1012

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2213	1111	24,8300	6,54305	,055	-,1857	49,8457
	1112	5,7200	7,38428	1,000	-22,3948	33,8348
	1113	8,0300	7,50066	1,000	-20,5213	36,5813
	1121	18,4400	7,05920	,896	-8,4641	45,3441
	1122	3,2900	8,09970	1,000	-27,5277	34,1077
	1123	9,2300	7,29638	1,000	-18,5561	37,0161
	1211	17,1700	7,12639	,977	-9,9832	44,3232
	1212	5,1600	7,16066	1,000	-22,1205	32,4405
	1213	17,3600	7,17656	,975	-9,9796	44,6996
	1221	9,8700	7,30096	1,000	-17,9332	37,6732
	1222	13,5800	6,84920	1,000	-12,5500	39,7100
	1223	2,9100	7,68504	1,000	-26,3356	32,1556
	2111	-,7200	7,84020	1,000	-30,5523	29,1123
	2112	-1,3200	7,51360	1,000	-29,9199	27,2799
	2113	-3,2000	7,93367	1,000	-33,3867	26,9867
	2121	5,9200	7,35546	1,000	-22,0869	33,9269
	2122	2,8000	7,54082	1,000	-25,9022	31,5022
	2123	2,5900	7,78721	1,000	-27,0417	32,2217
	2211	4,6000	7,18473	1,000	-22,7700	31,9700
	2212	19,2400	6,26990	,469	-4,7991	43,2791
	2221	13,4700	7,10803	1,000	-13,6151	40,5551
	2222	13,9400	7,40173	1,000	-14,2401	42,1201
	2223	24,0600*	6,17085	,040	,3700	47,7500
2221	1111	11,3600	5,30328	,999	-8,8448	31,5648
	1112	-7,7500	6,31196	1,000	-31,7700	16,2700
	1113	-5,4400	6,44773	1,000	-29,9805	19,1005
	1121	4,9700	5,92837	1,000	-17,5864	27,5264
	1122	-10,1800	7,13571	1,000	-37,3721	17,0121
	1123	-4,2400	6,20890	1,000	-27,8657	19,3857
	1211	3,7000	6,00822	1,000	-19,1600	26,5600
	1212	-6,3100	6,04882	1,000	-31,3247	14,7047
	1213	3,8900	6,06765	1,000	-19,1964	26,9764
	1221	-3,6000	6,21427	1,000	-27,2462	20,0462
	1222	,1100	5,67669	1,000	-21,4935	21,7135
	1223	-10,5600	6,66131	1,000	-35,9215	14,8015
	2111	-14,1900	6,83973	1,000	-40,2390	11,8590
	2112	-14,7900	6,46277	,994	-39,3883	9,8083
	2113	-16,6700	6,94668	,980	-43,1317	9,7917
	2121	-7,5500	6,27822	1,000	-31,4408	16,3408
	2122	-10,6700	6,49440	1,000	-35,3897	14,0497
	2123	-10,8800	6,77893	1,000	-36,6946	14,9346
	2211	-8,8700	6,07730	1,000	-31,9932	14,2532
	2212	5,7700	4,96235	1,000	-13,1800	24,7200
	2213	-13,4700	7,10803	1,000	-40,5551	13,6151
	2222	,4700	6,33237	1,000	-23,6282	24,5682
	2223	10,5900	4,83660	,998	-7,9045	29,0845

Based on observed means.

Multiple Comparisons

Dependent Variable: TIME

Dunnett T3

(I) O64128	(J) O64128	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
2222	1111	10,8900	5,69090	1,000	-10,8151	32,5951
	1112	-8,2200	6,64096	1,000	-33,4875	17,0475
	1113	-5,9100	6,77013	1,000	-31,6694	19,8494
	1121	4,5000	6,27751	1,000	-19,3913	28,3913
	1122	-10,6500	7,42832	1,000	-38,9325	17,6325
	1123	-4,7100	6,54309	1,000	-29,6057	20,1857
	1211	3,2300	6,35297	1,000	-20,9459	27,4059
	1212	-8,7800	6,39138	1,000	-33,1011	15,5411
	1213	3,4200	6,40920	1,000	-20,9685	27,8085
	1221	-4,0700	6,54818	1,000	-28,9850	20,8450
	1222	-,3600	6,04039	1,000	-23,3614	22,6414
	1223	-11,0300	6,97385	1,000	-37,5677	15,5077
	2111	-14,6600	7,14447	1,000	-41,8515	12,5315
	2112	-15,2600	6,78446	,996	-41,0741	10,5541
	2113	-17,1400	7,24693	,986	-44,7248	10,4448
	2121	-8,0200	6,60890	1,000	-33,1656	17,1256
	2122	-11,1400	6,81460	1,000	-37,0691	14,7891
	2123	-11,3500	7,08629	1,000	-38,3184	15,6184
	2211	-9,3400	6,41834	1,000	-33,7630	15,0830
	2212	5,3000	5,37461	1,000	-15,2532	25,8532
	2213	-13,9400	7,40173	1,000	-42,1201	14,2401
	2221	-,4700	6,33237	1,000	-24,5682	23,6282
	2223	10,1200	5,25873	1,000	-10,0177	30,2577
2223	1111	,7700	3,95981	1,000	-14,3206	15,8606
	1112	-18,3400	5,23414	,148	-38,3820	1,7020
	1113	-16,0300	5,39708	,569	-36,7065	4,6465
	1121	-5,6200	4,76455	1,000	-23,8342	12,5942
	1122	-20,7700	6,20272	,237	-44,5841	3,0441
	1123	-14,8300	5,10938	,639	-34,3862	4,7262
	1211	-6,8900	4,86354	1,000	-25,4893	11,7093
	1212	-18,9000*	4,91361	,046	-37,6942	-,1058
	1213	-6,7000	4,93677	1,000	-25,5843	12,1843
	1221	-14,1900	5,11590	,766	-33,7716	5,3916
	1222	-10,4800	4,44749	,986	-27,4615	6,5015
	1223	-21,1500	5,65052	,069	-42,8135	,5135
	2111	-24,7800*	5,85980	,012	-47,2586	-2,3014
	2112	-25,3800*	5,41505	,002	-46,1265	-4,6335
	2113	-27,2600*	5,98429	,003	-50,2234	-4,2966
	2121	-18,1400	5,19339	,153	-38,0233	1,7433
	2122	-21,2600*	5,45276	,039	-42,1533	-,3667
	2123	-21,4700	5,78872	,077	-43,6717	,7317
	2211	-19,4600*	4,94862	,034	-38,3905	-,5295
	2212	-4,8200	3,49002	1,000	-18,1012	8,4612
	2213	-24,0600*	6,17085	,040	-47,7500	-,3700
	2221	-10,5900	4,83660	,998	-29,0845	7,9045
	2222	-10,1200	5,25873	1,000	-30,2577	10,0177

Based on observed means.

*. The mean difference is significant at the ,05 level.

EK-5 SPSS Program Çıktıları

Varyans Analiz Sonuçları

Tez CD'si içerisinde sunulmuştur.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: ÖZEL, Mesut
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 24.08.1967 - Konya
Medeni hali	: Evli
Telefon	: 0 (312) 402 56 50
Faks	: 0 (312) 402 56 16
e-mail	: mesutozel@yahoo.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Kara Harp Okulu / Elektrik Elektronik Bölümü	1990
Lise	Maltepe Askeri Lisesi	1986

İş Deneyimi

Yıl	Yer
1990-2005	İçişleri Bakanlığı
2005-Devam	Milli Savunma Bakanlığı

Yabancı Dil

İngilizce

Hobiler

Futbol, Yüzme, Bisiklet, İngilizce, Briç.