GÜVENLİ İLETİŞİM İÇİN
PDA'LARDA AES ŞİFRELEME ALGORİTMASININ
UYGULANMASI

Ahmet AKSOY

YÜKSEK LİSANS TEZİ
BİLGİSAYAR EĞİTİMİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

KASIM 2010
ANKARA

Ahmet AKSOY tarafından hazırlanan GÜVENLİ İLETİŞİM İÇİN PDA'LARDA AES ŞİFRELEME ALGORİTMASININ UYGULANMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Remzi YILDIRIM
Tez Yöneticisi

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

Başkan: : Doç. Dr. Fatih V. ÇELEBİ

Üye : Yrd. Doç. Dr. Remzi YILDIRIM

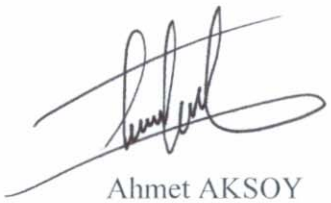
Üye : Doç. Dr. H. Haldun GÖKTAŞ

Tarih : 30/11/2010

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

TEZ BİLDİRİMİ

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



Ahmet AKSOY

GÜVENLİ İLETİŞİM İÇİN
PDA'LARDA AES ŞİFRELEME ALGORİTMASININ
UYGULANMASI
(Yüksek Lisans Tezi)

Ahmet AKSOY

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Kasım 2010

ÖZET

Teknolojinin gelişmesiyle cep bilgisayarları (Personal Digital Asistant) gelişerek hayatımıza girmiştir. PDA sayesinde yazılımlar mekandan bağımsız hale gelerek hayatımızda kolaylık sağlarlar. PDA'larda veri güvenilirliğinin sağlanması gerekir. Bu amaçla AES şifreleme algoritması ayrıntılı olarak incelenmiştir ve bu çalışmada cep bilgisayarları için veri güvenilirliğini arttırmaya yönelik bir uygulama geliştirilmiştir. Bu uygulama, Microsoft SQL Server veri tabanı ve Microsoft Visual Studio.NET 2008 Editöründe C# programlama dili kullanılarak geliştirilmiştir. Uygulama, XML Web Servisi ve Windows Mobile 6.5 Professional projesinden oluşmaktadır. Şifreleme algoritması olarak da Gelişmiş Şifreleme Standardı (Advanced Encryption Standard, AES) seçilmiştir.

Bilim Kodu : 702
Anahtar Kelimeler : PDA, AES, web servisi, şifreleme, şifre çözme
Sayfa Adedi : 60
Tez Yöneticisi : Yrd. Doç. Dr. Remzi YILDIRIM

APPLICATION OF AES ENCRYPTION ALGORITHM IN PDAs FOR A SECURE COMMUNICATION

(M.Sc. Thesis)

Ahmet AKSOY

GAZI UNIVERSITY
INFORMATICS INSTITUTE

November 2010

ABSTRACT

With the advance of the technology, PDAs have also evolved. PDA has freed the softwares from location and let us ease our life by saving time. Data security has to be provided on PDAs. For that purpose, AES encryption algorithm has been deeply studied and an application has been developed to improve data security on PDAs. This application has been created with Microsoft SQL Server database and Microsoft Visual Studio .NET 2008 Edition using C# programming language. Application consists of XML Web Service and Windows Mobile 6.5 Professional project. AES (Advanced Encryption Standard) has been chosen for encryption algorithm.

Science Code : 702
Key Words : PDA, AES, web service, encryption, decryption
Page Number : 60
Adviser : Assist. Prof. Dr. Remzi YILDIRIM

TEŞEKKÜR

Çalışmam boyunca maddi ve manevi yardımları ve katkılarıyla beni yönlendiren değerli hocam Yrd. Doç. Dr. Remzi YILDIRIM'a, yine maddi ve manevi desteğini hiçbir zaman esirgemeyen aileme, arkadaşlarıma ve özellikle kıymetli eşime teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Simgeler	**Açıklama**
GF(a)	a elemanlı Galois alanı
GF(a^b)	a^b elemanlı Galois alanı
GF(2^n)	2^n elemanlı Galois alanı
Nb	Kelime (32 bit) cinsinden durum'un uzunluğu
Nk	Kelime (32 bit) cinsinden anahtar uzunluğu
Nr	Tur sayısı
RCon	Anahtar üreteci tur sabiti
$\oplus$	Exclusive-OR (XOR)
Si	i'inci durum baytı

Kısaltmalar	**Açıklama**
AES	Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
CAB	Kabine Dosyası (Cabinet File)
CE	Kompakt Basımı (Compact Edition)
CLR	Ortak Dil Çalışma Zamanı (Common Language Runtime)
CTS	Ortak Tip Sistemi (Common Type System)
DES	Veri Şifreleme Standardı (Data Encryption Standard)

Kısaltmalar	**Açıklama**
DLL	Dinamik Bağlantı Kitaplığı (Dynamic Link Library)
DTK	Geliştirici Araç Kiti (Developer Tool Kit)
EXE	Çalıştırılabilir Dosya (Executable file)
FIPS	Federal Bilgi İşlem Standardı (Federal Information Processing Standard)
GPS	Küresel Konumlandırma Sistemi (Global Positioning System)
HTTP	Hipermetin Aktarma İletişim Kuralı (Hypertext Transfer Protocol)
IDE	Entegre Geliştirme Ortamı (Integrated Development Environment)
IIS	İnternet Bilgi Sunucu (Internet Information Server)
IP	İnternet Protokol Adresi (Internet Protocol Address)
MARS	Çarpma, Toplama, Döndürme ve Yerine koyma (Multiplication, Addition, Rotation and Substitution)
NBS	Ulusal Yayın Derneği (National Broadcasting Society)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
PDA	Kişisel Sayısal Asistan (Personel Digital Asistant)
RC6	Ron’s Code 6

Kısaltmalar	**Açıklama**
SDK	Yazılım Geliştirme Kitleri (Software Development Kits)
SOAP	Basit Nesne Erişim Protokolü (Simple Object Access Protocol)
URL	Tek Düzen Kaynak Bulucu (Uniform Resource Locator)
W3C	Dünyaca Yaygın Web Konsorsiyomu (World Wide Web Consortium)
XML	Genişletilebilir İşaretleme Dili (Extensible Markup Language)
3 DES	Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standard)
.NET CF	.NET Compact Framework

1. GİRİŞ

İletişim geçmişten günümüze hayatımızda önemli bir yere sahiptir. Eğitim, öğretim, alış veriş, sosyal faaliyetler ve insani ilişkiler gibi yaşamsal ihtiyaçlarımızın giderilmesini sağlayan bir araçtır. İletişim, iletmek istediğimiz bilginin belirlenmiş bir ortamda belirli kurallar dahilinde göndericiden alıcıya iletilmesi sürecidir.

İletişim sürecinde diğer insanların öğrenmesi sonucu maddi ve manevi zarara neden olabilecek bilgilerin güvenli iletilmesi gerekmektedir. Bilgilerin iletildiği ortamda güvenliğinin sağlanması gerekir. Buda gönderici ile alıcı arasında ortak gizli bir metot ile gerçekleştirilir. Mesela "tez" ifadesi iletilirken her bir harfinin yerine kendisinden sonra gelen 7. harf kullanılarak "bjf" gizli verisi ortama bırakılır ve bu verinin "tez" ifadesi olduğunu sadece bu metodu bilen alıcı anlar. Böylece verinin ortamda güvenli iletilmesi sağlanmış olur. Bu metot şifrelemedir ve iletişimin var olmasından beri kullanılmaktadır.

Son yıllarda internetin yaygınlaşmasıyla insanların sanal ortamdaki paylaşımları da artmıştır. İnternet, insanlara zamandan ve mekandan bağımsız olarak kolay iletişim sağladığı için büyük ölçüde rağbet görmektedir. Örneğin banka işlemleri, fatura ödemeleri, e-ticaret işlemleri, e-mail ve bunun gibi ihtiyaçlarımızı kolayca karşılar. Bu kadar çok kişisel bilginin paylaşıldığı bu ortamda kişilerin zarar görme ihtimali yüksektir. Verilerin bu ortamlarda kopyalanması, silinmesi, değiştirilmesi ve bozulması gibi birçok tehdit vardır. Bu tehditlerin ortadan kaldırılabilmesi için çeşitli şifreleme metotları geliştirilmiştir.

Şifreleme, teknolojinin gelişimi ile paralel olarak gelişmiştir. İnsanlar tarafından kırılanlar geçerliliğini yitirirken yerlerini daha gelişmişleri almıştır. Bu süreç gelecekte de bu şekilde devam edecektir.

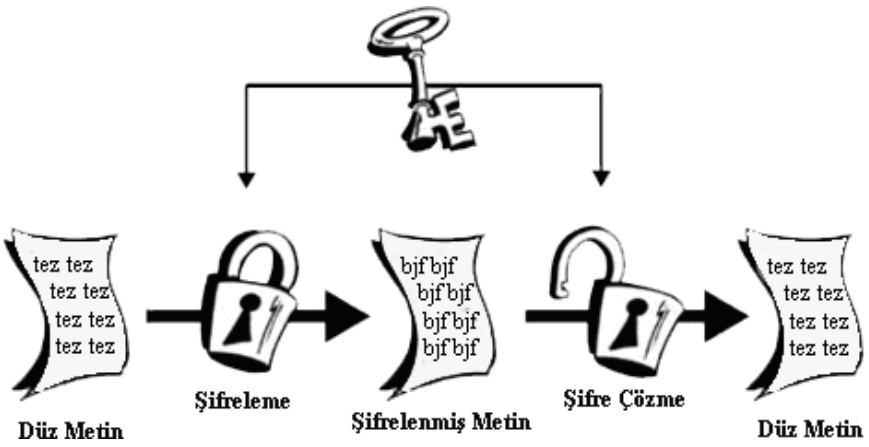
Kriptoloji, matematiğin hem şifre bilimi (kriptografi), hem de şifre analizini (kriptanaliz) kapsayan bir dalıdır. Şifre biliminin amacı, veri güvenliğini sağlamaktır ve şifre analizinin amacı ise şifreleri çözmektir. Şifreleme bilginin gizlenmesidir.

Şifrelemenin amacı ise verinin istenmeyen kurum, kuruluş ve şahıslar tarafından öğrenilmesini engellemektir. Şifre çözme (deşifre) işlemi ise şifreli verinin anlamlı hale çevrilmesi işlemidir. Günümüzdeki kriptografi, şifreleme ve şifre çözmeden daha fazlasını içerir. Kimlik denetimi gizlilik kadar önemlidir. Herhangi bir iletiye adımızı ekleyip ağ üzerinden gönderdiğimiz zaman kimliğimizi ispatlamak için elektronik yöntemlere ihtiyaç duyarız. Kriptografinin buna sunduğu çözüm ise sayısal imzadır [1].

Şifrelemede şifrelenecek veri düz metin (plaintext), kodlanmış veri ise şifrelenmiş veri (ciphertext) olarak adlandırılır. Düz metinin şifreli metine dönüştürülmesi işlemine şifreleme (encryption) denir. Şifreli metnin düz metine geri dönüştürülmesine ise şifre çözme (decryption) denir. Şifreleme için kullanılan bu metotlar kriptografi (cryptography) alanını oluşturur. Bu metotlar şifreleme sistemi veya şifre olarak da bilinir [2].

Şifreleme sistemi, şifreleme ve şifre açma olmak üzere iki adımdan oluşur. Şifrelemede şifrelenecek veri belli kuralar dahilinde farklı bir veriye dönüştürülür. Bu veri şifrelenmiş veridir. Şifre çözmede şifrelenmiş veri şifreleme işleminin tersi yapılarak asıl veriye dönüştürülür. Şifrelemede ve şifre çözmede anahtar kullanılabilir. Anahtar sayılardan oluşmaktadır. Anahtarın uzunluğu büyüdükçe şifrelemenin güvenliği de artar. İşlemci hızları arttıkça anahtar uzunlukları da mecburen artmıştır.

Eğer Ali, veriyi Veli'ye göndermek isterse şifreleme anahtarı kullanarak veriyi şifreler. Veli de gelen şifreli veriyi şifre çözme anahtarı kullanarak çözer. Eğer şifreleme sisteminde şifreleme işleminde kullanılan anahtar ile şifre çözme işleminde kullanılan anahtar daima birbirine eşit ise bu sistem simetrik şifreleme sistemidir. Basit olarak simetrik şifreleme sistemi Şekil 1.1.'deki gibi gösterilir. Eğer anahtarlar birbirinden farklı ise asimetrik şifreleme sistemidir [3].



Şekil 1. 1. Simetrik şifreleme sistemi

Simetrik şifreleme, blok şifreleme (block ciphers) ve akış şifreleme (stream ciphers) olarak ikiye ayrılır. Akış şifrelemede düz metin ardışık bitlere ayrılır ve anahtar oluşturucu tarafından üretilmiş akış anahtarı ile her bir bit şifrelenir. Eğer akış anahtarı p karakterden sonra tekrar ederse akış şifreleme periyodiktir aksi halde periyodik değildir. Blok şifrelemede blok şifreleme algoritması kullanılır. Şifrelenecek veri, veri bloğu halinde alınır ve anahtar ile belli işlemlere tabi tutularak aynı boyutta şifrelenmiş veri bloklarına dönüştürülür [4].

1977'de şimdiki adı NIST olan Ulusal Standartlar Bürosu (National Bureau of Standards, NBS) tarafından standartlaştırılan geniş kitlelerde kullanılan ilk modern blok şifreleme algoritması, veri şifreleme standardı (DES) idi. Bu şifreleme 64 bitlik veri bloklarını 56 bitlik anahtar kullanarak şifrelemekteydi. DES standartlaştırıldığında anahtar boyutunun çok küçük olduğuna ve potansiyel kuvvetli saldırılara karşı savunmasız olduğuna karar verildi. Ancak 1997 yılına kadar DES'e karşı başarılı olan kuvvetli saldırı rapor edilmedi. 1999'da DES ile şifrelenmiş veri, donanım ve yazılım ile bir günden daha az sürede kırıldı [5].

Veri şifreleme standardı olarak DES (Data Encryption Standard), uzun bir süre yaygın olarak kullanılmıştır. Daha sonra bilgisayar teknolojisindeki gelişmelere bağlı olarak çözümlenmiştir. Bunun en büyük nedeni anahtar uzunluğunun yetersiz olmasıdır. DES in güvensiz hale gelmesiyle yeni bir şifreleme sistemi arayışına

girilmiştir ve DES'in yerini gelişmiş şifreleme standardı (Advanced Encryption Standard, AES) almıştır.

AES, uzunluğu 128, 192 ve 256 bit olan anahtar kullanabilen ve anahtar ile 128 bitlik veri bloklarını şifreleyebilen simetrik blok şifreleme algoritmasıdır [6]. Son yıllarda birçok şifreleme metodu kullanılmaktadır.

Son yıllarda bilgisayarlar cebimize dahi girmeyi başararak cep telefonu görevini de üstlenmiştir. İnternet gibi teknolojileri desteklemesinden dolayı cep bilgisayarlarının (Personel Digital Asistant, PDA) yazılım dünyasında kullanımı her geçen gün artmaktadır. Bir lokantada adisyon işlemleri için kullanımından tutunda bankacılık işlemlerine kadar girmiştir. Bu nedenle cep bilgisayarlarında veri güvenliği de önemli hale gelmiştir.

Aynı dilde yazılan veya farklı dillerde yazılan uygulamalar birbirleriyle internet üzerinden veri alış verişi yapabilmektedir. Bunun için XML Web Servisi uygun bir teknolojidir ve standart olduğu için işletim sistemlerinin tamamıyla uyumlu bir şekilde çalışır. Veri XML (Extensible Markup Language) biçiminde ilerler.

Bu çalışmada XML web servisi (Web Service) kullanılarak veriler PDA'lardan gelişmiş şifreleme standardı ile şifrelenerek internetteki herhangi bir sunucudaki Microsoft SQL Server programı ile haberleşmesini sağlayan uygulama geliştirilmiştir. Bu uygulama Microsoft Visual Studio 2008 editöründe C# dili ile geliştirilmiştir. Bu çalışma AES algoritması, XML Web Servisler, cep bilgisayarları ve sonuç bölümlerinden oluşmaktadır.

2. AES ŞİFRELEME ALGORİTMASI

Bu bölümde AES şifreleme algoritmasında kullanılan matematiksel işlemler ve algoritmanın adımları incelenecektir.

2.1. AES Şifreleme Algoritmasının Gelişimi

NIST, Ocak 1997'de adına AES diyecekleri yeni bir şifreleme standardını geliştirmek için bir girişimin başladığını duyurdu. Bu yeni şifreleme standardı, eski veri şifreleme standardı olan DES ve 3DES (Triple - DES)'in yerine federal bilgi işleme standardı (Federal Information Process Standard, FIPS) olmalıydı [6, 9].

Çizelge 2. 1. NIST'in kabul ettiği 15 aday algoritma ve geliştiricilerinin listesi

Aday Algoritmalar	**Katılımcılar - (Ülke)**	**Katılımcı Türü**
CAST-256	Entrust (CA)	Şirket
Crypton	Future Systems (KR)	Şirket
DEAL	Outerbridge, Knudsen (USA-DK)	Araştırmacılar
DFC	ENS-CNRS (FR)	Araştırmacılar
E2	NTT (JP)	Şirket
Frog	TecApro (CR)	Şirket
HPC	Schroeppel (USA)	Araştırmacı
LOKI97	Brown et al. (AU)	Araştırmacılar
Magenta	Deutsche Telekom (DE)	Şirket
Mars	IBM (USA)	Şirket
RC6	RSA (USA)	Şirket
Rijndael	Daemen and Rijmen (BE)	Araştırmacılar
SAFER+	Cylink (USA)	Şirket
Serpent	Anderson, B iham, Knudsen (UK-IL-DK)	Araştırmacılar
Twofish	Counterpane (USA)	Company

NIST, Eylül 1997'de minimum gereksinimleri 128 bit blok uzunluğuna, 128, 192 ve 256 bitlik anahtar uzunluğunu destekleyen simetrik blok şifreleme sistemi olarak duyurdu. Fakat bu gereksinim daha sonra bırakıldı. Bazı katılımcılar algoritmalarında değişken blok uzunluğu tutmaya karar verdi [6-8].

Zamanında tamamlanıp kabul edilen Çizelge 2.1'deki 15 aday algoritmadan Ağustos 1999'da 5 tanesinin finale kaldığını NIST yayınladığı raporla duyurdu. Bu 5 algoritma MARS, RC6, Rijndael, Serpent ve Twofish'dir [6, 7].

NIST Ekim 2000'de 1997'den beri yapılan yoğun çalışmaların sonunda gelişmiş şifreleme standardı olarak Joan Daemen ve Vincent Rijmen tarafından dizayn edilen Rijndael algoritmasını ilan etmiştir [6-9].

2.2. AES Algoritmasında Kullanılan Matematiksel İşlemler

AES algoritmasında kullanılan bütün bitler sınırlı alan elemanlarını kullanarak yorumlanırlar. Sınırlı alan elemanları toplanabilir, çarpılabilir fakat bu işlemler sayılarda kullanılan işlemlerden farklıdır [10]. Bu farklılıklar ilerleyen konularda incelenecektir.

2.2.1. GF(2^8) alanı ve polinom gösterimi

GF(a) , a bir asal sayı olmak koşuluyla a sayıda elemana sahip bir Galois alanıdır. İlk eleman 0 olduğu için son eleman $\{a-1\}$'dir. Örneğin GF(2), 2 asal sayı olduğundan bir Galois alanıdır ve 0 ve 1 elemanlarından oluşur.

Galois alanları genişletilebilir. GF(a) a elemanlı iken GF(a^b) genişletilmiş sonlu alanı ise b adet GF(a) elemandan oluşur. AES algoritmasında kullanılan Galois alanı GF(2^8)'dir. GF(2^8) alanı 8 adet GF(2) elemanlıdır.

Sonlu alanın elemanları birkaç farklı şekilde gösterilebilir. $\{b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0\}$ bitlerinden oluşan bir baytlık b, katsayıları $\{0,1\}$'den oluşan polinom olarak Eş. 2.1.'deki gibi gösterilebilir [11].

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \quad (2.1)$$

Örnek 2.1. Onaltılık gösterimi $\{57\}$, ikilik gösterimi $\{01010111\}$ sayısının polinom gösterimi:

$$x^6 + x^4 + x^2 + x + 1$$

2.2.2. Toplama işlemi

GF(2^8)'de iki elemanın toplanması, bu iki elemanı polinom olarak ifade edip bu iki polinomun toplamından elde edilen toplam polinomundaki katsayılara mod 2 işlemi yapılır. Elde edilen sonuç GF(2^8)'de toplama işleminin sonucudur. Örnek 2.2 ve Örnek 2.3'te ayrıntılı olarak incelenmiştir [10].

Diğer bir ifadeyle GF(2^8)'de iki elemanın toplanması, ikilik sistemde her bir bitin XOR işlemine tabi tutulmasıyla gerçekleştirilir. $\{a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0\}$ ve $\{b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0\}$ için toplam $\{c_7\ c_6\ c_5\ c_4\ c_3\ c_2\ c_1\ c_0\}$ olsun. $c_i = a_i \oplus b_i$'dir.

Örnek 2.2.

$(x^6 + x^5 + x^2 + x) + (x^5 + x^2 + 1) = x^6 + x + 1$ (Polinom Gösterimi)

$\{01100110\} \oplus \{00100101\} = \{01000011\}$ (İkili Gösterim)

$\{66\} \oplus \{25\} = \{43\}$ (Onaltılı Gösterim)

Örnek 2.3.

$a = \{10101000\} \Rightarrow a(x) = x^7 + x^5 + x^3$

$b = \{10111011\} \Rightarrow b(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$a \oplus b = \{00010011\}$ ve $a(x) + b(x) = 2x^7 + 2x^5 + x^4 + 2x^3 + x + 1$

Burada $a(x) + b(x)$ polinomundaki katsayılara mod 2 işlemi uygulandığında

$c(x) = x^4 + x + 1$

toplam polinomu elde edilir.

2.2.3. Çarpma işlemi

GF(2^8) alanında ve polinom gösteriminde çarpma işlemi, iki polinomun karşılıklı çarpma işleminin yapılmasıyla elde edilir. Ancak sonuç GF(2^8) alanının dışarısında olabilir. Bundan dolayı çarpma işleminin sonucunda oluşan polinomu indirgenemez polinom ile indirgeme yapmak gerekir. İndirgeme işlemi için çarpım polinomunu indirgenemez polinom ile mod işlemi yapılır [10].

İndirgenemez polinom 1 ve kendisi dışında böleni olmayan polinomdur. $m(x)$, $a(x)$ ve $b(x)$ polinomları GF(2^8)'de tanımlı olmak üzere: $m(x)$ polinomu bu alanda tanımlı hiçbir polinomun çarpımı şeklinde ($m(x) = a(x) \times b(x)$) ifade edilemiyorsa $m(x)$ polinomu GF(2^8) alanında indirgenemez polinomdur [11].

GF(2^8) alanında çarpma işleminde indirgenemez polinom olarak, onaltılık gösterimde $1\{1b\}$, iki tabanındaki gösterimi $1\{00011011\}$ olan $m(x) = x^8 + x^4 + x^3 + x + 1$ polinomu kullanılır [7].

Örnek 2.4. $\{66\} \bullet \{25\} = \{91\}$'dir. Çünkü:

$$\{66\} = \{01100110\} \equiv x^6 + x^5 + x^2 + x$$
$$\{25\} = \{00100101\} \equiv x^5 + x^2 + 1$$
$$c(x) = a(x) \bullet b(x)$$
$$c(x) = (x^6 + x^5 + x^2 + x) \bullet (x^5 + x^2 + 1)$$
$$= x^{11} + x^8 + x^6 + x^{10} + x^7 + x^5 + x^7 + x^4 + x^2 + x^6 + x^3 + x$$
$$= x^{11} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + x,$$

Sonuç GF(2^8) alanının dışında olduğundan indirgeme işlemi uygulanırsa:

$$(x^{11} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$= x^7 + x^4 + 1 \equiv \{10010001\} = \{91\}$$

sonucu elde edilir.

İndirgeme işlemi ikinci bir yöntem ile de yapılır. İndirgeme polinomu 0'a eşitlenerek ($x^8 + x^4 + x^3 + x + 1 = 0$) ve polinomun en yüksek dereceli terimi olan x^8 eşitliğin sol tarafında yalnız bırakılarak $x^8 = x^4 + x^3 + x + 1$ eşitliği elde edilir ve çarpma işleminin sonucunda oluşan polinomda x^8 terimi yerine eşiti olan $x^4 + x^3 + x + 1$ yazılarak indirgeme işlemi yapılır. 8 ve daha üzeri katsayılı terim kalmayıncaya kadar bu işlem tekrar tekrar yapılır [10].

Bu yöntemi Örnek 2.4.'te elde edilen çarpma sonucuna uygular isek:

$$a(x) \bullet b(x) = x^{11} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + x$$
$$= x^8 \cdot x^3 + x^8 \cdot x^2 + x^8 + x^5 + x^4 + x^3 + x^2 + x$$

x^8 terimi yerine $x^4 + x^3 + x + 1$ yazalım,

$$= (x^4 + x^3 + x + 1) \cdot x^3 + (x^4 + x^3 + x + 1) \cdot x^2 + (x^4 + x^3 + x + 1) + x^5 + x^4 + x^3 + x^2 + x$$
$$= x^7 + x^6 + x^4 + x^3 + x^6 + x^5 + x^3 + x^2 + x^4 + x^3 + x + 1 + x^5 + x^4 + x^3 + x^2 + x$$
$$= x^7 + x^4 + 1 \equiv \{10010001\} = \{91\}$$

elde edilir. Sonuçta elde edilen polinomun derecesi 8'den küçüktür. İkilik gösterime çevrilince GF(2^8) alanının içerisinde olacaktır.

2.2.3.1. X ile çarpma işlemi

$$a(x) = a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x^1 + a_0 \tag{2.2}$$

$a(x)$ polinomunun x ile çarpılması sonucunda $c(x)$

$$c(x) = x \bullet a(x) \tag{2.3}$$

polinomu elde edilir. $a(x)$ polinomunun x polinomu ile çarpılması sonucunda derecesi 8 olan aşağıdaki polinom elde edilir.

$$a_7 x^8 + a_6 x^7 + a_5 x^6 + a_4 x^5 + a_3 x^4 + a_2 x^3 + a_1 x^2 + a_0 x \tag{2.4}$$

Bu polinomun $m(x)$ indirgenemez polinomuyla indirgenmesi işlemi ile $c(x)$ polinomu elde edilir. İndirgenme işlemi bu polinomun GF(2^8) alanının içinde olduğunda uygulanmazken GF(2^8) alanın dışında olduğunda ise uygulanır. Yani b_7 katsayısı 1 olduğunda x^8'li bir terim oluşur. Bundan dolayı GF(2^8) alanının dışındadır ve $m(x)$ polinomu ile indirgenmelidir. Ancak b_7 katsayısı 0 ise x^8'li bir terim oluşmamıştır. Dolayısıyla GF(2^8) alanının içerisindedir ve indirgenme işlemine gerek yoktur [10,11].

Örnek 2.5. $\{66\} \bullet \{13\} = \{90\}$'dır. Çünkü:

$$\{66\} \bullet \{02\} = \{cc\}$$
$$\{66\} \bullet \{04\} = \{cc\} \bullet \{02\} = \{83\}$$
$$\{66\} \bullet \{08\} = \{83\} \bullet \{02\} = \{1d\}$$
$$\{66\} \bullet \{10\} = \{1d\} \bullet \{02\} = \{3a\}$$

olduğundan

$$\begin{aligned} \{66\} \bullet \{13\} &= \{66\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\ &= \{66\} \oplus \{cc\} \oplus \{3a\} \\ &= \{90\} \end{aligned}$$

elde edilir.

2.2.4. Katsayıları Galois alanında ($GF(2^8)$) tanımlı polinomlar

AES algoritmasında bazı işlemlerde 4 bayttan oluşan kelimeler $[a_0, a_1, a_2, a_3]$ aşağıdaki gibi 4 terimli polinomlar olarak kabul edilir. Bu polinomlar:

$$a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0 \tag{2.5}$$
$$b(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0 \tag{2.6}$$

Bu iki polinomun toplama işlemi, karşılıklı olarak katsayıların XOR işlemi yapılması ile olur:

$$a(x) + b(x) = (a_3 \oplus b_3) x^3 + (a_2 \oplus b_2) x^2 + (a_1 \oplus b_1) x + (a_0 \oplus b_0) \tag{2.7}$$

Bu iki polinomun çarpılması ise iki adımda elde edilir. Birinci adımda cebirsel olarak bu iki polinom çarpılır ($c(x) = a(x).b(x)$) ve

$$c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \tag{2.8}$$

polinomu elde edilir. Buradaki:

$$\begin{aligned}
c_0 &= a_0 \bullet b_0 \\
c_1 &= a_1 \bullet b_0 \oplus a_0 \bullet b_1 \\
c_2 &= a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \\
c_3 &= a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3 \\
c_4 &= a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3 \\
c_5 &= a_3 \bullet b_2 \oplus a_2 \bullet b_3 \\
c_6 &= a_3 \bullet b_3
\end{aligned} \tag{2.9}$$

tanımlıdır.

Bu sonuç ($c(x)$), 4 baytlık kelimeyi temsil etmez. Bundan dolayı ikinci adımda $c(x)$ polinomuna 4. dereceden bir polinomla mod işlemi yapılır. Bu işlemden sonra $c(x)$ 4'den daha küçük bir derece olabilir. AES algoritması için bu işlemi $x^4 + 1$ polinomu gerçekleştirir. Bu yüzden:

$$x^i \bmod\left(x^4 + 1\right) = x^{i \bmod 4} \tag{2.10}$$

$a(x)$ ve $b(x)$'in bu modüler ürünü $a(x) \otimes b(x)$'ten elde edilen $d(x)$ polinomunu verir ve $d(x)$ aşağıdaki gibi ifade edilir:

$$d(x) = d_3x^3 + d_2x^2 + d_1x + d_0 \tag{2.11}$$

bununla

$$
\begin{aligned}
d_0 &= (a_0 \bullet b_0) \oplus (a_3 \bullet b_1) \oplus (a_2 \bullet b_2) \oplus (a_1 \bullet b_3) \\
d_1 &= (a_1 \bullet b_0) \oplus (a_0 \bullet b_1) \oplus (a_3 \bullet b_2) \oplus (a_2 \bullet b_3) \\
d_2 &= (a_2 \bullet b_0) \oplus (a_1 \bullet b_1) \oplus (a_0 \bullet b_2) \oplus (a_3 \bullet b_3) \\
d_3 &= (a_3 \bullet b_0) \oplus (a_2 \bullet b_1) \oplus (a_1 \bullet b_2) \oplus (a_0 \bullet b_3)
\end{aligned} \tag{2.12}
$$

$a(x)$ sabit polinom olduğu zaman bu ifade Eş. 2.13'te gösterilen matris formundaki gibi yazılabilir:

$$
\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \tag{2.13}
$$

Çünkü GF(2^8)'in üzerinde $x^4 + 1$ indirgenemez polinom değildir. Bundan dolayı 4 terimli çarpma her zaman ters çevrilebilir değildir. Ancak AES algoritmasında her zaman ters çevrilebilir olması gerekmektedir. Bu nedenle AES algoritmasında tersi olan Eş. 2.14'de gösterilen polinom seçilmiştir [7, 11, 18].

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \tag{2.14}$$

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\} \tag{2.15}$$

2.3. AES Algoritmasının Özellikleri

AES algoritmasında giriş bloğu, çıkış bloğu ve durum (state) 128 bittir. $Nb = 4$'tür ve durum, giriş ve çıkış bloklarındaki 32 bitlik kelime sayısını gösterir.

AES algoritmasında anahtar 128, 192 veya 256 bit uzunluklarında olabilir. Anahtardaki 32 bitlik kelime sayısını Nk gösterir. Nk, anahtar uzunluğuna göre sırayla 4, 6 veya 8 olur [2].

AES algoritmasında Nr'de tur sayısını gösterir. Nk ve Nb'nin değerine göre Nr Çizelge 2.2.'deki gibi değişir [12].

Çizelge 2. 2. Anahtar uzunluğuna göre tur sayısının değişimi

	Anahtar Uzunluğu (Nk kelime)	**Blok Uzunluğu (Nb kelime)**	**Tur Sayısı (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES algoritmasında bazı işlemlerin tekrar tekrar yapıldığı yapıya tur denir. AES algoritmasında şifreleme işleminde ilk işlem tur anahtarı eklemedir. Son turda:

Bayt yer değiştirme

Satır öteleme

Tur anahtarı ekleme

işlemleri yapılırken diğer turlarda sırayla $Nr-1$ kez:

Bayt yer değiştirme

Satır öteleme

Sütun karıştırma

Tur anahtarı ekleme

işlemleri yapılır. Şifre çözme işleminde işlemler tersten yapılır. İlk işlem tur anahtarı eklemedir. Sonra $Nr-1$. turdan 1. tura kadar:

Ters satır öteleme

Ters bayt yer değiştirme

Ters sütun karıştırma

Tur anahtarı ekleme

işlemleri yapılırken son turda ise aşağıdaki işlemler yapılır [13].

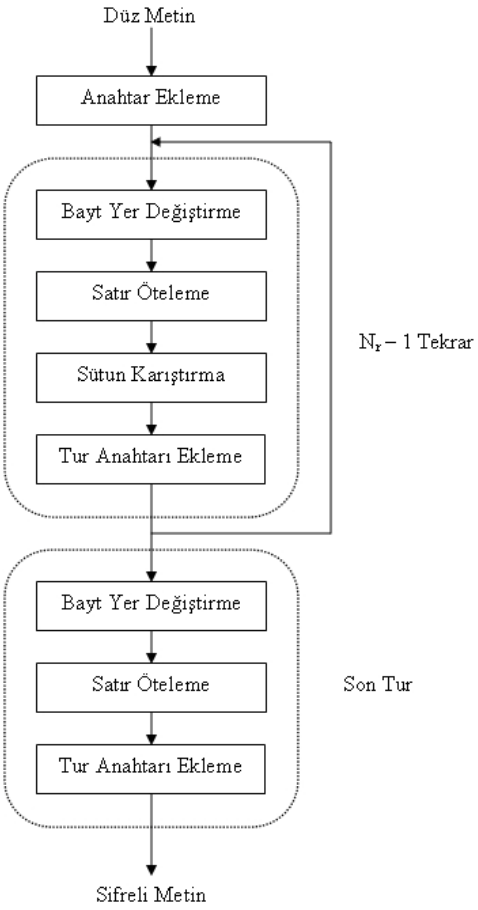
Ters bayt yer değiştirme

Ters satır öteleme

Tur anahtarı ekleme

2.3.1. Şifreleme işlemi

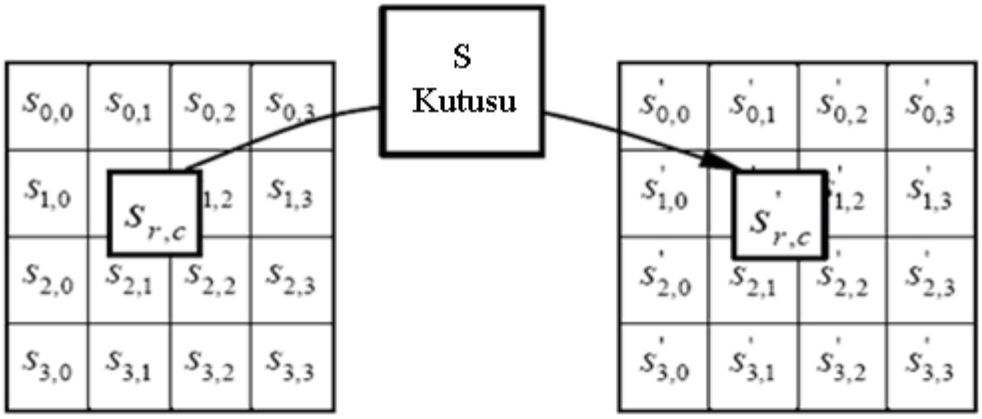
Şifreleme algoritması Şekil 2.1.'de gösterilmektedir.



Şekil 2. 1. AES şifreleme algoritması

2.3.1.1. Bayt yer değiştirme

Bayt yer değiştirme işlemi doğrusal olmayan bir dönüşümdür. Durum bloğundaki her bir baytı yer değiştirme tablosu (S-Kutusu) kullanarak başka bir bayta dönüştürür. Bayt yer değiştirme işlemi Şekil 2.2.'de de görüldüğü gibi her baytı ayrı ayrı değiştirmektedir [2,10].



Şekil 2. 2. Durumun her baytının S kutusu ile değiştirilmesi

S kutusu iki dönüşümün birleşimiyle oluşur:

1. Giriş baytının polinomlarda yapıldığı gibi çarpma işlemine göre tersi alınır.
2. GF(2) alanı üzerinde tanımlı Afin dönüşümü

$$b_i^{'} = b_i + b_{(i+4)\bmod 8} + b_{(i+5)\bmod 8} + b_{(i+6)\bmod 8} + b_{(i+7)\bmod 8} + c_i \tag{2.16}$$

uygulanır ve $0 \le i < 8$ için burada b_i baytın i. biti ve c_i, $\{63\}$ veya $\{01100011\}$ değerinin i. bitidir. Burada soldaki değişkendeki asal $(b^{'})$, sağdaki değerle güncellenebilen değeri gösterir [7,10].

S kutularındaki Afin dönüşüm elemanı Eş. 2.17.'de gösterildiği gibi matris biçiminde ifade edilebilir:

Bayt yer değiştirme işleminde kullanılan S kutusu Çizelge 2.3.'de gösterildiği gibi onaltılık formdadır.

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{2.17}$$

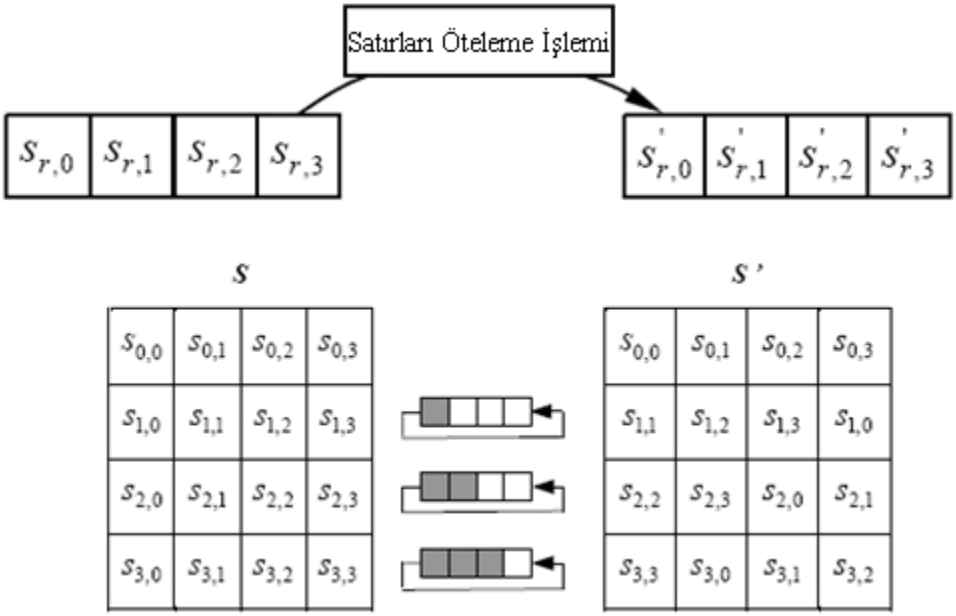
Çizelge 2. 3. S kutusu: xy baytı için yer değiştirme değerleri (onaltılık tabanda)

		Y															
		0	1	2	3	4	5	6	7	8	9	a	B	c	d	E	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	Af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	B2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	F3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	E4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	Ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Örnek 2. . Eğer $S_{1,1} = \{25\}$ ise sonuç değeri S kutusunda, satır indisi '2' ve sütun indisi '5' 'in kesiştiği hücredeki bayttır. Dolayısıyla $S_{1,1}' = \{3f\}$ olur.

2.3.1.2. Satırları öteleme

Satırları öteleme işleminde 4x4 matris halinde olan durum bloğunun son 3 satırındaki baytlar dairesel olarak sağdan sola doğru her bir satır farklı sayıda kaydırılır. Birinci satıra $(r = 0)$ kaydırma işlemi yapılmaz. İkinci satır 1 sütun kaydırılır ve bu işlemin sonunda 2. satır 1. sütundaki bayt, 2. satır 4. sütuna gelir. Üçüncü satır 2 ve dördüncü satır 3 sütun kaydırılır. Şekil 2.3.'de kaydırma işlemi gösterilmiştir [10,11].



Şekil 2. 3. Durumun son 3 satırının çevrimsel kaydırılması işlemi

2.3.1.3. Sütunları karıştırma

Sütunları karıştırma işleminde, durum bloğunun her bir sütunu dört terimli polinom olarak sütun sütun Eş. 2.20.'de ki gibi ifade edilen çarpım matrisiyle çarpılarak yeni sütun oluşturulur. Çarpım matrisi:

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \tag{2.18}$$

polinomundan Eş. 2.20.'deki gibi oluşturulur:

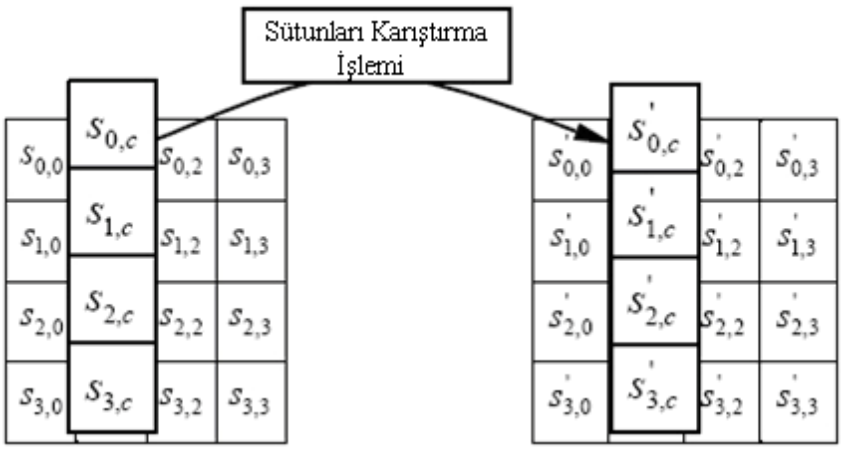
$$s'(x) = a(x) \otimes s(x): \tag{2.19}$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \qquad 0 \le c < Nb \text{ için} \tag{2.20}$$

Bu çarpma sonucunda sütun içerisindeki 4 bayt aşağıdaki gibi oluşmuştur:

$$\begin{aligned} s'_{0,c} &= (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c} \\ s'_{0,c} &= s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c} \\ s'_{0,c} &= s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c}) \\ s'_{0,c} &= (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}) \end{aligned} \tag{2.21}$$

Sütun karıştırma işleminin sütun sütun yapıldığı Şekil 2.4.'de gösterilmektedir:



Şekil 2. 4. Durum bloğunda sütun sütun yapılan sütun karıştırma işlemi

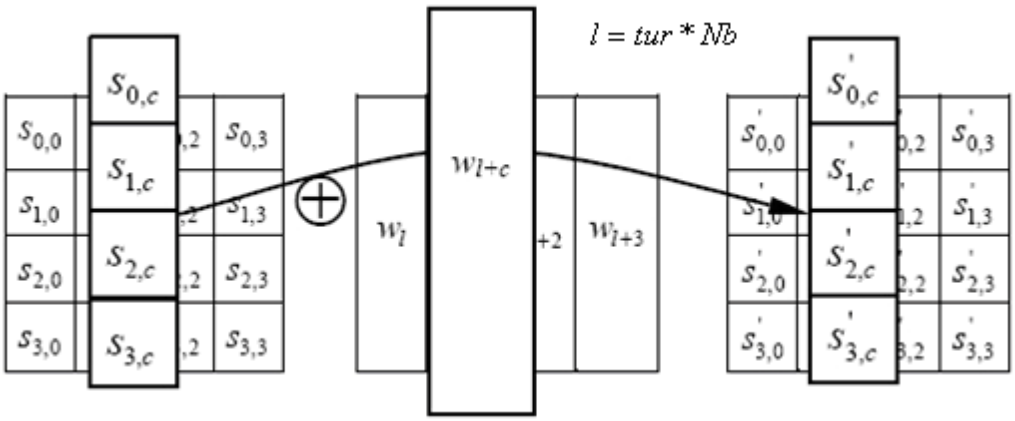
2.3.1.4. Tur anahtarı ekleme

Tur anahtarı ekleme işleminde durum bloğu, tur anahtarı ile XOR işlemine tabi tutulur. Her turun anahtarı, anahtar üreteci ile Nb kelime oluşturulur. Bölüm 2.3.2'de anahtar üretme işlemi anlatılmaktadır. Bu Nb kelime durumun sütunlarına XOR işlemi ile eklenir:

$0 \le c < Nb$ için,

$$\left[s'_{0,c},\ \ s'_{1,c},\ \ s'_{2,c},\ \ s'_{3,c}\right] = \left[s_{0,c},\ \ s_{1,c},\ \ s_{2,c},\ \ s_{3,c}\right] \oplus \left[w_{tur*Nb+c}\right] \qquad (2.22)$$

tanımlıdır. Burada $\left[w_i\right]$ anahtar üretecinin oluşturduğu kelimedir, bölüm 2.3.2 de anlatılmıştır ve "tur" değeri $0 \le tur < Nb$ aralığındadır. Şifreleme işleminde, $tur = 0$ olduğu zaman ilk tur anahtarı ekleme işlemi yapılmış olur ve bu işlem uygulamanın ilk turundan önce yapılan işlevidir. $1 \le tur < Nr$ olduğu zamanda şifrelemenin Nr adet turunda tur anahtarı ekleme işlemiş yapılır. Tur anahtarı ekleme işlemi Şekil 2.5.'de gösterilmiştir. Burada $l = tur * Nb$ 'dir [2,7,10].



Şekil 2. 5. Durum bloğundaki sütun sütun yapılan sütun karıştırma işlemi

2.3.2. Anahtar üreteci

AES algoritmasında anahtar üreteci girdi olarak her birinin uzunluğu 4 bayt olan *Nk* kelime alır ve $\mathrm{Nk}*(\mathrm{Nr}+1)$ kelimelik doğrusal bir dizi üretir. *Nk* kelime ilk anahtar ekleme ve diğer *Nr* turun her biri için tur anahtarı ekleme işlemini sağlaması için yeterlidir. Şekil 2.6.'da anahtar üretecinin temsili kodu gösterilmiştir:

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)

begin
      word temp
      i = 0
      while (i < Nk)
          w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
          i = i+1
      end while
      i = Nk
      while (i < Nb * (Nr+1)]
          temp = w[i-1]
          if (i mod Nk = 0)
              temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
          else if (Nk > 6 and i mod Nk = 4)
              temp = SubWord(temp)
          end if
          w[i] = w[i-Nk] xor temp
          i = i + 1
      end while
End
```

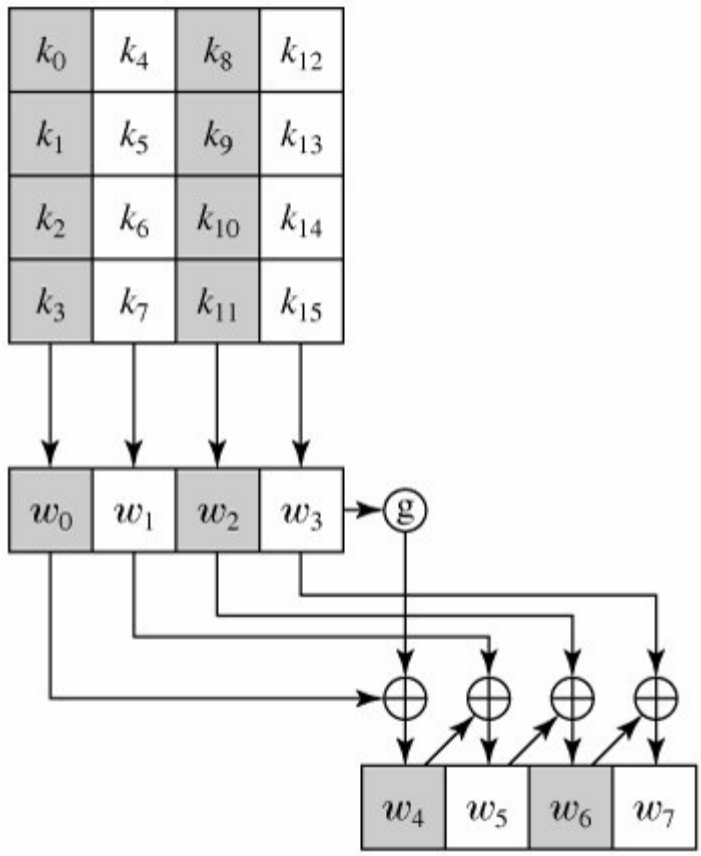
Şekil 2. 6. Anahtar üreteci sözde kodu

Anahtar, anahtar üretecindeki ilk *Nk* kelimeye kopyalanır. Anahtar üretecindeki kalan kelimeler ilk *Nk* kelimede işlemler yapılarak bir anda üretilir. Her eklenen kelime bir önceki kelime ve *Nk* önceki kelimeye bağlıdır. Şekil 2. 6. 'da da görülen 4 durumun üçünde basit XOR işlemi yapılmaktadır. Kelime (w) dizisinin *Nk* katı elemanları için biraz daha karışık işlemler uygulanır. 128 bit şifreleme anahtarı için Şekil 2.7.'de gösterildiği gibi kelime dizisinin ilk 8 kelimesinin oluşumu, ilk 4 kelimesi anahtardan oluşturulup ikinci 4 kelimesi ise g sembolü ile gösterilen karmaşık bir işlev ile oluşturulur. g işlevi aşağıdaki alt işlevlerden oluşur [2,10]:

1. “RotWord” işlevi, bir kelimede sağa doğru bir baytlık dairesel kaydırma yapar. Örneğin kelimemiz $[a_0,\ a_1,\ a_2,\ a_3]$ olsun. “RotWord” işleminden sonra kelimemiz $[a_1,\ a_2,\ a_3,\ a_0]$ olur.

2. “SubWord” işlevi, S-kutusu kullanarak giriş kelimesinin her baytına bayt yer değiştirme işlemi yapar.

3. Birinci ve ikinci adımın sonucu $Rcon[j]$ ile XOR işlemine tabi tutulur.



Şekil 2. 7. 128 bit anahtar için AES anahtar üreteci

Tur sabiti sağdaki 3 baytı daima 0 olan kelimedir. Böylece tur sabiti ile kelimenin sadece soldaki baytı XOR işleminden etkilenir. Tur sabiti her tur için farklıdır ve $RC[1]=1,\ \ RC[j]=2\cdot RC[j-1]$ ile GF(2^8) alanında tanımlı çarpma işlemiyle oluşturulan RC değerleriyle $Rcon[j]=(RC[j],\ 0,\ 0,\ 0)$ olarak tanımlanır. RC değerleri Çizelge 2.4.’te gösterildiği gibi onaltılık tabandadır [2].

Çizelge 2. 4. Onaltılık gösterimde j değerleri için RC değerleri

j	1	2	3	4	5	6	7	8	9	10
RC[j]	1	2	4	8	10	20	40	80	1B	36

Örnek 2.6. 8. tur anahtarı EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F olsun. 9. tur anahtarının ilk 4 baytı aşağıdaki gibidir:

i (decimal)	temp	RotWord İşlevi Sonrası	SubWord İşlevi Sonrası	Rcon (9)	Rcon ile XOR İşlevi Sonrası	w[i - 4]	w[i]=temp XOR w[i - 4] İşlemi Sonrası
36	7F8D292F	8D292F7F	5DA515D2	1B000000	46A515D2	EAD27321	AC7766F3

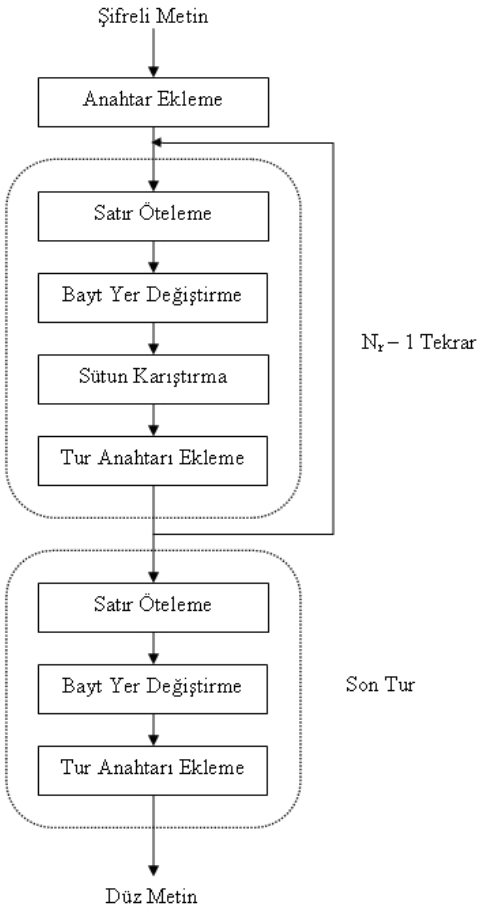
Ekler bölümünde 128, 192 ve 256 bitlik şifreleme anahtarı için anahtar üreteci örnekleri yer almaktadır [10].

2.3.3. Şifre çözme işlemi

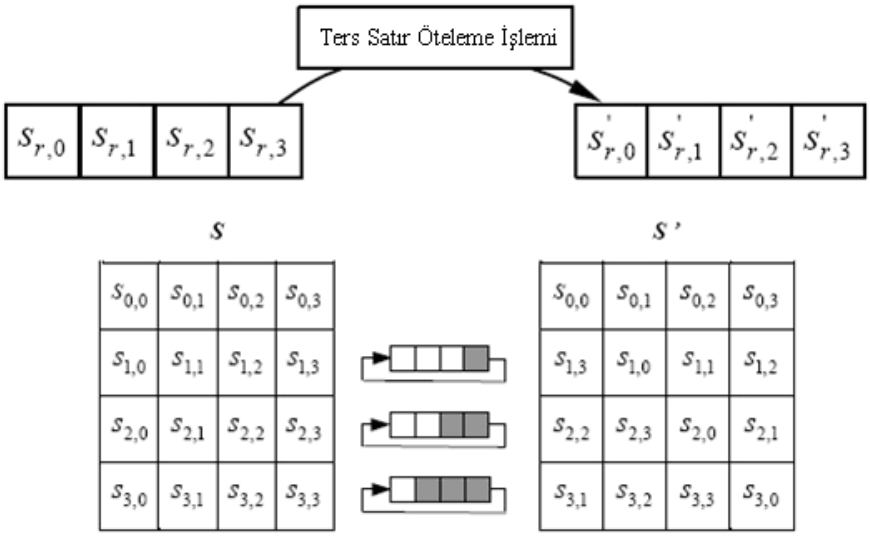
Şifre çözme işlemi, şifreleme işlemindeki işlemlerin terslerinin ters sırada uygulanması işlemidir. Şifre çözme algoritması Şekil 2.8.'de gösterilmektedir.

2.3.3.1. Ters satır öteleme

Satır öteleme işleminin tersidir. Durum bloğunun son 3 satırındaki baytlar dairesel olarak farklı sayıda kaydırılır. Birinci satır kaydırılmaz. İkinci satır 1 sütun, üçüncü satır 2 sütun ve dördüncü satır 3 sütun soldan sağa doğru Şekil 2.9.'daki gibi kaydırılır [11].



Şekil 2. 8. AES şifre çözme algoritması



Şekil 2. 9. Durum bloğunun son 3 satırında yapılan ters satır öteleme işlemi

2.3.3.2. Ters bayt yer değiştirme

Ters bayt yer değiştirme işlemi, bayt yer değiştirme işleminin tersidir. Durum bloğunun her bir baytını Çizelge 2.5.'te gösterilen ters S kutusu kullanarak başka bir bayta dönüştürür [10].

Çizelge 2. 5. Ters S kutusu: xy baytı için ters yer değiştirme değerleri (onaltılık tabanda)

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

2.3.3.3. Ters sütun karıştırma

Ters sütun karıştırma işlemi, sütun karıştırma işleminin tersidir. Bu işlemde durum bloğunun her bir sütununa katsayıları GF(2^8) alanında tanımlı olan polinomlar konusunda da anlatıldığı gibi işlemler yapılır. Sütunlar GF(2^8) üzerinde polinomlar olarak kabul edilir. Bu işlemde her bir sütun çarpım matrisinde sütun sütun çarpılarak yeni sütunlar oluşturulur. Çarpım matrisi burada $a^{-1}(x)$ polinomundan oluşturulur.

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\} \tag{2.23}$$

$a^{-1}(x)$ polinomunda çarpım matrisi

$$s'(x) = a^{-1}(x) \otimes s(x): \tag{2.24}$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \qquad 0 \le c < Nb \text{ için} \tag{2.25}$$

gibi tanımlıdır. Bu çarpımın sonucunda sütun içindeki 4 bayt

$$\begin{aligned} s'_{0,c} &= (\{0e\} \bullet s_{0,c}) \oplus (\{0b\} \bullet s_{1,c}) \oplus (\{0d\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c}) \\ s'_{1,c} &= (\{09\} \bullet s_{0,c}) \oplus (\{0e\} \bullet s_{1,c}) \oplus (\{0b\} \bullet s_{2,c}) \oplus (\{0d\} \bullet s_{3,c}) \\ s'_{2,c} &= (\{0d\} \bullet s_{0,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0e\} \bullet s_{2,c}) \oplus (\{0b\} \bullet s_{3,c}) \\ s'_{3,c} &= (\{0b\} \bullet s_{0,c}) \oplus (\{0d\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0e\} \bullet s_{3,c}) \end{aligned} \tag{2.26}$$

gibi oluşur.

2.3.3.4. Ters anahtar ekleme

Anahtar ekleme işleminde durum bloğundaki baytlar anahtar ile XOR işlemine tabi tutuluyordu. XOR işlemi kullanıldığından anahtar ekleme işleminin terside yine kendisidir.

3.AES ŞİFRELEME ALGORİTMASININ PDA ÜZERİNDE UYGULANMASI

Bu bölümde sırasıyla uygulamada kullanılan araçlar ve AES şifreleme algoritmasının güvenli iletişim için PDA üzerinde geliştirilen bir uygulaması anlatılacaktır. Bu uygulamada cihaz olarak HTC firmasının üretmiş olduğu HD2 modeli, programlama platformu olarak Visual Studio .NET 2008, programlama dili olarak C#, işletim sistemi olarak Windows Mobile 6.5 Professional, Web Servis olarak XML Web Service ve veritabanı olarak da SQL Server kullanılmıştır. Uygulamada verilerin güvenliği AES şifreleme algoritması ile arttırılmıştır.

3.1. Windows Mobile ve PDA

Microsoft firmasının yıllardır ürettiği ve geliştirdiği uygulamalar standart hale gelmiştir. Microsoft, Windows Mobile teknolojisi ile standartlaşmış formlarını kalıplarından çıkarmıştır. Bu değişimle daha görsel ve başarılı uygulamalar sunar hale gelmiştir ve zaman ilerledikçe de gelişmeye devam etmektedir. Her yeni Windows Mobile sürümü bir önceki sürümün hatalarından arındırılarak ve geliştirilerek yeniliklerle hayata sunulur. Fakat bu gelişimlerde genellikle genel çizgi aşılmaz. Windows mobile yazılımların temeli CE (Compact Edition)'dir.

Windows Mobile işletim sistemi taşınabilir cihazlar için işletim sistemi açısından büyük değişimler yapmış bir teknolojidir. Yani Windows Mobile, PDA ve son teknoloji mobil cihazlar için geliştirilmiş bir işletim sistemidir diyebiliriz.

Bu uygulamada mobil cihazlardan Windows Mobile işletim sisteminin uygulandığı PDA (Personal Digital Asistant) kullanılmıştır. PDA'lara Pocket PC yani taşınabilir cep bilgisayarı da denir. Aynen bir bilgisayar gibi kendine özel işletim sistemine sahiptir. Yukarıda belirttiğimiz gibi bu işletim sistemi Windows Mobile'dir. İlave olarak cep telefonu özelliği taşır. Boyut olarak küçük olduğundan dolayı taşınması kolay olan bu bilgisayarlarda kişisel bilgilerin, isimlerin, adreslerin, hesapların, belgelerin ve benzeri bilgilerin bulunduğu veritabanı sistemine sahiptir. Gelişen teknoloji ile günümüzde bu kendi küçük ama özellikleri büyük PDA'ların cep

telefonu, görsel ekranı, güçlü işlemcisi, çoklu ortam işlemleri, video oynatma, fotoğraf çekimi, yer bildirimi (navigasyon) ve GPS özellikleri ile kullanımı bir hayli yaygınlaşmıştır. Kullanım alanlarına göre özellikleri de değişmektedir.

Windows Mobile uygulamaları yapılırken geliştirme ve derleme için Visual Studio ortamında yardım ve kolaylık sunan birçok özellik mevcuttur.

3.2. XML Web Servisler

Mevcut teknolojiler ile işletmelerin birbirleri ile iletişimi sorun oluşturmaktaydı. İşletmelerin internet taleplerinin büyümesiyle daha gelişmiş bir teknolojiye ihtiyaç vardı [14].

Örneğin; bir hastanenin ya da emniyet müdürlüğünün içişleri bakanlığına kimlik numarası ile kimlik bilgisi sorgusu yapması gibi kurumlar arası bilgi alış veriş işlemlerinde birçok sorun yaşanmaktaydı.

Farklı işletim sistemleri, farklı programlama dilleri, farklı nesne modelleri veri alışverişinde büyük problemlere sebep oluyordu. Web Servisler bu tip problemleri çözmek için geliştirildi.

Web Servisler sayesinde farklı işletim sistemlerindeki ve farklı programlama dilleriyle geliştirilen programlar arasındaki veri alışverişi sorunsuz sağlanır. SOAP, HTTP ve XML gibi iyi desteklenen internet standartlarını kullanması sayesinde bütün platformlarla uyum içinde çalışır [15].

XML Web Servis, .NET gibi güncel uygulama platformlarına uyum sağlaması ve bu platformlarda kolayca geliştirilmesi, işletim sistemlerinden ve platformlardan bağımsız olması, internet üzerinden kullanıcıların uygulamalara kolayca ulaşım sağlaması ve bu kadar geniş kitlelere ulaşırken güven problemi oluşturmaması açısından avantajlıdır.

Web Servis SOAP protokolünü kullanan bir Web uygulamasıdır. SOAP üç amaç için tasarlanmıştır [14].

1. İnternet üzerinde çalışabilmelidir,
2. Basit ve uygulaması kolay olmalıdır,
3. XML tabanlı olmalıdır.

SOAP Web Servisi ile istemci arasındaki iletişimin nasıl olacağını belirler. XML temellidir. İki uygulamanın internet üzerinden birbirleri ile nasıl iletişim kuracağını belirleyen bir protokoldür [15].

Web Servis her türlü uygulama için yeni bir etkileşim düzeyine erişim yeteneği sağlar. Web Servis HTTP üzerinden herhangi bir istemci tarafından çağrılabilen nesneler ve metotlardır [14-16].

XML'de bir Web Servis hizmetidir. XML Türkçe olarak genişletilebilir işaretleme dili anlamına gelmektedir. Öğrenilmesi kolaydır ve XML bir standarttır. Web' de yapılandırılmış biçimde bulunan verileri kullanma olanağı sağlar. XML ile veri oluşturmak ve veri okuyup, işlemek basittir. XML platformdan bağımsız çalışır.

XML Web Servisler bir kullanıcı arabirimine sahip olmayıp, kendine ait standart bir arayüze sahiptir. Bir XML Web Servisi standart Web protokollerini yani XML, http ve SOAP'ı kullanır. Bu Web standartlarını destekleyen herhangi bir sunucu üzerinde çalışır. Bu standartlar W3C standardı olduğu için hemen hemen tüm işletim sistemleri ve farklı programlama dilleri tarafından desteklenir. Farklı dil ve platformları desteklemesinden dolayı XML Web Servisleri internet üzerinde veri alışverişi için kullanılır.

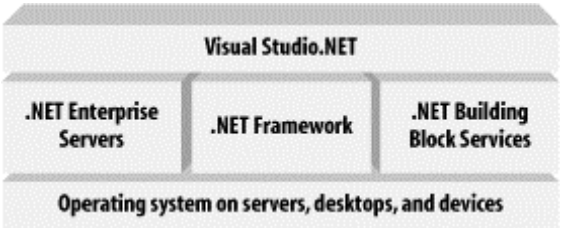
3.3. Visual Studio .NET 2008

Visual Studio 2000 yılından bu yana gelişimini sürdürmektedir. Visual Studio .NET platformu ara kod tabanlı çalışma mantığına sahiptir. Uyumlu diller kullanılarak

istenilen ara kodun üretilmesini sağlar. .NET, farklı diller arasında uyumlu olabilme özelliğine sahiptir. Microsoft firması .NET'i, geliştirilen uygulamaların windows işletim sistemlerinde platformdan bağımsız olarak çalışması amacı ile üretmiştir.

.NET platformu, PDA gibi yeni nesil mobil cihazlar için de hızlı ve kolay bir şekilde yazılım geliştirmek için kullanılır. Mobil cihazlarda kullanılırken farklı olarak .NET framework yerine .NET compact framework gerekmektedir. Visual Studio, Visual Basic, C#, C++ dillerinin geliştirme ortamlarını ve özelleştirilmiş kütüphanelerini içerisinde bulundurur.

Hızlı ve kolay yazılım geliştirilebilmesinden dolayı avantajlıdır. Bileşen tabanlı çalışma ortamı sağlar. Windows uygulamalarının yanı sıra web uygulamaları geliştirmek için de yaygın olarak kullanılmaktadır. .NET platformu Şekil 3.1.'de olduğu gibi 5 ana bileşenden oluşmaktadır. Bu 5 ana bileşenden en alt tabakayı işletim sistemi oluşturur. Bu alt tabakada Windows CE, Windows ME, Windows 2000, Windows XP, Windows Vista vb. Windows işletim sistemlerinden biri olabilir [14-17].



Şekil 3. 1. .NET platformu

İşletim sisteminin üzerinde ise Application Server, BizTalk Server, Commerce Server, Exchange Server, Host Integration Server, Internet Security ve Acceleration Server ürünlerini içeren .NET Enterprise Server bulunur [16].

.NET platformunun en üst tabakası yeni bir geliştirme aracı olan Visual Studio .NET'tir. Visual Studio 6.0'ın devamı niteliğindedir. Farklı dilleri ve hata ayıklama,

XML Şema Editörü gibi birçok yeni özellikleri destekleyen IDE (Integrated Development Environment)'dir.

.NET'in merkezinde Microsoft .NET Framework bulunmaktadır. .NET Framework, Windows platformu üzerinde geliştirilen uygulamaların geliştirme ve çalıştırma altyapısıdır. Bütün .NET dillerinin kullanabildiği ortak framework sınıfları ve CLR (Common Language Runtime)'yi içerir.

3.3.1. .NET compact framework

Her zaman, her yerden, her cihazdan bilgiye ulaşmak için sağlam bir altyapıya ihtiyaç vardır ve bu alt yapı platformdan bağımsız olmalıdır. Bu ihtiyaç .NET Framework ile sağlanmaktadır. .NET Framework, web uygulamalarını, web servislerini ve windows uygulamalarını, .NET'de veriye ulaşımı, CLR (Common Language Runtime), CTS (Common Type System) ve .NET Programlama dillerini yani tüm gereksinimleri içinde bulundurur.

PDA gibi mobil cihazlarda Mobil .NET uygulamalarını çalıştıran ve .NET Framework platformunun, mobil cihazların niteliklerine göre geliştirilmiş haline ise .NET compact framework denir. Kısacası .NET Framework' ün özel bir sürümüdür. PDA'larda çalışması için Mobil.NET'de geliştirilen uygulama, .NET CF (Compact Framework)'e ihtiyaç duyar [19].

Visual Studio .NET kullanarak Windows Mobile cihazları için yazılım geliştirmek kolay ve zevklidir. Visual Studio .NET Compact Framework, .NET Framework'e paralel olan class kütüphanelerini sağlar. Fakat bu kütüphaneler tamamıyla özdeş değildir. Visual Studio .NET Compact Framework ile .NET Framework' ün çalışma mantığı aynıdır [15,16, 20].

Visual Studio .Net'de Windows Mobile için yazılım geliştirmede kullanılan IDE ile Windows uygulamaları için kullanılan IDE aynıdır. Bu sayede yeni bir IDE

öğrenmeye gerek yoktur. Windows Mobile sadece farklı bir program tipi oluşturma işlemidir.

Windows Mobile ile Windows masaüstü işletim sistemleri kullanılan hata düzeltme programları, görsel tasarım şekilleri, kullandığı kütüphaneler, kullandığı diller, yardım yapısı ve daha birçok ortak niteliklere sahiptirler.

Visual Studio .NET'de mobile için yazılım geliştirirken .NET CF kullanılır. VS 2003'de 1.0 versiyonu, 2005'de 2.0 versiyonu, 2008'de 2.0 veya 3.5 versiyonlarıyla yazılım geliştirilebilinir. Bu yazılımlar geliştirilirken de C#, Visual Basic ve C++ dilleri kullanılabilir.

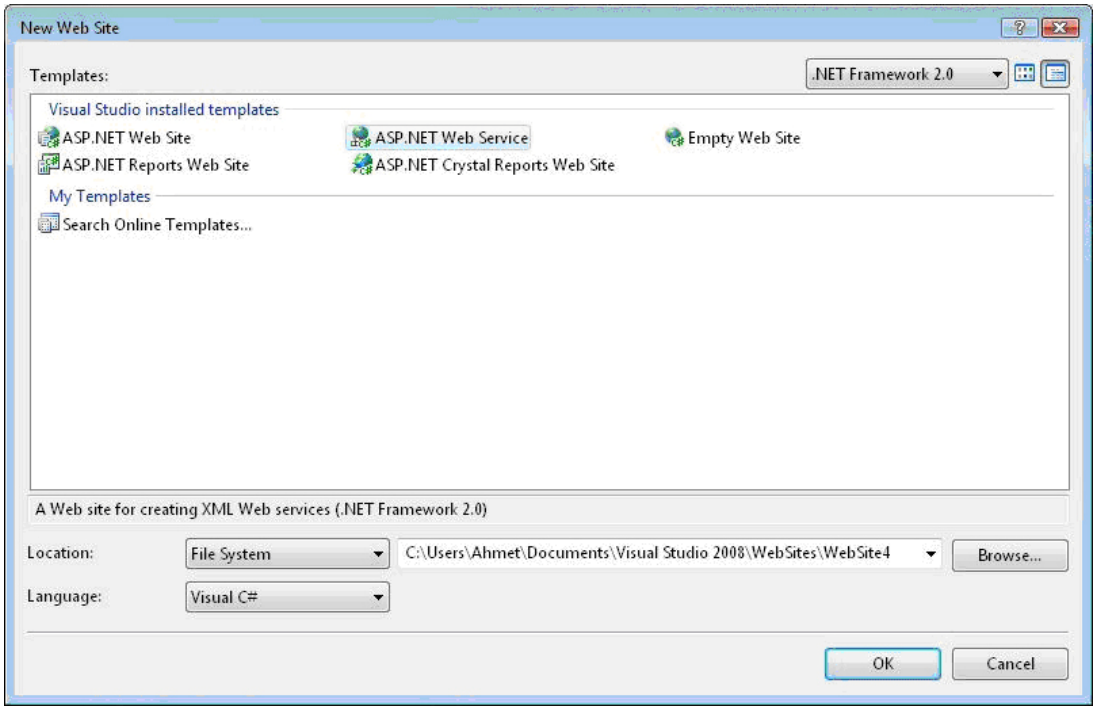
3.3.2. Visual Studio .NET ile bir web servis oluşturmak

Visual Studio .NET ile bir Web Servisi oluşturmak için Microsoft Visual Studio 2008 editöründe;

File menüsünde bulunan New menüsündeki Web Site menüsü tıklanır, sonra Şekil 3.2.'de gösterilen New Web Site iletişim kutusu açılır.

Açılan kutudan hangi .NET Framework sürümü kullanılmak isteniyor ise seçilir ve Templates bölümünden ASP. NET Web Service seçeneği ve Language bölümünden Visual C# dilini seçerek, Location bölümüne web servisin dosyalarının hangi klasörde oluşturulacağını belirterek OK butonuna tıklanır. Böylece Web Servis projemizi geliştirmeye başlanır.

Web servis oluşturduğumuzda Service.asmx, Service.cs ve Web.config isimli dosyalar otomatik olarak oluşmaktadır. Service.asmx dosyası web servisin uygulama dosyasıdır. Internet Information Server (IIS) Service.asmx dosyasını çalıştırır. Web servisindeki web metotları service.asmx dosyasının uzantısı .cs olan kod dosyasına yazılmaktadır. Şekil 3.3.'de gösterildiği gibi bu dosya service.asmx dosyasında CodeBehind özelliğinde belirtilir. Varsayılan olarak service.cs dosyasıdır.



Şekil 3. 2. New web site iletişim kutusu

```
<%@ WebService Language="C#" CodeBehind="~/App_Code/Service.cs"
Class="Service" %>
```

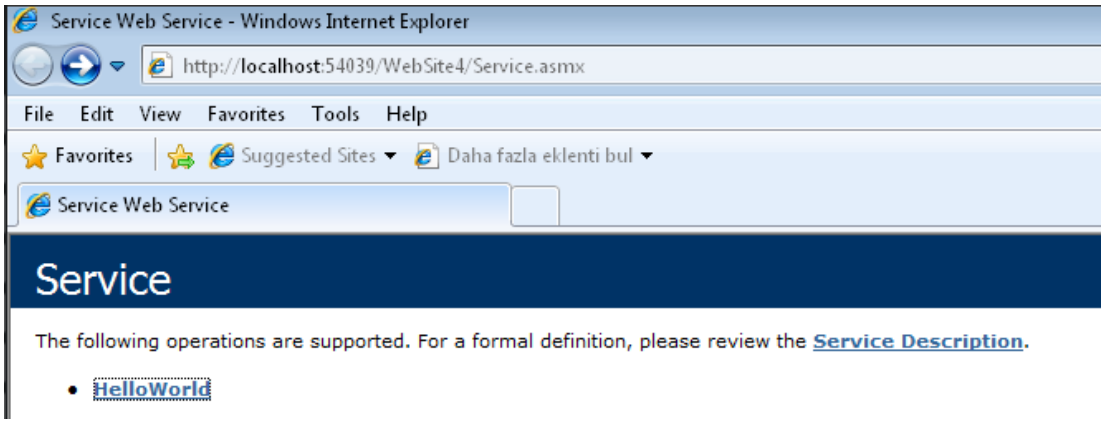
Şekil 3. 3. Service.asmx dosyasının özelliklerini belirten kod

Service.cs dosyasında web serviste kullanılacak web metotları yazılır. Herhangi bir metodun web metot olabilmesi için Şekil 3.4.'de gösterildiği gibi metottan önceki satırda [WebMethod] ifadesi yer almalıdır. Aksi halde o metot internet üzerinde çalışmaz. Örnek web metodu Şekil 3.5.'de gösterildiği gibi web tarayıcısında çalışmaktadır.

Web.config dosyası web servisimiz için gereken XML tabanlı ayar dosyasıdır. Uygulamada oluşan hatanın ziyaretçilere gösterilip gösterilemeyeceği, uygulamanın bölgesel ayarları, kimlik denetimi, veritabanı bağlantı bilgileri ve kullanıcıların yetki tanımlamaları gibi ayarlamalar bu dosya üzerinde yapılabilir.

```
using System;
using System.Web;
using System.Web.Services;
using System.Web.Services.Protocols;

[WebService(Namespace = "http://tempuri.org/")]
[WebServiceBinding(ConformsTo = WsiProfiles.BasicProfile1_1)]
public class Service : System.Web.Services.WebService
{
    public Service () {

        //Uncomment the following line if using designed
components
        //InitializeComponent();
    }

    [WebMethod]
    public string HelloWorld() {
        return "Hello World";
    }

}
```

Şekil 3. 4. Service.cs dosyasında örnek bir web metot oluşturma sözde kodu

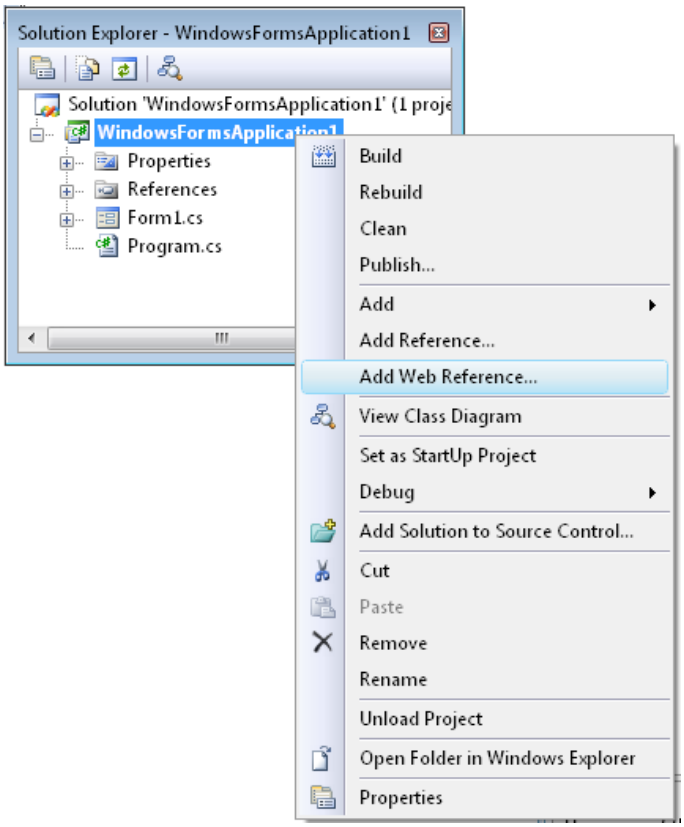


Şekil 3. 5. Web servisin helloword web metodu

3.3.3. Visual Studio .NET ile uygulamaya bir web servis eklemek

Visual Studio .NET'te oluşturulmuş olan bir projede yayınlanan web servisi projemizde kullanmak için; Web Servisi, web referansı olarak projeye eklememiz gerekmektedir. Bu işlem "Project" menüsünden "Add Web Reference" menüsüne veya Şekil 3.6.'daki gibi "Solution Explorer" penceresinde sağ tuş tıklanarak açılan

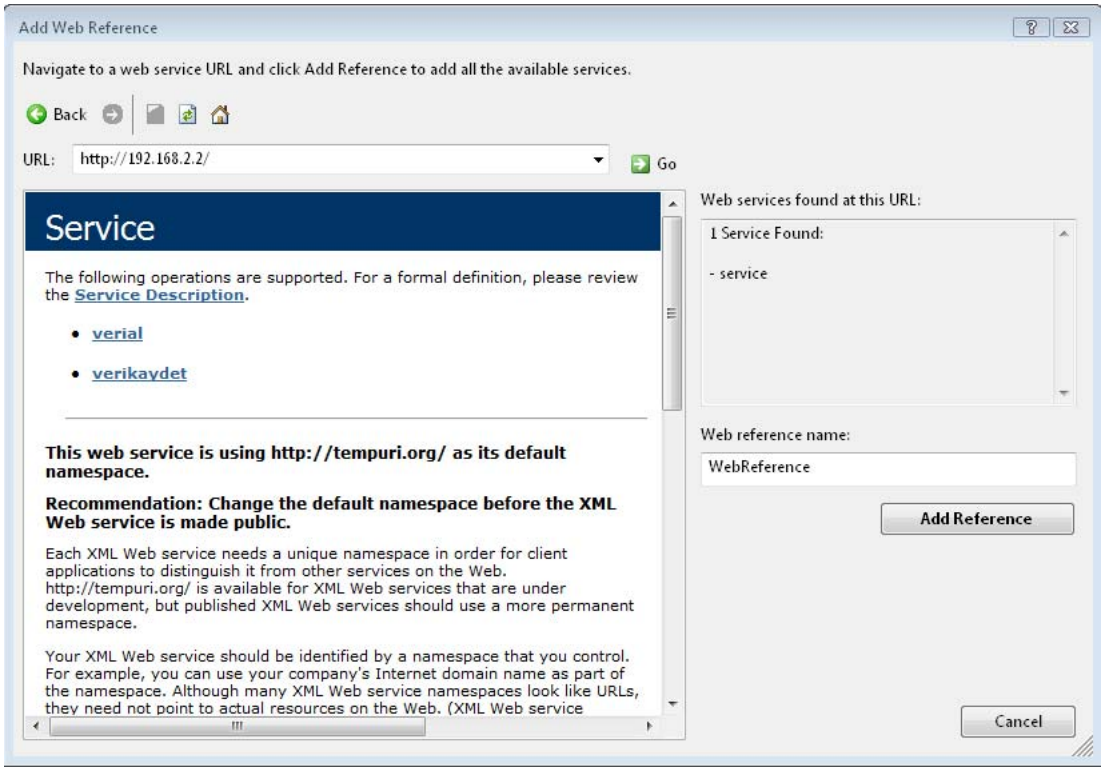
menüdeki “Add Web Reference” menüsüne tıklanarak Şekil 3.6.’da gösterilen “Add Web Reference” penceresi açılır.



Şekil 3. 6. Solution Explorer penceresinden Web Reference ekleme

“Add Web Reference” penceresinde URL kısmına web servisin yayınlandığı sunucunun IP adresi yazılarak “Go” butonu tıklanır. Bu işlemden sonra yayınlanan web servis ve metotları Şekil 3.7.’de gösterildiği gibi “Add Web Reference” penceresindeki tarayıcıda gözükür. “Web Reference Name” bölümüne web servisin referansının adı yazılarak “Add Reference” butonu tıklanır.

Web servisi uygulamaya eklendikten sonra web metodu kullanmak için web servis bir nesne olarak oluşturulmalıdır ve bu sınıfın ilgili metodu çağrılarak işlem yapılır. Örnek kod Şekil 3.8.’deki gibi ifade edilmektedir.



Şekil 3. 7. Add Web Reference penceresi

```
WebReference.Service servis = new WebReference.Service();
gelen = servis.verial(islem.sifrele(textBox1.Text));
```

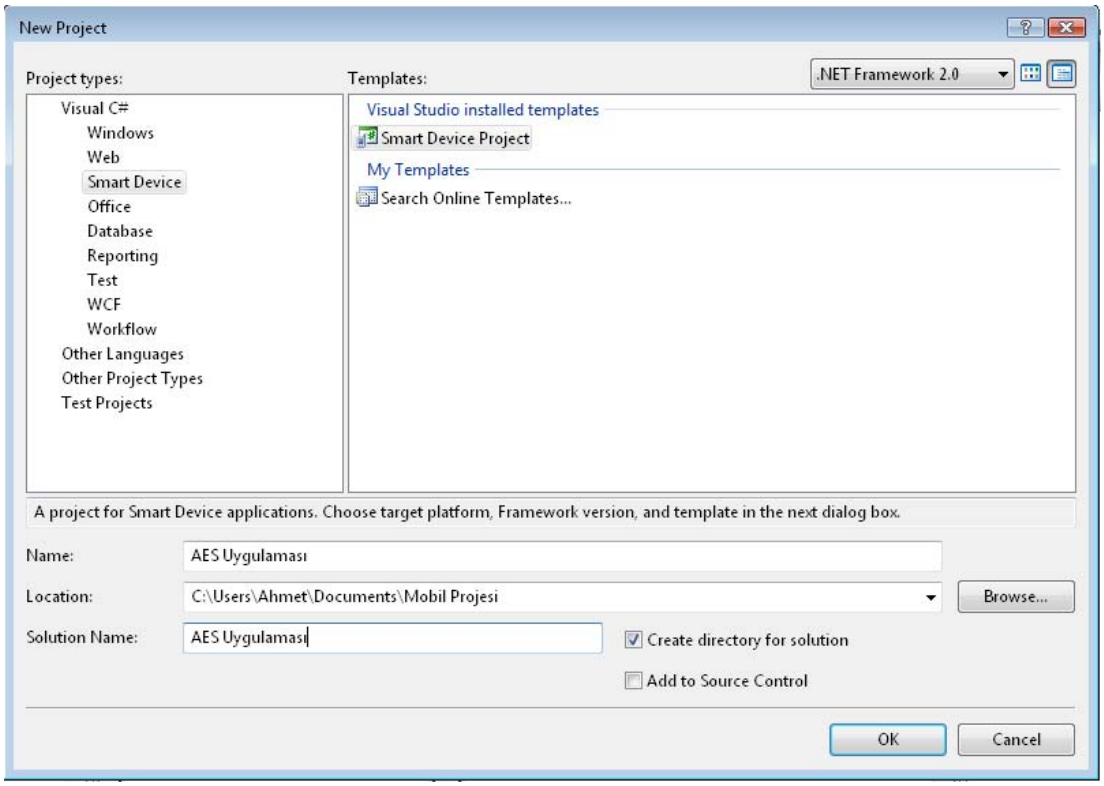
Şekil 3. 8. Uygulamada eklenen web servisin web metodunun çağrılması

3.3.4. Visual Studio .NET ile PDA uygulaması oluşturmak

Visual Studio .NET 2008'de PDA uygulaması oluşturmak için ilgili "Windows Mobile 6 Professional Software Development Kits (SDK)" aracının kurulması gerekmektedir. Uygulamada kullanılan cihazın işletim sistemi "Windows Mobile 6.5 Professional" sürümüne uygun olan "Windows Mobile 6.5 Professional Developer Tool Kit (DTK)" aracıdır.

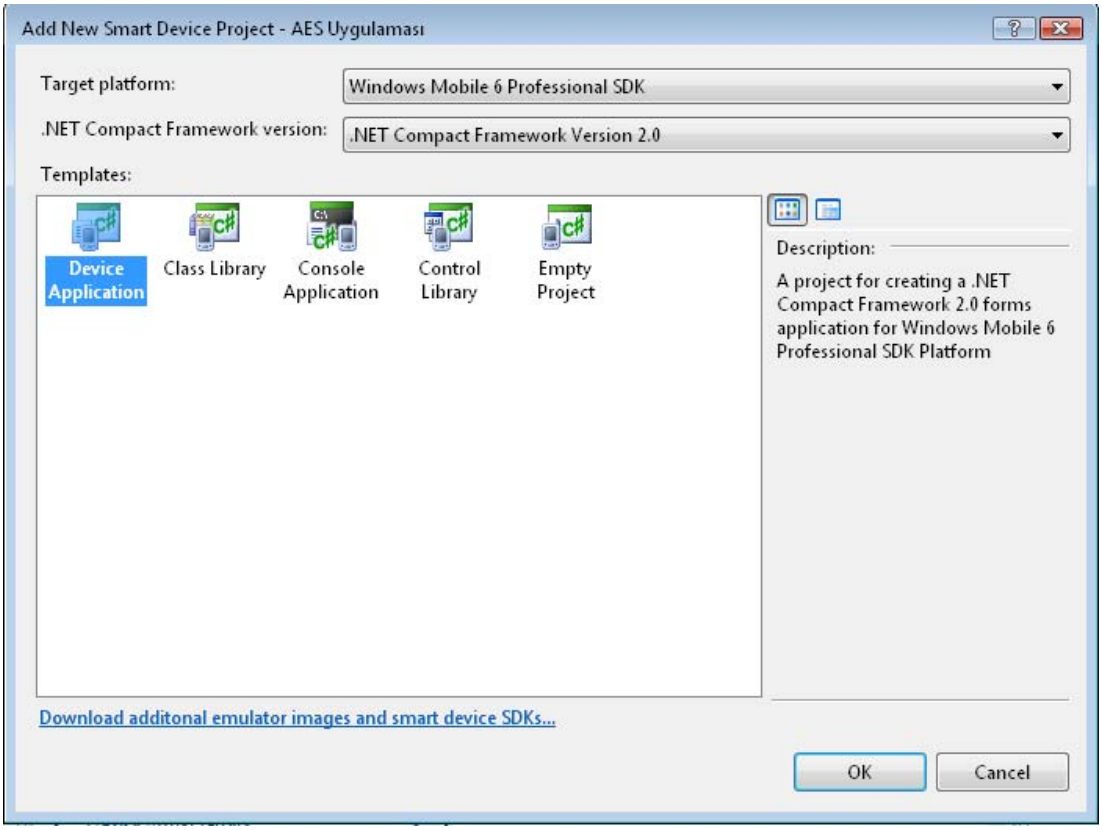
Windows mobil uygulaması geliştirmek için "File" menüsünden "New Project" tıklanır. Ekrana gelen Şekil 3.9.'da gösterilen "New Project" penceresindeki proje

tiplerinden Smart Device Project tipi seçilir ve Project Template bölümünden Smart Device Project Template'i seçilir. Sonra projenin ismi ve adresi yazılır ve OK butonuna tıklanır.



Şekil 3. 9. New project iletişim kutusu

Bir sonraki adımda Şekil 3.10.'da gösterilen "Add New Smart Device Project" penceresi açılır. Bu pencereden "template" bölümünden "Device Application" ve "Framework" versiyonu seçme bölümünden ".NET Compact Framework" versiyonu seçilir. "OK" butonuna tıklanır. Şekil 3.11.'de gösterilen form tasarlanmak üzere açılır.

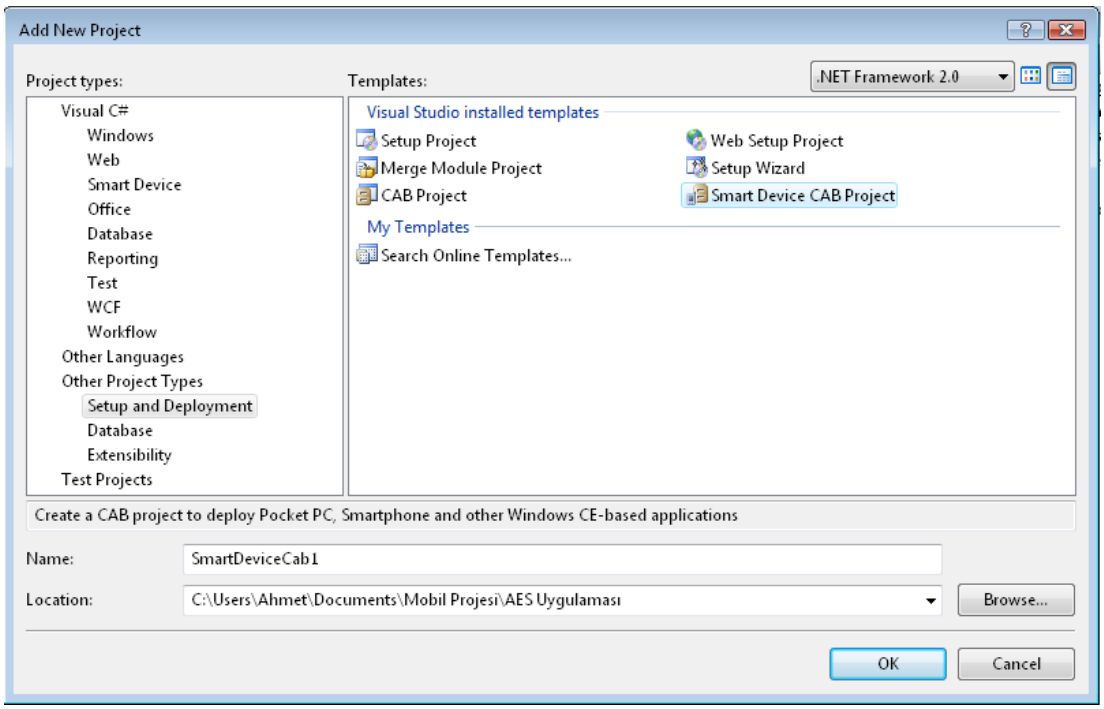


Şekil 3. 10. Add new smart device Project penceresi

Şekil 3. 11. Smart device formu

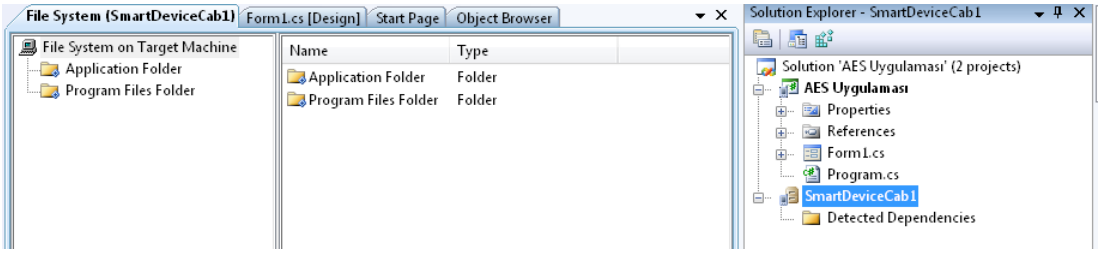
3.3.5. Visual Studio .NET ile PDA uygulamasına paket oluşturmak

Visual Studio ortamında geliştirilen Smart Device Projesinin PDA'larda çalışması için kurulum paketi hazırlanması gerekmektedir. Oluşturulan paket CAB uzantılıdır. Visual Studio 2008'de kurulum projesi oluşturma işlemi için File menüsündeki Add menüsünde bulunan New Project menüsü tıklanarak açılan Şekil 3.12.'de gösterilen pencereden Other Project Types seçeneğinden Setup and Deployment proje tipi seçilir. Template bölümünden Smart Device CAB Project 'i seçip projenin ismini ve oluşturulacak klasör belirlendikten sonra OK butonuna tıklanır.



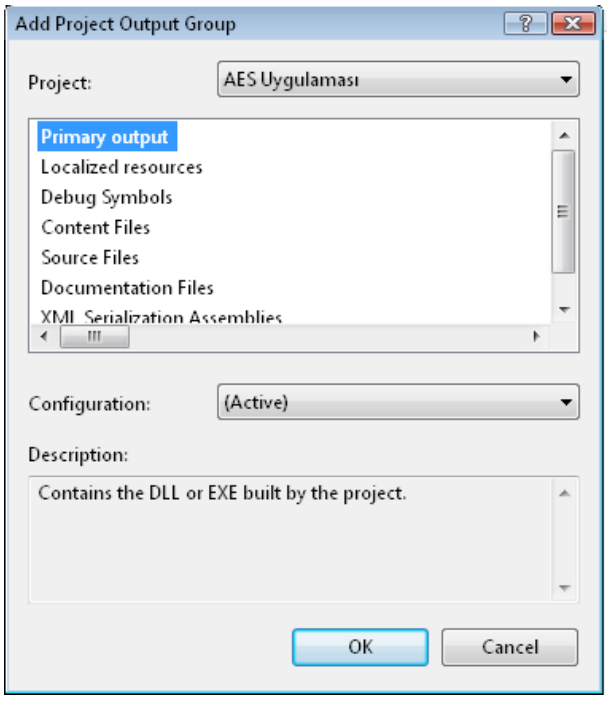
Şekil 3. 12. Kurulum paketi oluşturmak için Add New Project penceresi

Şekil 3.13.'te gösterildiği gibi kurulum projesi PDA uygulamasının içerisine oluşturulur.

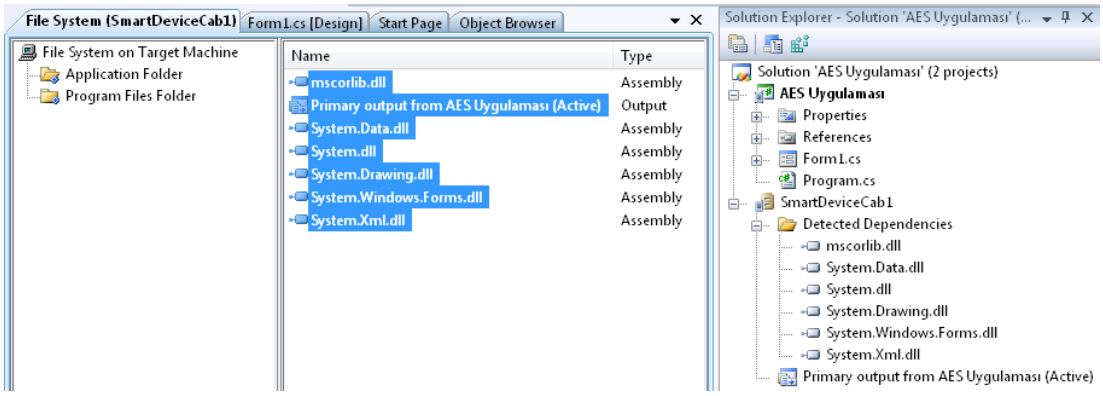


Şekil 3. 13. Kurulum projesinin projedeki gösterimi

Şimdi "Aplication Folder" üzerinde sağ tuş tıklayıp açılan menüden "Add" menüsünden "Project Output" menüsüne tıklayarak Şekil 3.14.'te gösterilen "Add Project Output Group" penceresinden "Primary Output" seçeneğini seçerek ve "Configuration" seçeneğinden de "Active" seçeneğini seçerek "OK" butonuna tıklanır. Böylece Şekil 3.15.'te gösterildiği gibi projemizin "dll" ve "exe" dosyaları "Cab" dosyasına eklenir.



Şekil 3. 14. Add project output group penceresi



Şekil 3. 15. Projenin exe ve dll dosyalarının eklenmiş hali

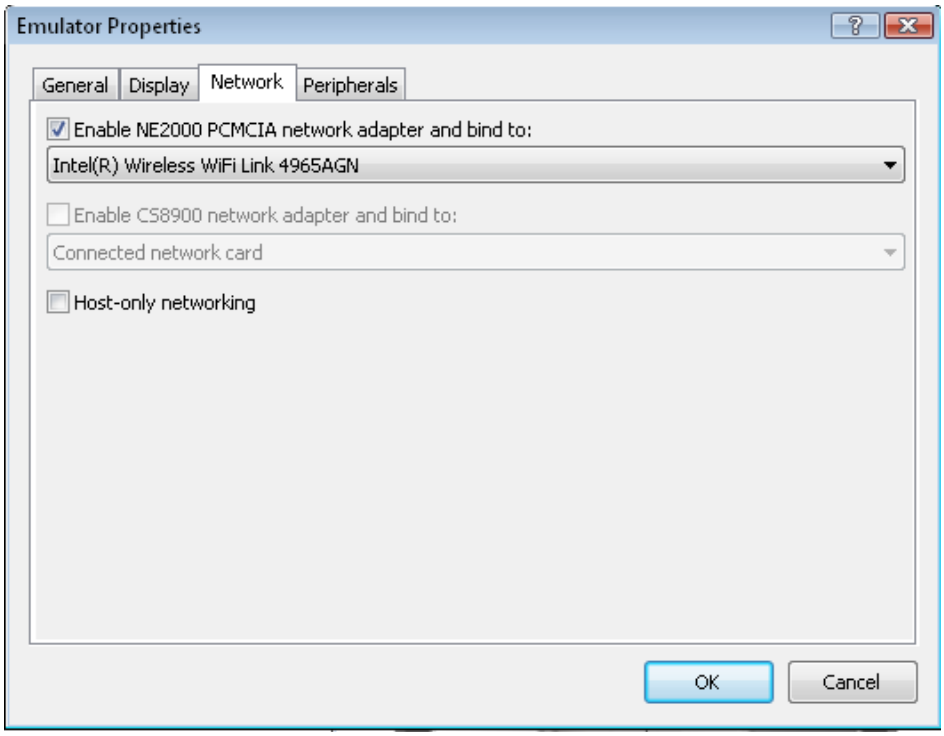
Bu haliyle kurulum projemizi built edince kurulum dosyamız olan CAB dosyası oluşur. Bu CAB dosyasını PDA'ya kurabiliriz.

3.3.6. Windows Mobile 6.5 Professional emülatörleri

Emülatörler ise Visual Studio ortamında geliştirdiğimiz yazılımları test etmemiz için kullanılır. Geniş bir yelpazede mobil cihazlarda Windows Mobile işletim sistemleri kullanılmaktadır. PDA'ları uygulama geliştirirken temin etmek maliyeti arttırır. Bu nedenle sanal donanım ve Windows Mobile işletim sisteminin farklı sürümlerini destekleyen Şekil 3.16.'da gösterilen emülatörler her türlü kodu çalıştırır.

Emülatörler asıl cihazın taklididir ve aynı yeteneklere sahiptir. Orijinal Windows Mobile uygulamalarını çalıştırabilirler. Şekil 3.17.'de gösterildiği gibi Emülatörün özellikleri penceresindeki "Network" sekmesinden ağ ayarlarını yaparız. Bu sayede emülatörler bilgisayarımızın internetini de sanal olarak kullanabilirler. Bu işlemin başarılı bir şekilde çalışması için "Microsoft Virtual PC" programını kurmak gerekmektedir. Emülatörlerde "breakpoint" özelliği sayesinde kodların çalışmasını izleyebilir ve hataları kontrol edebiliriz.

Şekil 3. 16. Windows Mobile 6.5 Professional işletim sistemli emülatör



Şekil 3. 17. Emülatör Properties penceresi

3.4. Geliştirilen Uygulamanın Test Edildiği PDA'nın Özelikleri

Uygulamamızda Şekil 3.18.'de gösterilen HTC firmasının ürettiği HD2 PDA ürünü kullanılmıştır. Bu bölümde uygulamada kullanılan PDA'nın özellikleri Çizelge 3.1.'de gösterilmektedir.

Çizelge 3. 1. HTC HD2 cihazının özellikleri

İşletim Sistemi	Windows Mobile 6.5
İşlemci	Qualcomm 1GHz Snapdragon
Dahili Bellek	ROM 1GB; RAM 576MB
Uyumluluk	* WiFi: 802.11 b/g * GPS/AGPS
Boyutlar	122x67x11mm
Ağırlık	157g (with battery)
Ekran	4.3-inch HD touch-sensitive screen with 480 x 800 WVGA resolution
Teknoloji	GSM: 850/900/1800/1900 MHz WCDMA/HSPA: 1700 MHz (AWS) / 2100 MHz
Batarya	1230 mAh Talk Time: 380 min (GSM) Standby Time: 490 hours (GSM) (The above are subject to network and phone usage)
Hoparlör	Built-in microphone, speaker
Kamera	5MP, including widescreen capture, digital zoom and 2x LED Flash
Ses/Görüntü	* Windows Media® Player * Albums * Pictures & Videos * FM Radio * Audio supported formats: .aac, .amr, .m4a, .mid, .mp3, .mp4, .qcp, .wav, .wma * Video supported formats: .wmv, .asf, .mp4, .3gp, .3g2, .m4v, .avi
G/Ç Arabirimi	Bluetooth® 2.1 with Enhanced Data Rate, WiFi: 802.11 b/g
Büyüme	microSD™ memory card (SD 2.0 compatible) (up to 32GB)
Kutu İçeriği	16GB MicroSD Card MicroUSB Cable Travel Charger
Kullanıcı Arabirimi	* HTC Sense user experience * Capacitive touchscreen with pinch-to-zoom and haptic capability * G-Sensor * Proximity sensor * 3.5 mm headset jack

Şekil 3.18. Uygulamanın test edildiği cihaz

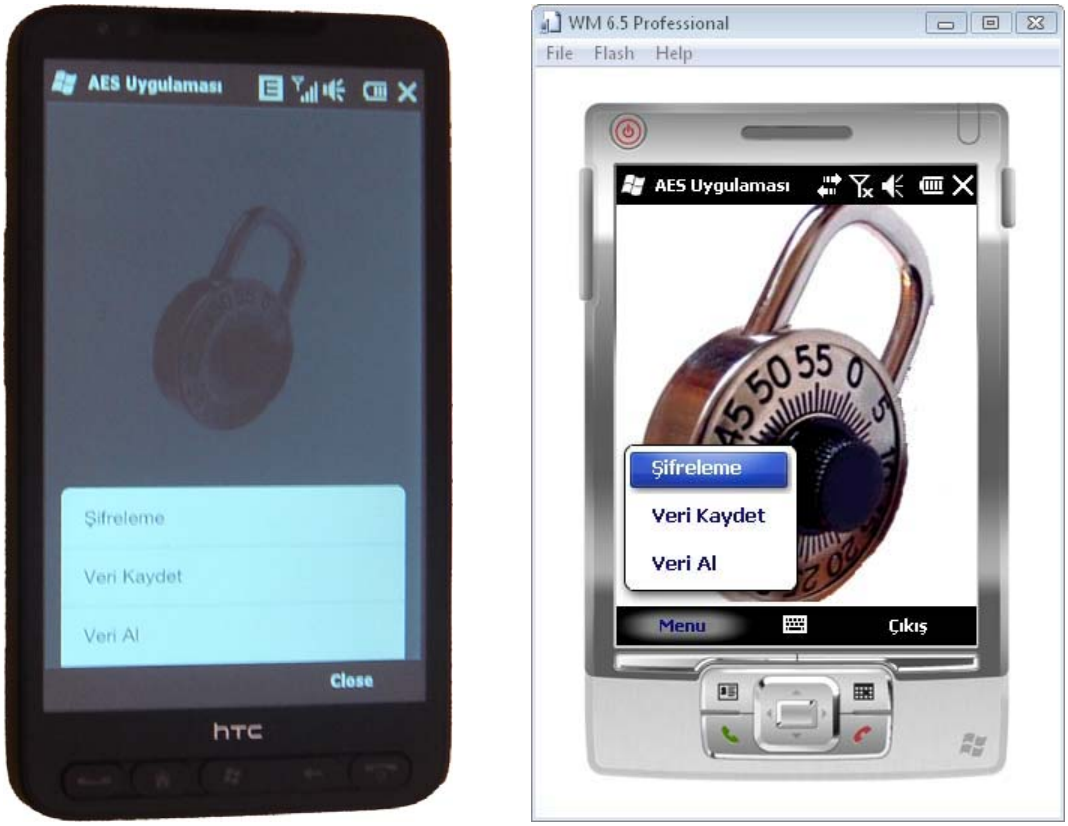
3.5. Geliştirilen Uygulama

Bu konuda geliştirilen uygulamaların çalışma sistemi anlatılacaktır. Geliştirilen çalışma bir XML web servis ve PDA için geliştirilen uygulamadan oluşturulmaktadır. Bu konuda alt başlıklar halinde uygulamaya ait 4 adet ekran incelenecektir. Bu ekranlar aşağıdaki gibidir.

Ana Menü Ekranı
Şifreleme Ekranı
Veri Kaydetme Ekranı
Veri Alma Ekranı

3.5.1. Ana menü ekranı

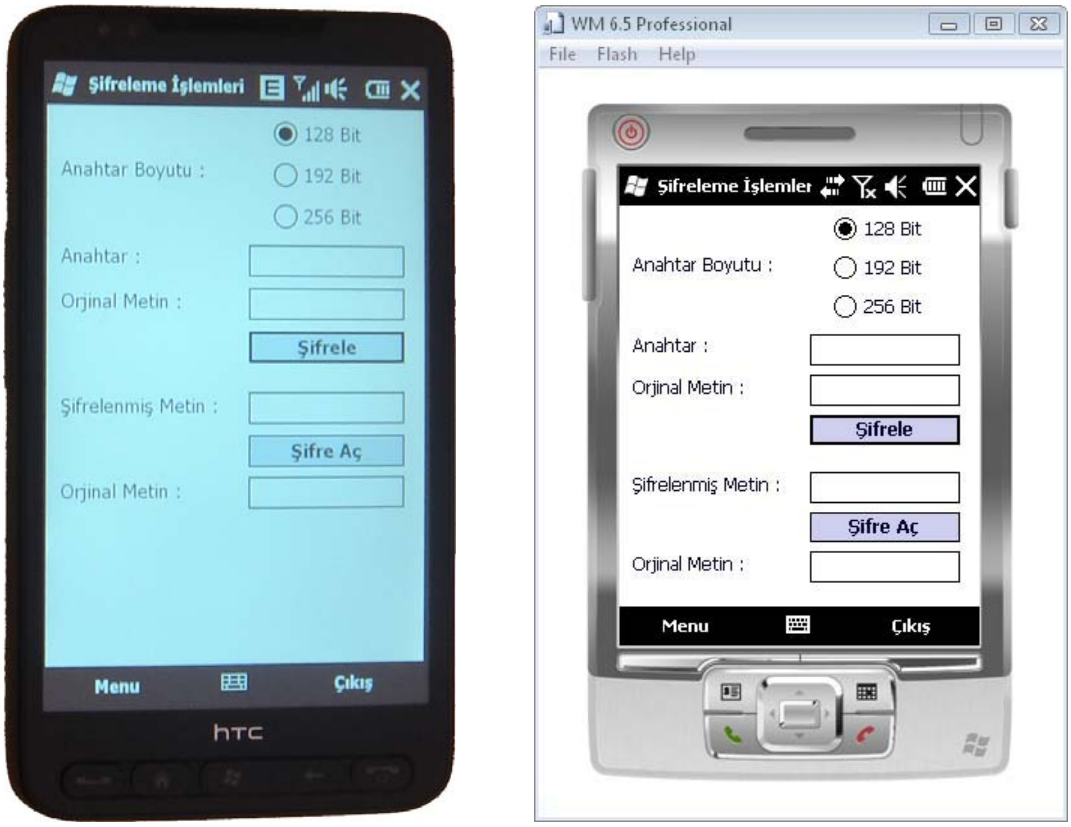
Ana menü ekranı programda ilk çalışan ekrandır. Menü bölümünden gerçekleştirmek istediğimiz seçeneğe ulaşırız. Buradaki menüde Şifreleme, Veri Kaydet ve Veri Al – Çıkış menü öğeleri bulunmaktadır. Ana menü ekranı Şekil 3.19.'da gösterilmiştir.



Şekil 3. 19. Ana menü ekranının PDA'da ve emülatörde gösterimi

3.5.2. Şifreleme ekranı

Bu ekran AES şifreleme algoritmasının PDA'da belirtilen bir anahtar ile şifreleme ve şifre çözme işleminin yapıldığı ekrandır. Anahtar boyutunu seçerek, seçilen boyuta uygun anahtarı ve şifrelenecek metni ilgili metin kutularına yazarak şifrele butonuna tıklanır. Şifrelenmiş metin, ilgili metin kutusunda gösterilir. Şifre çözme işleminde de şifrelenmiş metin aynı anahtar girilince şifre aç butonu ile şifresi çözülerek ilgili metin kutusunda gösterilir. Eğer kullanıcı anahtarı farklı girer ise şifre çözme işlemi gerçekleşir. Fakat doğru metne ulaşılmamış olur. Şifreleme ekranı Şekil 3.20.'de gösterilmektedir.

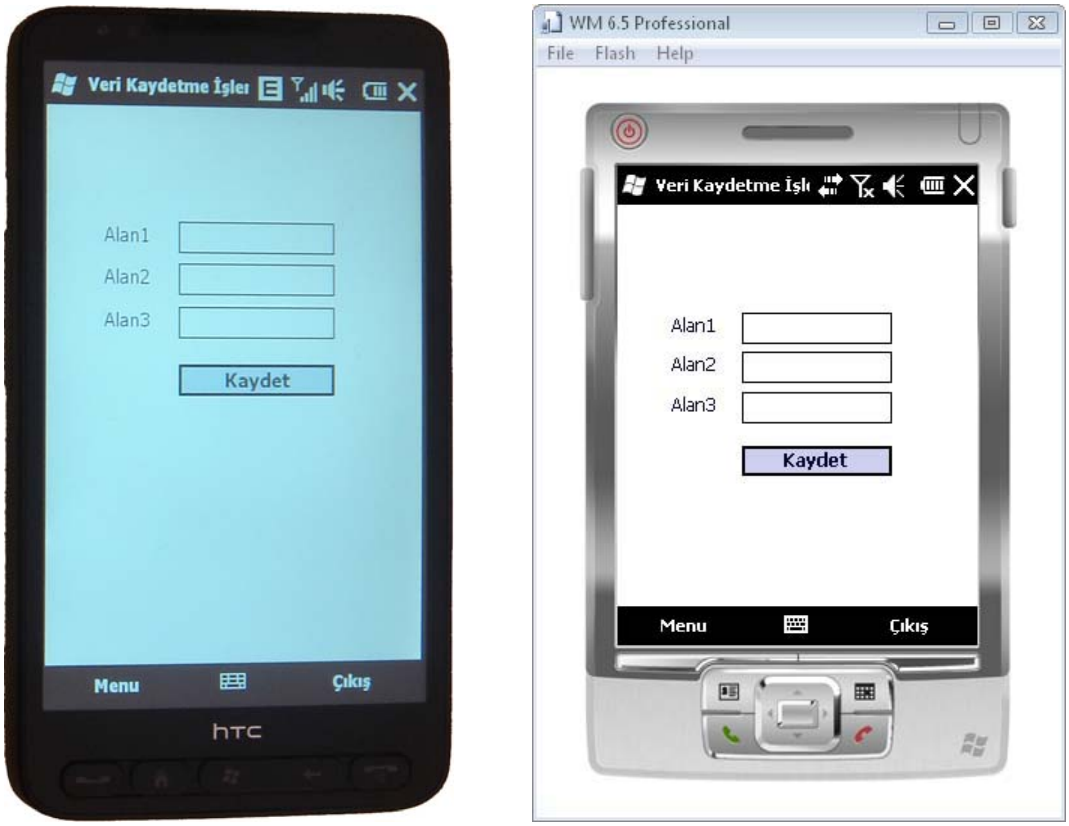


Şekil 3. 20. Şifreleme ekranının PDA'da ve emülatörde gösterimi

3.5.3. Veri kaydetme ekranı

Şekil 3.21.de' gösterilen veri kaydetme ekranında; internet üzerinde bulunan SQL Server veri tabanı sunucusundaki veri tabanına, web sunucu üzerinde yayınlanan web servisteki veri kaydet web metodu kullanılarak PDA ile internet üzerinden veri kaydetme işlemi yapılır.

Bu işlemde veri tabanındaki bir tablonun 3 alanına veri kaydedilir. Formda bulunan 3 alan doldurulup kaydet butonuna tıklanır. Sonra veriler şifrelenerek web servisteki veri kaydet web metodu aracılığı ile şifreli veriler, şifreleri çözülerek veri tabanına kaydedilir. PDA'da kayıt işlemi başarılı bir şekilde gerçekleştirilmiştir mesajı verilir. Bu işlemde şifrelenmiş veriler XML biçiminde internet üzerinden sunucuya ulaşmıştır ve web servis ile şifreleri çözülerek veri tabanına kaydedilmiştir.

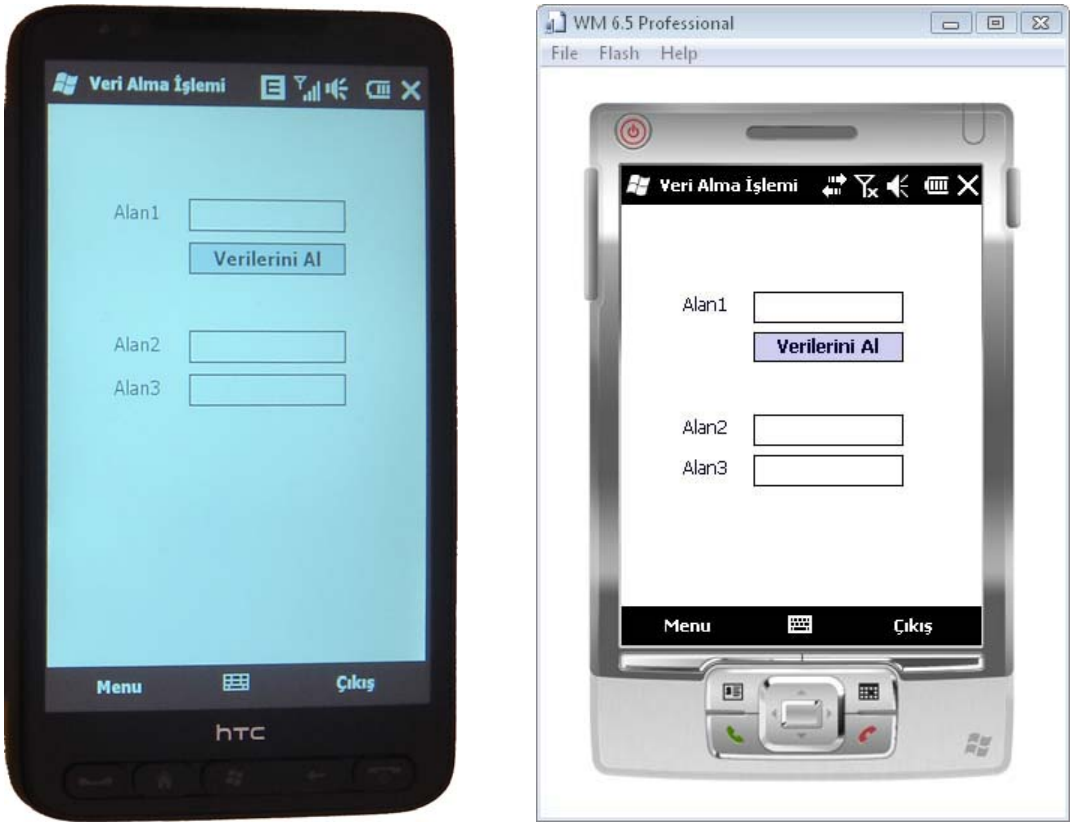


Şekil 3. 21. Veri Kaydet ekranının PDA'da ve emülatörde gösterimi

3.5.4. Veri alma ekranı

Şekil 3.22.'de gösterilen veri alma ekranında internet üzerindeki SQL server veri tabanından uygun sorgulama ile elde edilen veriler PDA'ya getirilir.

Bu işlemde veri tabanında 3 alanı bulunan tablodaki verilerden sorgulama yapılır. Formda bulunan alan1 metin kutusuna veri tabanındaki tablodan istenen verinin alan1 değeri yazılır ve veri al butonu tıklanır. Metin kutusuna yazılan bu değer şifrelenerek web servisteki veri al web metodu ile şifresi açılarak tablodan gerekli sorgulama yapılır ve sorgulama sonucunda elde edilen veriler şifrelenerek PDA'ya iletilir. Gelen verilerin şifreleri PDA'da açılarak ilgili metin kutularına aktarılır ve kullanıcıya veriler başarılı bir şekilde alınmıştır mesajı verilir. Bu işlemde veriler veri tabanına gönderilirken ve veriler alınırken ortamda şifrelenmiş olarak XML biçiminde ilerlemektedir.



Şekil 3. 22. Veri Alma ekranının PDA'da ve emülatörde gösterimi

4. SONUÇ VE ÖNERİLER

Güvenli iletişimi sağlamak için bir AES uygulaması ile şifreleme sistemi geliştirilmiştir. Bu uygulama geliştirilirken gelişen teknolojiyle hayatımızda geniş bir kullanım alanına sahip olan mobil cihazlardan PDA tercih edilmiştir. PDA'da uygulanarak anlatılan bu şifreleme sistemindeki veri güvenliği ise AES şifreleme algoritması ile yapılmıştır.

AES şifreleme algoritması şifreleme alanında önemli bir yere sahiptir. AES güvenilirliği NIST tarafından kabul edilmiş bir standarttır. AES' in kullanımı oldukça yaygındır.

AES şifreleme algoritması hızlı ve güvenlidir. Yapısal olarak AES bir blok şifreleme algoritmasıdır. Bu tez çalışmasında AES şifreleme algoritması; algoritmada kullanılan matematiksel işlemler, anahtar uzunlukları, tur sayısı, her bir turda yapılan işlemler, şifreleme anahtarı oluştururken kullanılan algoritma, şifreleme ve şifre çözme özellikleri anlatılmıştır.

PDA'larda güvenli iletişim için AES şifreleme algoritması ile geliştirilen uygulamanın kullanımı adım adım anlatılmıştır. Bu uygulama bir XML Web Servisi ve Windows Mobile 6.5 Professional projesinden oluşmaktadır. Veriler PDA'dan şifrelenerek XML Web Servis sayesinde XML biçiminde ortamda ilerledikten sonra şifreleri çözülerek SQL Server veri tabanına kaydedilmektedir. Veri alırken de veriler ortamda yine şifrelenmiş ve XML biçiminde ilerlemektedir.

Şifreleme anahtarı ise mobil uygulamasının içerisinde ve web serviste de bir dll dosyasında bulunmakta olup anahtar ortamda bulunmamaktadır. Bu sayede ortamda veriler ele geçirilse dahi doğru şifreleme anahtarını bilmeyenler tarafından düz metin elde edilemez. Bu sebeple veriler sadece şifreleme anahtarını bilenler tarafından anlamlı hale gelmektedir. Bu çalışmada ortamda ilerleyen verilerin istenmeyen kişiler tarafından anlamlı hale getirilmesi zorlaştırılmıştır. Ancak verilerin değiştirilmesi, silinmesi ve kopyalanması ile ilgili bir işlem yapılmamıştır.

XML web servisi kullanılarak platform bağımsızlığı sağlanmıştır. Böylece istenilen veri tabanı sunucusuna erişim sağlanabilir ve herhangi bir mobil cihaz ile bu uygulama kullanılabilir. Bu uygulamada SQL server veri tabanı kullanılmıştır. Arzu edildiği takdirde diğer veri tabanı sunucuları kolaylıkla kullanılabilir.

Web servise erişebilen istenmeyen kurum, kuruluş ve şahıslar veri tabanı sunucusuna erişebilir. Bundan dolayı XML web servisin de güvenliği sağlanmalıdır. PDA için geliştirilen uygulamada kullanıcı yetkilendirme işlemleri yapılmalıdır.

Bu çalışmada geliştirilen uygulamada metin şifreleme üzerinde durulmuştur. Uygulamamız geliştirilerek ses, resim ve video şifrelemek için de kullanılabilinir. Bu sayede özellikle mobil cihazlar için internet destekli şifreli sesli görüşme ve şifreli görüntülü görüşme uygulamaları geliştirilebilir.

KAYNAKLAR

1. İnternet : Kamu Sertifikasyon Merkezi Kurumu "Kriptoloji" http://www.kamusm.gov.tr/tr/bilgideposu/belgeler/temelkavramlar.jsp (2010).

2. Stallings W., "Cryptography and Network Security: Principles and Practice", ***Prentice Hall,*** USA, 29-31, 62-173 (2005).

3. Bunchmann, J. A., "Introduction to Cryptography", S. Axler, F.W. Gehring, K.A. Ribet, ***Springer – Verlag***, New York, 71-72 (2002).

4. Mogollon, M., "Cryptography and Security Services Mechanisms and Applications", K. Klinger, J. Neidig, S. Reed, K. M. Roth, M. Stocking, E. Meyer, ***Cybertech Publishing***, New York, 54-90 (2007).

5. Joux, A., "Algorithmic Cryptanalysis", D. R. Stinson, ***CRC Pres***, New York, 157-158 (2009).

6. Daemen, J., Rijmen, V., "The Design of Rijndael - AES - The Advanced Encryption Standard", ***Springer – Verlag***, Germany 1-8, 30-33 (2002).

7. Başkök, M. D., "AES şifreleme algoritmasının modellenmesi", Yüksek Lisans Tezi, ***Gazi Üniveristesi Fen Bilimleri Enstitüsü***, Ankara, 72-75 (2007).

8. Kayış, H., "AES Uygulamasının FPGA Gerçeklemelerine Karşı Güç Analizi Saldırısı", Yüksek Lisans Tezi, ***İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü,*** İstanbul, 10-32 (2006).

9. Yerlikaya, T., "Yeni şifreleme algoritmalarının analizi", Doktora Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, 89-97 (2006).

10. "Advanced Encryption Standard", ***Federal Information Processing Standard FIPS***, Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington DC, 1-33 (2001).

11. Daemen, J., Rijmen, V., "AES Proposal: Rijndael", ***First Advanced Encryption Conference***, Ventura, 1-37 (1998).

12. MOLLIN, R. A., "An Introduction to Cryptography Second Edition", ROSEN, K. H., ***Chapman & Hall/CRC***, the USA, 130-157 (2007).

13. Denis, T., S., "Cryptography for Developers", Heffernan, E., Johnson, S., ***Syngress Publishing*****,** 138-200 (2007).

14. Jorgensen, D., "Developing .NET Web Services with XML", Rebello, A., Nolan, C. B., ***Syngress***, The USA, 1-207 (2002).

15. 15. Yao, P., Durant, D., “Programming .NET Compact Framework 3.5”, ***Addison-Wesley***, The USA, 318-330 (2009).

16. Thai, T. L., Lam, H., “.NET Framework Essentials”, ***O'Reilly***, The USA, 5-160 (2002).

17. Dawes, A., “Windows Mobile Game Development”, ***Apress***, The USA, 1-24 (2010).

18. Sakallı, M. T., “Modern şifreleme yöntemlerinin gücünün incelenmesi”, Doktora Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, 49-63 (2006).

19. Williams, D. H., “PDA Robotics Using Your Personal Digital Assistant to Control Your Robot”, ***McGraw-Hill***, New York, 1-4 (2003).

20. Milroy, S., Cox, K., Safford, D., Barker, L., Kalani, A. and Lee, W. M., “. N ET Mobile Web Developer’s Guide”, ***Syngress***, The USA, 1-97, 173-204 (2002).

EKLER

EK-1. 128 Bitlik anahtar üreteci işlemleri

Şifreleme Anahtarı = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

$N_k = 4$ için anahtar üreteci adımları [10]:

w0 = 2b7e1516 w1 = 28aed2a6 w2 = abf71588 w3 = 09cf4f3c

i (dec)	temp	RotWord() İşleminden Sonra	SubWord() İşleminden Sonra	Rcon[i/Nk]	Rcon ile XOR İşleminden Sonra	w[i–Nk]	w[i]= temp XOR w[i-Nk]
4	09cf4f3c	cf4f3c09	8a84eb01	01000000	8b84eb01	2b7e1516	a0fafe17
5	a0fafe17					28aed2a6	88542cb1
6	88542cb1					abf71588	23a33939
7	23a33939					09cf4f3c	2a6c7605
8	2a6c7605	6c76052a	50386be5	02000000	52386be5	a0fafe17	f2c295f2
9	f2c295f2					88542cb1	7a96b943
10	7a96b943					23a33939	5935807a
11	5935807a					2a6c7605	7359f67f
12	7359f67f	59f67f73	cb42d28f	04000000	cf42d28f	f2c295f2	3d80477d
13	3d80477d					7a96b943	4716fe3e
14	4716fe3e					5935807a	1e237e44
15	1e237e44					7359f67f	6d7a883b
16	6d7a883b	7a883b6d	dac4e23c	08000000	d2c4e23c	3d80477d	ef44a541
17	ef44a541					4716fe3e	a8525b7f
18	a8525b7f					1e237e44	b671253b
19	b671253b					6d7a883b	db0bad00
20	db0bad00	0bad00db	2b9563b9	10000000	3b9563b9	ef44a541	d4d1c6f8
21	d4d1c6f8					a8525b7f	7c839d87
22	7c839d87					b671253b	caf2b8bc
23	caf2b8bc					db0bad00	11f915bc
24	11f915bc	f915bc11	99596582	20000000	b9596582	d4d1c6f8	6d88a37a
25	6d88a37a					7c839d87	110b3efd
26	110b3efd					caf2b8bc	dbf98641
27	dbf98641					11f915bc	ca0093fd
28	ca0093fd	0093fdca	63dc5474	40000000	23dc5474	6d88a37a	4e54f70e
29	4e54f70e					110b3efd	5f5fc9f3
30	5f5fc9f3					dbf98641	84a64fb2
31	84a64fb2					ca0093fd	4ea6dc4f

EK-1 (Devam). 128 Bitlik anahtar üreteci işlemleri

32	4ea6dc4f	a6dc4f4e	2486842f	80000000	a486842f	4e54f70e	ead27321
33	ead27321					5f5fc9f3	b58dbad2
34	b58dbad2					84a64fb2	312bf560
35	312bf560					4ea6dc4f	7f8d292f
36	7f8d292f	8d292f7f	5da515d2	1b000000	46a515d2	ead27321	ac7766f3
37	ac7766f3					b58dbad2	19fadc21
38	19fadc21					312bf560	28d12941
39	28d12941					7f8d292f	575c006e
40	575c006e	5c006e57	4a639f5b	36000000	7c639f5b	ac7766f3	d014f9a8
41	d014f9a8					19fadc21	c9ee2589
42	c9ee2589					28d12941	e13f0cc8
43	e13f0cc8					575c006e	b6630ca6

EK-2. 192 Bitlik anahtar üreteci işlemleri

Şifreleme Anahtarı = 8e 73 b0 f7 da 0e 64 52 c8 10 f3 2b
80 90 79 e5 62 f8 ea d2 52 2c 6b 7b

$N_k = 6$ için anahtar üreteci adımları [10]:

w0 = 8e73b0f7 w1 = da0e6452 w2 = c810f32b
w3 = 809079e5 w4 = 62f8ead2 w5 = 522c6b7b

i (dec)	temp	RotWord() İşleminden Sonra	SubWord() İşleminden Sonra	Rcon[i/Nk]	Rcon ile XOR İşleminden Sonra	w[i–Nk]	w[i]= temp XOR w[i-Nk]
6	522c6b7b	2c6b7b52	717f2100	01000000	707f2100	8e73b0f7	fe0c91f7
7	fe0c91f7					da0e6452	2402f5a5
8	2402f5a5					c810f32b	ec12068e
9	ec12068e					809079e5	6c827f6b
10	6c827f6b					62f8ead2	0e7a95b9
11	0e7a95b9					522c6b7b	5c56fec2
12	5c56fec2	56fec25c	b1bb254a	02000000	b3bb254a	fe0c91f7	4db7b4bd
13	4db7b4bd					2402f5a5	69b54118
14	69b54118					ec12068e	85a74796
15	85a74796					6c827f6b	e92538fd
16	e92538fd					0e7a95b9	e75fad44
17	e75fad44					5c56fec2	bb095386
18	bb095386	095386bb	01ed44ea	04000000	05ed44ea	4db7b4bd	485af057
19	485af057					69b54118	21efb14f
20	21efb14f					85a74796	a448f6d9
21	a448f6d9					e92538fd	4d6dce24
22	4d6dce24					e75fad44	aa326360
23	aa326360					bb095386	113b30e6
24	113b30e6	3b30e611	e2048e82	08000000	ea048e82	485af057	a25e7ed5
25	a25e7ed5					21efb14f	83b1cf9a
26	83b1cf9a					a448f6d9	27f93943
27	27f93943					4d6dce24	6a94f767
28	6a94f767					aa326360	c0a69407
29	c0a69407					113b30e6	d19da4e1
30	d19da4e1	9da4e1d1	5e49f83e	10000000	4e49f83e	a25e7ed5	ec1786eb

EK-2 (Devam). 192 Bitlik anahtar üreteci işlemleri

31	ec1786eb					83b1cf9a	6fa64971
32	6fa64971					27f93943	485f7032
33	485f7032					6a94f767	22cb8755
34	22cb8755					c0a69407	e26d1352
35	e26d1352					d19da4e1	33f0b7b3
36	33f0b7b3	f0b7b333	8ca96dc3	20000000	aca96dc3	ec1786eb	40beeb28
37	40beeb28					6fa64971	2f18a259
38	2f18a259					485f7032	6747d26b
39	6747d26b					22cb8755	458c553e
40	458c553e					e26d1352	a7e1466c
41	a7e1466c					33f0b7b3	9411f1df
42	9411f1df	11f1df94	82a19e22	40000000	c2a19e22	40beeb28	821f750a
43	821f750a					2f18a259	ad07d753
44	ad07d753					6747d26b	ca400538
45	ca400538					458c553e	8fcc5006
46	8fcc5006					a7e1466c	282d166a
47	282d166a					9411f1df	bc3ce7b5
48	bc3ce7b5	3ce7b5bc	eb94d565	80000000	6b94d565	821f750a	e98ba06f
49	e98ba06f					ad07d753	448c773c
50	448c773c					ca400538	8ecc7204
51	8ecc7204					8fcc5006	01002202

EK-3. 256 Bitlik anahtar üreteci işlemleri

Şifreleme Anahtarı = 60 3d eb 10 15 ca 71 be 2b 73 ae f0 85 7d 77 81
1f 35 2c 07 3b 61 08 d7 2d 98 10 a3 09 14 df f4

$N_k = 8$ için anahtar üreteci adımları [10]:

w0 = 603deb10 w1 = 15ca71be w2 = 2b73aef0 w3 = 857d7781
w4 = 1f352c07 w5 = 3b6108d7 w6 = 2d9810a3 w7 = 0914dff4

i (dec)	**temp**	**RotWord() İşleminden Sonra**	**SubWord() İşleminden Sonra**	**Rcon[i/Nk]**	**Rcon ile XOR İşleminden Sonra**	**w[i–Nk]**	**w[i]= temp XOR w[i-Nk]**
8	0914dff4	14dff409	fa9ebf01	01000000	fb9ebf01	603deb10	9ba35411
9	9ba35411					15ca71be	8e6925af
10	8e6925af					2b73aef0	a51a8b5f
11	a51a8b5f					857d7781	2067fcde
12	2067fcde		b785b01d			1f352c07	a8b09c1a
13	a8b09c1a					3b6108d7	93d194cd
14	93d194cd					2d9810a3	be49846e
15	be49846e					0914dff4	b75d5b9a
16	b75d5b9a	5d5b9ab7	4c39b8a9	02000000	4e39b8a9	9ba35411	d59aecb8
17	d59aecb8					8e6925af	5bf3c917
18	5bf3c917					a51a8b5f	fee94248
19	fee94248					2067fcde	de8ebe96
20	de8ebe96		1d19ae90			a8b09c1a	b5a9328a
21	b5a9328a					93d194cd	2678a647
22	2678a647					be49846e	98312229
23	98312229					b75d5b9a	2f6c79b3
24	2f6c79b3	6c79b32f	50b66d15	04000000	54b66d15	d59aecb8	812c81ad
25	812c81ad					5bf3c917	dadf48ba
26	dadf48ba					fee94248	24360af2
27	24360af2					de8ebe96	fab8b464
28	fab8b464		2d6c8d43			b5a9328a	98c5bfc9
29	98c5bfc9					2678a647	bebd198e
30	bebd198e					98312229	268c3ba7
31	268c3ba7					2f6c79b3	09e04214

EK-3 (Devam). 256 Bitlik anahtar üreteci işlemleri

32	09e04214	e0421409	e12cfa01	08000000	e92cfa01	812c81ad	68007bac
33	68007bac					dadf48ba	b2df3316
34	b2df3316					24360af2	96e939e4
35	96e939e4					fab8b464	6c518d80
36	6c518d80		50d15dcd			98c5bfc9	c814e204
37	c814e204					bebd198e	76a9fb8a
38	76a9fb8a					268c3ba7	5025c02d
39	5025c02d					09e04214	59c58239
40	59c58239	c5823959	a61312cb	10000000	b61312cb	68007bac	de136967
41	de136967					b2df3316	6ccc5a71
42	6ccc5a71					96e939e4	fa256395
43	fa256395					6c518d80	9674ee15
44	9674ee15		90922859			c814e204	5886ca5d
45	5886ca5d					76a9fb8a	2e2f31d7
46	2e2f31d7					5025c02d	7e0af1fa
47	7e0af1fa					59c58239	27cf73c3
48	27cf73c3	cf73c327	8a8f2ecc	20000000	aa8f2ecc	de136967	749c47ab
49	749c47ab					6ccc5a71	18501dda
50	18501dda					fa256395	e2757e4f
51	e2757e4f					9674ee15	7401905a
52	7401905a		927c60be			5886ca5d	cafaaae3
53	cafaaae3					2e2f31d7	e4d59b34
54	e4d59b34					7e0af1fa	9adf6ace
55	9adf6ace					27cf73c3	bd10190d
56	bd10190d	10190dbd	cad4d77a	40000000	8ad4d77a	749c47ab	fe4890d1
57	fe4890d1					18501dda	e6188d0b
58	e6188d0b					e2757e4f	046df344
59	046df344					7401905a	706c631e

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : AKSOY, Ahmet

Uyruğu : T.C.

Doğum tarihi ve yeri : 1983 Yozgat

Medeni hali : Evli

e-mail : ahmetaksoy2001@hotmail.com.

Eğitim

Derece	*Eğitim Birimi*	*Mezuniyet tarihi*
Lisans	Gazi Üniversitesi/BÖTE	2007
Önlisans	GOP Üniversitesi/Bilgisayar Programcılığı Programı	2002

Yabancı Dil

İngilizce

Hobiler

Bilişim Teknolojileri, Yazılım, Masa Tenisi