KABLOSUZ AĞLARDA ERİŞİM GÜVENLİĞİ VE KİMLİK DOĞRULAMA

Mustafa YILDIRIM

YÜKSEK LİSANS

BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2014

ANKARA

Mustafa YILDIRIM tarafından hazırlanan "KABLOSUZ AĞLARDA ERİŞİM GÜVENLİĞİ VE KİMLİK DOĞRULAMA" adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Suat ÖZDEMİR .....
Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Prof. Dr. M. Ali AKCAYOL .....
Bilgisayar Mühendisliği Anabilim Dalı, GÜ

Doç. Dr. Suat ÖZDEMİR .....
Bilgisayar Mühendisliği Anabilim Dalı, GÜ

Doç. Dr. Süleyman TOSUN .....
Bilgisayar Mühendisliği Anabilim Dalı, AÜ

Tez Savunma Tarihi: 12.02.2014

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Şeref SAĞIROĞLU .....
Fen Bilimleri Enstitü Müdürü

TEZ BİLDİRİMİ

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

Mustafa YILDIRIM

KABLOSUZ AĞLARDA ERİŞİM GÜVENLİĞİ VE KİMLİK DOĞRULAMA

(Yüksek Lisans Tezi)

Mustafa YILDIRIM

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Şubat 2014

ÖZET

Teknolojik gelişmelerin baş döndürücü şekilde ilerlediği çağımızda kablosuz ağ teknolojileri hayatımızın vazgeçilemez bir parçası haline gelmiştir. Gerek yüksek hızlı internet erişim maliyetlerinin düşmesi gerekse kablosuz ağ teknolojisine sahip dizüstü bilgisayar, akıllı cep telefonu, tablet bilgisayarlar gibi taşınabilir cihazların yaygınlaşması hemen her yerden internet erişim imkânı sağlamıştır. Fakat bilginin havada özgürce yolculuk yapabildiği bu ortamlarda güvenlik zafiyetleri de artmıştır. Günümüzde kablosuz yerel alan ağlarında erişim güvenliği ve kimlik doğrulama için kullanılan güvenlik protokolleri profesyonel olmayan saldırganların bile kırabileceği hale gelmiştir. Bu çalışmada kablosuz yerel alan ağlarında erişim güvenliği sağlamak ve kimlik doğrulaması yapmak için 3 farklı güvenlik yöntemi önerilmiştir. Bu yöntemler sırası ile eliptik eğri kriptografisi, mobil imza ve SMS ile tek kullanımlık şifre gönderme tekniklerine dayalı olup günümüzde kullanılan yöntemlere göre daha fazla güvenlik sağlamaktadır. Bu çalışmada kablosuz ağlarda erişim güvenliği ve kimlik doğrulama için ilk kez açık anahtar altyapısına sahip eliptik eğri kriptografisi ile erişim güvenliği ve kimlik doğrulamaya yasal yükümlülük ekleyen mobil imza önerilmiştir. Ayrıca okul, hastane, hava alanı gibi kamuya açık alanlarda ön tanımlamaya ihtiyaç olmaksızın hızlı ve güvenli erişim ve kimlik doğrulama sağlayan tek kullanımlık şifreleme yöntemi önerilmiştir.

Önerilen yöntemler gerçek ortamda uygulanarak çalışabilirlikleri gösterilmiştir.

Bilim Kodu : **902.1.014**
Anahtar Kelime : **kablosuz ağ güvenliği, eliptik eğri kriptografisi, mobil imza, tek kullanımlık şifreleme**
Sayfa Adedi : **72**
Tez Yöneticisi : **Doç. Dr. Suat ÖZDEMİR**

AUTHENTICATION AND ACCESS CONTROL IN WIRELESS NETWORKS

(M.Sc. Thesis)

Mustafa YILDIRIM

GAZİ UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

February 2014

ABSTRACT

Wireless network technologies are become an essential part of our life. The decreasing the costs of high speed internet access as well as widespread usage of internet enabled portable devices such as laptops or smart phone make internet access from nearly everywhere. However, security gaps are increased in this environment where information roams freely over the air. Today, wireless local area network access security and authentication protocols have become breakable even by non-professional attackers. In this study, to provide access security and authentication in wireless local area networks, three different security methods are proposed. These methods are elliptic curve cryptography, mobile signature, SMS and one time password. The proposed methods provide more security than today's methods. To the best of our knowledge, elliptic curve cryptography with public key infrastructure and mobile signature for wireless local area network access are proposed for the first time. Also, one time password method is proposed for access security in the public open areas such as school, hospital and airport. The proposed methods are tested and their applicability is proven.

Science Code : **902.1.014**
Key Words : **wireless security, elliptic curve cryptography, mobile signature, one time password**
Page Number : **72**
Supervisor : **Assoc. Prof. Dr. Suat ÖZDEMİR**

TEŞEKKÜR

Bu tez çalışmasının hazırlanmasında yardımlarını esirgemeyen, sabır ve anlayışla bana daima yol gösteren, destek olan değerli danışman hocam Sayın Doç. Dr. Suat ÖZDEMİR'e teşekkürü bir borç bilirim.

Ayrıca uzakta olsalar da varlığını hep yanımda hissettiğim, yaşamım boyunca benden sevgi ve desteklerini esirgemeyen, zor zamanlardaki en büyük destekçim aileme sonsuz sevgi ve teşekkürlerimi sunarım.

Son olarak, yardım ve anlayışlarından dolayı T.C. Merkez Bankası bünyesindeki mesai arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Kısaltmalar	**Açıklama**
AAA	Açık Anahtar Altyapısı
AES	Advanced Encryption Standard (Gelişmiş Kodlama standardı)
ASP	Active Server Pages (Aktif Sunucu Sayfaları)
CAPTCHA	Completely Automated Public Turing test to tell Computers and Human Apart (İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi)
CMAC	Cipher Based Message Authetication Code (Şifre Tabanlı Mesaj Kimlik Doğrulama)
CC	Common Criteria (Ortak Kriterler)
DES	Data Encryption Standard (Veri Şifreleme Standart)
DoS	Denial of Service (Servis Dışı Bırakma)
DSA	Digital Signature Algorithm (Dijital İmza Algoritması)
EAL	Evaluation Assurance Level (Değerlendirme Garanti Seviyesi)
EAP	Extensible Authentication Protocol (Genişletilebilir Kimlik Doğrulama Protokolü)
ECC	Elliptic Curve Cryptography (Eliptik Eğri Kriptografisi)
ECDSA	Elliptic Curve Digital Signature Algorithm (Eliptik Eğri Dijital İmza Algoritması)
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
ETSI	European Telecommunications Standard Institute (Avrupa Telekomünikasyon Standartlar Komitesi)
GSM	Global System for Mobile Communications (Mobil İletişimler İçin Küresel Sistem)

Kısaltmalar	Açıklama
HMAC	Hash Based Message Authentication Code (Özet Tabanlı Mesaj Doğrulama Kodu)
HSM	Hardware Security Module (Donanımsal Şifreleme Modülü)
HOTP	HMAC based One Time Password (Hmac Bazlı Tek Kullanımlık Şifreleme)
HTTPS	Secure Hypertext Transfer Protocol (Güvenli Hiper Metin Aktarım İletişim Kuralı)
ICV	Integrity Check Value (Bütünlük Kontrol Değeri)
IDEA	International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)
IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IETF	Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü)
IIS	Internet Information Services (İnternet Bilgi Servisleri)
IP	Internet Protocol Address (İnternet Protokol Adresi)
IV	Initial Vector (Başlangıç Vektörü)
MAC	Media Access Control (Ortam Erişim Kontrolü)
MAC	Message Authetication Code (Mesaj Doğrulama Kodu)
MD5	Message-Digest Algorithm (Mesaj Özet Algoritması)
MERNİS	Merkezî Nüfus İdare Sistemi
MIC	Message Integrity Code (Mesaj Bütünlük Kodu)
OATH	Initiative for Open Authentication (Açık Kimlik Doğrulama Girişimi)
ORM	Object Relational Mapping (Nesne ile İlişkisel Haritalama)
OTP	One Time Password (Tek Kullanımlık Şifre)
PDA	Personal Digital Assistant (Kişisel Sayısal Yardımcı)
PKCS	Public Key Cryptography Standards (Açık Anahtarlı Kriptografi Standardı)

Kısaltmalar	Açıklama
PSK	Pre-Shared Key (Ön Paylaşımlı Anahtar)
RADIUS	Remote Authentication Dial-In User Service (Uzaktan Aramalı Kullanıcı Kimlik Doğrulama Servisi)
RC4	Rivest Cipher 4 (Rivest Şifresi 4)
RFC	Request For Comments (Yorumlar için Talep)
RIPEMD	RACE Integrity Primitives Evaluation Message Digest (RACE Bütünlük Asli Mesaj Değerlendirme Özeti)
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm (Güvenli Özetleme Algoritması)
SIM	Subscriber Identity Module (Abone Kimlik Modülü)
SMS	Short Message Service (Kısa Mesaj Hizmeti)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSID	Service Set Identifier (Hizmet Takımı Tanıtıcısı)
SSL	Secure Soket Layer (Güvenli Giriş Katmanı)
TKIP	Temporal Key Integrity Protocol (Geçici Anahtar Bütünlüğü Protokolü)
TOTP	Time based One Time Password Algorithm (Zaman Bazlı Tek Kullanımlık Şifreleme)
URL	Uniform Resource Locator (Tekdüzen Kaynak Bulucu)
USB	Universal Serial Bus (Evrensel Seri Veriyolu)
VPN	Virtual Private Network (Sanal Özel Ağ)
WEP	Wired Equivalent Privacy (Kabloluya Eşdeğer Gizlilik)
WPA	Wi-Fi Protected Access (Wi-Fi Korumalı Erişim)

1. GİRİŞ

Kablosuz ağlar, kablosuz haberleşme yeteneğine sahip cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır [1], Bu ağlar özellikle taşınabilir cihazların artmasına paralel olarak çoğalmıştır. Kablosuz ağ teknolojisi hem pratik hem de kullanışlı olması nedeni ile hayatın vazgeçilmez bir parçası haline gelmiştir. Bu teknoloji iletim ortamı olarak kablolu iletişime göre daha serbest olan havayı kullanmaktadır. İletim ortamının hava olması kullanım kolaylığı getirmekle beraber erişim güvenliği noktasında önemli zafiyetlere sebep olmaktadır.

Kablosuz ağlar farklı frekans aralıkları ve farklı kullanım alanlarına göre 3 sınıfa ayrılmaktadır [1]. Bunlardan ilki kişisel alan ağlarıdır. Kişisel alan ağları 1 ile 20 metre arası mesafeye sahip, düşük iletişim hızına sahip birebir haberleşme için kullanılan ağlardır. En önemli örnekleri kızılötesi (infrared) ve bluetooth'dur. Bir diğer kablosuz ağ sınıfı yerel alan ağlarıdır. Yerel alan ağları IEEE (Institute of Electrical and Electronics Engineers - Elektrik ve Elektronik Mühendisleri Enstitüsü), 802.11 standardı ile tanımlanan, yüksek hızlı iletişime olanak sağlayan, 10 ila 100 metre mesafeye kadar erişim imkanı sağlayan ağlardır. Son kablosuz ağ sınıfı ise geniş alan ağlarıdır. Baz istasyonları üzerinden yaklaşık 50 km kadar alan kaplayarak 75 Mbps'lik hızlara ulaşabilen ağ türüdür.

Kablosuz yerel alan ağlarında erişim güvenliği ve kimlik doğrulama için çeşitli güvenlik seviyelerinde kriptografik yöntemler kullanılmaktadır [2]. Risk seviyesine göre WEP (Wired Equivalent Privacy - Kabloluya Eşdeğer Gizlilik), WPA (Wi-Fi Protected Access - Wi-Fi Korumalı Erişim) gibi erişim kontrolü protokolü ile birlikte kimlik doğrulama amaçlı EAP (Extensible Authentication Protocol - Genişletilebilir Kimlik Doğrulama Protokolü) ve türevleri kullanılmaktadır. Bu önlemlerin yanı sıra yerel alan ağlarında IP (Internet Protocol Address - İnternet Protokol Adresi) veya MAC (Media Access Control - Ortam Erişim Kontrolü) adresi ile filtreleme, SSID (Service Set Identifier - Hizmet Takımı Tanıtıcısı) gizleme gibi çeşitli güvenlik önlemleri de alınmaktadır. Önlemlerin olmasına rağmen bilgisayarların işlem

kapasitesinin artması, internet erişiminin hızlanması, internet korsanlarının (hacker) artması gibi nedenlerle güvenlik açıkları her geçen gün artmaktadır. Özellikle kablosuz yerel alan ağlarına karşı kablosuz ağ dinleme (sniffer), sözlük atakları, erişim noktasına DoS (Denial of Service - Servis Dışı Bırakma) saldırıları, sahte SSID yayını yapma, WEP şifresini kırma için paket toplama, kimlik sahteciliği, MAC adresi sahteciliği veya kaba kuvvet saldırısı gibi birçok saldırı türü ortaya çıkmıştır.

Farklı ölçeklerdeki kuruluşlar farklı hızda ve türde internet erişimine ihtiyaç duyarlar. Artık yüksek hızlarda internet erişimi gerek maliyet gerekse teknoloji açısından daha kolay elde edilebilir hale gelmiştir. İnternet erişimi için kullanılan en önemli teknoloji kablosuz ağ teknolojisidir. Kablosuz ağ teknolojisi ile birlikte dizüstü bilgisayarlar, akıllı telefonlar, tabletler gibi taşınabilir cihazların yaygınlaşması ile hemen hemen her yerde internete erişim imkânı olabilmektedir. Kablosuz ağlara izinsiz erişimi engellemek için günümüzde WEP ya da WPA gibi simetrik anahtar algoritmaları kullanan protokoller ile erişim güvenliği ve kimlik doğrulama sağlanmaktadır. Ancak bu algoritmalar ile ilgili güvenlik zafiyetleri olduğu görülmektedir [3]. Özellikle ziyaretçilerine internet erişim imkânı sunmak zorunda olan kamu kurum ve kuruluşları, hastaneler, üniversiteler gibi yerlerde hem güvenli şekilde kablosuz erişim imkânı sağlamak hem de olası güvenlik açıklarının önüne geçmek için kablosuz yerel alan ağlarında erişim güvenliği ve kimlik doğrulama yöntemlerinin daha etkin olması gerekmektedir.

Kötü amaçlı bir kişinin yetkisiz olarak kablosuz ağa dâhil olması durumunda ağ içerisindeki tüm kullanıcıların bilgi güvenliği tehdit altına girmiş olmaktadır. Dahası bu tip kullanıcılar, ağ içerinde çeşitli saldırılar gerçekleştirerek ağın internet erişimini ya da ağ içerisindeki veri alışverişini engelleyebilmektedir [4]. Sonuç olarak kişi ve kuruluşlar maddi ve/veya manevi zararlara uğrayabilmektedir. Bu gibi tehlikelere karşı alınacak en önemli önlem saldırgan kişilerin daha ağa dâhil olmadan erişimlerini engellemek ve kimliklerini tespit etmektir.

Bu bağlamda kablosuz yerel alan ağına erişimi daha kolay ve güvenli hale getirebilmek ve etkin kimlik doğrulama protokolleri kullanabilmek için yeni güvenlik teknolojilerinden faydalanılması gerekmektedir.

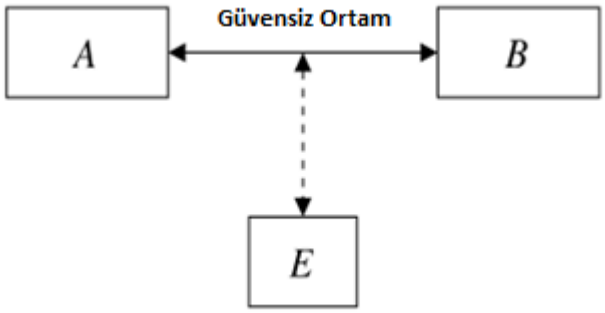
Bu tez çalışmasında kablosuz yerel alan ağlarında erişim güvenliğini sağlamak ve kimlik doğrulaması yapmak için 3 farklı güvenlik yöntemi geliştirilmiştir. Bu yöntemlerden ilki yakın zamanda literatürde yerini alan küçük boyutta anahtar kullanmasına rağmen güçlü bir güvenlik sağlayan AAA (Açık Anahtar Altyapısına) dayanan ECC (Elliptic Curve Cryptography - Eliptik Eğri Kriptografisi) temelli yöntemdir [5]. Bir diğeri ise elektronik imza sürecini cep telefonu ve özel SIM (Subscriber Identity Module - Abone Kimlik Modülü) kartlar ile gerçekleştiren mobil imza [6] teknolojisidir. Son olarak cep telefonuna tek kullanımlık şifre göndererek kablosuz yerel alan ağına erişim kontrolü ve kimlik doğrulama sağlayan sistem geliştirilmiştir.

Tezin kalan kısmı şu şekilde düzenlenmiştir; 2. Bölümde modern kriptografik yöntemler açıklanmıştır. Simetrik, asimetrik anahtarlı yöntemler incelenmiş, birbirleri ile karşılaştırılarak avantaj ve dezavantajları ortaya konulmuştur. Simetrik ve asimetrik anahtarlı yöntemleri birleştiren hibrit yöntem açıklanmıştır 3. Bölümde kablosuz ağ erişim güvenliği ve kimlik doğrulama için kullanılan WEP ve WPA protokolleri açıklanmıştır. Protokollerin şifreleme algoritmaları, bütünlük kontrol sistemleri, kimlik doğrulama yöntemlerinin yanında güvenlik zafiyetleri de ortaya konulmuştur. 4. Bölümde eliptik eğri kriptografisi üzerinde durulmuştur. Eğrinin matematiksel temelleri olan grup, halka, alan gibi tanımlar açıklanmış, eğri üzerinde toplama ve çarpma işlemleri gerçekleştirilmiştir. Eliptik eğri kullanılarak şifreleme ve deşifreleme incelenmiştir. Eliptik eğri kriptografisinde Diffie-Hellman anahtar değişim protokolünün uygulanması gösterilmiştir. 5. Bölümde mobil imza senaryosu ve mobil imza altyapısı kullanılarak erişim güvenliği ve kimlik doğrulama sağlanmasının faydaları açıklanmıştır. 6. Bölümde tek kullanımlık şifrelemenin çalışma prensibi özetlenmiş. MAC (Message Authetication Code - Mesaj Doğrulama Kodu) [7], HMAC (Hash Based Message Authentication Code - Özet Tabanlı Mesaj Doğrulama Kodu) [8], HOTP (HMAC based One Time Password - HMAC Bazlı Tek

Kullanımlık Şifreleme) [8], TOTP (Time Based One Time Password Algorithm - Zaman Bazlı Tek Kullanımlık Şifreleme) [9] gibi algoritmalar açıklanmıştır. 7. Bölümde eliptik eğri kriptografisi ve tek kullanımlık şifreleme algoritmaları kullanılarak erişim güvenliği ve kimlik doğrulama gerçekleştiren tez uygulaması açıklanarak performans değerlendirmelerinde bulunulmuştur. Günümüzde kullanılan WEP ve WPA gibi protokoller ile kıyaslanmış, getirdiği yenilikler ve güvenlik avantajları üzerinde durulmuştur. Tez uygulaması geliştirilirken alınan diğer önlemler olan ECC ile üretilmiş SSL (Secure Soket Layer - Güvenli Giriş Katmanı) sertifikası, CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart - İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) testi ve SQL (Structured Query Language - Yapılandırılmış Sorgu Dili) enjeksiyonu gibi güvenlik mekanizmaları özetlenmiştir. Sonuç bölümünde ise yeni önerilen güvenlik mekanizmalarının avantajları vurgulanmıştır.

2. KRİPTOGRAFİK SİSTEMLER

Kriptografi bilginin güvenli iletimini sağlamak için geliştirilen matematiksel yöntemler olarak tanımlanabilir. Kelime yunanca saklı, gizli anlamına gelen "kryptein" ile yazmak anlamına gelen "graphein" kelimelerinin birleşiminden oluşmaktadır [10].



Şekil 2.1. Temel iletişim modeli

Yukarıdaki şekil kriptografinin kullanıldığı temel iletişim modelini göstermektedir. Şekil 2.1'de A ve B iletişim kurmak istemektedir fakat iletişim kanalı güvensizdir. Burada A ve B cep telefonu aracılığı ile iletişim kurmak isteyen 2 kişi ise E bu konuşmayı dinlemek isteyen kötü amaçlı bir kişi olabilir veya A bir web tarayıcısı aracılığı alışveriş yapmak isteyen biri ise B bir alışveriş sitesi olabilir ve E internet üzerindeki trafiği dinleyen bir yazılım olabilir. E, A kullanıcısına ait kredi kartı bilgilerini ele geçirebilir. Başka bir senaryo ise A internet üzerinden B'ye e-posta göndermek isteyen bir kişi ise E bu e-postayı B'ye ulaşmadan yakalayıp okuyabilen veya üzerinde değişiklik yapan bir saldırgan olabilir. Son senaryo ise A bir kullanıcının banka hesabına ulaşabilmesi için kullanılan bir akıllı kart iken, B bankaya ait sunucu olabilir. Bu durumda E iletim hattını monitörleyerek kullanıcıya ait hesap bilgilerini ele geçirmeye çalışan bir bilgisayar korsanı olabilir [11].

Yukarıdaki senaryolarda da görüldüğü gibi iletişim sırasında güvensiz bir kanal kullanmak telafisi mümkün olmayan büyük problemlere neden olabilmektedir. Kriptografi biliminin temel amacı insanların bu senaryolardaki gibi olumsuzluklarla

karşılaşmasını engellemektir. Bunu yaparken çok farklı algoritmalar kullansa bile temelde şu şekilde bir yol izler; gönderici alıcıya iletmek istediği açık veriyi güvensiz haberleşme ortamına yollamadan önce karar verilmiş bir anahtar veya herhangi bir kriptografik yöntem yardımı ile şifreler. Şifreleme işlemi tamamlandıktan sonra şifreli veri haberleşme kanalı aracılığıyla alıcıya gönderilir. Şifreli veri haberleşme ortamında üçüncü kişilerin eline geçse bile bir şey ifade etmemektedir. Çünkü veri sadece doğru anahtara sahip alıcı tarafından açık veriye çevrilebilir.

Yukarıda bahsedilen kriptografik sistemlerin sağlaması gereken temel özellikler aşağıda sıralanmıştır [12] [13];

Gizlilik: Kısaca veriyi görmeye yetkili herkesin görmesi, görme izni olmayan hiç kimsenin görememesi olarak özetlenebilir.

Bütünlük: Verinin sadece yetkili kullanıcılar tarafından değiştirilebilmesi, bunun dışında kalanların ise verinin bütünlüğünü bozamamasıdır. Bütünlük kavramı verinin değiştirilmesini, fazladan veri eklenmesini, var olan verinin bir kısmının veya tamamının değiştirilmesini, silinmesini kapsar. Kriptografi biliminde bütünlüğü sağlamanın önemi kadar bütünlüğü bozulmuş verinin tespiti de önemlidir. Özellikle özet (hash) fonksiyonları burada kullanılmaktadır.

İnkâr Etmeme (Reddedilemezlik): Tarafların gönderdikleri veriler veya yaptıkları işlemleri inkâr edememesidir. Bir başka ifade ile göndericinin veriyi kendisinin gönderdiğini inkâr edememesi, aynı şekilde alıcının da aldığı veriyi inkâr edememesidir.

Kimlik Doğrulama: Gönderici ve alıcının karşılıklı kimliklerini doğrulayabilmeleridir.

Erişim Kontrolü: Erişim izni olmayan üçüncül kişi veya uygulamaların güvenli ortamdaki kaynaklara ulaşa”mayacağı garantisidir. Erişim kontrolü sağlanması için

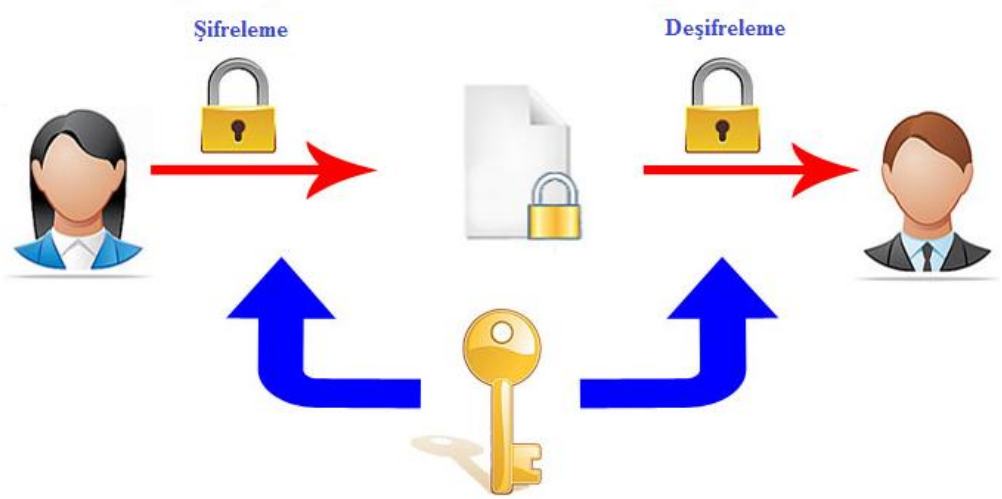
erişim sağlamaya çalışan her varlık tanınmalı ve kaynaklardan sadece kendisine izin verilen şekilde yararlanması sağlanmalıdır.

Erişilebilirlik: Erişime özel olarak yetkilendirilmiş kişilerin ihtiyaç duydukları anda gerekli bilgiye veya hizmete ulaşabilir ve kullanılabilir olması garantisidir.

Yukarıda bahsedilen özellikler kriptografik algoritmalar ile sağlanmaktadır. Günümüzde yaygın olarak kullanılan algoritmalar genel olarak şifrelemede kullanılan anahtarın özelliklerine göre iki gruba ayrılmıştır. Bunlar simetrik ve asimetrik anahtarlı kriptografi olarak isimlendirilmektedir.

2.1. Simetrik Anahtarlı Kriptografi

1940'lı yılların sonlarında Caulde Shannon'un yayınladığı teorik makale simetrik veya gizli anahtarlı şifrelemenin temellerini oluşturmuştur. Bu çalışma simetrik anahtarlama yöntemi birçok modern kriptografi sistemin temeli olmuştur [14]. Simetrik anahtarlı sistemler tek, gizli anahtarlı kriptografi sistemleri olarak da adlandırılmaktadır. Şekil 2.2'de görüldüğü gibi bu sistemde gönderici ve alıcı taraf aynı anahtarla veya bir anahtardan diğeri kolaylıkla elde edilebilecek anahtarlarla hem şifreleme hem de deşifreleme yapılmaktadır. Kullanılan bu anahtara gizli anahtar (secret key) denilmektedir.



Şekil 2.2. Simetrik anahtarlı kriptografi

Simetrik anahtarlı yöntemler blok ve akan şifreleme olarak iki gruba ayrılmaktadır [15].

2.1.1. Blok şifreleme

Blok şifreleme şifrelenecek veriyi sabit uzunluklara bloklara bölerek belirlenmiş simetrik anahtarla şifrelenmesidir. Blok şifreleme ile şifrelenmek istenen veri seçilen blok uzunluğunun tam katı değil ise veriye yeterli sayıda anlamsız bitler eklenerek tamamlanır. Veriden oluşturulan bloklar bir döngü ile ayrı ayrı şifrelenir. Özellikle büyük boyuttaki verilerin şifrelenmesinde tercih edilir. Blok şifrelemenin en dikkate değer örnekleri AES (Advanced Encryption Standard - Gelişmiş Kodlama standardı) [16], DES (Data Encryption Standard - Veri Şifreleme Standart) [17], ve IDEA (International Data Encryption Algorithm- Uluslararası Veri Şifreleme Algoritması) [18] algoritmalarıdır.

2.1.2. Akan şifreleme

Akan şifreleme her bir adımda şifrelenecek veriye ait bir biti şifrelemektedir. Akan şifreleme yüksek hızlı iletişim için en iyi yöntemlerden biridir. Özellikle donanımsal şifrelemede blok şifrelemeye göre oldukça iyi performans göstermektedir. En temel

örnekleri RC4 (Rivest Cipher 4 - Rivest Şifresi 4) [19], A5/1 [20], A5/2 [20], Panama [21], algoritmalarıdır.

RC4 algoritması 1987 yılında RSA (Rivest, Shamir, Adleman) [22] Security firmasından Ron Rivest tarafından geliştirilmiştir. Algoritma 1994 yılına kadar şirketin ticari sırı olarak kalmış bu tarihten sonra açıklanmıştır. RC4 algoritması şifreleme yapabilmek için sözde rastlantısal sayı üreteçlerinden yararlanır. Bu üreteç tahmini zor sayı dizisi üretir. Üretilen sözde rastlantısal sayı dizisi ile açık metin bit bazında XOR işlemine tabi tutularak şifreleme işlemi yapılır. Şifre çözme işlemi de aynı şekilde şifreli metne XOR işlemi uygulanarak elde edilir.

Simetrik anahtarlı sistemlerin bir kısım zayıf yönleri bulunmaktadır. Bu sistemlerde güvenlik anahtar boyu ile orantılıdır. Örneğin 90'lı yıllara kadar güveli olarak bilinen DES algoritması ile üretilen 56 bit uzunluğundaki anahtar, 1998 yılında yayınlanan "Cracking DES" kitabında kaba kuvvet saldırısı ile birkaç gün içinde kırılabileceği ortaya konulmuştur. 56 bitlik DES algoritması yerine 168 bitlik Triple DES [23] algoritması önerilmiştir. Bir diğer çalışma Distributed.net ve gönüllüleri tarafında yapılan birkaç yıl süren ve binlerce kişisel bilgisayarın kullanılması ile gerçekleştirilen çalışma ile 64 bitlik anahtar boyuna sahip RC5 algoritmasının da kırılabileceği ortaya konulmuştur. Bu nedenle anahtar boyu yeterli uzunlukta seçilmesi gerekmektedir. Bir diğer problem ise kimlik doğrulama ve verinin bütünlüğünün sağlanmasındaki güçlüktür. Simetrik anahtarlı şifrelemede asimetrik anahtarlı şifrelemede olduğu gibi göndericiye ait özel anahtar olmayıp, hem gönderici hem de alıcı aynı anahtar ile işlem yapmaktadır. Göndericinin kimliğini anahtar ile doğrulayabilecek bir mekanizma simetrik anahtarlı sistemlerde mevcut değildir. Simetrik anahtarlı sistemlerin haberleşmede kullanılmasında en büyük zafiyet ise anahtarın taraflar arasında güvenli bir şekilde paylaşılmasıdır. Günümüz elektronik iletişiminde hemen hemen tüm ortamlar güvensiz sayılmakta, ayrıca insanlar daha önce hiç iletişim kurmadıkları kişiler veya sistemlerle güvenli iletişim kurma ihtiyaçları olmaktadır. Bu ihtiyacın giderilmesinde aynı anahtar ile güvenlik sağlayan simetrik anahtarlı algoritmanın anahtar paylaşımı problemi doğmaktadır.

Anahtar paylaşımı problemine çözüm 1977 yılında Diffie ve Hellman tarafından önerilmiş olan yöntemle aşılmıştır [24].

2.2. Asimetrik Anahtarlı Kriptografi

Asimetrik diğer bir ismiyle açık anahtarlı kriptografik sistemlerde şifreleme ve şifre çözme için kullanılan anahtarlar birbirinden farklıdır. Bu tür sistemlerde her kullanıcının açık ve özel olmak üzere bir çift anahtarı vardır. Bu anahtarların en önemli özelliği anahtarlardan hiçbiri hem şifreleme hem de şifre çözme işleminde kullanılamaz. Anahtarlardan birinin şifrelediğini ancak ve ancak diğer anahtar açmaktadır. Bu anahtarlardan açık olanı herkes tarafından bilinmektedir. Özel anahtar ise yalnızca anahtar sahibi tarafından bilinmektedir. Ayrıca bir kişiye ait açık anahtardan yola çıkarak özel anahtarının hesaplanması teorik olarak çok zordur. Bu zorluğu anahtarlar arasındaki çarpanlara ayırma veya ayrık logaritma problemlerinin çözüm güçlüğü gibi matematiksel yöntemler sağlamaktadır [25].

Asimetrik anahtarlı kriptografi yönteminin getirdiği en büyük avantaj, daha önce hiç bir araya gelip ortak gizli anahtar belirlemeyen tarafların, güvensiz iletişim ortamında güvenli bir iletişim kurabilmesini sağlamasıdır. Şekil 2.3'deki örnekte daha önce hiçbir bağlantısı olmayan A ve B kişisi internet gibi güvenli olmayan bir ortamda gizli bir metin paylaşmak istemektedir. A metni önce kendi özel anahtarı ile daha sonrada B'nin herkes tarafından bilinen açık anahtarı ile şifreler ve internet üzerinden şifreli metni B kullanıcısına gönderir. Böylelikle yalnızca B kullanıcısının açabileceği bir şifreli metin oluşturulmuş olmaktadır. Gönderim sırasında şifreli metin üçüncül kişilerin eline geçse dahi şifreyi çözebilmesi için B kullanıcısının özel anahtarına sahip olması gerekmektedir fakat herkes B kullanıcısının sadece açık anahtarını bilebilmekte ve açık anahtardan özel anahtarı tahmin etme ihtimali olmamaktadır. Şifreli metni alan B kullanıcısı ise öncelikle kendi özel anahtarı ile daha sonrada A'nın açık anahtarı ile şifreli metni açık metne çevirebilmektedir. Şifreli metin sadece A kullanıcısının açık anahtarı ile düz metne çevrilebildiğinde gönderenin A kullanıcısı olduğuna dairde kimlik doğrulaması yapılmış olmaktadır.

Şekil 2.3. Asimetrik anahtarlı kriptografi

Asimetrik anahtarlı kriptografik sistemlerin diğer bir önemli kullanım alanı ise elektronik imza teknolojisidir. Elektronik imza sistemleri asimetrik anahtarlı şifrelemenin tam tersi şekilde çalışmaktadır. Kişi imzalaması gereken dokümanı sadece kendisinin bildiği özel anahtarı ile imzalarken, bu imzanın kime ait olduğunu öğrenmek isteyen diğer kullanıcılar, kişinin açık anahtarı ile imzayı doğrulaya bilmektedir [26]. İmzanın doğası gereği imzalanan metnin gizliliği değil metni kimin imzaladığı önemlidir. Özel anahtarı ile imzalanan metin kişinin herkes tarafından bilinen açık anahtarını üzerinde barındıran elektronik sertifika ile doğrulanmaktadır. Aynı yöntem asimetrik anahtarlı sistemlerde kimlik tespiti için kullanılabilmektir.

Asimetrik anahtarlı algoritmalardan modern kriptografik sistemlerde de kullanılan en önemli örnekleri RSA, DSA (Digital Signature Algorithm - Dijital İmza Algoritması) [27], Diffie-Hellman [28], ElGamal [28], ve ECC algoritmalarıdır. Bu yöntemlerden RSA algoritması tamsayıların çarpanlarına ayrılmasına dayanan yöntem ile DSA, Diffie-Hellman, ElGamal ve ECC ise ayrık logaritma problemine dayanarak şifreleme yapmaktadır [22] [29]. Algoritmaların matematiksel yöntemleri farklı olsa bile hemen hepsi büyük sayılar (özellikle asal sayılar) üzerindeki karmaşıklıktan

yararlanmaktadır. Bu algoritmalardan günümüzde en sık kullanılanlarından RSA algoritmasını bir örnekle açıklamak gerekirse [5]:

İki adet çok büyük asal sayı (p, q) seçilir. Seçilen asal sayıların büyüklüğü şifrelemenin gücünü gösterir.

p = 23 ve q = 41 iki asal sayı alınır.
N: Açık anahtar olmak üzere;
N = p * q = 23 * 41 = 943
(p - 1) * (q - 1) ile aralarında asal olan bir adet e sayısı seçilir.
(p - 1) * (q - 1) = 22 * 40 = 880 ile arasında asal olan 7 sayısı e olarak seçilir.
Şifrelemek istenilen mesaj 35 sayısı olsun;
C: Şifreli mesaj
$C = M^e \bmod N = 35^7 \bmod 943 = 545$

Şifreli metni açmak için önce özel anahtarımızı hesaplıyoruz;
d: Özel anahtar
e * d =1 mod (p - 1) * (q - 1)
7 * d = 1 mod (880) ise d = 503 olur.
Şifreli metni çözme için
M: Açık metin
$M = C^d \bmod N = 545^{503} \bmod 943 = 35$

2.3. Simetrik ve Asimetrik Anahtarlı Algoritmaların Karşılaştırılması

Simetrik ve asimetrik anahtarlı sistemler kıyaslandığında her ikisinin de avantaj ve dezavantajları olduğu görülmektedir. Asimetrik anahtarlı sistemlerin simetrik anahtarlı sistemlere kıyasla avantajlı olduğu yönlere bakacak olursak, asimetrik yöntemde her kullanıcının gizli tutması gereken sadece bir adet özel anahtarı varken, simetrik yöntemde (n) adet kullanıcı var ise her kullanıcı için gizli tutulması gereken (n - 1) adet anahtar vardır. Bu da anahtarın saklanması gereken güvenli depolama

alanının yükünü artırmaktadır. Asimetrik yöntemin bir diğer önemli avantajı ise anahtar paylaşımı için güvenli bir iletişim ortamına ihtiyacın olmamasıdır. Böylelikle güvensiz bir iletim ortamında olan iki kişi daha önce aralarında hiçbir ortak anahtar veya sır paylaşmamış olmalarına rağmen güvenli bir şekilde haberleşebilmektedirler. Bu yöntem kullanılarak dünyanın neresinde olursa olsun daha önce hiç görüşmediğimiz kişilerle internet gibi güvensiz ortam üzerinden güvenli iletişim kurabilmemize olanak sağlamaktadır.

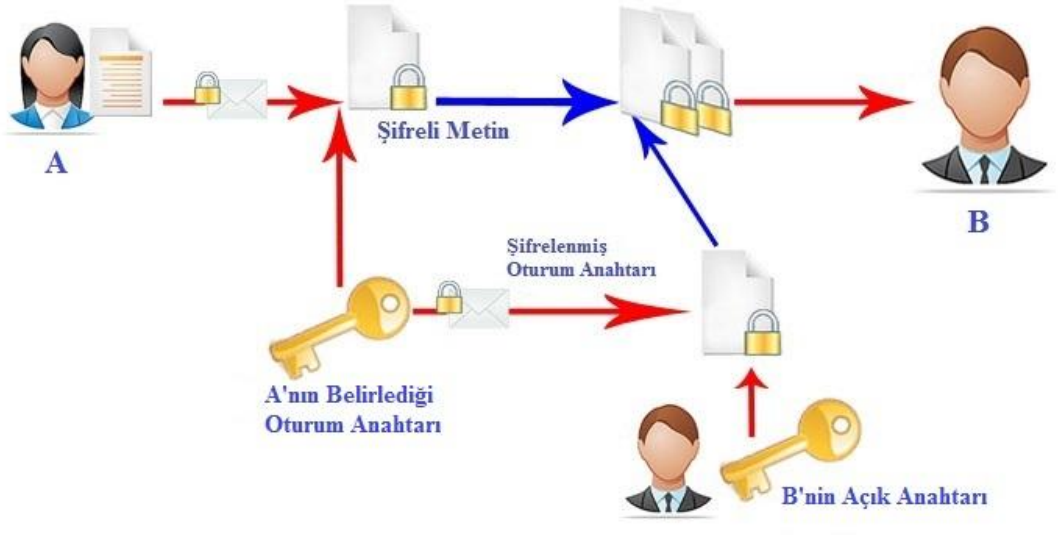
Asimetrik anahtarlı yöntemlerin simetrik yöntemlere göre dezavantajlarının en önemlisi asimetrik anahtarlı sistemlerin simetriğe göre çok yavaş çalışmasıdır. Bu yavaşlığın en önemli sebebi anahtar uzunluğu ve hesaplama karmaşasıdır [10]. Asimetrik yöntemlerin bir diğer dezavantajı ise güveliğin tek yönlü fonksiyonların hesaplanmasının kolay olmasına rağmen tersinin hesaplanmasının imkânsız olmasına dayanmaktadır. Buradaki imkânsızlık neredeyse tersinin hesaplanmasının imkânsız olmasıdır. Fakat bu bir varsayımdır, henüz kesin olarak imkânsız olduğu ispatlanmamıştır. Asimetrik anahtarlı yöntemlerin bir diğer dezavantajı ise eğer aynı veri birden fazla kişiye gönderilecek olursa bu veri ayrı ayrı her alıcının açık anahtarı ile şifrelenmesi gerekmektedir. Bu da sisteme büyük bir yük getirmektedir.

2.4. Hibrit Yöntemler

Bu problemi çözebilmek için günümüzde simetrik ve asimetrik anahtarlı yöntemleri bir arada kullanan hibrit yöntemler geliştirilmiştir. Hibrit yöntemler basitçe açıklanması gerekirse şifrelenecek veri simetrik anahtar ile şifrelenirken bu anahtarın kendisi asimetrik yöntem ile şifrelenmektedir. Böylelikle simetrik anahtarlama yönteminin hızından, asimetrik anahtarlama yönteminin güvensiz ortamda haberleşme kolaylığından yararlanılmış olunmaktadır [30].

Şekil 2.4'de A kullanıcısı hibrit yöntem ile B kullanıcısına veri göndermektedir. Bunu yaparken A kullanıcısı AES, DES, IDEA gibi simetrik şifreleme algoritmalarından birini kullanarak oturum anahtarı üretip, o anahtar ile veriyi şifrelemektedir. Ayrıca oturum anahtarını da B kullanıcısının açık anahtarı ile

şifrelemektedir. A hem simetrik anahtarla şifrelenmiş veriyi hem de B kullanıcısının açık anahtarı ile şifrelenmiş oturum anahtarını güvensiz ortamdan B kullanıcısına göndermektedir.



Şekil 2.4. Hibrit yöntem ile şifreleme

Hibrit yöntem ile yapılan şifreleme ile büyük boyutlara sahip veri B'nin açık anahtarıyla şifrelenmemektedir. Bunun yerine simetrik algoritmalarla oluşturulan oturum anahtarıyla şifrelenmektedir. Böylelikle hem şifreleme işlemi daha kısa sürmüş hem de kaynak tasarrufu sağlanmış olmaktadır. Veriye göre çok küçük boyutlarda olan oturum anahtarı ise B kullanıcısının açık anahtarı ile şifrelenmektedir. Böylelikle Simetrik anahtarlı yöntemin kaynak tasarrufu ve hızı elde edilmekle birlikte asimetrik anahtarlı yönteminde şifreleme gücü kullanılmaktadır.

Şekil 2.5. Hibrit yöntem ile şifre çözme

Şekil 2.5'de B kullanıcısı aldığı şifreli veriyi açabilmek için öncelikle özel anahtarı ile oturum anahtarının şifresini çözmekte, daha sonra oturum anahtarı ile şifreli veriyi açmaktadır. Bu işlemi yaparken B'de, A'da olduğu gibi asimetrik anahtarlı yönteme göre hız ve kaynak tasarrufu sağlamaktadır.

3. KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK

Kablosuz ağlar, kablosuz haberleşme yeteneğine sahip (802.11, bluetooth, infrared, GSM (Global System for Mobile Communications - Mobil İletişimler İçin Küresel Sistem) vb.) [1] cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır. Kablosuz ağ teknolojisinde iletişim radyo sinyalleri aracılığıyla korumasız hava ortamında gerçekleştiği için, birçok güvenlik riski barındırmaktadır. Kablosuz ağların başlıca güvenlik riskleri; ağa sızma, trafiğin dinlenip verilerin çözülmesi, ağ topolojisinin ortaya çıkması, istenmeyen yetkisiz erişim noktalarına bağlanılması, istenmeyen yerlere servis verilmesi ve DoS saldırılarıdır [1]. Kablosuz ağlarda güvenlik, kablosuz ağlarla ilgili yaşanan sorunların başında gelmektedir [31].

Bu sorunların yaşanmaması, verinin bütünlüğünün ve gizliliğinin temel seviyede muhafaza edebilmesi için en azından aşağıdaki temel güvenlik önlemlerinin alınması gerekmektedir [32].

- Kablosuz ağ cihazları ile birlikte gelen, varsayılan ayarlar ve varsayılan kullanıcı ad ve parolaları değiştirilmelidir. 30 yıldan fazladır ileri teknoloji ürünleri satan firmalar üzerinde yapılan araştırmaya göre kullanıcıların çoğunluğunun aldıkları ürünleri varsayılan yapılandırma ayarları ile kullanıldığını göstermektedir [33].
- Sık kullanılan kablosuz ağ güvenliği algoritmalarından olan WEP, WPA gibi algoritmaların daha etkin biçimde kullanılması gerekmektedir.
- Erişim izni verilecek cihazların MAC adresi tanımlamaları ile erişim sağlanması gerekmektedir.
- SSID yayınını herkesin göremeyeceği şekilde gizli olarak yapılandırılmalıdır.
- Kablosuz ağa otomatik bağlan özelliği pasif hale getirilmelidir.
- Erişim sağlamak isteyen cihazlara otomatik IP adresi tanımlama yerine manuel olarak IP ataması yapılması seçilmelidir.
- Ağda virüs, truva atı (trojan), klavye tuşlarını izleyenler (keylogger), solucan gibi zararlı yazılımların izinsiz port açmalarına karşı önlemler alınmalıdır.

Yukarıdaki sayılan önlemler birçok kablosuz ağ tehdidine karşı bizleri koruyabilmektedir. Fakat bu önlemlerinde yetersiz kaldığı profesyoneller veya organize olmuş saldırganlar için daha ciddi önlemler alınması gerekmektedir. Birkaç örnek ile açıklama gerekirse;

SSID yayınını gizli hale getirsek bile kablosuz ağ dinleyiciler (sniffer) havadaki radyo sinyali trafiğini dinleyerek SSID'yi ele geçirebilir, aynı SSID ismi ile yayın yaparak ağınıza bağlanmak isteyen kullanıcıları kendi erişim noktalarına yönlendirebilirler [34] [35].

MAC adresi tanımı ile güvenlik sağlamak ilk bakışta çok etkin bir yöntem gibi görünmektedir. Ancak MAC adresi aslında gerçek bir güvenlik mekanizması değildir ve tüm MAC adresleri iletişim esnasında şifresizdir. Bir saldırgan NetStumbler gibi kablosuz ağı tarayan uygulamalar ile MAC adresini ele geçirebilir. Ağda yetkiye sahip bir MAC adresi ile kendi MAC adresini kolaylıkla yer değiştirebilir. Bu sadece bir kayıt değişimidir ve bu iş için kullanılan birçok yazılım bulunmaktadır. MAC adresi doğrulama ile erişim kontrolü etkin bir yöntem olsa bile tek başına güvenlik sağlamakta yetersizdir [33].

WEP ve WPA gibi kablosuz ağların güvenlik algoritmaları günümüzde en sık kullanılan erişim güvenliği ve kimlik doğrulama protokolleridir. Bu algoritmalar IEEE 802.11 standardı için geliştirilmiş şifreleme algoritmalarıdır. Bu güvenlik protokolleri veri bağlantı katmanında çalışmaktadırlar.

3.1. Kabloluya Eşdeğer Gizlilik (WEP)

WEP algoritması 802.11 standardı ile birlikte geliştirilmiş ilk güvenlik algoritmasıdır. Temel olarak üç önemli amaç için kullanılmıştır. Bunlar güvenilirlik, erişim kontrolü ve veri bütünlüğüdür.

WEP protokolü Ron Rivest'in bulduğu simetrik anahtarlı RC4 akış şifreleme algoritmasına dayanır. RC4 algoritması 24 bitlik bir IV (Initial Vector - Başlangıç

Vektörü) ve 40 veya 104 bitlik simetrik anahtarın birbirine eklenmesi ile oluşturulur. Oluşan bu yeni anahtar ile eldeki verinin uzunluğunda akış anahtarı elde edilir. Elde edilen akış anahtarı ile veri şifrelenir. Verinin bütünlüğünü korunduğunu doğrulama için WEP'de ICV (Integrity Check Value - Bütünlük Kontrol Değeri) hesaplanır. Başlangıç vektörü, akış anahtarı ile şifrelenmiş veri ve ICV sırasıyla alıcıya gönderilir. Alıcı şifreli metni çözebilmesi için başlangıç vektörü ile simetrik anahtarı birleştirir ve açık metni bulabilmek için şifreleme işleminin tersi sıra ile işlemleri gerçekleştirir [37].

3.1.1. WEP protokolü zayıflıkları

WEP protokolü çeşitli saldırılara karşı yapısı itibari ile zayıflıklara sahiptir. Ağı dinleyen bir saldırgan erişim noktasından açık metni istemciden ise şifreli metni elde edebilir. Yeteri kadar dinleme verisi elde ettiğinde simetrik anahtarı tahmin edebilecektir. Ayrıca WEP protokolünde tekrar saldırıları için herhangi bir güvenlik önlemi yoktur. Saldırgan simetrik anahtarı tahmin edemese bile göndericiden elde ettiği dinleme paketlerini alıcıya tekrar gönderirse verinin içeriğini bilmediği halde kendisini doğrulatabilir.

WEP protokolünde kullanılan RC4 algoritması IV olarak 24 bitlik bir dizi kullanır. 24 bitlik bir diziden yaklaşık olarak 17 milyon farklı IV üretilebilir. Bu durumda ise 802.11b standardına göre yaklaşık 7 saatte tüm olasılıklar denenebilir [36].

ICV lineer bir metot ile hesaplanmakta ve şifreli metnin arkasına eklenmektedir. ICV lineer metotla hesaplandığı için şifreli veride bir değişiklik yapıldığında ICV değeri de hesaplanabilmektedir [38].

WEP'de kimlik doğrulama tek yönlüdür. Sadece erişim noktası istemcinin kimlik doğrulamasını yapmaktadır. Erişim izni isteyen bir istemciye şifresiz bir paket gönderilir. İstemci aldığı paketi WEP anahtarı ile şifreler ve erişim noktası bu şifreli paketi doğrularsa istemcinin üye olması veya paket göndermesi izni verilir. Görüldüğü gibi erişim noktası istemciyi doğrulamaktadır fakat istemci erişim

noktasını doğrulaması gibi bir prosedür yoktur. Ağa zarar vermek isteyen bir saldırgan yakın bir yerde erişim noktası ekleyip normal ağın işleyişine zarar verebilir ve istemciler farkında olmadan bu zararlı erişim noktasına istek gönderebilirler.

3.2. Wi-Fi Korumalı Erişim (WPA)

WPA, Wi-Fi Alliance firması tarafından gerçekleştirilmiş bir güvenlik teknolojisidir. Temel amacı WEP'de karşılaşılan güvenlik açıklarını ortadan kaldırmaya yöneliktir. WEP teknolojisi ile çalışan cihazlarda hiçbir donanım değiştirmeden çalışabilecek şekilde tasarlandığı için kısa zamanda kullanımı yaygınlaşmıştır. WEP algoritmasının zayıflığından meydana gelen yetkisi olmayan kişilerin ağa erişimi, sahte erişim noktası kullanılabilmesi, kulak misafirliği (*eavesdropping*), MAC aldatması (MAC spoofing) gibi çeşitli saldırılara karşı daha dayanıklı bir sistem olarak geliştirilmiştir [39].

WPA oturum anahtarı ile grup anahtarı olmak üzere 2 farklı anahtar kullanmaktadır. Bu anahtarlar doğrulama sunucusunun veya erişim noktasının ürettiği ana anahtardan türetilmiştir. Oturum anahtarı her kullanıcı oturum açtığında veya ağa giriş yaptığında yeniden oluşturulan kullanıcı ile erişim noktası arası (unicast) iletişimde kullanılır. Grup anahtarı ise ağa dâhil tüm kullanıcıların bildiği ağda güvenli yayın yapılabilmesi için kullanılan (multicast) anahtardır.

WPA'nın WEP'den en önemli farklarından biri kimlik doğrulama yöntemini zorunlu hale getirmesidir. Kimlik yönetimi için 2 farklı seçenek sunmaktadır [40].

Bunlardan ilk ön paylaşımlı anahtarlı WPA-PSK (WPA Pre Shared Key – WPA Ön Paylaşımlı Anahtar) protokolüdür. Küçük işletmeler ve ev kullanımı için geliştirilmiştir. 8-63 arası karakter uzunluğuna sahip bir şifre belirlenir. Erişim noktası ile istemci tarafından önceden bilinmesi gerekmektedir. Kurumsal işletmeler için kullanımı uygun değildir.

Diğeri kimlik doğrulama yöntemi 802.1x yapısıdır. Port tabanlı ağ erişim kontrolü mekanizmasıdır. İstemci bağlanmak istediği erişim noktasına istek gönderir, erişim noktası bu isteği RADIUS (Remote Authentication Dial-In User Service - Uzaktan Aramalı Kullanıcı Kimlik Doğrulama Servisi) iletir. RADIUS sunucusu kimlik doğrulama ve yetkilendirme işlemini gerçekleştir ve sonucu erişim noktasına ve istemciye bildirir. Sonuca göre erişim noktası istemciye özel bir sanal port açar ve ağı şifrelemek için gerekli anahtarı oluşturur. [41].

3.2.1. Geçici Anahtar Bütünlüğü Protokolü (TKIP)

WPA şifreleme protokolü olarak TKIP [42] kullanmaktadır. Bu protokol WEP teknolojisinin de kullandığı RC4 algoritmasını kullanmaktadır. Fakat TKIP, WEP'de yaşanan problemleri ortadan kaldırmak için çeşitli önlemler almıştır. İlk önlem başlangıç vektörü uzunluğunu 48 bite çıkarmak ve anahtar boyu 128 bite çıkarılmıştır. Sadece bu değişiklilerle anahtar tekrarlama süresi 100 yıl olmaktadır. TKIP her bir paketi farklı anahtar ile şifrelemektedir. Ayrıca her paket için ardışık bir sıra numarası vererek tekrar saldıranlarını da önlemektedir [43].

3.2.2. Mesaj Bütünlük Kodu (MIC)

WEP algoritmasından kullanılan ICV lineer metot ile hesaplandığı için tahmin edilmesi kolaydır. WPA'da bu protokolü çözebilmek için Michael olarak bilinen MIC algoritması kullanılmıştır. MIC, 8 baytlık bir bütünlük hesaplayan koddur. Bu kod oluşturulurken alıcı ve gönderici MAC adresleri ile veri sağlama bitleri (checksum) oluşturulur [43].

3.2.3. WPA protokolü zayıflıkları

WPA protokolü WEP'deki birçok güvenlik açığını kapatmaktadır. Sadece kaba kuvvet saldırısı (brute-force attack) ile kırılması teorik olarak mümkün olsa bile çok zaman alacağı için neredeyse imkânsızdır. Fakat bu sistemdeki en büyük güvenlik açığı insandan kaynaklanmaktadır. Ağ şifresi seçilirken unutulmaması için sadece

alfa nümerik karakterler kullanılmaktadır. Doğum tarihleri, önemli yıllar, tuttuğunuz takımın adı, insan adları, sözlüklerden seçilmiş kelimeler, cep telefonu numaraları, tarihsel öneme sahip yıllar, il plaka numaraları, sadece harfler ya da rakamlardan oluşan sekiz haneli şifreler WEP kadar basit olmasa da rahatlıkla kırılabilmektedir. Bu şifrelere örnek vermek gerekirse;

- 19861986 (tarih çiftleri),
- 14531986 (önemli tarih, doğum tarihi çiftleri),
- bjk1974, ahmet1990, 14531453 (önemli tarih çiftleri)

Bu örnekleri çoğaltmak mümkündür. Saldırganlar bu açığı kullanarak çok vakit kaybetmeden birkaç bilgisayar ile şifreyi bulabilmektedirler. Sadece rakamlardan oluşan 8 karakterli bir şifrenin basit bir bilgisayarla yaklaşık 5 günde çözülebilmektedir [44].

Tez çalışmasında yukarıda bahsedilen güvenlik zafiyetleri aşabilmek ve modern kriptografik yöntemler arasından kablosuz ağ erişim kontrolü ve kimlik doğrulama yapmak için 3 farklı güvenlik protokolü; eliptik eğri kriptografisi, mobil imza ve tek kullanımlık şifreleme önerilmiştir. Tezin devam eden bölümünde bu protokoller açıklanacaktır.

4. ELİPTİK EĞRİ KRİPTOGRAFİSİ (ECC)

Eliptik eğri kriptografisi birbirinden bağımsız olarak 1985 yılında Neal Koblitz [45] ve Victor Miller [46] tarafından önerilmiştir. ECC önceki bölümde ayrıntılı olarak açıklanan asimetrik anahtarlı şifreleme sistemini kullanmaktadır. Bilgisayar teknolojisinin ve telekomünikasyon sektörünün geldiği seviye göz önünde tutulursa simetrik anahtarlı sistemlerdeki anahtarın güvenli şekilde paylaşımı çok büyük problemler oluşturmuştur. Bu nedenle karşılıklı haberleşmede kanal güvenliği aranmaksızın güvenli iletişim kurulmasını sağlayan asimetrik anahtarlı yöntemler modern kriptografi içerisinde büyük önem kazanmıştır. ECC asimetrik anahtarlı yöntemler arasında anahtar boyu çok kısa olmasına rağmen çok yüksek seviyelerde güvenlik sağlamasıyla dikkat çekmiştir. Örneğin 1024 bitlik bir RSA algoritması ile oluşturulan güvenliği, ECC sadece 160 bit ile karşılayabilmektedir [47]. Aşağıdaki çizelge ECC ile diğer kriptografik sistemler arasındaki anahtar boyuna göre güvenlik seviyeleri kıyaslamasını göstermektedir.

Çizelge 4.1. ECC, RSA, DSA anahtar boyu karşılaştırması [48]

	Bant Genişliği		Anahtar Uzunluğu	
	2000 bitlik veri için imza boyutu (Bit)	100 bitlik veri için imza boyutu (Bit)	Açık Anahtar (Bit)	Gizli Anahtar (Bit)
RSA	1024	1024	1088	2048
DSA	320	2048	1024	160
ECC	320	321	161	160

Eliptik eğri algoritmasında güvenlik ayrık logaritma probleminin çözüm zorluğuna dayanmaktadır. $a^i = b \pmod p$ işleminde a ve i verildiğinde b'yi hesaplamak kolay iken; a ve b verildiğinde i'yi hesaplamak ($i = \log_a b$) zor bir problemdir.

4.1. ECC'de Kullanılan Matematiksel Kavramlar

Eliptik eğri algoritmasına girmeden önce algoritmanın tanımında geçen grup, Abelian grup, alan, sonlu alan, Galois alan, gibi matematiksel kavramlar açıklanacaktır.

Tanım 1: Grup

Herhangi bir G kümesi Δ ikili işleminde kapalılık, birleşme, etkisiz eleman, ters eleman aksiyomlarını sağladığında <G, Δ> grubu denir.

Kapalılık: $\forall x, y \in G$ için $x \Delta y \in G$

Birleşme:$\forall x, y, z \in G$ için $(x \Delta y) \Delta z = x \Delta (y \Delta z) \in G$

Etkisiz Eleman: $\forall x \in G$ için $x \Delta e = e \Delta x = x$ olan $e \in G$

Ters Eleman : $\forall x \in G$ için $x \Delta y = y \Delta x = e$ olan $y \in G$

Tanım 2:Abelian Grup

İkili işlemde değişme özelliği olan gruplardır. Değişmeli grup olarak da adlandırılır.

Değişme Özelliği : $\forall x, y \in G$ için $x \Delta y = y \Delta x$

Tanım 3: Halka

Halka <A; +, *> bir A bir küme + ve * ise A kümesi üzerinde tanımlanmış işlemler olmak üzere aşağıdaki özellikle sağlanırsa A üzerinde bir halka tanımlanmış olur.

- <A, +> değişmeli bir grup olmalıdır.
- "*" işlemi A üzerinde kapalılık ve değişme özelliğine sahip olmalıdır.
- "*" işleminin A üzerinde etkisiz elemanı olması gerekmektedir.
- $\forall x, y, z \in A$ için $(x + y) * z = (x * z) + (y * z)$

Tanım 4: Alan

Bir A kümesi üzerinde tanımlanmış + ve * işlemleri için aşağıdaki aksiyomlar sağlanıyorsa bir alan oluşur.

- <A, +> ve <A, *> bir Abelian grup olmalıdır.
- <A, +> sadece toplama işleminin etkisiz elemanı için bir ters elemanı bulunmayabilir.
- <A; +, *> bir halka oluşturmalıdır. Yani * işleminin + işlemi üzerinde dağılma özelliği olmalıdır.

Yukarıdaki özellikleri sağlayan gerçel sayılar kümesi bir alan örneğidir.

Tanım 5: Sonlu Alan

Yukarıda tanımlanan alanın sonlu sayıda eleman içermesi durumunda sonlu alan olarak adlandırılır. Sonlu alanın eleman sayısı alanın derecesini gösterir. Derecesi aynı olan alanlar matematiksel olarak aynı yapıdadır sadece elemanların gösterimi farklıdır.

Bir sonlu alan p asal, m tam sayı olmak üzere $q = p^m$ şeklinde bir asalın kuvveti olması gerekir. Bu alan F_q şeklinde gösterilir.

Tanım 6:Galois Alan

Galois alan p asal sayı olmak üzere eleman sayısı p olan Z_p= {0, 1, 2, 3, … , p-1} üzerinde modülo p'de toplama ve çarpma işlemlerinin tanımlanması ile oluşturulan sonlu alandır. GF(p) ile gösterilir.

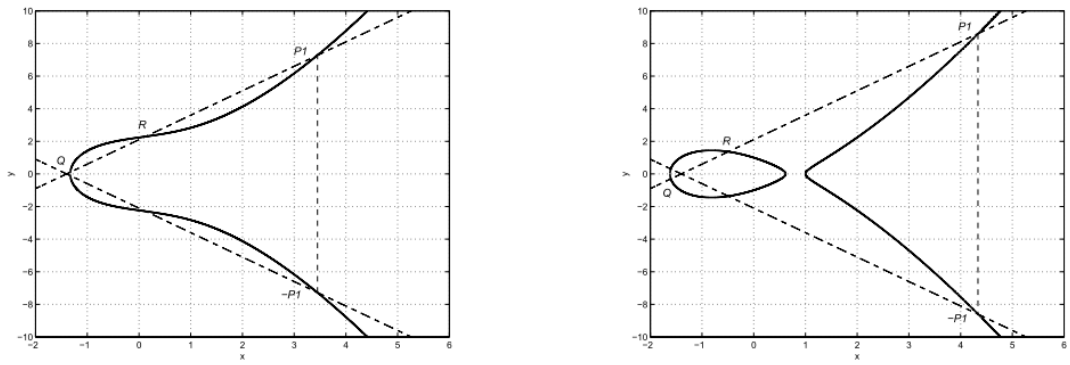
4.2. Eliptik Eğri Temelleri

Eliptik eğriler kübik eşitliklerdir. Bir alan üzerinde Weierstrass denkleminin çözüm kümesi ve sonsuz Ó noktasının birleşiminden oluşmaktadır [49].

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

a, b, c, d, e gerçel sayılardır. Denklem üzerinde özel toplama ve çarpma işlemi tanımlanmaktadır. Çözüm kümesi toplama işlemi ile Abelian grup oluşturmaktadır.

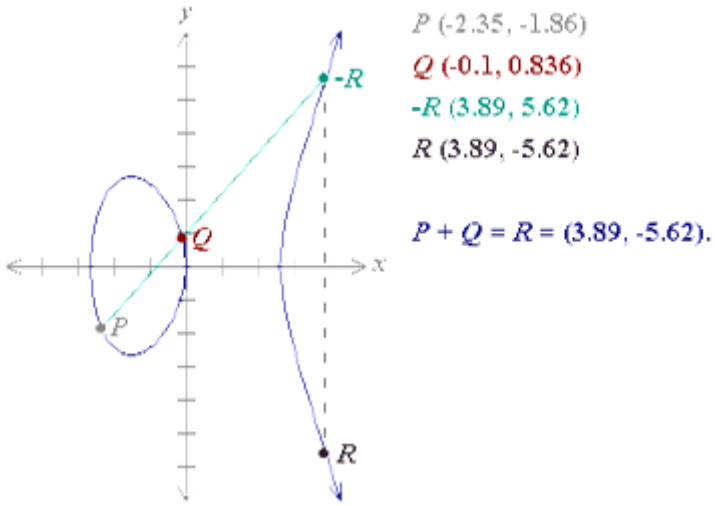
Çözüm kümesi üzerinde oluşturulan grubun birim elemanı y ekseni üzerinde olduğu varsayılan sonsuzdaki Ó noktasıdır. Eğer eliptik eğriyi bir doğru 3 noktadan keserse bu noktaların toplamı sonsuzluktaki Ó noktasına eşittir. Aşağıda $y^2 = x^3 + 2x + 5$ ve $y^2 = x^3 - 2x + 1$ eliptik eğrilerinin şekilleri gösterilmektedir.



Şekil 4.1. $y^2 = x^3 + 2x + 5$ ve $y^2 = x^3 - 2x + 10$ [50]

Eliptik eğrilerde çözüm kümesi bir grup oluşturulduğuna göre, bu grup üzerinde nokta toplama ve nokta çarpma işlemi yapılabilmektedir. P ve Q eliptik eğri üzerinde birbirinden farklı iki nokta olmak üzere bu noktaların toplamı aşağıdaki gibi bulunmaktadır.

P ve Q noktaları bir doğru ile birleştirilir. Bu doğru eliptik eğriyi -R gibi bir başka noktada keser. Bu noktanın x eksenine göre simetriği R = P + Q toplamını vermektedir. Eğer P ve Q noktaları aynı nokta ise bu durumda P noktasından çizilen teğetin eğri ile kesişim noktasının x eksenine göre simetriği alınarak bulunur. Aşağıdaki şekilde $y^2 = x^3 - 7x$ eğrisi üzerinde toplama işlemi gösterilmiştir.



Şekil 4.2. $y^2 = x^3 - 7x$ [50]

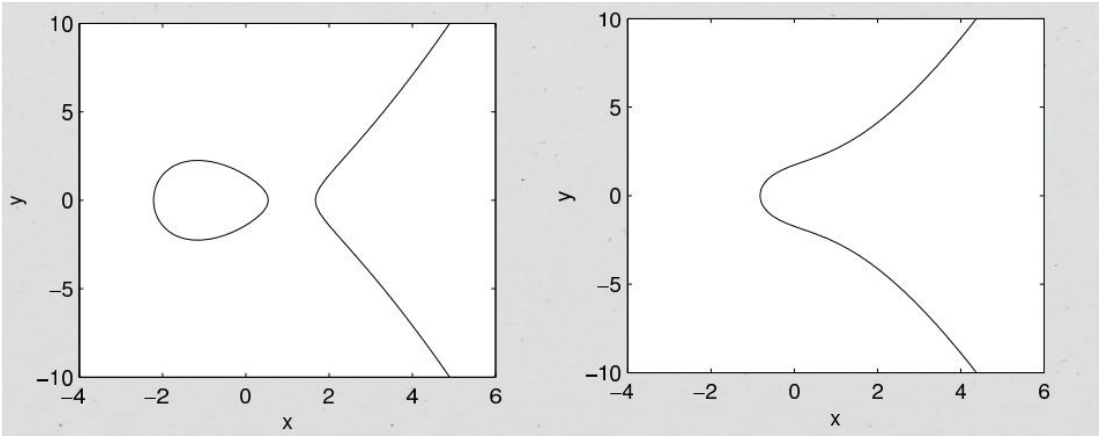
4.3. Galois Alan Üzerinde Tanımlı Eliptik Eğriler

Eliptik eğri kriptografisi sonlu Galois alanı $E_p(a, b)$ üzerinde tanımlı bir formu üzerinde gerçekleştirilmektedir. Eğrinin genel gösterimi aşağıdaki gibidir.

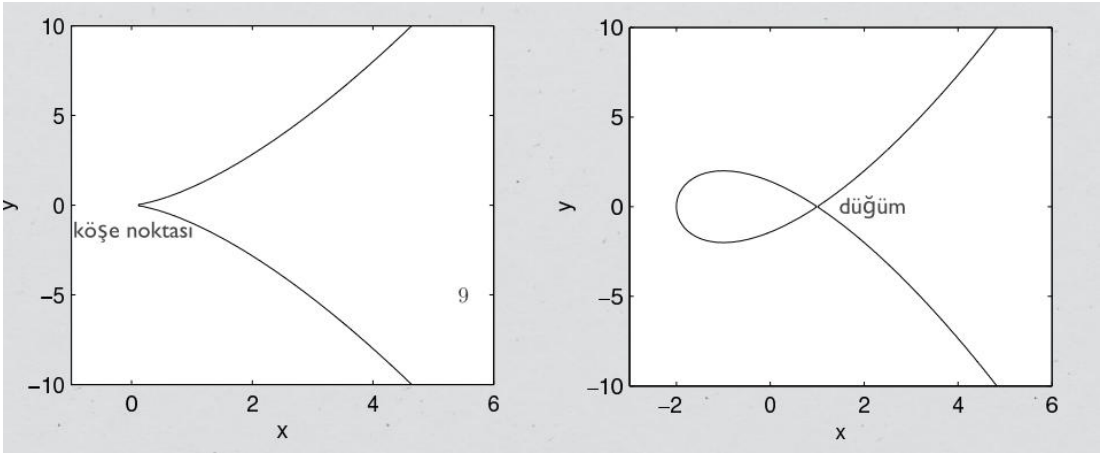
$$y^2 = x^3 + ax + b \pmod p$$

p asal sayı ve a, b sayıları p'den küçük negatif olmayan iki tamsayı olmak üzere $4a^3 + 27b^2 \neq 0 \pmod p$ olması gerekmektedir.

Eliptik eğri denkleminin diskriminantı -16 $(4a^3 + 27b^2)$ dir. Diskriminantı 0 olan eğriler tekildir ve süreksiz (pürüzsüz) eğrilerdir. Süreksiz eğri denklemleri her yerde türevli ve herhangi bir kırılma noktası olmayan eğrilerdir. $4a^3 + 27b^2 = 0$ olan eğriler şifreleme için güvenli değillerdir [48]. Eliptik eğriler $y = \sqrt{x^3 + ax + b}$ şeklinde ifade edilebildiğinden x eksenine göre simetriktirler. Şekil 4.4 ve Şekil 4.5'de diskriminantı 0 olan ve olmayan eğriler gösterilmiştir.



Şekil 4.3. $y^2 = x^3 - 4x + 2$ ($4a^3+27b^2<0$) ve $y^2 = x^3 + 3x + 3$ ($4a^3+27b^2>0$) [50]



Şekil 4.4. $y^2 = x^3$ ve $y^2 = x^3 - 3x + 2$ grafikleri ($4a^3+27b^2= 0$) [50]

Örneğin p = 23, a = b = 1 olsun. Eğri denklemi $y^2 = x^3 - 3x + 2$ olmaktadır. Bu durumda $4.1^3 + 27.1^2 = 8 \bmod (23)$ dir, $8 \neq 0 \bmod (23)$ dır.

4.4. Eliptik Eğrilerde Toplama Ve Çarpma İşlemi

P=(x_1, y_1) ve Q=(x_2, y_2) eliptik eğri E_p(a, b) üzerinde noktalardır. Ó sonsuzluk noktasıdır. Eliptik eğri E_p(a, b) üzerinde aşağıdaki toplama kuralları geçerlidir:

1) P + Ó = Ó + P = P
2) Eğer $x_1 = x_2$ ve $y_1 = -y_2$ ise P = (x_1, y_1) ve Q = (x_2, y_2) = (x_1, $-y_1$) = -P dir. Bu durumda P + Q = Ó.

3) Eğer $Q \neq -P$ ise P + Q toplamı (x_3, y_3) dir ve aşağıdaki gibi bulunur:

$x_3 = \lambda^2 - x_1 - x_2 \bmod (p)$

$y_3 = \lambda (x_1 - x_3) - y_1 \bmod (p)$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q \end{cases}$$

Eliptik eğri üzerinde çarpma işlemi yapabilmek için toplama işleminden faydalanılmaktadır. Çarpma işlemi bir örnek ile açıklanacaktır.

P = (3, 10) ve $P \in E_{23}(1, 1)$. $2P = (x_3, y_3)$ bulmak gerekirse:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod p = \frac{3 * 3^2 + 1}{2 * 10} \pmod{23} = \frac{5}{20} \pmod{23} = 4^{-1} \pmod{23} = 6$$

$x_3 = \lambda^2 - x_1 - x_2 \pmod p = 6^2 - 3 - 3 \pmod{23} = 30 \pmod{23} = 7$

$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p = 6 (3 - 7) - 10 \pmod{23} = -34 \pmod{23} = 12$

$2P = (x_3, y_3) = (7, 12)$ olmaktadır. Eğer kP gibi bir çarpma işlemi yapılacak ise toplam k kez aynı toplama işlemi gerçekleştirilmektedir. Örneğin 19P gibi bir çarpma işlemi uygulanacaksa hesaplama kolaylığı açısından 19P => P + P = 2P, 2P + 2P = 4P, 4P + 4P = 8P, 8P + 8P = 16P, 16P + 2P + P = 19P gibi hesaplanabilmektedir.

Fakat k birkaç yüz basamaklı bir sayı ise kesişim noktalarının çokluğundan hem işlem yavaşlayacak hem de yuvarlama sırasında işlem hataları yapılacaktır. Bu kriptografik işlemlerde istenmeyen bir durumdur. Bu nedenle eliptik eğri Z_p veya Z_2^m de tanımlanmaktadır. Z_p yazılımsal olarak Z_2^m ise donanımsal olarak gerçekleşmesi

kolaydır. Eliptik eğrilerde ayrık logaritma probleminin temelinde Z_p gibi sınırlı bir alanda seçilen bir P noktasının yeterince büyük bir k ile çarpılması yatmaktadır.

4.5. Açık Metni Eliptik Eğri Üzerindeki Noktalar ile Eşleştirme

Eliptik eğri ile şifrelemede öncelikle açık metin eliptik eğri üzerindeki noktaya dönüştürülmesi gerekmektedir. Bu dönüşüm birebir olmalıdır. Bu nedenle şifreleyeceğimiz mesaj birimine yetecek kadar eliptik eğri (F_q) üzerinde nokta bulunması gerekmektedir. Bunun için Hasse teorimi kullanılır.

Tanım: Hasse Teoremi
Sonlu alanda eliptik eğri üzerindeki nokta sayısını tahmin etmek için Hasse Teoremi kullanılır. Teorem hakkında ilk çalışmalar Emil Artin tarafından gerçekleştirildi. 1936 yılında Hasse makalesinde ispatladı. Hasse'nin teoremi daha sonra daha kolay bir ispat yöntemi ile Manin tarafından da ispatlandı. Teorem nokta tahminin de kabul edilebilir küçüklükte hata ile sonuç vermektedir [51]. N, Fq üzerinde tanımlanmış olan eliptik eğri üzerindeki noktaları göstermek üzere:

$$|N - (q + 1) \leq 2\sqrt{q}|$$

Örnek: E: $y^2 = x^3 + 14x + 14$ eğrisi F_{19} olmak üzere:

$$|N - (19 + 1) \leq 2\sqrt{19}|$$
$$-8.718 \leq N - 20 \leq 8.718$$
$$11.282 \leq N \leq 28.718$$
$$12 \leq N \leq 28$$

Açık metin (M) eliptik eğri üzerine yerleştirilmek istenilirse; sabit blok boylu birimlere (m) ayrılmalıdır. $k \in N$ olmak üzere, $0 \leq m \leq M$ ve $q > Mk$ olması gerekmektedir. $1 \leq j \leq k$ olacak şekilde $mk + j$ formunda 1 den Mk ya kadar tamsayılar yazılır. Verilen bir m için ve $j = 1, 2, \ldots, k$ ya kadar $mk + j$ şeklinde F_q

elemanı x elde edilir. Bu x kullanılarak $y^2 = f(x) = x^3 + ax + b$ denklemi kullanılarak f(x) elde edilir. f(x) değeri y^2'ye eşit olmasından dolayı tam kare olmalıdır. Eğer tam kare değer elde edilemezse j değeri bir artırılarak tekrar denenir.

Bir örnekle açıklama gerekirse t karakterini F_{491} alanında E: $y^2 = x^3 + 7x + 9$ eğrisi üzerine yerleştirmek gerekirse [52]:

Öncelikle $4a^3 + 27b^2 \neq 0 \pmod p$ olması gerektiğinden $4.7^3 + 27.9^2 = 3559 = 122 \neq 0 \pmod{491}$

Bu eğri şifrelemede kullanılabilir.

$|N - (491 + 1) \leq 2\sqrt{491}|$
$-44{,}317 \leq N - 492 \leq 44.317$
$11.282 \leq N \leq 28.718$
$448 \leq N \leq 536$

Hasse teoremine göre alfabeyi şifrelemek için yeterli noktaya sahiptir.

k = 10 ve $0 \leq m < 26 = M$ olmak üzere alfabe $a \equiv 0$ olacak şekilde sayı değerleri ile eşlenir.
$q > 26 * 10$
Eğri üzerine yerleştirilmek istenen karakter $t \equiv 19$ olmaktadır. mk + j değeri, k = 1, 2, ... , k = 10'a kadar hesaplanarak (19 * 10 + 1 den 19 * 10 + 10) x değerleri ile birebir eşlenir.

mk + j	191 192 193 194 195 196 197 198 199 200
x	191 192 193 194 195 196 197 198 199 200

x = 191'den başlanarak f(x) denkleminde yerine konulur.
$f(x) = 191^3 + 7 * 191 + 9$

$= 6969217$

$= 454 \bmod (491)$

$\neq y^2$

$\forall\, y \in F_{491}$

454 tam kareye eşit olmadığından bir sonraki değer olan 192'ye geçilir.

$f(x) = 192^3 + 7 * 192 + 9$

$= 7079241$

$= 3 \bmod (491)$

$= 113^2$

mod (491) de $3 \equiv 113^2$ olduğundan t değeri eğri üzerinde P_t (192, 113) noktası ile temsil edilir.

Örnekte görüldüğü gibi her x değeri için bulunan f(x) değeri y^2 gibi bir tam kareye eşit olması gerekmektedir. Tam kare kontrolü için karesel rezidü (quadratic residues) formülü kullanılır.

Tanım: Karesel Rezidü ve Legendre Sembolü

p, tek ve asal sayı olmak üzere, $x^2 \equiv a \pmod p$ denkliği için 3 durum vardır [52];

- a mod (p) de karesel rezidü değildir. Denklemin çözümü yoktur
- a mod (p) de 0'a denktir. Denklemin sadece bir çözümü vardır.
- a mod (p) de karesel rezidüdür. Denklemin iki kökü vardır.

Legendre Sembolü a bir tamsayı ve $p > 2$ asal sayı olmak üzere Legendre sembolü (a/p) aşağıdaki gibi hesaplanır.

$$(a/p) = \begin{cases} 0, & p|a \text{ ise} \\ 1, & a \bmod (p)' \text{de karesel rezidü ise} \\ -1, & a \bmod (p)' \text{de karesel rezidü değil ise} \end{cases}$$

(a/p) aşağıdaki gibi hesaplanır;

$(a/p) \equiv a^{(p-1)/2} \bmod (p)$

4.6. Eliptik Eğri Şifreleme

RSA ve Diffie-Helman algoritmalarının temel aritmetik işlemi çarpma iken, ECC'de toplamadır. Fakat çarpım aslında temelde tekrarlı bir toplama işlemidir.

$k * G = G + G + G + ... + G \bmod (p)$

Eliptik eğride şifrelenmek istenen açık metin öncelikle yukarıda bahsedildiği gibi eğri üzerinde uygun noktalar (Qm) ile eşleştirilmesi gerekmektedir. Daha önce belirlenmiş olan k değeri ve eğri üzerinde P taban noktası çarpılarak kP noktası hesaplanır. Bu değer (kP) ve şifrelenmek istenen veri için bulduğumu Qm değeri toplanarak şifreli veri Qc = Qm + kP hesaplanır. Oluşan bu yeni noktanın sadece x koordinatı xc karşı tarafa gönderilir.

Alıcı daha önceden paylaşılmış olan k ve P değerlerini çarparak kP değerini hesaplar. xc bilgisi karşı tarafından gönderilmiştir. Alıcı xc ile Qc'yi tekrar hesaplar ve açık metni bulabilmek için Qm = Qc - kP işlemini gerçekleştirir.

4.7. Eliptik Eğri Kriptografisinde Diffie-Hellman Anahtar Değişimi

1976 yıllında ilk kez Whitfield Diffie ve Martin Hellman tarafından ilk açık anahtar şeması önerilmiştir [53]. Diffie-Hellman anahtar değişim protokolü sonlu bir alanda (Örneğin; Galois alanında) bir asal sayının, tam sayı modülü üzerinde üstelleştirilmesine dayanır.

Alice ve Bob q, a, b $\in Z_p$ parametreleri seçer E_p (a, b) oluşturulur ve bunun üzerinden bir G noktası seçilir. G noktası açık parametredir.

Alice ve Bob kendilerine özel olacak E_A ve E_B gibi iki nokta seçerler. Her biri kendine ait özel noktaları ile G noktasını işleme sokar ve açık anahtarlarını (D_A ve D_B) oluşturur;

$D_A = E_A * G \bmod (p)$
$D_B = E_B * G \bmod (p)$

Alice ve Bob haberleşmede kullanacakları ortak anahtarı aşağıdaki gibi hesaplar;

Alice $K = D_A * E_B$ (Alice'in kapalı anahtarı * Bob'un açık anahtarı)
Bob $K = D_B * E_A$ (Bob'un kapalı anahtarı * Alice'in açık anahtarı)

Böylelikle Alice ve Bob aynı K değerini hesaplar

$K = D_A * E_B = D_B * E_A$
$K = (E_A * G) * E_B = (E_B * G) * E_A$
$K = E_A * E_B * G$

Bu durumda D_A, D_B ve E_B bilen birisi K'yı hesaplayamaz. Problemin zorluğunun artırılması için derecesi yüksek bir G noktası seçilmesi gerekmektedir [54].

5. MOBİL İMZA

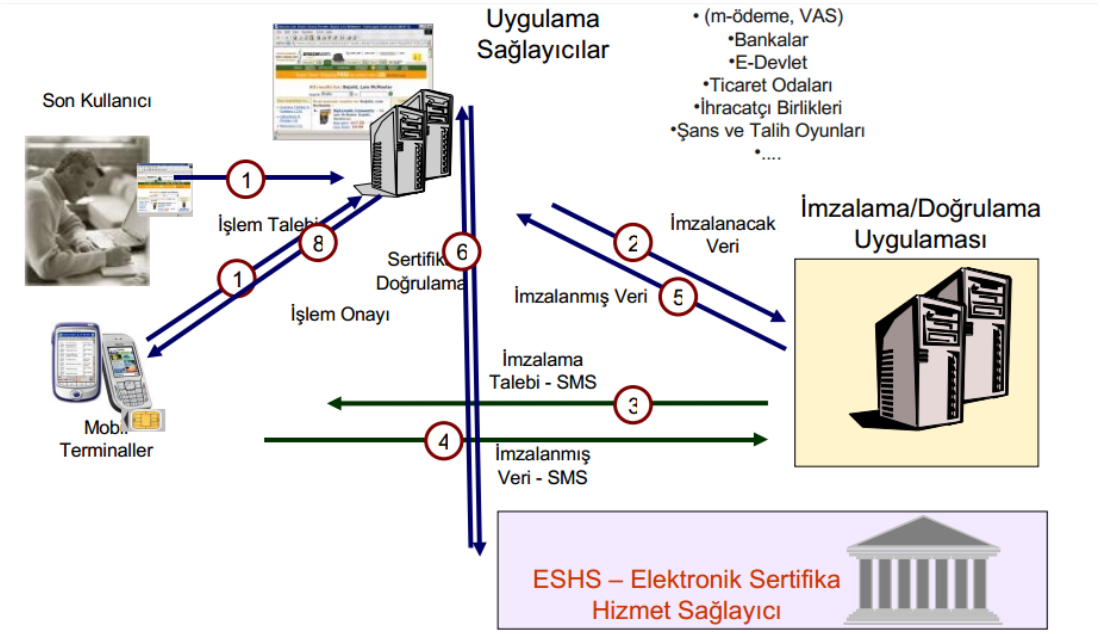
İletişim teknolojilerinin hızla gelişmesi, bilgiye her noktadan erişim ihtiyacı mobil ve kablosuz sistemlere olan talebi artırmakta ve hayatın vazgeçilmez bir parçası haline getirmektedir [55]. Bu gelişmelerle birlikte mobil ortamlarda yapılan iş ve işlemler çoğalmakta, bu ortamlara olan güven ihtiyacı ön plana çıkmakta, yüksek seviyede bilgi ve iletişim güvenliğine ihtiyaç duyulmaktadır. Ülkemizde 5070 sayılı Elektronik İmza Kanunu [56] ile bu ortamlara güven sorununu ortadan kaldırmak, iş ve işlemlerin hukuken de geçerli olmasını sağlamak için düzenlenmiştir. Bu kanunda tarif edilen ıslak imza ile eşdeğer mobil imza, hem uluslararası standartlara hem de 5070 sayılı Elektronik İmza Kanununa uygundur ve yasal olarak geçerlidir. Mobil imza kısaca elektronik imzanın özel GSM SIM kartları kullanılarak atılmasını sağlayan servistir.

Ülkemizde mobil imza servisi yeni kurulmasına rağmen kullanım kolaylığı, yüksek güvenlik ve yasal bağlayıcılıkları nedeniyle giderek yaygınlaşmaktadır. Ayrıca elektronik imza ile aynı yasal geçerliliğe sahip olmasına rağmen elektronik imzaya göre yıllık ücret tarifleri çok daha uygundur. Bu nedenle e-Devlet kapısındaki birçok uygulama artık mobil imza destekler hale gelmiştir. Böylelikle en üst seviyede güvenlik sağlanırken vatandaşlarında kâğıt ortamında gerçekleştirdikleri birçok işlemi e-devlet uygulamaları ile kolayca gerçekleştirebilmektedir. Mobil imzanın yukarıda bahsedilen yönlerinden dolayı ülkemizde çok kısa zamanda yaygınlaşacağı bilinmektedir. Mobil imza ülkemizdeki birçok kritik uygulamada yer bulmasına rağmen henüz kablosuz ağlarda erişim güvenliği için kullanılmamıştır.

5.1. Mobil İmza Senaryosu

Mobil imza çalışma senaryosu aşağıdaki şekilde gösterildiği gibi öncelikle kullanıcı bilgisayarında veya mobil cihazından imzalamak istediği belgeyi görüntüler (1). İmzalamak için telefon numarasını girer ve imzalama işleminin gerçekleşmesi için operatör tarafındaki imzalama sunucusuna imzalanacak veri iletilir (2). İmzalama sunucusu işlemini gerçekleştirmek için imzalama talebini kişinin mobil cihazına

SMS (Short Message Service - Kısa Mesaj Hizmeti) olarak bildirir (3), İmzalayacak kullanıcı SMS'i onaylar ve imzalama sunucusuna onay mesajı döner ve imzalama işlemi gerçekleştirilir (4). İmzalanmış veri, kişinin genel anahtarı ve nitelikli elektronik sertifikası isteği gönderen sunucuya iletilir (5). Sunucu imzalanmış verinin imzasının geçerli olup olmadığını kontrol etmek için ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) imzalanmış veri, açık anahtar ve nitelikli elektronik sertifikayı gönderir. ESHS elektronik sertifikanın geçerliliği, imzalı verinin sertifika sahibi kişi tarafından imzalandığı gibi tüm güvenlik kontrollerinden geçirir. Bu kontrollerin tamamından geçen imzalanmış veride herhangi bir güvenlik sorunu ile karşılaşılmazsa Uygulama sunucusuna imzalanmış verinin doğruluğunu onaylar (6).



Şekil 5.1. Mobil imza senaryosu [57]

5.2. Mobil İmza Altyapısı

Mobil imza, mobil cihazların özelliklerinden bağımsız olarak teknik gereksinimlerinin tanımlandığı ETSI (European Telecommunications Standard Institute - Avrupa Telekomünikasyon Standartlar Komitesi) tarafından yayımlanan standartlarda "bir kullanıcının bir antlaşmayla ilgili kararının onayını mobil bir aletle almak için kullanılan evrensel yöntem" olarak tanımlanmaktadır [58].

Mobil imza, elektronik imza gibi açık anahtar altyapısı kullanarak ıslak imza ile aynı yasal sorumluluğu taşımaktadır. Mobil cihazlar için üretilen özel SIM kartlar ülkemizin de sertifika otoritesi 17 ülkeden biri olduğu CC (Common Criteria - Ortak Kriterler)'in belirlediği EAL +4 (Evaluation Assurance Level - Değerlendirme Garanti Seviyesi) seviyesinde anahtar saklama özelliğine sahiptirler. Bu kartların en önemli güvenlik özelliği içerisinde bulundurduğu özel anahtarı hiçbir şekilde dışarı çıkarmamasıdır [58].

Elektronik imzada olduğu gibi mobil imzada açık anahtar altyapısını kullanmaktadır. Bu altyapıda özel ve açık anahtarların üretilmesi ve açık anahtarın dağıtılması gerekmektedir. Açık anahtarın dağıtılması, kime ait olduğunu belirtilmesi, güvenilir bir makamdan alınıp alınmadığının kontrolü gibi bilgileri bir arada bulunduran güvenli elektronik sertifika oluşturulmaktadır. Bu sertifika dağıtımı, sertifika güven zincirinin oluşturulması kayıp, çalınma veya buna benzer diğer sebeplerle sertifikanın iptal edilmesi, anahtarların yedeklenmesi, gibi hizmetleri sağlayan ESHS makamlar kurulması gerekmektedir [58]. Bu makamlar mobil imza servis sağlayıcı operatörlerin dışından kurulan bağımsız sertifika hizmeti veren kuruluşlardır. Mobil imza telekomünikasyon operatörü, ESHS kuruluşlar ile ortak çalışma ile AAA kullanarak bu altyapının sağladığı gizlilik, bütünlük, kimlik doğrulama ve inkâr edememe gibi unsurları mobil imza kullanıcılarına sunmaktadırlar.

Mobil imzada e-imza gibi elektronik ortamlarda yapılan işlemlerin hukuki geçerlilik kazanılması için kullanılmaktadır. Elektronik imza son zamanlarda elektronik ödeme sistemleri, devlet portalları, kayıtlı elektronik posta hizmetleri, elektronik fatura gibi çok farklı uygulama alanlarında kullanılmaktadır [59 - 61]. Fakat bununla beraber e-imza teknolojisinde imzalamak için kullanılan özel anahtar ortak kriterlerin (CC) belirlediği EAL+4 seviyesinde güvenlik önlemine sahip cihazlar ile taşınması gerekmektedir. Bu cihaz genellikle akıllı kartlar veya akıllık çubuklar ile taşınmakta ve bilgisayarlara USB (Universal Serial Bus - Evrensel Seri Veri Yolu) portlarından bağlanarak çalışmaktadır. Bu nedenle günümüzde yaygın olarak kullanılan cep telefonu, PDA (Personal Digital Assistant - Kişisel Sayısal Yardımcı), tablet gibi mobil cihazlar ile kullanılamaz olmaktadır. Mobil cihazlardaki bu sorunun

çözülebilmesi için gizli anahtarın mobil cihazlar için üretilen aynı güvenlik seviyesine sahip özel SIM kartlar ile taşınması sağlanmaktadır.

Kriptografik işlemler şifreleme, deşifreleme, gibi genellikle çok büyük işlem kapasitesi gerektirmektedir. Elektronik ortamda imzalama ve imzanın doğrulanması da birer kriptografik işlemdir. Bu nedenle genellikle HSM (Hardware Security Module - Donanımsal Şifreleme Modülü) gibi özel cihazlar kullanılmaktadır. Mobil cihazlardaki kısıtlı enerji ve kapasite problemlerinden dolayı imzalama ve doğrulama işlemleri yapılabilmesi için gerekli kaynak bulunmamaktadır. Mobil imza altyapısı bu kaynak yetersizliğini de göz önünde bulundurarak imzalama ve doğrulama gibi işlemleri servis sağlayıcı operatöre yüklemektedir. Böylelikle mobil cihaz donanımdan bağımsız ve mobil cihazın kaynaklarını kullanmadan imzalama işlemi yapılmaktadır.

Kablosuz yerel alan ağlarında erişim güvenliği ve kimlik doğrulama için mobil imzanın seçilmesinde en büyük etken bu yöntemin kablosuz ağ donanımına ve mobil cihaza herhangi bir kriptografik işlem yaptırmadan güvenlik sağlamasıdır. Böylelikle çok büyük bir kaynak tasarrufu yapılmış ve aynı zamanda asimetrik anahtar altyapısı kullanılarak asimetrik anahtarlamanın güvenlik seviyesinde şifreleme yapılmış olmaktadır. Bu yöntemin kablosuz ağlardaki erişim güvenliğine sağlayacağı bir diğer önemli katkı ise günümüzde kullanılan kablosuz erişim protokollerinin hemen hepsinde bulunan "Erişim Taahhütnamesi" için yasal sorumluluk içerecek şekilde imzalanması olacaktır. Hâlihazırda kullanılan sistemlerde sözleşmenin altından bulunan “okudum ve kabul ediyorum” gibi düğmelere basarak onay verilmesi yasal olarak hiçbir şey ifade etmemektedir. Fakat bu sözleşmenin mobil imza gibi hukuki dayanağı olan bir yöntemle imzalanarak onaylanması herhangi bir yasa dışı olayda hukuki dayanak olarak sunulmasını sağlayacaktır.

Mobil imzanın ülkemizde yaygınlaşması ile kamusal alanlardaki kablosuz ağ bağlantısındaki erişim güvenliği ve kimlik doğrulamaya büyük katkı sağlayacaktır. Herhangi bir kamusal alanda ağa dâhil olmak isteyen kullanıcı sistem yöneticisi ile hiç iletişim kurmasına gerek kalmadan mobil imzası ile erişim taahhütnamesini

imzalamak suretiyle tüm yasal sorumluluğu üzerine alarak ağ dâhil olacaktır. Böylelikle kullanıcı hava alanı, tren istasyonu ve diğer kamu kurum ve kuruluşlarında kısa bir süreliğine kullanacağı ağa dâhil olabilmek için sistem yöneticisi ile irtibata geçme zahmetinden kurtulmuş olacaktır. Sistem yöneticisi tarafında ise büyük bir iş yükü azalması sağlanmış olurken, aynı zamanda kullanıcılardan yasal geçerliliği olan mobil imzalarını alarak güvenlik sağlamış olacaklardır. Kamusal alanlarda kablosuz ağlarda mobil imza ile erişim kontrolü ve kimlik doğrulama uygulamasının hayata geçmesi ile kullanıcıların zahmetsizce ağa dâhil olabilmeleri ülkemizde aynı zamanda mobil imzanın yaygınlaşmasına da katkı sağlayacaktır.

6. TEK KULLANIMLIK ŞİFRE (OTP)

İnternet gibi güvenilir olmayan iletişim ortamlarında en muhtemel saldırılardan biri kötü niyetli kullanıcılar tarafından ortamın dinlenmesi olmaktadır [39]. Bunun için iletim hattından paket yakalayan programlar, port dinleyiciler veya klavye tuşlarını izleyenler gibi yöntemler kullanılmaktadır. İnternet ortamın hala en çok kullanılan kimlik doğrulama yöntemi ise kullanıcı adı ve statik şifre ile doğrulamadır.

Yukarıda bahsedilen saldırı türleri ile statik şifreli kimlik doğrulama yöntemlerini kolayca aşmak mümkün olmaktadır. Bu tür saldırılara karşı bilgi güvenliğini koruma altına almanın en başarılı yollarından biri tek kullanımlık şifreleme yöntemidir. Böylelikle saldırganlar sizin paketlerinizi yakalasa veya klavyenizi izleyerek şifrenizi ele geçirse bile şifrenin tek kullanımlık olmasından dolayı herhangi bir tehdit oluşturmaktadır.

Yemleme (phishing) saldırıları internet kullanıcılarının bilgi güvenliğini tehdit eden çok ciddi bir başka saldırı türüdür. Yemleme saldırısı özetle saldırganların çok sayıda kullanıcıya rastlantısal olarak gönderdikleri sahte e-posta veya kısa mesajla kredi kartı numaraları, kullanıcı şifreleri gibi kritik bilgilerini ele geçirmeye çalışmalarıdır. Kullanıcılar beklemedikleri bu mailde yazılan direktifleri izleyerek sahte bir web sitesine yönlendirilir ve burada kritik bilgilerinin girilmesi istenir. Örneğin kredi kartı bilgileri ile internet üzerinden güvenli alışveriş yapılabilme veya para transferi için kullanılan paypal.com sitesi yerine saldırgan kullanıcıyı paypa1.com gibi bir URL (Uniform Resource Locator - Tekdüzen Kaynak Bulucu)'ye yönlendirir. Bu sahte web sitesinin görünümü hemen hemen gerçek site ile aynı şekilde dizayn edilir. Aynı anda birçok kullanıcıya giden mail üzerinden verilen link ile birçok kullanıcı fark etmeden sonu 1 ile biten sahte siteye yönlendirilir. Bu sitede kullanıcı kimlik bilgileri veya kredi kartı bilgisi gibi bilgiler girilmesi için zorlanır. Araştırmalar sonucunda çalınan kullanıcı ismi ve parolalarının %70'inden fazlası yemleme saldırısı ile gerçekleştirilmektedir. Kullanıcı ismi ve parola gibi bilgileri ele geçiren saldırganlar bu bilgiler ile kurbanın daha değerli bilgilerine ulaşabilmektedirler.

Yemleme saldırılarının oluşturabileceği tehditlere karşı çeşitli güvenlik önlemleri alınmaktadır. Yemlemeye karşı sahte mail tespiti için kullanılan filtreler, domain isimlerinde kullanılan kelimelerin uzaklıklarını ölçen algoritmalar, site içinde kullanılan resim veya anahtar kelimeleri kıyaslayan uygulamalar geliştirilmiştir. Fakat bu önlemler dahi tam olarak yemleme saldırılarını engelleyememektedir. Yemleme saldırılarına karşı koruma önlemlerinden en etkilisi tek kullanımlık şifreleme yöntemidir. Sabit bir şifre yerine her kullanımda değişen şifre kullanmak, saldırganların yemleme saldırısı yaparak şifreyi elde etmesini engelleyemese bile tek kullanımlık olmasından dolayı kısa süre içerisinde geçersiz olacaktır.

Statik şifreleme yönteminin tek kullanımlık şifrelemeye göre bir diğer dezavantajı ise insanların şifre olarak seçtikleri kelime veya sayıların kolayca tahmin edilebilmesinden kaynaklanmaktadır. Çağımızda insanlar mail hesapları, kredi kartı şifreleri, web sitelerine ait üyelik parolaları gibi birçok şifreyi hatırlamak durumunda kalmaktadırlar. Hatırlamalarının kolay olabilmesi için doğum tarihi, telefon numaraları, tuttuğu takımın adı gibi basit ve tahmin edilebilir şifreler kullanmaktadırlar. Bu da tekrarlama atağına karşı güvenilirlik azaltmaktadır. Tek kullanımlık şifre ise insanların şifre hatırlamasına gerek kalmaksızın güvenlik sağlamakta ve tekrarlama ataklarını kesin olarak önlemektedir.

6.1. Tek Kullanımlık Şifrenin Çalışma Prensibi

Sistem tarafından üretilen tek kullanımlık şifreler kullanıcıya güvenli ikincil bir kanaldan iletilmesi gerekmektedir. Şifre, sistem yöneticisi tarafından belirlenen bir süre içinde geçerliliği sona ermektedir. Bu nedenle şifrenin iletileceği ikincil kanalın iletim süresinin kısa olması gerekmektedir. En sık kullanılan ikincil kanallar e-posta, kısa mesaj servisleri (SMS) ve gerçek zamanlı anlık mesaj servisleridir. Bu servislerden gelen şifrenin belirlenen süre içinde sisteme girilmesi gerekmektedir. Eğer bu süre içinde girilemezse şifre geçerliliğini kaybetmektedir. OTP'nin kaba kuvvet saldırısı ile aşılmaması için ise sistem yöneticisinin belirlediği sayıda yanlış giriş yapılması durumunda, yine sistem yöneticisinin belirlediği süre kadar sisteme giriş yapılması engellenmektedir.

OTP farklı metotlar ile uygulanmaktadır. Bunlardan ilki zaman ile senkronize üretilen tek kullanımlık şifredir. Bu yöntemde belirli bir zaman aralığı için şifre üretilir. Bu metotta kullanıcının saati ile sunucu sistem saati aynı olmalıdır. Zaman bağımlı tek kullanımlık şifrelemede en büyük problem kullanıcı ve sistem saatinin senkronize çalıştırabilmektir. Oluşturulan şifre belirlenen zaman aralığı içinde geçerli olması nedeniyle zaman aralığının sürenin ayarlanması büyük önem arz etmektedir. Süre çok kısa olursa kullanıcı ikincil kanaldan şifreyi almadan geçersiz konuma düşer ve sistem kullanılamaz hale gelir. Eğer gereğinden fazla uzun olursa aynı şifrenin tekrar kullanımına sebep olunabilir. Bu da sistemin araya girme saldırısına açık hale getirebilir [62]. Bu nedenle genellikle tercih edilmemektedir.

Bir diğer metot sayaca dayalı şifre belirleme yöntemidir. Yöntemde sayacın başlangıç değeri ve kullanıcının sahip olduğu tek kullanımlık şifre oluşturan cihaz (token) ile sistem arasında paylaşılan gizli anahtar ile şifre oluşturulur. Eğer şifre yanlış ise daha önce belirlenmiş olan bir aralıkta sayaç artırılarak tekrar denenir. Eğer bu denemeler sonucunda olumsuz sonuç alınırsa şifre yanlış kabul edilir. Fakat kullanıcı şifrenin doğruluğundan emin ise sayaçların senkronizasyonu kontrol edilir. Sisteme başarılı giriş yapılan her durumda sayaç kullanıcı cihazı ve sunucu tarafından güncellenir [63].

Tek kullanımlık şifrelemede uygulanılan başka bir yöntem ise bir önceki üretilen şifreyi başlangıç değeri alarak matematiksel bir algoritma ile yeni şifreyi üretmektir [64].

6.2. Özet Fonksiyonları

Tek kullanımlık şifre oluşturmada en sık kullanılan yöntem anahtarlı özet (hash) fonksiyonudur. Özet fonksiyonları modern kriptografinin temel araçlarındandır. Veri bütünlüğünü korumak için kullanılır. Bunu yapmak için geri dönüşümsüz (tek yönlü) fonksiyonlar kullanır. Bir diğer deyişle tek yönde çözüm hesaplamak çok hızlı ve kolay iken aksi yönde işlem yapmak çok zordur. Özet fonksiyonları modern kriptografi de veri bütünlüğünü kontrol etmek için kullanılmaktadır. Haberleşmede

gönderici taraf iletmek istediği veriyi bu fonksiyonlar ile işleme sokar ve özet değeri elde eder. Veri ve özet değeri alıcıya gönderilir, alıcı verinin tekrar özetini alır ve karşı tarafın gönderdiği özet ile kıyaslar. Eğer özetler eşlenirse veri iletim kanalından değişmeden geldiği ispatlanmış olur. Günümüzde en sık kullanılan özet fonksiyonları MD5 (Message-Digest Algorithm - Mesaj Özet Algoritması), RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest - RACE Bütünlük Asli Mesaj Değerlendirme Özeti) ve SHA (Secure Hash Algorithm - Güvenli Özetleme Algoritması) ailesi algoritmalarıdır. İyi bir özet fonksiyonun aşağıdaki özellikleri sağlaması gerekmektedir [65];

- Özet fonksiyonu mesaj uzunluğundan bağımsız olmalıdır, her boyuttaki mesaj uygulanabilir olmalıdır.
- Özet fonksiyonu tüm mesaj boyutları için sabit uzunlukta çıktı üretmelidir.
- Yazılımsal veya donanımsal olarak herhangi bir girdi için özet kolayca hesaplanabilir olmalıdır.
- Özet biliniyorken özeti oluşturan ana veri bulunması zor olmalıdır.
- Farklı verilere ait iki özetin aynı olma olasılığı (collision - çakışma) çok zor olmalıdır.

Özet algoritmaları anahtarlı ve anahtarsız olmak üzere iki ana alt gruba ayrılmaktadır. Anahtarsız olan özet fonksiyonları sadece veri bütünlüğünü kontrol etmektedirler. Anahtarlı özet fonksiyonları ise veri bütünlüğü ile birlikte anahtar sahibinin kimlik doğrulamasını da yapabilmektedirler. Tek kullanımlık şifre üretirken anahtarlı olan özet fonksiyonlarından yararlanılmaktadır.

6.3. Mesaj Doğrulama Kodu (MAC)

Güvensiz ortamda iletişimin bütünlüğünü sağlamak ve kimlik doğrulama yapmak başlıca gerekliliklerdendir. Gizli anahtara dayalı bütünlük kontrolü sağlayacak mekanizmalar “Mesaj Doğrulama Kodları” (MAC) olarak tanımlanır. Anahtarsız özetleme fonksiyonları iletimi esnasında mesaj kazara veya kasti olarak değiştirilmiş

ise bu değişikliği tespit etmeye yaramaktadır. Anahtarsız özet fonksiyonları böylelikle sadece gönderilen mesajın bütünlüğünü kontrol edebilirken mesaj doğrulama kodları bütünlük ile birlikte kimlik doğrulamada yapmaktadırlar [66] [67].

M açık metin, K gizli anahtar olmak üzere f(M, K) MAC algoritmasıdır. K anahtarı (a, b) gibi bir çift katsayıdan oluşmaktadır. K = (a, b) iken f(M, K) = y = aM + b şeklinde tanımlanır.

|M| = n olmak üzere M mesajının bit sayısını göstermektedir.
P asal sayı olmak üzere |p| > n
Z_p= { 0, 1, 2, 3, ... , p-1 } modül p de tanımlı bir alandır ve +, -, *, / işlemleri tanımlıdır. Z_p alanında tanımlı işlemler aşağıdaki özelliklere sahiptir;

- + işlemine göre değişme ve birleşme özelliğine sahiptir. Birim elemanı 0'dır.
- * işlemine göre değişme ve birleşme özelliğine sahiptir ve birim elemanı 1'dir.
- Tüm elemanların toplama göre tersi vardır.
- 0 hariç tüm elemanlar çarpmaya göre tersinirdir.

MAC değerinin hesaplanabilmesi için Z_p den rastgele bir a, b çifti seçilir. f(M, K) = aM + b mod (p) değeri hesaplanır.

|f(M, k)| = |p| olduğundan MAC uzunluğu mesaj ile aynıdır. MAC değerinin açık mesaj kadar uzun olması istenir bir durum değildir. Bu nedenle p küçük bir değer seçilir. M =M_1, M_2, M_2, … M_t olacak şekilde parçalara bölünür ve her bir parça 0 <= M_i < p şartını sağlaması gerekmektedir.

$f(M, k) = € a_i M_i + b \pmod p$

Hattı dinleyen saldırgan M, y, p değerinin ele geçirebilir fakat a ve b katsayılarına ulaşamaz. y = aM + b (mod p) değerini sağlayan birden fazla katsayı çifti vardır.

Eğer saldırgan M' gibi bir değeri alıcıya kabul ettirmek isterse yeni bir MAC değeri hesaplaması gerekmektedir.

$f(M', k) = a_i M + (y - a_i M) \pmod p = a_i (M' - M) + y \pmod p$

Bu durumda saldırganın a_i değerini tahmin etmesi gerekmektedir. Z_p gibi bir alan içerisinde ait herhangi bir değer olacağından saldırganın doğru değeri tahmin etme ihtimali 1/p'dir.

Eğer gönderici ve alıcı aynı gizli anahtarı 2 kez kullanırsa, hattı dinleyen saldırganın elinde 2 bilinmeyenli 2 denklem olacaktır. Bu durumda a ve b değerleri buluna bilmektedir.

$y = f(M, k) = aM + b \pmod p$
$y' = f(M', k) = aM' + b \pmod p$
$a = y - y' / M - M' \; b = y - aM$

Anahtarsız özet fonksiyonları sadece mesaj bütünlüğünü korurken, MAC'ler kimlik doğrulamada yapabilmektedir. Anahtarsız özet fonksiyonlarının çok sayıda olmasına rağmen MAC algoritmaları fazla bulunmamaktadır. En çok bilinen MAC algoritmaları HMAC, CMAC algoritmalarıdır.

6.4. Özet Tabanlı Mesaj Doğrulama Kodu (HMAC)

HMAC algoritması 1996 yılında Mihir Bellare, Ran Canetti ve Hugo Krawczyk tarafından ortaya atılmıştır. Anahtar tabanlı mesaj doğrulama kodlarının özel bir versiyonudur. HMAC gizli bir anahtar ile özet fonksiyonunu kapsayan mesaj doğrulama kodunu hesaplamak için kullanılan özel bir yapıdır. Tek kullanımlık şifreleme algoritmalarının büyük çoğunluğu HMAC'i kullanır. Buradaki özet fonksiyonu MD5 veya SHA ailesinden (SHA-1, SHA-256, SHA-512 gibi) herhangi bir fonksiyon olabilir. Kullanılan özet fonksiyonuna göre MAC algoritmasına HMAC-MD5, HMAC-SHA1 veya HMAC-SHA2 gibi isimler tanımlanır. HMAC

algoritmalarını gücü; kullanılan özet algoritmasına, özet çıktısının boyutuna ve kullanılan gizli anahtara bağlıdır [68].

Bir mesajın HMAC'i hesaplanırken mesaj sabit uzunluklu parçalara bölünür. Örneğin MD5 ve SHA-1 algoritmaları için mesaj 512 bitlik bloklara ayrılır. Oluşan HMAC mesaj doğrulama kodunun uzunluğu ayrılan blokların uzunluğuna eşittir. İstenirse budama operasyonu geçirilerek HMAC daha kısa hale getirilebilir.

6.5. HMAC Bazlı Tek Kullanımlık şifreleme (HOTP)

HOTP algoritması OATH (Initiative for Open Authentication - Açık Kimlik Doğrulama Girişimi) tarafından 2005 yılında IETF (Internet Engineering Task Force - Internet Mühendisliği Görev Gücü)'da Java uygulaması ile birlikte yayınlanmıştır. Algoritma uzak bağlantı yapan VPN Virtual Private Network - Sanal Özel Ağ), kablosuz ağlar, web uygulamaları gibi birçok alanda kabul görmüştür. Algoritma çalıştığında 6 veya 8 karakterli nümerik şifre üretmektedir. HOTP algoritmasının sadece nümerik karakter vermesinin sebebi telefon gibi kısıtlı cihazlarda şifre girişinin kolay olmasıdır. Algoritmanın gücü kullanılan gizli anahtarın gücü ile doğru orantılıdır. En az 128 bit uzunluğunda anahtar kullanılması gerekmektedir.

s ikili (binary) dizisini göstermek üzere |s| dizinin uzunluğunu göstermektedir.
s[i] ise i. bitteki değeri ifade etmektedir. s = s[0], s[1], ... , s[n-1] olmak üzere n = |s|'yi ifade etmektedir.
s değeri onluk sisteme çevrilebilmesi için ikili dizisini sayıya çeviren StToNum fonksiyonu tanımlanır. Örneğin; StToNum (110) = 6

C: 8 baytlık sayaç değeri
K: istemci sunucu arasındaki ortak gizli anahtar

HOTP (K, C) = Budama (HMAC-SHA-1 (K, C))

HMAC hesaplanması için SHA-1 SHA-2, MD5 gibi özet algoritmalarından biri seçilir. HMAC-SHA-1 değeri hesaplanınca HMAC algoritmasından çıkan değer budama (truncate) fonksiyonuna sokulur ve 4 baytlık ikili dizisine çevrilir. Çıkan ikili dizi StToNum fonksiyonuna sokularak nümerik değer elde edilir.

HS = HMAC-SHA-1 (K, C)
Sbits = Budama (HS)
HOTP = StToNum (Sbits)

160 bitlik bir anahtar ve SHA-1 algoritması kullanıldığında HS değeri 20 baytlık olur. Bu değer budama fonksiyonu ile 4 bayta düşürülür. StToNum değeri 4 baytlık ikili dizisini 10 basamaklık nümerik değeri çevirir.

6.6. Zaman Bazlı Tek Kullanımlık Şifreleme (TOTP)

TOTP ilk olarak 2008 yılında OATH üyesi birkaç araştırmacı tarafından yayınlanmıştır. TOTP algoritması HOTP algoritmasının zamana bağlı olarak geliştirilmiş bir versiyonudur [9].

Temel olarak TOTP = HOTP (K, T) tanımlanır. Burada K önceden belirlenmiş gizli anahtardır. T ise başlangıç süresi ile sistem saati arasındaki farktan hesaplanan bir tamsayıdır. T = (Sistem zamanı – T0) / X dir. T0 başlangıç zamanı varsayılan değeri 0 dır. X ise varsayılan değeri 30 veya 60 saniye olan zaman aralığıdır. X değeri süresince tek kullanımlık şifre aynı kalmaktadır [9].

Örneğin; X değeri 30 saniye T0 değeri 0 olarak ayarlanmış ise sistem zamanı 30. saniyeden 59. saniyeye kadar T = 1'dir, saniye 60 olduğunda T = 2 olacaktır.

7. GELİŞTİRİLEN KABLOSUZ ALAN AĞ GÜVENLİK UYGULAMASI

Bu bölümde kablosuz yerel alan ağ güvenliği için geliştirilen web uygulaması açıklanmıştır. Ağ güvenliği sağlayabilmek için uygulamada eliptik eğri kriptografisi ve tek kullanımlık şifreleme kullanılmıştır.

Tez için hazırlanan web ara yüzünü geliştirmek için Microsoft Visual Studio platformunda ASP.NET (Active Server Pages - Aktif Sunucu Sayfaları) web uygulaması geliştirme teknolojisi ve C# dili kullanılmıştır. Tez uygulaması için ASP.NET web uygulama geliştirme ortamı seçilmesinin sebebi Microsoft .NET Framework'ün sağladığı kolaylıklardır. Framework web uygulaması geliştirmesi sırasında en çok sıkıntı yaşanan inşa edebilme (build), yayım (deploy), hata ayıklama (debug)'da çok büyük kolaylıklar tanımıştır. Ayrıca geliştireceğimiz güvenlik uygulaması gereği gelişmiş bir matematik ve kriptografi kütüphanesine ihtiyaç duyulmaktadır. .NET Framework'ü matematik (System.Math) ve güvenlik (System.Security) sınıfları sayesinde uygulama geliştirme esnasında zaman tasarrufu sağlamıştır.

Veri tabanı olarak ise Microsoft SQL Server 2008 ve veri tabanı ile nesneye yönelik programlama arasındaki ilişkiyi kuran Entity Framework'ü kullanılmıştır. Entity Framework, .NET platformunda ORM (Object Relational Mapping - Nesne ile İlişkisel Haritalama) araçlarındandır. Birçok kolaylığının yanında en önemli özelliği veri tabanındaki tablolara uygun nesneler oluşturmasıdır.

Uygulama çalışabilmesi için web ara yüzünü ve veri tabanını barındıran sunucu ve yüksek bant genişliği ve yönlendirme özelliğine sahip akıllı ağ anahtarı (switch) gerekmektedir. Çalışmamız esnasında sunucu olarak Intel Core i7 2.2 Ghz işlemcili 8 Gb Ram'e sahip 64 bit makine kullanılmıştır. Yönlendirme özellikli uygun ağ anahtarına sahip olunmadığından yönlendirme testleri yapılamamıştır.

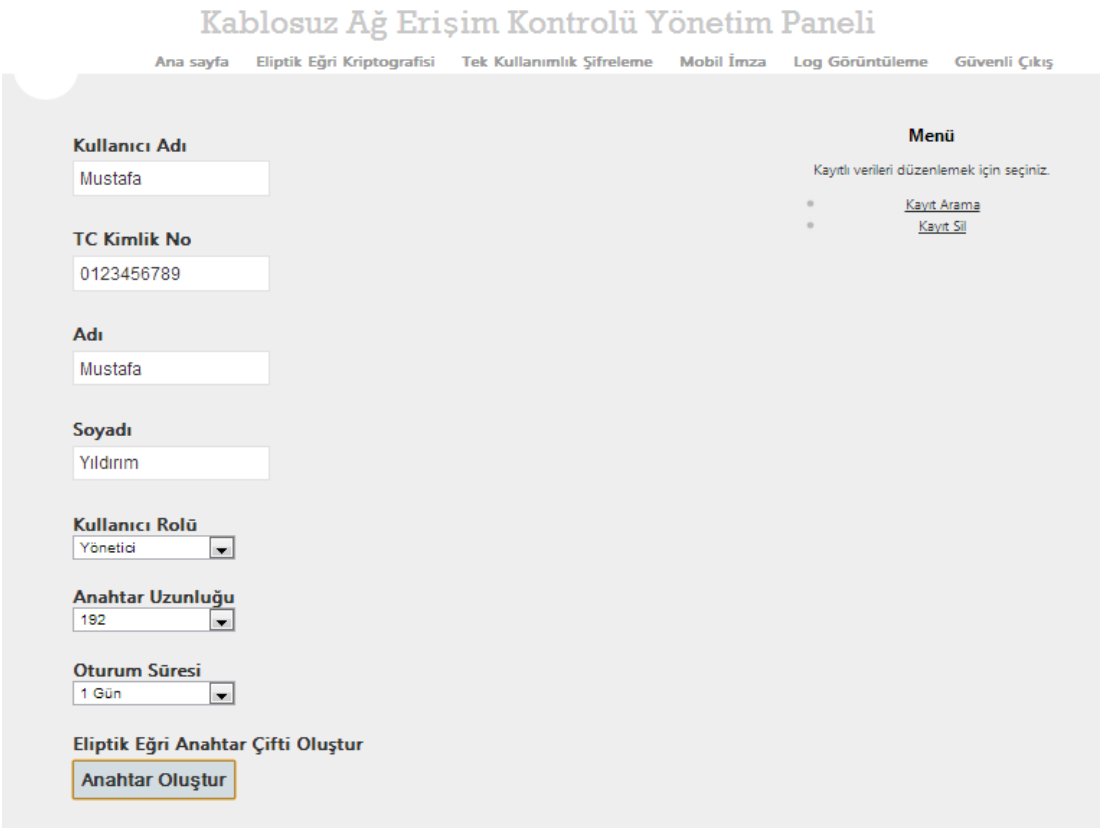
Uygulama, ağa dâhil olmak isteyen kullanıcı dizüstü bilgisayar, akıllı telefon, tablet gibi kablosuz ağ özelliği olan cihazla ağ anahtarına istek göndermesi ile

başlamaktadır. Akıllı ağ anahtarı bu istek üzerine kullanıcıya geçici ip atar. Örneğin kullanıcı 10.0.0.1 gibi geçici bir ip alır. Akıllı ağ anahtarı 10'lu ip bloğundaki kullanıcıları sadece ağ güvenliği için geliştirilen web ara yüzüne erişimine izin verir. Kullanıcılar bu ara yüz yardımı ile eliptik eğri kriptografisi veya tek kullanımlık şifreyle oturum açarlar. Oturum açabilen kullanıcıların ip adresleri 10'lu bloktan çıkarılarak farklı ip bloğuna atanır. Örneğin 192.0.0.1 gibi bir ip alan kullanıcı uygulamanın belirlediği oturum zamanı içerisinde kablosuz ağı özgürce kullanabilir.

Uygulamada oturum açmanın iki farklı yolu vardır. Bunlardan ilki eliptik eğri kriptografisi diğer ise tek kullanımlık şifrele sistemidir.

7.1. Eliptik Eğri Kriptografisi (ECC) Gerçeklemesi

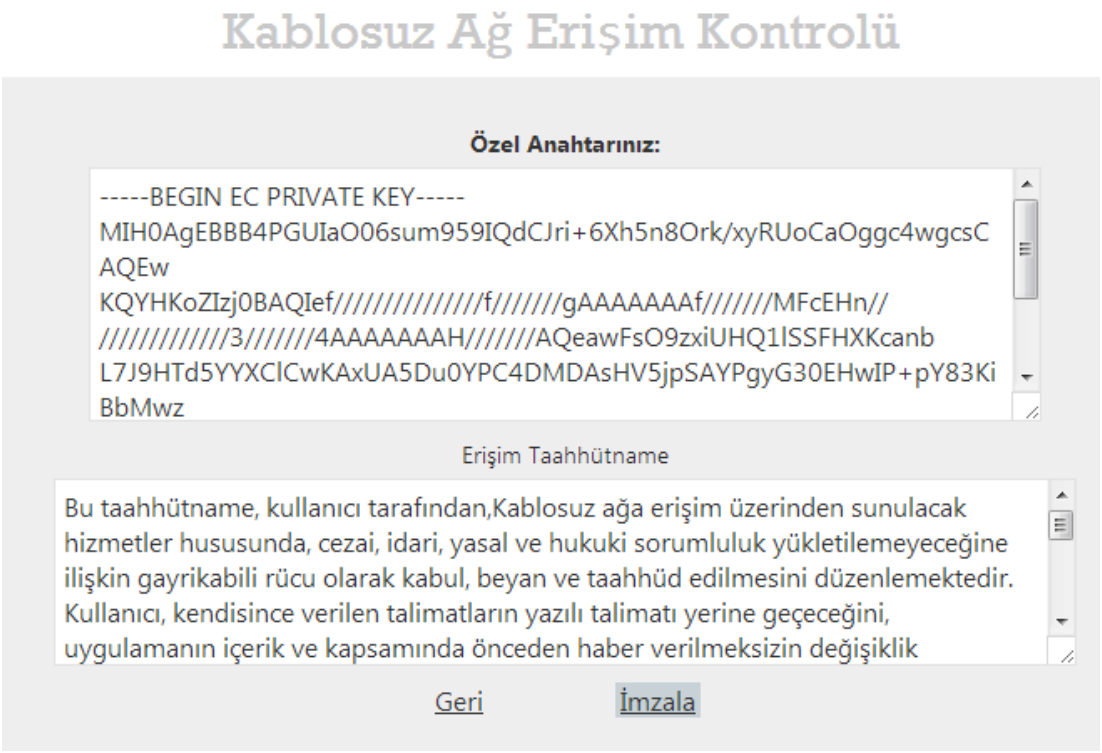
Asimetrik anahtarlı kriptografi yöntemlerinden olan eliptik eğri kriptografisi ile kullanıcının kablosuz ağa bağlanabilmesi için öncelikle sistem yöneticisinden özel ve genel anahtarını alması gerekmektedir. Sistem yöneticisi kullanıcının isteği doğrultusunda Şekil 7.1'deki gibi kullanıcıya rolü (yönetici veya kullanıcı), oturum süresi (1 saat, 8 saat, 1 gün veya 1 hafta) ve anahtar uzunluğu (192, 239, 256 bit) belirler. Bu belirlemelerden sonra istenilen uzunlukta açık ve gizli anahtar oluşturulur. Oluşturulan anahtarlar Şekil 7.2'de görüldüğü gibi kaydet butonuna basılarak hem veri tabanına hem de kullanıcıya verilmek üzere dosyaya kaydedilir. Bu anahtarlar güvenli bir kanaldan kullanıcıya iletilir.



Şekil 7.1. Kullanıcı ECC kayıt formu

Şekil 7.2. ECC ile üretilen açık ve özel anahtar

Kullanıcı vatandaşlık numarası ve sistem yöneticisinden aldığı anahtar ile giriş yapmak istediğinde Şekil 7.3'deki gibi erişim taahhütnamesini kabul etmesi ve özel anahtarı ile taahhütnameyi imzalaması gerekmektedir. Kullanıcının özel anahtarı ile imzaladığı taahhütnameden dönen imza değeri sistem veri tabanında kayıtlı olan açık anahtarı ile doğrulanabilirse sisteme başarılı bir giriş yapmış olmaktadır.



Şekil 7.3. ECC anahtarı ile taahhütname imzalama

Kullanıcı oturum açtığı andan itibaren sistem yöneticisinin belirlediği oturum saati süresince kablosuz ağı kullanabilecektir. Oturum açılması esnasında vatandaşlık numarası, oturum açış zamanı, imzalanan veri ve imza değeri gibi tüm önemli bilgiler veri tabanına kaydedilmektedir.

Eliptik eğri kriptografisi için Bouncy Castle açık kaynak kodlu kriptografi kütüphanesinden yararlanılmıştır. Anahtar üretimi (GenerateKeys), imza değeri alma (GetSignature) ve imza doğrulama (VerifySignature) için kullanılan fonksiyonlar Şekil 7.4'de gösterilmiştir.

```
public void GenerateKeys(int keySize,string path, string keyName)
{
    var gen = new ECKeyPairGenerator();
    var secureRandom = new SecureRandom();
    var keyGenParam = new KeyGenerationParameters(secureRandom, keySize);
    gen.Init(keyGenParam);
    var key = gen.GenerateKeyPair();
    publicKey = (ECPublicKeyParameters)(key.Public);
    privateKey = (ECPrivateKeyParameters)(key.Private);
    var textWriter = new StreamWriter(path+keyName+"_private.key");
    var pemWriter = new PemWriter(textWriter);
    pemWriter.WriteObject(key.Private);
    pemWriter.Writer.Flush();
    textWriter.Close();

    textWriter = new StreamWriter(path + keyName + "_public.key");
    pemWriter = new PemWriter(textWriter);
    pemWriter.WriteObject(key.Public);
    pemWriter.Writer.Flush();
    textWriter.Close();

    publicKey = (ECPublicKeyParameters)readPublicKey(path + keyName + "_public.key");
    privateKey = (ECPrivateKeyParameters)readPrivateKey(path + keyName + "_private.key");

}
public byte[] GetSignature(string plainText, ECPrivateKeyParameters privateKey)
{
    var encoder = new ASCIIEncoding();
    var inputData = encoder.GetBytes(plainText);
    var signer = SignerUtilities.GetSigner("ECDSA");
    signer.Init(true, privateKey);
    signer.BlockUpdate(inputData, 0, inputData.Length);
    return signer.GenerateSignature();
}
public bool VerifySignature(ECPublicKeyParameters publicKey, string plainText, byte[] signature)
{
    var encoder = new ASCIIEncoding();
    var inputData = encoder.GetBytes(plainText);
    var signer = SignerUtilities.GetSigner("ECDSA");
    signer.Init(false, publicKey);
    signer.BlockUpdate(inputData, 0, inputData.Length);
    return signer.VerifySignature(signature);
}
```

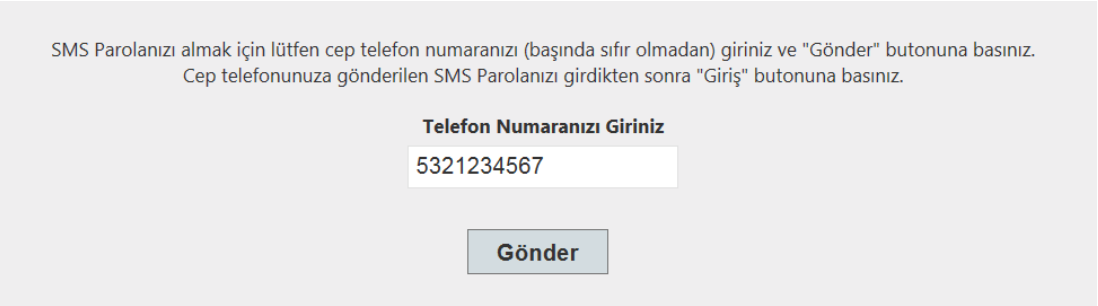
Şekil 7.4. ECC anahtar üretimi, imzalama ve imza doğrulama fonksiyonları

Anahtar üretimi fonksiyonu anahtar uzunluğu, oluşturulan anahtarın kayıt yeri ve anahtar ismi parametrelerini almaktadır. İmza değeri fonksiyonu imzalanacak açık metni ve imzalayacak kullanıcının özel anahtarını parametre olarak almakta ve imza değerini bayt olarak geri döndürmektedir. İmza doğrulama fonksiyonu ise imza atan kişinin açık anahtarını, açık metni ve imza değerini almakta geriye doğru (true) veya yanlış (false) olarak değer döndürmektedir.

7.2. Tek Kullanımlık Şifreleme (OTP) Gerçeklemesi

Tek kullanımlık şifre gerçeklemesinde düşünülen senaryo kullanıcının kablosuz yerel alan ağ erişim sistem yöneticisine daha önce herhangi bir bilgi vermeksizin sadece telefonuna gönderilen tek kullanımlık şifre ile ağa dâhil olabilmesi üzerine kurgulanmıştır. Bu nedenle eliptik eğri gibi kullanıcının daha önceden sistem yöneticisi ile temasa geçmesine gerek yoktur.

Ağa dahi olmak isteyen kullanıcı eliptik eğride olduğu gibi akıllı ağ anahtarı tarafından kablosuz ağ erişim kontrolü sağlayan web ara yüzüne yönlendirilir. Kullanıcı erişim taahhütnamesini kabul edip Şekil 7.5'deki cep telefonunu numarasını girerek tek kullanımlık şifre isteğinde bulunur.



Şekil 7.5. OTP isteği

Sistem aldığı cep telefonu numarasının daha önce giriş yapıp yapmadığını veri tabanından kontrol eder. Eğer ilk kez giriş yapıyorsa kullanıcıya ait ortak gizli anahtar oluşturur, sayacı birden başlatır ve özet tabanlı tek kullanımlık şifre (HOTP) oluşturur. Eğer daha önce giriş yapmış ise ortak gizli anahtarı veri tabanından alınır ve son sayaç numarası bir artırılarak yeni tek kullanımlık şifresi oluşturulur. Oluşturulan şifre SMS geçidi (SMS gateway) yardımı ile kullanıcının cep telefonuna gönderilir. SMS deki şifre 3 dakika içerisinde sisteme doğru olarak girildiği takdirde kullanıcı başarılı bir şekilde oturum açmış olur. Şekil 7.6'da görüldüğü gibi 3 dakika içerisinde girilemeyen şifreler geçersiz duruma düşer ve sistem kullanıcıyı başlangıç sayfasına yönlendirir.

Şekil 7.6. SMS ile gelen OTP'nin giriş ekranı

Uygulama tek kullanımlık şifre ile erişim sırasında telefon numarası, oturum gizli anahtarı, OTP, ip adresi, tarih gibi tüm gerekli kütük (log) bilgilerini veri tabanına kaydetmektedir. Ayrıca kütüklerin özeti (hash) alınarak kayıtların bütünlüğü korunmaktadır. Başarılı giriş yapılması durumunda Şekil 7.7'deki görüldüğü gibi 2 saatlik oturum süresi başlamış olur.

Şekil 7.7. Başarılı giriş sayfası

Tek kullanımlık şifre oluşturulmasında OtpSharp ve .NET framework'e ait güvenlik (System.Security.Cryptography) kütüphanesi kullanılmıştır. Oluşturulan şifrenin gönderilebilmesi için SMS geçidi hizmeti veren bir web servis kullanılmıştır.

Kullanıcı ilk kez tek kullanımlık şifre ile erişim sağlamak istiyorsa, uygulama .NET kütüphanesi aracılığı ile 256 bit anahtar uzunluğuna sahip bir oturum anahtarı üretilir

ve sayaç değeri 1 yapılır. Eğer daha önce giriş yapılmış ise veri tabanından önceki oluşturulan anahtar çekilir ve sayaç bir artırılır. Çizelge 7.1 de örnek telefon numarası, sayaç değeri, gizli anahtar ve tek kullanımlık şifre değerleri gösterilmiştir.

Çizelge 7.1. OTP, sayaç ve oturum anahtarı

Telefon Numarası	Sayaç No	Oturum Anahtarı	OTP
511 111 11 11	1	6bc6d7489af203b01c955b945c585102d12653fdaa66ee93606d8508ab72640b28bac4ff2d091c28ab0904530dee14166cf95220abd60a90f3223c36ce99f43c	231081
522 222 22 22	1	157fda685a82c4de5973e035712b9be1a3d80fbb42bed5db0efcff81a712b2be8672d5f1ba63fb0d235a1c3a3a581f0190bbda54c0b9142e077c11c72093e483	789495
533 333 33 33	1	94690552991849460b0a671c5fc5c55cd8d5da7849bb5c648cd8e670ea6909829bb4bbe78c9e48a3d1cd2c2617f52e99af372314ea712a9035bd90e5aeee6eb5	590193
511 111 11 11	2	6bc6d7489af203b01c955b945c585102d12653fdaa66ee93606d8508ab72640b28bac4ff2d091c28ab0904530dee14166cf95220abd60a90f3223c36ce99f43c	329676
511 111 11 11	3	6bc6d7489af203b01c955b945c585102d12653fdaa66ee93606d8508ab72640b28bac4ff2d091c28ab0904530dee14166cf95220abd60a90f3223c36ce99f43c	865360
522 222 22 22	2	157fda685a82c4de5973e035712b9be1a3d80fbb42bed5db0efcff81a712b2be8672d5f1ba63fb0d235a1c3a3a581f0190bbda54c0b9142e077c11c72093e483	058266

7.3. Alınan Diğer Güvenlik Önlemleri

Bu bölümde erişim güvenliği için geliştirilen web uygulamasının güvenliğinin sağlanabilmesi için alınan diğer güvenlik önlemlerinden bahsedilecektir. Bilindiği üzere özellikle güvenlik sistemlerinde küçük bile olsa bir güvenlik açığının olması tüm sistemin güvensiz hale gelmesine yetmektedir. Bu nedenle literatür çalışması sırasında çok sık karşımıza çıkan SQL enjeksiyonu (SQL injection), kablosuz ağ dinleme (sniffer), paket yakalama veya veri bütünlüğünü bozma gibi saldırılara karşı önlemler alınmıştır.

7.3.1. ECC ile üretilmiş SSL sertifikalı yayın

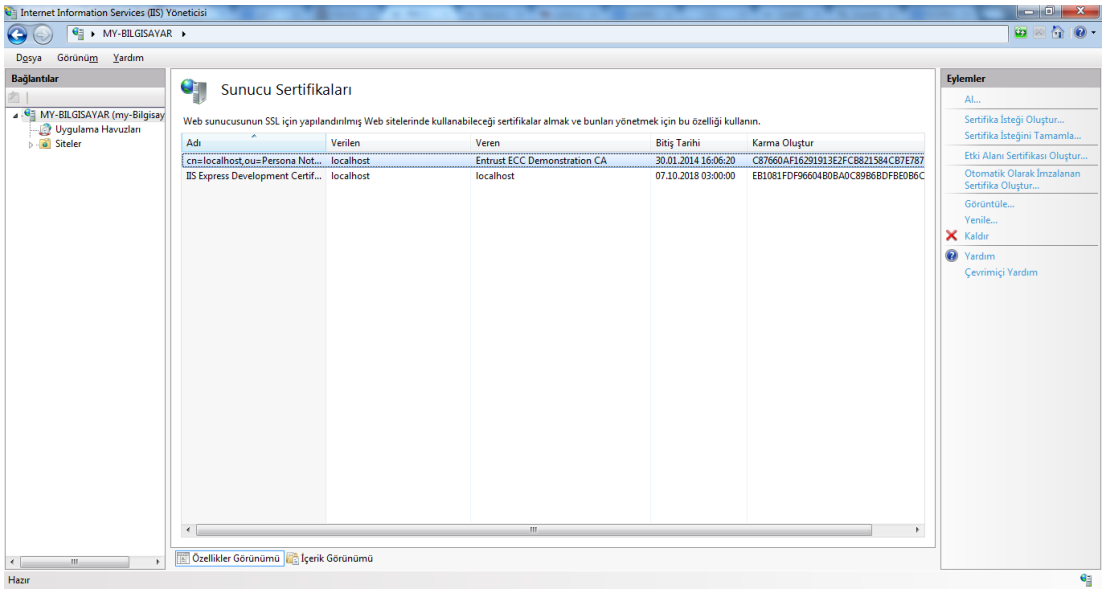
Netspace firması tarafında 1994 yılında geliştirilen sonraki yılda IETF tarafından standartlaştırılan SSL (Güvenli Giriş Katmanı - Secure Soket Layer) [69] protokolü temel olarak web tarayıcı ile web sunucusu arasındaki http trafiğini şifrelemek için kullanılmaktadır. SSL sertifikası açık anahtarlı kriptografi temellidir.

SSL sertifikası asimetrik anahtarlı kriptografi de en yaygın kullanılan X.509 sertifika ailesine dâhildir. X.509 standardı 1999 yılında IETF tarafından RFC 2459 (Request For Comments - Yorumlar için Talep) olarak yayınlanmıştır. X509 ailesinden olan SSL sertifikasının oluşturan temel bölümler sertifikayı yayınlayan kurumun veya sertifika sahibinin adı, açık anahtar, geçerlilik süresi (başlangıç ve bitiş tarihleri), açık anahtar algoritması (RSA, DSA, ECC gibi), sertifika makamının imzalama algoritması (RSA-MD5, RSA-SHA-1, ECDSA (Elliptic Curve Digital Signature Algorithm)), sertifika makamının imzasıdır [70].

Sertifika makamı (VeriSign, GlobalSign gibi), sertifikayı veren ve doğruluğunu garanti eden kuruluştur. Sertifika makamı sahip olduğu kök sertifikadan yeni sertifikalar üretirler. Kök sertifikadan üretilen yeni sertifikalar ile imzalanan veriler kök sertifika sahibi kuruluşun güvencesi altında olmaktadır.

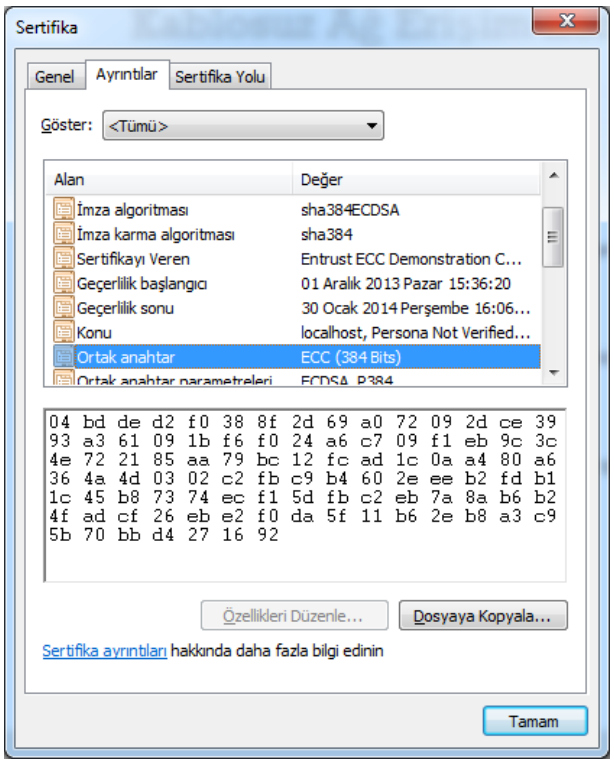
Uygulama için Entrust firması tarafından üretilen SSL sertifikası kullanılmıştır. Sertifika ECC 384 bit anahtar boyuna sahiptir. Aynı güvenlik seviyesinin sağlanabilmesi için yaklaşık RSA 2048 bitlik bir anahtar kullanımına ihtiyaç vardır. Anahtar boyunun kısalması hem istemci hem de sunucu için güvenlik seviyesini düşürmeden büyük bir kaynak tasarrufu sağlamaktadır. 384 bitlik ECC anahtarı ile istemci ve sunucu arasındaki iletişim sırasında paketleri şifreleyecek olan oturum anahtarı, veri bütünlüğünü kontrol edecek algoritma paylaşılır. İstemcinin ilk istekte bulunduğu anda SSL sertifikasındaki açık anahtar ile yapılan bu işlem el sıkışma olarak adlandırılır. El sıkışma işlemi başarılı olarak tamamlanması durumunda istemci sunucu arasındaki bütün paketler oturum anahtarı ile şifrelenir.

Web uygulaması Microsoft IIS (Internet Information Services - İnternet Bilgi Servisleri) yayınlanmıştır. Yapılan yayının SSL sertifikası ile yapılabilmesi için Entust firmasında alınan PKCS#12 (Public Key Cryptography Standards - Açık Anahtarlı Kriptrografi Standardı) formatındaki özel anahtar IIS üzerinden Şekil 7.8'deki gibi sunucu sertifikalarına eklenmiştir. Anahtarın eklenmesi ile site HTTPS (Secure Hypertext Transfer Protocol - Güvenli Hiper Metin Aktarım İletişim Kuralı) olarak 443. porttan yayın yapabilir hale gelmiştir.



Şekil 7.8. SSL sertifikası eklenmesi

Kullanıcı kablosuz yerel alan ağ erişim kontrolü uygulaması web ara yüzene eriştiğinde, web tarayıcısı üzerinde asma kilit simgesi görecektir. Simge SSL sertifikası ile güvenli iletişim kurulacağını göstermektedir. Simge üzerine çift tıklamayla Şekil 7.9'daki gibi sertifika bilgilerine ulaşılmaktadır.



Şekil 7.9. ECC 384 bitlik SSL sertifikası

7.3.2. CAPTCHA testi

CAPTCHA (İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi - Completely Automated Public Turing test to tell Computers and Human Apart) [71] testi Carnegie Mellon Üniversitesi'nde geliştirilmiştir. Testin temeli 1912 - 1954 yıllarında yaşayan matematik ve bilgisayar bilimci Alan Turing tarafında atılmıştır. Alan Turing yaptığı çalışmalarda makinelerin insanlar gibi düşünme yetisine sahip olup olamayacağını araştırmıştır. Bunun için Turing testi adını verdiği bir test önermiştir. Bu testte sorgulayıcı göremediği bir alanda bulunan insan ve makineye sorular yöneltmektedir. Soruların cevapları ses gizlenerek sadece klavye ile girilmekte ve sorgulayıcının ekranına yazı olarak düşmektedir. Sorgulayıcı sorduğu

sorulara aldığı cevaplara göre insanı makineden ayıramaz ise makine Turing testini geçmiş olmaktadır.

CAPTCHA Turing testindeki gibi makine ve insan ayrımı yapılması için kullanılmaktadır. Bunu yapmak için arka planda rastgele oluşturduğu sayıyı grafik olarak çizip sadece insanların okuyabileceği bir forma döndürmektedir. Oluşturulan grafik üzerindeki sayıları internet robotu (bot) okuyamaz olacaktır.

Erişim kontrolü uygulamasının tek kullanımlık şifre gönderme ara yüzünde cep telefonu numarası girerek SMS gönderme sırasında CAPTCHA yazılımı eklenmiştir. Böylelikle herhangi bir internet robotu sadece telefon numarası giriş bölümüne yazdığı numaralar ile SMS trafiğini gereksiz yere işgal edemeyecektir. Şekil 7.10'da oluşturulan CAPTCHA örneği gösterilmiştir.

Şekil 7.10. CAPTCHA örneği

7.3.3. Yapılandırılmış Sorgu Dili (SQL) enjeksiyonu

SQL dili çok sayıda veri tabanı ürünün desteklediği yapısal bir sorgulama dilidir. SQL birçok kişi tarafında programlama dili olarak bilinse de aslında bir programlama dili değildir. SQL, en basit tanımı ile verileri yönetmek ve üzerinde ekleme, güncelleme silme gibi işlemleri yapabilmek için tasarlanmıştır.

SQL enjeksiyonu sızma saldırılarının bir türüdür. Web uygulamalarında kullanıcıdan alına girdi bölümleri kullanılarak sisteme zarar veren SQL komutları göndermek tekniğidir. Özellikle kullanıcı adı ve parola ile giriş yapılan sistemlerde çok sık kullanılan aşağıdaki SQL cümlesi ile örnek vermek gerekirse;

"SELECT * FROM Kullanicilar WHERE KullaniciAdi = ' " + TextAdi + " ' AND Parola = ' " + TextParola + " ' ";

Bu cümle kullanıcı adını ve parolayı 'Kullanicilar' tablosunda eşleşmesi ile sisteme giriş için kullanılır. Saldırgan "TextAdi" bölümüne '1 or 1=1 – – gibi bir ifade yazdığından sorgumuz;

SELECT * FROM Kullanicilar WHERE KullaniciAdi = ‘ 1 or 1=1 -- AND Parola = '123'

Cümlemiz KullaniciAdi bölümü 1 ise veya 1 eşittir 1 ise giriş yapsın olmaktadır. -- işaret SQL komutlarında yorumun başladığını göstermektedir. Böylece parola kontrolü yapılmamış olur.

SQL enjeksiyonu saldırısı basit dahi olsa çok etkili bir güvenlik açığıdır. Saldırgan bu atakla kimlik doğrulama mekanizmalarını aşabilmektedir. Bu nedenle gerçekleştirilen uygulamada bu saldırıya karşı önlem alınmıştır. Kullanıcıdan giriş yapması beklenilen tüm alanlarda SQL dilindeki özel karakterleri süzen bir filtre fonksiyonu tanımlanmıştır. Böylelikle saldırgan SQL dilinde "*", "--", """, "\", "=", gibi SQL dilinde özel anlamlara sahip karakter ve işaretlerin girmesi engellenmiştir.

7.4. Geliştirilen Protokollerin Var Olanlar ile Karşılaştırılması

Bu bölümde tez uygulamasında gerçeklenen güvenlik protokolleri kablosuz yerel alan ağlarında kimlik doğrulamada kullanılan WEP, WPA, WPA-2 gibi protokoller ile karşılaştırılmaktadır. Uygulamada gerçeklenen OTP protokolü, WEP veya WPA gibi kablosuz ağ cihazı üreticileri tarafından standart olarak kullanılmamakla birlikte çeşitli firmalar tarafından üretilen yazılım veya donanım ile ayrı bir ürün olarak alınabilmektedir. Fakat açık anahtar altyapısına sahip ECC ile kimlik doğrulama protokolü ise ilk kez önerilmiştir. Literatür çalışmalarına bakıldığında herhangi bir açık anahtar altyapısı kullanılarak kablosuz yerel alan ağlarda kimlik doğrulama protokolü önerilmemiştir. Geliştirilen uygulama üzerinde yapılan testler sonucu ECC algoritması ile erişim güvenliği ve kimlik doğrulamada başarılı sonuçlar vermiştir. Açık anahtar algoritmalarının hesaplama karmaşasından kaynaklanan yavaşlık kısıtlı kaynaklara sahip kablosuz ağ cihazları yerine sunucu üzerinde gerçekleşmesi sebebiyle hissedilemeyecek ölçüde azaltılmıştır. Ayrıca açık anahtarlı algoritmalarından bilişim dünyasında yaygın olarak kullanılan RSA, DSA gibi algoritmalarda yaşanan güvenlik seviyesinin yükseltilmesi için anahtar boyu uzun tutulması problemini aşan ECC algoritması kullanılmıştır. ECC algoritmasının kullanılması zaman ve kaynak tasarrufu sağlanmasında önemli katkı sağlamıştır.

Kablosuz ağ teknolojisine sahip taşınabilir cihazların artması ile insanların okul, hastane, otel, hava alanı gibi kamuya açık alanlarda var olan kablosuz ağa bağlanarak internet erişimi sağlama talepleri ortaya çıkmıştır. WEP, WPA gibi sabit parolaya bağlı protokollerle kamuya açık alanlarda erişim kontrolü ve kimlik doğrulama için yetersizdir. Tüm kullanıcıların aynı parola ile giriş yapması ve parolanın güvenli bir şekilde dağıtılması imkânsızdır. Bu güvenlik probleminin aşılması için kamu alanındaki ağdan yararlanmak isteyen kullanıcının vatandaşlık ve cep telefonu numarası alınarak tek kullanımlık şifre gönderme yöntemi ile güvenlik sağlanması önerilmiştir. Kullanıcıların girdiği vatandaşlık numarasını kontrol eden bir fonksiyon çalıştırılarak gerçek bir vatandaşlık numarası olup olmadığı kontrolü yapılmıştır. Cep telefonu numarasının ise tek kullanımlık şifreyi SMS yoluyla alabilmesi için doğru numarayı girmesi gerekmektedir. Uygulama kullanıcıdan alınan vatandaşlık

numarası, cep telefonu numarası, ip adresi, tarih gibi önemli tüm bilgileri veri tabanında özetleri ile birlikte saklamaktadır. Böylelikle kamuya açık alanlarda erişim güvenliği ve kimlik doğrulama WEP veya WPA protokollerine göre çok daha etkin bir şekilde gerçekleştirmektedir.

Var olan sistemlerde tüm kullanıcılar aynı parola ile ağa bağlanarak tek taraflı kimlik doğrulama yapmaktadır. Erişim noktasına bağlanmak isteyen istemciye parola kontrolü yaparak kimlik doğrulama sağlamaktadır. Fakat istemci doğru erişim noktasına bağlandığının kontrolünü yapamamaktadır. Bu açıktan dolayı saldırganlar aynı SSID ismini kullanarak istemcileri kendi erişim noktalarına çekmekte ve ağa giriş parolası veya diğer önemli bilgilerini alabilmektedirler. Uygulamada ECC algoritması kullanılmasıyla özel anahtara sahip istemciyi açık anahtar doğrulamakta, tam tersi işlemle istemci sunucuyu doğrulamaktadır.

WEP, WPA, WPA-2 gibi klasik erişim kontrolü protokollerde belirli karakter uzunluğuna sahip parola kullanılmaktadır. Parola alfa nümerik karakterlerden oluşmak zorundadır. Bu parolayı ağa bağlanmak isteyen kullanıcı hatırlamak durumunda kalmaktadır. İnsanların unutma zafiyetinde dolayı tahmin edilebilmesi kolay anlamlı sözcükler veya doğum tarihi, önemli yıllar, telefon numaraları gibi tahmini kolay sayılar parola olarak belirlenmektedir. WEP veya WPA protokollerindeki insan zafiyetinden kaynaklanan bu güvenlik boşluğunu yeni önerilen erişim kontrolü protokolleri aşmış durumdadır. ECC ile erişim kontrolü protokolünde kullanılan en küçük anahtar boyu 192 bittir. Anahtar sahibi özel anahtarını güvenli bir cihaz (token) aracılığı ile taşıdığı için hatırlama gibi bir zorunluluğu yoktur. 192 bit uzunluğundaki ECC anahtarının süper bilgisayarlar tarafından dahi tahmin edilebilmesi yıllar alacaktır. OTP ile erişim kontrolü sırasında ise kullanıcının hatırlaması gereken bir parola yoktur. OTP her girişte yeniden oluşturulduğu için saldırganlar tahmin edebilse bile sonraki girişte şifre değişmiş olacağında süreklilik sağlayamayacaklardır.

WEP algoritması bütünlük kontrolü için 32 bitlik lineer metot ile hesaplanan ICV algoritmasını, WPA ise 64 bit uzunluğundaki MIC (Message Integrity Code - Mesaj

Bütünlük Kodu) algoritmasını kullanmaktadır. Bütünlük kontrolü algoritmalarının en büyük problemi çakışma denilen iki farklı verinin aynı özete sahip olması durumudur. 128 bit uzunluğunda özet üreten MD5 algoritmasında çakışma bulmak için yaklaşık 2^{64} deneme yapmak gerekmektedir. Bu deneme sayısında 1 günde ulaşmak mümkün olduğunda daha önce uluslararası standartlarda kabul edilen MD5 algoritması standartlardan çıkartılmıştır [72]. WEP ve WPA da kullanılan bütünlük kontrolü algoritmalar ise MD5 algoritmasına göre çok daha az deneme sayısı ile çakışma yakalanabilmektedir. WEP ve WPA bütünlük kontrolü algoritmalarının yetersiz olduğu aşikârdır. Yeni önerilen ECC ve OTP yöntemlerinde ise bütünlük kontrolü için uluslararası standartlara uygun SHA 256 bitlik özetler kullanılmıştır. SHA 256 özet algoritması ayrıca veri tabanı kayıtlarının bütünlük kontrolü için kullanılmıştır.

8. SONUÇ ve ÖNERİLER

Bu tezde kablosuz yerel alan ağlarında erişim kontrolü ve kimlik doğrulama üzerine çalışılmıştır. Kablosuz erişim kontrolü ve kimlik doğrulama için ilk geliştirilen WEP protokolüdür. WEP protokolünün birçok güvenlik açığının olması nedeniyle sırasıyla WPA, WPA-2 gibi protokoller geliştirilmiştir. Fakat bilgisayarın işlem kapasitelerinin artması, internet hızını yükselmesi, siber korsanların organize olarak siber ordulara dönüşmesi gibi nedenlerden dolayı WPA algoritmaları erişim kontrolü ve kimlik doğrulamada yetersiz hale gelmiştir. Bununla birlikte kablosuz iletişim özelliğine sahip dizüstü bilgisayar, tablet, akıllı telefon gibi cihazların hayatımıza girmesiyle kablosuz ağlara olan ihtiyacımızda giderek artmıştır. Bu çalışmada günümüzde kullanılan erişim kontrolü ve kimlik doğrulama protokollerindeki güvenlik zafiyetlerinin giderilmesi için 3 farklı güvenlik seviyesine sahip erişim kontrolü ve kimlik doğrulama sağlayacak yöntem önerilmiştir.

Bunlardan ilki ve en yüksek güvenlik seviyesine sahip eliptik eğri kriptografisidir. ECC'si asimetrik anahtarlı yöntemlerdendir. WEP, WPA gibi protokoller simetrik anahtarlı şifreleme algoritmalarını kullanmaktadır. Literatür çalışmaları asimetrik anahtarlı kriptografi yöntemlerin simetrik anahtarlı yöntemlere göre çok daha güçlü bir güvenlik sağladığı gösterilmiştir. Bu nedenle kablosuz ağ teknolojisinde açık anahtarlı eliptik eğri kriptografisi ile erişim güvenliği ve kimlik doğrulama önerilmiştir. Açık anahtarlı yöntemlerin kimlik doğrulama ve güvenlik seviyesinin yüksek olmasına rağmen hesaplama karmaşasından kaynaklanan zaman ve performans kayıpları olabilmektedir. Fakat yapılan çalışmada erişim kontrolü ve kimlik doğrulama için kısıtlı kaynaklara sahip kablosuz ağ cihazları yerine yönlendirme yapılarak sunucu üzerinde işlemler yapılmıştır. Böylelikle olası zaman kayıplarının önüne geçilmiştir. Ayrıca asimetrik anahtarlı yöntemlerden kısa anahtar boyu ile yüksek seviye güvenlik sağlayan eliptik eğri kriptografisinin seçilmesi performansı artırmıştır. Tez kapsamında geliştirilen eliptik eğri ile erişim kontrolü ve kimlik doğrulama uygulamasında yapılan testlerde başarılı sonuçlar alınmıştır.

Önerilen bir diğer güvenlik protokolü günümüzde birçok farklı alanda uygulanan mobil imza teknolojisidir. Mobil imza bilindiği gibi ıslak imzaya denk, elektronik ortamlarda hukuki geçerlilik kazandıran bir teknolojidir. Bu teknolojinin arkasında yine asimetrik anahtarlı kriptografi bulunmaktadır. Ülkemizdeki GSM operatörleri mobil imza hizmeti verebilmektedir. Kablosuz ağda erişim güvenliği sağlayan uygulamalar kullanıcılardan "Erişim Taahhütnamesi" adı altında erişimde uyulması gereken kurallarla ilgili bir yazıyı kabul etmemizi istemektedirler. Fakat yazının kabul edilmesi hukuken hiçbir yaptırıma sahip değildir. Elektronik ortamda hukuken geçerlilik sağlanabilmesi için taahhütnamenin mobil veya elektronik imza ile imzalanması gerekmektedir. Var olan uygulamalarda bu durum eksik bırakılmıştır. Mobil imza ile kablosuz yerel alan ağlarında erişim kontrolü ve kimlik doğrulama yapılması durumunda imzalanan erişim taahhütnamesi hukuken geçerli bir evrak durumuna gelecektir. Tez uygulaması içerisinde mobil imza hizmeti veren operatörlerden destek alamadığımızdan dolayı mobil imza ile erişim kontrolü ve kimlik doğrulama uygulaması gerçekleştirilememiştir.

Önerilen son protokol ise tek kullanımlık şifre göndererek erişim kontrolü ve kimlik doğrulama yapmaktır. Diğer yöntemlere göre daha düşük güvenlik seviyesinde olmasına rağmen erişim güvenliği uygulamalarında en çok kabul gören yöntemdir. Bunun en önemli sebebi insanların taşınabilir cihazlar yardımıyla okul, hastane, hava alanı gibi kamuya açık yerlerde kablosuz ağa erişim sağlama taleplerinden kaynaklanmaktadır. Kamu alanlarındaki kablosuz ağdan yararlanmak isteyenlerin kullanıcılar kısa süre içerisinde kimlik doğrulaması yapılarak ağa dâhil edilmesi gerekmektedir. Bunun en kolay ve en etkin yolu kullanıcıdan cep telefonu numarası alınarak üretilen tek kullanımlık şifreyi gönderme olmaktadır. Statik parolaya bağlı WEP, WPA ve WPA-2 gibi protokoller ile kamuya açık ağlarda erişim kontrolü ve kimlik doğrulama yapmak neredeyse imkânsızdır. Tez uygulaması sırasında gerçekleştirilen HOTP algoritması kullanılarak tek kullanımlık şifre ile erişim güvenliği ve kimlik doğrulama protokolü, oluşturduğu 6 veya 8 basamaktan oluşan şifreyi SMS yolu ile kullanıcının cep telefonuna göndermektedir. Kullanıcı telefonuna gelen şifreyi 3 dakika içerisinde sisteme doğru şekilde girerek oturum

açabilmektedir. Yapılan testler tek kullanımlık şifre ile kısa süre içerisinde güvenli şekilde erişim kontrolü ve kimlik doğrulama yapıldığını göstermiştir.

Tez çalışması esnasında yapılan araştırmalar ve incelemeler sonucu kablosuz yerel alan ağ güvenliği hakkında birçok kazanım elde edilmiştir. Bu kazanımlar ışığında gelecekteki akademik ve sosyal hayata yönelik çalışmalar hakkında birkaç öneri sunulacaktır. Hayatımızda rahat şekilde fark edebileceğimiz kamusal alanlardaki kablosuz ağ erişiminin artması sonucu ağ erişim kontrolü ve kimlik doğrulamadaki sıkıntıları giderecek güvenli bir çözüme ihtiyaç vardır. Bunun için önerdiğimiz mobil imza gibi daha önce kablosuz ağ sistem yöneticisi ile irtibata geçmeden kimlik doğrulama yapabilecek bir protokolün ihtiyacıdır. Özellikle yakın gelecekte planlanan, şehirlerin tamamını kapsayan kablosuz ağ sistemlerinin kurulması ile erişime yasal sorumluluk yükleyen mobil imza yönteminin hayata geçirilmesi zorunlu hale gelecektir. Bir diğer öneri geliştirdiğimiz uygulama esnasında kişileri vatandaşlık numaralarını, vatandaşlık numaraları kontrol fonksiyonu ile kontrol ettirilmiştir. Bunun yerine MERNİS (Merkezî Nüfus İdare Sistemi) sistemi ile kontrol sağlamak kimlik doğrulama açısından daha etkin bir yöntem olacaktır. Aynı şekilde tek kullanımlık şifre gönderirken alınan telefon numaraları operatörlerden destek alınarak numara sahibinin vatandaşlık numarası veya adı ve soyadı gibi bilgilerle eşleştirme güvenliği artırıcı olacaktır. Kablosuz yerel alan ağ erişim güvenliği ve kimlik doğrulama uygulamasının kullanım yerindeki güvenlik hassasiyetine göre giriş çıkış saatleri veya SMS ile tek kullanımlık şifre gönderme zamanı sistem saati yerine daha hassas ve güvenilir olan atom saati kullanılarak zamanın kesinliği artırılabilir. Yapılacak son öneri ise kısa anahtar boyuna rağmen çok yüksek güvenlik sunan eliptik eğri kriptografisinin güvelik sistemlerinde yaygın şekilde kullanılması ile zaman, güç tasarrufu ve performans kazancını sağlamaya yönelik çalışmaların artırılması olacaktır.

KAYNAKLAR

1. Özdemir, B., "Kablosuz Yerel Alan Ağı Güvenliği Kılavuzu", ***Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü,*** Kocaeli, Türkiye, 8-14, (2008).

2. Regan, K., "Wireless LAN Security: Things You Should Know about WLAN Security", ***Network Security***, Amsterdam, The Netherlands,7-9, (2003).

3. Wilhelm, T., "Professional Penetration Testing (Second Edition)", ***Syngress,*** Waltham, USA , 323-338, (2009).

4. Schmoyer T.R., Lim Y.X., Oewn H.L.,"Wireless Intrusion Detection and Response: A case study using the classic man in the middle attack", ***Information Assurance Workshop***, New York, USA, 68-75, (2003).

5. Denis, T., "Crytography of Developers", ***Syngress Punlishing***, Rockland, MA, USA, 389,391-400, (2006).

6. Tokdemir, A.İ., "Mobil Elektronik İmza İşlemi Kullanıcı Kılavuzu", ***İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı***, Ankara, 3-4, (2013).

7. Zhang, L., Wu, W., Wang, P., Liang, B., "Another Look at CBC-MAC", ***Information Processing Letters***, Beijing, China, 302-307,(2012).

8. M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., Ranen, O., "HOTP: An HMAC-based One-Time Password Algorithm", ***IETF RFC 4226***, California, USA, 4-8, (2005).

9. M'Raihi, D., Machani, S., Pei, M., Rydell, J, "TOTP: Time-Based One-Time Password Algorithm", ***IETF RFC 6238***, California, USA, 3-5, (2011).

10. Schmeh, K., "Cryptography and Public Key Infrastructure on Internet", ***John Wiley & Sons Inc***, Bochum,Germany, 9-14, (2003).

11. Hankerson, D., Menezes, A., Vanstone, S., "Guide to Elliptic Curve Cryptography", ***Springer***, New York, USA, 1-21, (2003).

12. Menezes, A.J., Oorschot, P. C. V., Vanstone, S. A., "Handbook of Applied Cryptography", ***CRC Press***, Florida, USA, 361-367, (1997).

13. Stallings , W., "Cryptography and Network Security", ***Prentice Hall***, 2nd Ed., New Jersey, USA,1-28 (1999).

14. Shannon, C.E., "Communication Theory of Secrecy Systems", ***A Mathematical Theory of Cryptography,*** Newyork, USA, 657-715, (1946).

15. Schneier, B.,"Applied Cryptography: Protocols, Algorithms, and Source Code in C", ***John Wiley & Sons Inc***, 2nd Ed., New York, USA, 166- 168, (1996).

16. Cho, J., Soekamtoputra, S., Choi, K., Moon, J., "Power Dissipation and Area Comparison of 512-Bit and 1024-Bit Key AES", ***Computers and Mathematics with Applications,*** Chicago,USA , 1378-1383, (2013).

17. Raphael, C., Kuching, W., "Reducing the Exhaustive Key Search of The Data Encryption Standard (DES)", ***Computer Standards & Interfaces,*** Malaysia, 528-530, (2007).

18. Biryukov, A., Nakahara, J., Yıldırım, H.M., "Differential Entropy Analysis of the IDEA Block Cipher", ***Journal of Computational and Applied Mathematics*** Ankara, Turkey, 561–570, (2013).

19. Tomasevic, V., Bojanic, S., Taladriz, O.N., "Finding an internal state of RC4 stream cipher", ***Information Sciences***, Madrid, Spain, 1715-1727, (2007).

20. Biryukov, A., Shamir, A., Wanger, D., "Real Time Crytanalysis of A5 on a PC", ***Fast Software Encryption***, Rehovot, Israel, 1-18, (2000).

21. Daemen, J., Clapp, C., "Fast Hashing and Stream Encyption with PANAMA", ***Fast Software Encryption***, Lausanne, Switzerland, 60-74, (1998).

22. Rivest, R. L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", ***Communications of the ACM***, New York, USA, 120-126, (1978).

23. Yingze, Y., Ying, Z., "Delaying Function Construction Based on Triple DES", ***Procedia Engineering,*** Wuhan, China, 3483-3486, (2012).

24. Diffie, W., Hellman, M. E., "New Directions in Cryptography", ***IEEE Transactions on Information Theory***, 644-654, (1976).

25. Dulaney, E., "CompTIA Security+ Study Guide: Exam SY0-301", ***Sybex***, 5th Ed., Hoboken NJ, USA, 307-309, (2011).

26. Bhunia, C.T., "Information Technology Network and Internet", ***New Age International***, Daryaganj, New Delhi, 403-405, (2005).

27. Shao, Z., "Batch Verifying Multiple DSA-type Digital Signature", ***Computer Networks***, Zhejiang, China, 383-389, (2001).

28. Akyıldız, E., Ashraf, M., "An Overview of Trace Based Public Key Cryptography Over Finite Fields", ***Journal of Computational and Applied Mathematics***, Ankara, Turkey, 599-621, (2013).

29. Stinson, D.R., “Cryptography Theory and Practice”, ***CRC Press Company***, 2nd Ed. Chapman & Hall/CRC, 363-365, (2002).

30. Güvenoğlu, E.,"Bilgi Güvenliği ve Şifreleme-Bilgi Sistemleri Güvenliği Ders Notları", ***Maltepe Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi*** İstanbul, Türkiye,(2012).

31. Aydin, M.A., Tanriverdi, Ö., Zaim, A. H., Durukan, Ş., Gürkaş, G.Z., "Kablosuz Ağlarda Yönlendiriciler ve Yönlendirici Hafızasının Analizi", ***Mühendislik Bilimleri Genç Araştırmacılar Kongresi,*** Istanbul, Türkiye, 8-15, (2005).

32. Şahinaslan, Ö., Şahinaslan, E., Kantürk, A., "Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık", ***3.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu***, Ankara, Türkiye, 1-6, (2010).

33. Bautts, T., Barnes, C., Ouellet, E., “Hack Proofing Your Wireless Network”, ***Syngress Publishing,*** Rockland, USA, 224-253 (2002).

34. Kindervag, J., "The Five Myths of Wireless Security", ***Telecommunication and Network Security***, 7-16, (2006).

35. Arbaugh, W.A., Shankar, N., Wan, Y.C., "Your 802.11 Wireless Network Has No Clothes", ***Wireless Communications***, 44-51, (2002).

36. Conway, R., Cordingley, J.,” Code Hacking : A Developer's Guide to Network Security”, ***Charles River Media***, 353-359, (2013).

37. Manley, M.E., McEntee, C.A., Molet, A.M., Park, J.S., "Wireless Security Policy Development for Sensitive Organizations", ***Systems, Man and Cybernetics (SMC) Information Assurance Workshop***,150-157, (2005).

38. İnternet: Cisco Systems Documentation, "A Comprehensive Review of 802.11 Wireless Lan Security and The Cisco Wireless Security Suite", http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf , (2014).

39. Wiley, J., Gudaitis, T., Jabbusch, J., Rogers, R., Lowther, S., “Low Tech Hacking: Street Smarts for Security Professionals”, ***Syngress***, Waltham, USA, 121-135, (2012).

40. İnternet: Wi-Fi Alliance, "Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise", http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf , (2014).

41. Gezgin, D.M., Buluş, E., Buluş, H.N.,”The Security Suggestions for Wireless Access Points”, ***Trakia Journal of Sciences***, Edirne, Türkiye, 134-137, (2009).

42. Gezgin, D.M., Buluş, E., "RC4 Tabanlı WPA'da Kullanılan TKIP Şifrelemesinin İncelenmesi", ***IV.İletişim Teknolojileri Ulusal Sempozyumu,*** Adana, Türkiye, 107-112, (2009).

43. Yüksel E., Soytürk, M., Ovatman, T., Örencik, B., " Telsiz Yerel Ağlarında Güvenlik Sorunu" ***Ağ ve Bilgi Güvenliği Ulusal Sempozyumu,*** 23-30, (2005).

44. İnternet: Bilgi Güvenliği, "Kablosuz Ağların Karanlık Tarafı", http://www.bilgiguvenligi.gov.tr/kablosuz-aglar/kablosuz-aglarin-karanlik-tarafi.html, (2014).

45. Koblitz, N., "Elliptic Curve Cryptosystem", ***Mathematics of Computation***, 203-209, (1987).

46. Miller, V., Williams, H.C., "Uses of Elliptic Curves in Cryptograpy", ***Advances in Cryptology CRYPTO'85***, 417-426, (1985).

47. Gupta, K., Silakari, S., "ECC over RSA for Asymmetric Encryption: A Review", ***International Journal of Computer Science Issues,*** MP, India, 370-375, (2011).

48. Blake, I.F., Seroussi, G., Smart, N.P., "Advances in Elliptic Curve Crypography", ***Cambridge University Press***, İngiltere, 3-19, (2005).

49. Washington, L., "Elliptic Curve Number Theory and Cryptpgrapy", ***CRC Press, Maryland***, USA, 9-59, (2008).

50. Chouinard, J.Y., "Design of Secure Computer Systems CSI4138/CEG4394 Notes on Elliptic Curve Cryptography", ***Ottawa University***, Canada,1-23 (2002).

51. Tolkov, I., "Counting Points on Elliptic Curves: Hasse's Theorem and Recent Developments", ***Washington University Anvanced Calculus Term Paper***, Washington,USA, 1-12, (2013).

52. Caelli, W,J., Dawson, E.P., "PKI, Elliptic Curve Cryptography and Digital Signature", ***Computers & Security***, 47-66, (1999).

53. Diffie, W., Hellman, M., "New Direction in Cryptograpy", ***IEEE Transaction on Information Theory***, 644-654, (1976).

54. Ahirwal, R. R., Ahke, M., "Elliptic Curve Diffie-Hellman Key Exchange Algorirthm for Securing Hypertext Information on Wide Area Network", ***International Journal of Computer Science and Information Technologies***, 363-368, (2013).

55. Atlığ, C., Uçar, E., Uçar, Ö., "Mobil ve Kablosuz Sistemlerde Bilgi Erişim Özellikleri", ***Akademik Bilişim 2006 + BilgiTek IV***, Pamukkale Üniversitesi, Denizli, 440-443, (2006).

56. Elektronik İmza Kanunu, Kanun no:5070. ***T.C. Resmi Gazete***, Sayı 25355, (2004).

57. İnternet: Ulusal Mobil Devlet Konferansı, "Mobil Devlet & Mobil İmza", http://www.mdevlet.org/wp-content/uploads/2009/06/can_orhun_mobil_dewlet_mobil_imza1mb.pdf (2014).

58. Sağıroğlu, Ş., Kabasakal, D., Alkan, M., "Mobil Elektronik İmza, Altyapısı ve Türkiye", ***Gazi Üniv. Müh. Mim. Fak. Der.,*** Ankara, Türkiye, 49-56, (2008).

59. Hassinen, M., Hyppönen, K., Haataja, K., "An Open, Pki-Based Mobile Payment System", ***Proceedings of The Emerging Trends in Information and Communication***, 86-100, (2006).

60. Asokan, N., Schunter, M., "Optimistic Fair Exchange***", Handbooks in information***, 365-392, (2009).

61. Kalionzoglou, A., Boutsi, P., Polemi, D., "EInvoke: Secure E-Invoicing Based on Web", ***Electronic Commerce Research***, 337-353, (2006).

62. Özdemir, S., Karacan, H., "İnternet Bankacılığı için İmgesel Bağıl Konum Tabanlı Tek Kullanımlık Şifre Sistemi", ***ISCTURKEY***, Ankara, Türkiye, 194-199, (2010).

63. Türk, Ö., Özer, A.B., "Kaos Tabanlı Özet Fonksiyon Kullanılarak Tek Kullanımlık Şifre Üretimi", ***Fırat Üniversitesi Elektrik-Elektronik Bilgisayar Sempozyumu,*** Elazığ, Türkiye, s. 6-9, (2011).

64. Kim, M., Lee, B., Kim, S., Won, D., "Weaknesses and Improvements of One-Time Password Authentication Scheme", ***International Journal of Future Generation Communication and Networking***, 29-38, (2009).

65. Yüksel, A., "Tek Kullanımlık Kimlik Doğrulamalı Anahtar Değişim Yazılım Uygulamasının Geliştirilmesi", Yüksek Lisans Tezi, ***Hacettepe Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, Türkiye, 27-39, (2006).

66. FIPS PUB 198, "The Keyed-Hash Message Authentication Code (HMAC)", ***Federal Information Processing Standards Publication,*** Gaithersburg, (2002).

67. Stallings, W., "Cryptography and Network Security Principles and Practices Fourth Edition", ***Prentice Hall***, 362-394, (2005).

68. Krawczyk, H., Bellare, M., Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", ***IETF RFC 2104***, Newyork, USA, 1-11, (1997).

69. İnternet: Önal, H., "SSL Kullanımı ve Sayısal Sertifika, İmza İşleri", http://csirt.ulakbim.gov.tr/dokumanlar/ssl_sayisal_sertifikalar.pdf , (2014).

70. İnternet: UEKAE, TÜBİTAK. "Açık Anahtar Altyapısı Eğitim Kitabı", http://www.kamusm.gov.tr/dosyalar/kitaplar/aaa/ , (2014).

71. Ahn, L., Blum, M., Hopper, N. J., Langford, J., "CAPTCHA: Using Hard AI Problems for Security", ***Advances in Cryptology – EUROCRYPT***, Warsay, Poland, 294–311, (2003).

72. Thompson E., "MD5 Collisions and The İmpact on Computer Foresics", ***Digital Investigation***, Lindon, USA, 36-40, (2005).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: YILDIRIM, Mustafa
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 27.09.1986, Çorum
Medeni hali	: Bekâr
Telefon	: 0 (537) 471 50 72
Faks	: 0 (332) 353 16 49
e-mail	: yildirim.mustafa@tcmb.gov.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Çankaya Üniversitesi Endüstri Mühendisliği (Çift Anadal)	2011
Lisans	Çankaya Üniversitesi Bilgisayar Mühendisliği	2010
Lisans	Kocaeli Üniversitesi Bilgisayar Öğretmenliği	2006 (Terk edilmiş)
Lise	Çorum Atatürk Lisesi	2003

İş Deneyimi

Yıl	Yer	Görev
2012-Halen	Türkiye Cumhuriyet Merkez Bankası	Endüstri Mühendisi
2011-2012	Enerji ve Tabii Kaynaklar Bakanlığı	Bilgisayar Mühendisi
2010-2011	E-İmza Bilişim A.Ş.	Bilgisayar Mühendisi

Yabancı Dil

İngilizce