MOBİL TELEFONLAR İÇİN POLYBIUS ALGORİTMASI İLE ŞİFRELİ MESAJLAŞMA UYGULAMASI

MEHTAP ALTUĞ

YÜKSEK LİSANS TEZİ
ELEKTRONİK BİLGİSAYAR EĞİTİMİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Ocak 2012
ANKARA

Mehtap ALTUĞ tarafından hazırlanan MOBİL TELEFONLAR İÇİN POLYBIUS ALGORİTMASI İLE ŞİFRELİ MESAJLAŞMA UYGULAMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Fecir DURAN

Tez Yöneticisi

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

Başkan : Prof. Dr. Şeref SAĞIROĞLU

Üye : Prof. Dr. Ömer Faruk BAY

Üye : Yrd. Doç. Dr. Fecir DURAN

Tarih : 05 / 01 / 2012

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.

Mehtap ALTUĞ

MOBİL TELEFONLAR İÇİN POLYBIUS ALGORİTMASI İLE ŞİFRELİ MESAJLAŞMA UYGULAMASI

(Yüksek Lisans Tezi)

Mehtap ALTUĞ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2012

ÖZET

Cep telefonu kullanımının giderek yaygınlaşması hem bireysel iletişimin hem de e-bankacılık, e-ticaret, e-eğitim gibi hizmetlerin mobil ortamda artarak kullanılmasını sağlamaktadır. Bu kullanım sıklığı IMEI klonlama, spam yazılımlarla mesajların başka bir telefona yönlendirilmesi, yasal ve yasal olmayan dinlemeler gibi güvenlik açıklarını da beraberinde getirmektedir. Güvenlik açıklarını azaltabilmek amacıyla bu tez çalışmasında, cep telefonlarında mesaj yoluyla gerçekleştirilen işlemler ve iletişim için AltugSec adı verilen şifreli mesajlaşma uygulaması geliştirilmiştir. Şifreleme işlemi için asimetrik algoritmalara göre daha hızlı olan ve hafızada daha az yere gereksinim duyan simetrik şifreleme algoritmalarından Polybius algoritması kullanılmıştır. Ayrıca güvenlik seviyesini yükseltmek amacıyla uygulamaya kullanıcı tarafından belirlenen anahtar bilgisi eklenmiştir.

Bilim Kodu : **702.1.014**
Anahtar Kelime : **mobil cep telefonları, mobil programlama, şifreleme, polybius algoritması**
Sayfa Adedi : **77**
Tez Yöneticisi : **Yrd. Doç. Dr. Fecir DURAN**

AN ENCRYPTED MESSAGING APPLICATION FOR MOBİLE PHONES WITH POLYBIUS ALGORITHM

(M. Sc. Thesis)

Mehtap ALTUĞ

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

January 2012

ABSTRACT

The increasing prevalence of mobile phone usage provides the services in mobile environment increasingly such as both individual communications as well as e-banking, e-commerce, e-learning. This sort of frequency of use cause security vulnerabilities such as cloning of IMEI, directing the messages into to another phone by spam software, recording conversations legally or illegally. In this thesis, in order to minimize security vulnerabilities, an encrypted messaging application has been developed which is called AltugSec for the communication and transactions carried out via SMS on mobile phones. For the encryption process, the Polybius algorithms, a part of the symmetric encryption algorithm used which is faster than asymmetric algorithms that require less space and more memory. In addition, in order to increase the security level, a key information was added to the application which is indicated by the user.

Science Code : **702.1.014**
Key Words : **mobile cell phones, mobile programming, encryption, polybius algorithm**
Page Number : **77**
Adviser : **Assist. Prof. Dr. Fecir DURAN**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Sayın Yrd. Doç. Dr. Fecir DURAN'a, çalışmalarım boyunca desteğini esirgemeyen değerli arkadaşlarım Sayın Özkan ÜNSAL, Sayın Namık Kemal KARASU ve ablam Sayın Akın ALTUĞ ÖZBODUROĞLU'na ve manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Kısaltmalar	Açıklama
AES	Gelişmiş Şifreleme Standardı
APN	Erişim Noktası Adı
ATM	Eş Zamansız Aktarım Modu
AUC	Kimlik Doğrulama Merkezi
BSS	Baz İstasyonu Alt Sistemi
CPU	Merkezi İşlem Birimi
DES	Veri Şifreleme Standardı
DSA	Dijital İmza Algoritması
E-KİMLİK	Elektronik Kimlik
E-ÖDEME	Elektronik Ödeme
E-İMZA	Elektronik İmza
E-ÇEK	Elektronik Çek
E-POSTA	Elektronik Posta
GPS	Küresel Konumlama Sistemi
GSM	Mobil İletişim İçin Küresel Sistem
HLR	Merkez Konum Kaydı
IDEA	Uluslararası Veri Şifreleme Algoritması
IMEI	Uluslar Arası Mobil İstasyon Cihaz Kimliği
IMSI	Uluslar Arası Mobil Abone Kimliği
IRDA	Kızılötesi
LAI	Konum Alanı Belirteci
MMS	Çoğul Ortam Servisleri
MS	Mobil İstasyon
MSC	Mobil Anahtarlama Merkezi
NSS	Ağ İstasyonu Alt Sistemi
PC	Kişisel Bilgisayar
PGP	Oldukça İyi Gizlilik
PIN	Kişisel Kimlik Numarasi

Kısaltmalar	Açıklama
POS	Satış Noktası
RAND	Rastgele
RC4	Rivest Şifreleme Versiyonu 4
RC5	Rivest Şifreleme Versiyonu 5
RFID	Radio Frekansı Tanımlama
RSA	Rivest Shamir Adleman
SET	Güvenli Elektronik İşlemi
SIM	Abone Kimlik Modülü
SMS	Kısa Mesaj Servisi
SMSC	Kısa Mesaj Servis Merkezi
SRES	İmzalı Yanıt
SSL	Güvenli Yuva Katmanı
TMSI	Geçici Mobil Abone Kimlik
VLR	Ziyaretçi Konum Kaydı
WAP	Geniş Alan Koruma
1G	1. Nesil
2G	2. Nesil
3G	3. Nesil
4G	4. Nesil
3DES	Üçlü Veri Şifreleme Standardı

1.GİRİŞ

Telefon XIX. yüzyılda ortaya çıkmış, hızlı bir gelişim geçirerek günümüzde iletişim sektörünün en önemli araçlarından biri olmuştur. Cep telefonu kişisel ve sosyal bilgiler sağlayan multimedya dijital bir platformdur [1]. Mobil iletişim sektöründeki hızlı ilerleme sayesinde sektörde faaliyet gösteren şirketlerin sayısında artış ortaya çıkmıştır.

Cep telefonunun bireylerin günlük hayatlarına girişi Avrupa ülkelerinde 1990'ların başına rastlamaktadır [2]. Cep telefonu teknolojisinin Türkiye ile tanışması 1994 yılında gerçekleşmiştir ve cep telefonu kullanıcı sayısı hızlı bir artış göstermiştir [3]. Türkiye'deki hanelerin % 50,2'si cep telefonu teknolojisinden yararlanmaktadır [4].

Ülkemizde cep telefonu kullanım oranının oldukça yüksek olması bireysel iletişim dışında e-bankacılık, e-ticaret, e-eğitim, e-sağlık gibi hizmetlerinde mobil ortamda yaygınlaşmasını sağlamaktadır. İnsanların zaman ve mekan kısıtlaması olmadan bu hizmetlere erişebilmesi, GSM (Global System for Mobile Communication) kullanım oranlarını ve kullanım alanlarını hızla arttırmaya devam edecektir.

Cep telefonlarına olan ilginin yüksek olması, bu alandaki teknolojinin de hızla gelişmesine neden olmaktadır. Günümüzde bilgisayarlara gitgide daha fazla benzeyen akıllı cep telefonları denilen bu cihazların çeşidi ile beraber kullanım oranları da artmaktadır. Bu artış ile beraber sayısal ortamda karşılaşılan güvenlik problemleri mobil dünyada da kendini göstermeye başlamıştır. Bu gelişmeler doğrultusunda, mobil cihazlarda güvenliğin sağlanması ve yeni güvenlik önlemleri alınması gerekmektedir.

Bankacılık işlemlerinde en çok kullanılan kanallardan biri ya da tamamlayıcısı olan kısa mesaj servisi güvenliğin gerekli olduğu en önemli alanlardan biridir. Mobil bankacılığın en basit ve en kolay uygulanabilir biçimi müşterilerin telefon ile arama yapmaları ya da yazılı mesaj göndermeleridir. Mobil aygıtlar bankacılık işlemlerinde kullanılırken sistem güvenliği açısından çeşitli tehlike ve saldırılara maruz

kalabilmektedir. Ayrıca kullanıcıların kişisel bilgilerini bulundurdukları cep telefonları kolay çalınabilmekte ve kaybedilebilmektedir.

Cep telefonlarının yaygın kullanımları göz önüne alınarak bir telefonun gerçek kullanımını rapor etmek ve mobil cep telefonu programı kullanımını keşfetmek amaçlı yapılan bir çalışmada, bir denek grubuna cep telefonu kullanım anketi uygulanmıştır. Anketin sonuçlarına göre; cep telefonları ile ilgili mevcut gizlilik endişelerinin olduğu tespit edilmiştir. Yapılan bir başka çalışmada, 1996 yılında Kuzey Amerika'da cep telefonu dolandırıcılığının büyük bir gelir kaybına neden olduğu, bu nedenle cep telefonunda kimlik doğrulama, güvenlik ve gizliliğin önemli konular olduğu vurgulanmaktadır. Yapılan araştırmalar, cep telefonlarında bilgi güvenliğinin önemini ve bilgi gizliliğine duyulan ihtiyacı desteklemektedir [5].

Bilgi güvenliği, elektronik ortamlarda bilgilerin saklanması ve taşınması esnasında izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür [6]. Bilgi güvenliği; başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin ortadan kaldırılması ile sağlanmaktadır. Bilgi güvenliği konusunda zafiyetlerle karşılaşılmaması için, bazı önlemler alınması gereklidir. Ancak, tüm önlemler alınmış dahi olsa, sürekli gelişen saldırı teknikleri yüzünden sistemlerin %100 güvenli olduğu düşünülmemelidir [7].

Bilgi güvenliği sağlamada kullanılan temel araç kriptografidir. Kriptografi bilgi güvenliğini inceleyen ve anlaşılabileni anlaşılamaz yapan bir bilim dalıdır. Gizlilik, güvenilirlik, veri bütünlüğü, kimlik doğrulama, özgünlük ve inkâr edilemezlik gibi konular kriptografinin önemli çalışma alanlarıdır [5].

Cep telefonlarının yaygın kullanımı ve bireysel iletişim dışında pek çok amaç için kullanılması güvenlik açıklarını da beraberinde getirmektedir. IMEI klonlama, yasal ve yasal olmayan dinlemeler, spam yazılımlarla mesajların başka bir telefona yönlendirilmesi başlıca güvenlik açıkları arasında sayılabilir [8].

Bu güvenlik açıklarının önüne geçilebilmesi için kriptolu telefonlar geliştirilmiştir. Almanya'da Deutche tarafından tasarlanmış ve Türkiye'ye ithal edilmiş, piyasaya sunulmuş olan ilk kriptolu telefon Enigma T301TR'dir. Bu telefon en gelişmiş şifreleme teknolojisini kullanarak standart GSM şebekelerinde sesli iletişim için güçlü uçtan uca şifreleme sağlayan telefondur [9].

ASELSAN ve Teknomobil Uydu Haberleşme A.Ş. tarafından ise Türkiye'nin ilk yüzde yüz yerli kriptolu haberleşme cihazı geliştirilmiştir. 2110 MEMK adı verilen cep telefonu yasa dışı dinlenme ihtimalini ortadan kaldırmaktadır. Bu telefonla dünyanın her yerinde, uydu üzerinden güvenli haberleşme yapmak mümkündür [10].

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), tamamen özgün ve milli bir yazılımla kripto özellikli cep telefonu geliştirmiştir. Yeni teknoloji, özellikle milli gizlilik içeren bilgilerin cep telefonları aracılığıyla güvenli paylaşılmasına olanak tanımaktadır.

Bunlara ek olarak Nokia tarafından geliştirilmiş ve kullanıcılarına ücretsiz olarak sunduğu Mobile Cipher 1.0.3 adında mobil şifreleme uygulaması bulunmaktadır [11].

Gerçekleştirilen bu tez çalışmasında en önemli iletişim aracı olan cep telefonları arasında, mesajlaşma gerçekleşirken güvenliği sağlamak amacıyla mesajların şifreli olarak gönderilip alınması sağlanmaktadır. Bu şekilde mesajlaşma gerçekleştiğinde önemli bir mesaj sadece gönderici ve alıcı tarafından okunabilecek, bilgi gizliliğinin ihlali ortadan kaldırılmış olacaktır. Geliştirilen program kısıtlı hafıza 856K, RAM 748K ve işlemci hızına 201MHz sahip mobil telefonlarda da çalışabilmektedir. Açık mesajı hızlı bir şekilde 0.01sn şifreleyerek anlaşılamaz mesaj haline getirmektedir. Açık mesaj 256 karakterden fazla ve RAM 1MB'ın altında olduğu durumda bile şifreleme işlemi başarılı bir şekilde gerçekleşmektedir.

Tez beş bölümden meydana gelmektedir. Giriş bölümünün devamı olarak tezin ikinci bölümünde, GSM ve cep telefonlarının genel yapısı, kullanım amaçları, kullanım

sıklığı gibi araştırmalara yer verilmektedir. Üçüncü bölümde, kriptoloji, kriptografi, kriptografide kullanılan önemli algoritmalar, şifreleme algoritmalarının performansı belirlenirken dikkat edilen kriterler, kriptoanaliz ve şifreli metine yönelik bazı saldırı çeşitleri üzerinde durulmuştur. Dördüncü bölümde, Polybius şifreleme algoritması kullanılarak gerçekleştirilen şifreli mesajlaşma uygulamasına yer verilmektedir. Sonuç ve değerlendirme bölümünde ise kullanılan şifreleme algoritmasının performansı değerlendirilmekte ve bu algoritmaya karşı yapılabilecek saldırılara karşı alınabilecek önlemlerle ilgili önerilerde bulunulmaktadır.

2. GSM VE CEP TELEFONU

Teknolojinin hızlı gelişmesi insanların haberleşme alanındaki ihtiyaçlarına yeni boyutlar kazandırmıştır. Devamlı hareket halinde olan kişilerin telefon haberleşmesinde karşılaştıkları imkansızlıklar, elektromanyetik dalgaların telekomünikasyon aracı olarak kullanılabileceği fikrini doğurmuş ve bu amaçla çalışmalar başlamıştır. Gezgin iletişim ilk olarak A.B.D.'de 1940'lı yılların sonlarında, Avrupa'da ise 1950'li yılların başlarında tek hücreli analog araç telefonları kullanılmaya başlanmıştır [12].

Ticari olarak ilk cep telefonu 1973'te yapıldı. İlk hücresel analog gezgin telefon sistemleri 1980'lerin başında kullanılmaya başlanmıştır. Bu sistemler, birinci nesil (1G) analog teknolojiyi kullanmakta olup, kullanıcıların zamanla artan ses kalitesi, kapsama alanı, kapasite gibi ihtiyaçlarına cevap vermekte yetersiz kalmıştır. Bu yetersizlik ikinci nesil (2G) sayısal teknolojinin çıkmasını zorunlu kılmıştır. Günümüzde kullanılan GSM (Global System for Mobile) standartlarındaki cep telefonları, 2G sayısal teknolojiyi kullanan sistemlere örnek olarak gösterilebilir. 2G gezgin telefonlar, ilk kez 1991'in ortalarında piyasaya sürülmüş ve kullanımı büyük bir hızla yaygınlaşmıştır [13].

GSM, başlangıçta bir Avrupa standardı olarak tasarlanmış ve çok hızlı olarak tüm dünyaya adapte edilmiştir. GSM sisteminin genel yapısı, gezgin istasyon (MS, Mobile Station-Gezgin Birim İstasyon), baz istasyonu alt sistemi (BSS-Base Station Subsystem) ve şebeke anahtarlama alt sistemi (NSS-Network Subsystem) olmak üzere yapısal olarak üç ana bileşene ayrılabilir. MS, kablosuz haberleşme için kullanılması gerekli olan cep telefonu ve SIM kartı birimlerinden oluşmaktadır. Abone kimlik doğrulama modülü olarak bilinen SIM (Subscriber Identity Module-Abone Tanımlama Modülü) kartında, şebeke tarafından tanımlanmış ve şebekeye giriş için kullanılan aboneyle ilgili bilgiler bulunmaktadır [14].

Gezgin telefon sistemleri sayesinde telefon haberleşmesinin yeri günlük hayatımızda yeni bir anlam kazanmış ve bu sistem iş ve sosyal hayatımızı değiştirmekle kalmamış, veri iletiminin de gezgin şebekeler aracılığıyla temin edilmesi ile bu sistemler hayatımızın vazgeçilmez bir öğesi haline gelmiştir [13].

Artık günümüzde bilgi işleme ve gösterme tekniklerinin kullanılarak kullanıcıyı evrensel bir bilgi ağının parçası haline getirmeyi hedefleyen sistemlere ise üçüncü nesil sistemler (3G) denilmektedir. 3G ile hız saniyede kilobit yerine megabit ile ölçülmektedir. Bu sayede televizyon yayını, canlı bağlantı gibi yüksek hıza ihtiyaç duyan uygulamalar hayata geçirilebilmektedir [15]. 3G teknolojisinden sonra ise her zaman her yerde daha hızlı ve daha kaliteli iletişim sağlayacak olan sistemler ise 4G olarak sınıflandırılmaktadır [16].

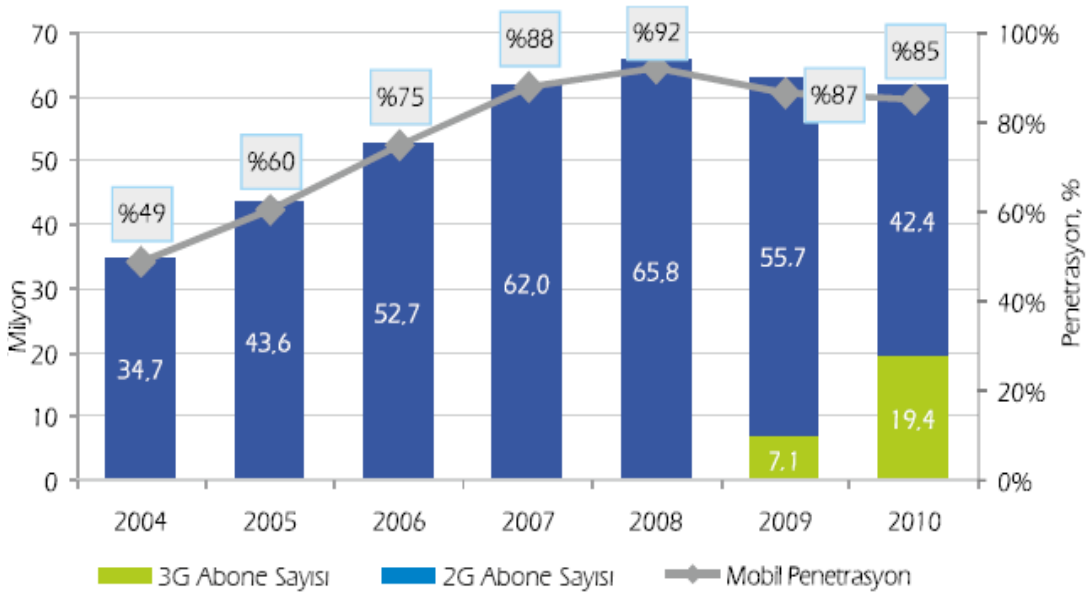
Gezgin cihazlar o kadar hızlı gelişme kaydetmişlerdir ki artık onlar üzerinde de PC'lerde olduğu gibi bir işletim sistemi kurulup çalıştırılabilmektedir. İşletim sistemleri gezgin cihazlarla kullanıcılar arasında bir ara yüz görevi görmektedir. Bunun yanında birçok görevi yerine getirmektedir. Bunlar arasında kısa film seyretme, mp3 yükleme, dinleme, birçok resim formatını görüntüleyebilme, mikro programlama dilleri ile yazılmış uygulamaları çalıştırma, görsel oyunları yükleme, oynama ve bunların dışında birçok özellik mevcuttur [17]. Gezgin cihazlara yüklü işletim sistemlerinden yaygın olarak kullanılanlar arasında Symbian OS, Windows CE/ Pocket PC, Palm OS, Pocket Linux sayılabilir [16].

2.1. Cep Telefonlarının Yıllara Göre Kullanım Sıklığı

Tüm dünyada olduğu gibi ülkemizde de mobil telekomünikasyon sektörü hızlı bir gelişme göstermektedir. Ülkemiz sadece yerli yatırımcıların değil aynı zamanda yabancı sermayenin de ilgisini çekerek önemli bir cazibe merkezi haline gelmiştir.

2010 yılı sonu itibariyle Türkiye'de yaklaşık %85 penetrasyon oranına karşılık gelen 61,8 milyon mobil abone bulunmaktadır. Şekil 2.1'de abone sayısı ve penetrasyon oranlarında yıllar itibariyle meydana gelen hızlı artış gözler önüne serilmektedir.

Bununla birlikte; 2009 yılı Temmuz ayında başlayan 3G hizmetleri ile 3G abone sayısı 2010 yılı sonu itibariyle 19 milyonu geçmiştir [18].



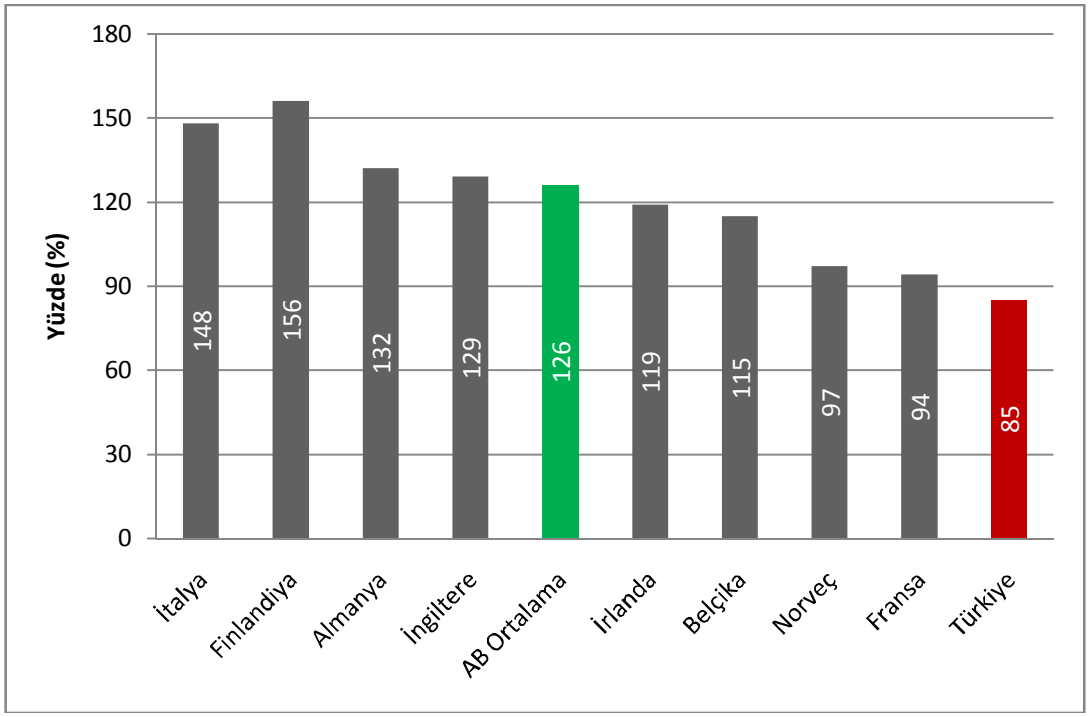
Şekil 2.1. Mobil abone sayısı ve penetrasyon oranı [18]

Çizelge2.1'de 3G hizmetlerine ilişkin veriler yer almaktadır. 2010 yılı 1. Çeyrekte 8,7 milyon olan 3G abone sayısı 2010 2. Çeyrekte 11,4 milyona ulaşırken, 3G hizmetiyle birlikte mobil internet hizmeti alan kullanıcı sayısı da 640.580'den 832.321'e yükselmiştir. Bu dönemde toplam mobil internet kullanım miktarı ise 2.568 TByte olarak gerçekleşmiştir [19].

Çizelge 2.1. 3G Hizmeti kullanıcı verileri [19]

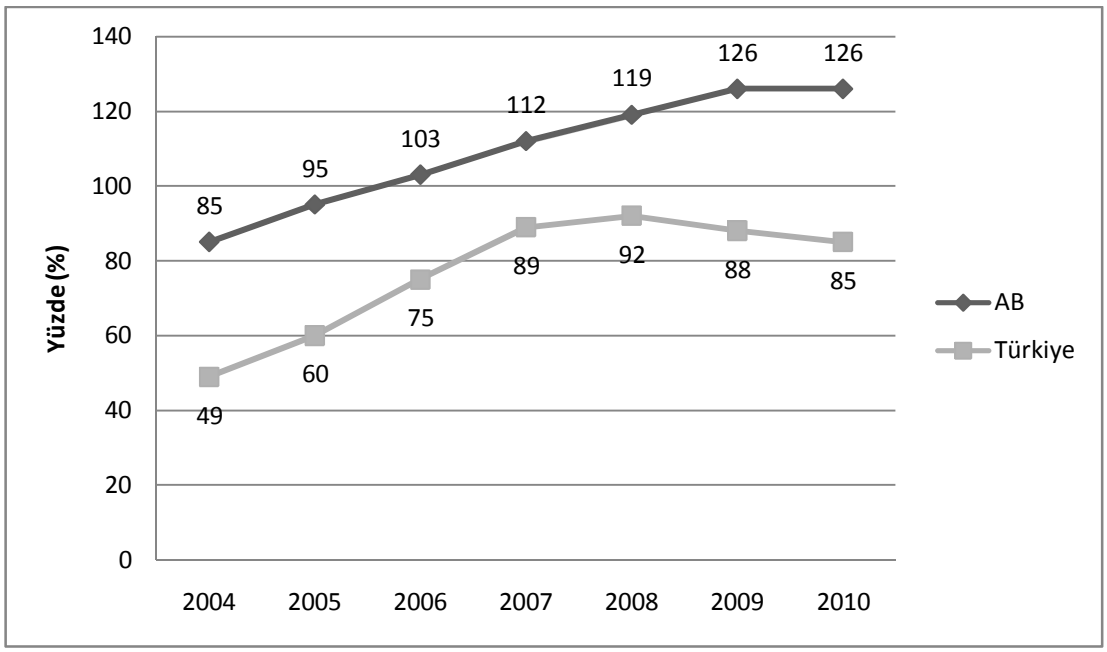
	2010 – 1. Çeyrek	**2010 – 2. Çeyrek**
3G Abone Sayısı	8.717.769	11.433.031
Mobil İnternet Kullanıcı Sayısı	640.580	832.321
Mobil İnternet Kullanım Miktarı, Gbyte	2.105.643	2.629.253

Şekil 2.2'de Türkiye ve bazı Avrupa ülkelerinde mobil penetrasyon oranları karşılaştırılmaktadır. Şekilde verilen AB ülkeleri verileri Haziran 2010, Türkiye verisi Aralık 2010'a aittir. Ekim2009 itibariyle AB ülkelerinde ortalama olarak %126 olan mobil penetrasyon oranı, Türkiye'de 2010yılı sonu itibariyle %85'dir [18].



Şekil 2.2. Türkiye ve bazı Avrupa ülkelerinin mobil penetrasyon oranları [18]

Yıllara göre mobil penetrasyondaki değişim AB ülkeleri ortalaması ve Türkiye karşılaştırması da Şekil2.3'te görülmektedir. 2004 yılından bu yana Türkiye'de mobil penetrasyon oranı AB'ye benzer şekilde artış eğilimindeyken, 2010 yılında Numara Taşınabilirliği düzenlemelerinin de etkisiyle düşüş yaşamıştır [18].



Şekil 2.3. Yıllara göre Türkiye ve AB ülkeleri mobil penetrasyon oranları [18]

2.2. Cep Telefonu ile Sağlanan Hizmetler

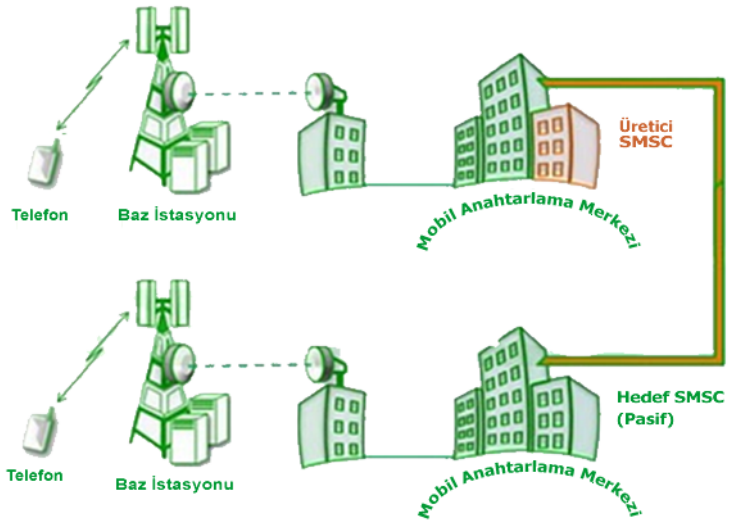
Cep telefonu ile sağlanan hizmetler, telefon modeline ve servis sağlayıcıya göre değişmekle beraber en yaygın olarak kullanılanları, sesli görüşme ve kısa mesaj hizmetidir [20]. Bunların yanı sıra, MMS göndermek, Ofis dökümanları, PDF Okumak, GPS, MP3 Player, Kamera, Veri Saklama, Wi-Fi, Kablosuz Internet, WAP, Internet APN-Kurumsal APN'ler amacıyla kullanılmaktadır [21].

2.2.1. Sesli görüşme

Sesli görüşme, cep telefonu kullanıcıları arasında karşılıklı ses verisinin taşınması yoluyla iletişim kurulması işlemidir.

2.2.2.Kısa mesaj servisi

SMS (Short Message Service-Kısa Mesaj Servisi), GSM şebekeleri üzerinden mobil telefon aracılığı ile ileti yollanması ve alınması işlemlerini kapsamaktadır. Bir SMS iletisi sayılardan ve harflerden oluşmaktadır. 160 karakter uzunluğundadır. Şekil 2.4'de görüldüğü gibi iletiler bir telefondan diğerine ulaştırılırken SMS servis merkezine (SMSC) gelir ve alıcının telefonuna yönlendirilir. Mobil telefon kullanıcısı SMS iletisi aldığında telefonunun alarmı ile uyarılır. Alıcı iletiyi okuduğunda buna cevap verebilir, saklayabilir veya başka bir telefona yönlendirebilmektedir.



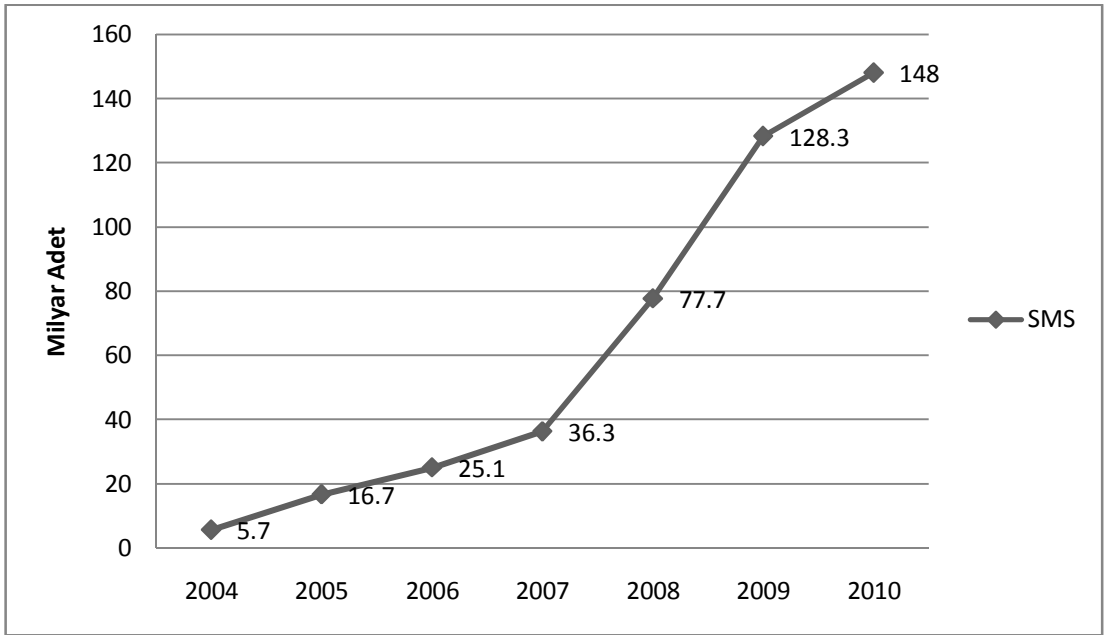
Şekil 2.4. SMS'in bir telefondan diğerine iletilmesi [22]

SMS uygulaması hızlı ve kolay bir duyuru aracıdır. Bu uygulama ile firmalar/kurumlar tüm müşterilerine, bayi ve iş ortaklarına tek bir işlem ile ulaşabilmekte; müşterilere/çalışanlara gönderecekleri SMS'ler ile doğum günü, bayram kutlamaları yapabilmekte; kampanyalar ya da yapacakları toplantı ve seminerler hakkında bilgi verebilmektedirler. Firmaların/kurumların oluşturabilecekleri şablonları kullanarak müşterilere, bayi ve iş ortaklarına toplu olarak SMS gönderilmesi ya da program içinde gerçekleştirilen bazı işlemler sonucunda otomatik olarak SMS gönderebilmektedir. Müşterilerin yanı sıra,

firma/kurum çalışanlarına da farklı amaçlarla SMS gönderilmesi sağlanabilmektedir. Ayrıca, insan kaynakları paketinde hazırlanan şablonlara göre de firma personeline SMS ile bilgilendirme yapılabilmektedir [23]. Bu gibi amaçlarla kullanılan kısa mesaj servisinin kullanım sıklığı her geçen gün artmaktadır.

Kısa mesaj servislerinin yıllara göre kullanım sıklığı

Şekil 2.5'de GSM işletmecilerinin toplam SMS sayılarındaki değişime yer verilmektedir. Gönderilen SMS sayısına bakıldığında özellikle 2008 yılındaki artış dikkat çekmektedir. Türkiye'de özellikle genç nüfus arasında yaygın olarak kullanılan SMS, GSM operatörlerinin teşvik edici kampanyaları ile hızlı bir artış yakalamıştır. 2010 yılında da benzer bir artış izlenmiş ve SMS sayısı 148 milyarı geçmiştir [18].



Şekil 2.5. Yıllara göre SMS miktarı [18]

Günlük hayatımızda sıklıkla kullanmakta olduğumuz SMS m-ticaret, mobil bankacılık olarak bilinen gelecekteki iş alanlarında çok hayati bir rol oynayacaktır. SMS'in bu gibi alanlarda kullanılması güvenilirlik endişesini ortaya çıkarmaktadır.

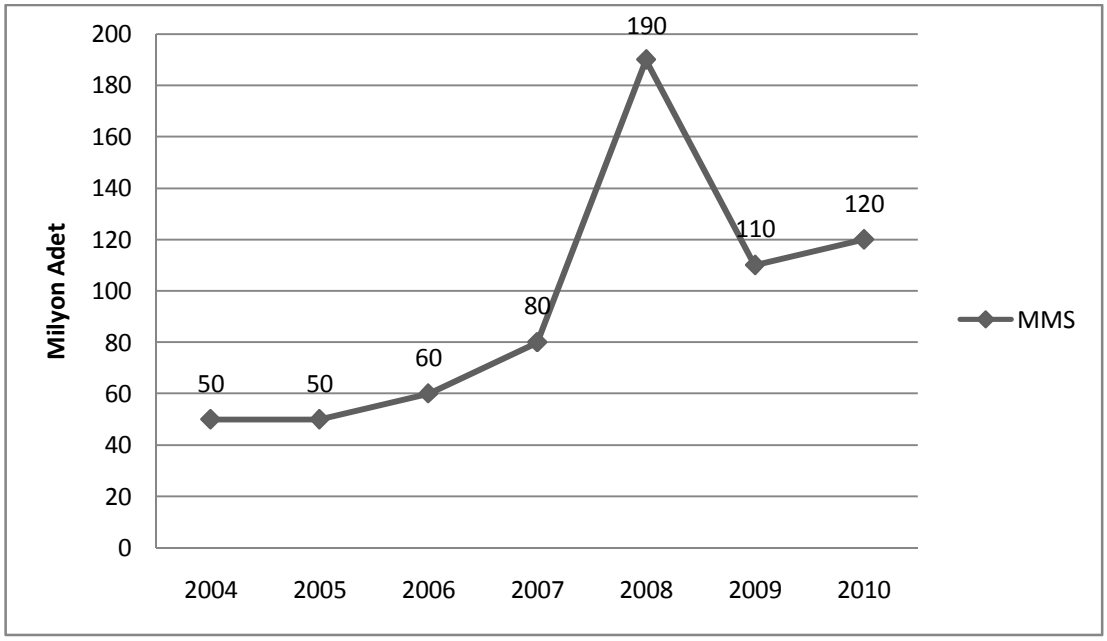
Yapılan bir çalışmada, günümüzde tam SMS güvenliği ile ilgili herhangi bir şema bulunmadığı için güvenlik şeması geliştirilmiştir. Geliştirilen bu şemada ilk olarak SMS düz metin halindedir ve daha sonra mevcut GSM şifreleme teknolojisi yardımı ile düz metin şifreli metin olarak çevrilmekte, daha sonra şifreli metin genel anahtar imza yardımı ile dijital olarak imzalanmış olmaktadır. Önerilen şema, m-ticaret veya mobil bankacılıkta ve güvenli mesajlaşmada en gerekli çıkışlar olan toplam özgünlük, veri bütünlüğü, gizlilik, yetki ve inkar edememeyi sağlayacaktır. Böylece SMS'in m-ticaret, mobil bankacılık gibi alanlarda kullanımı daha güvenli hale gelecektir [24].

2.2.3. Multimedya mesajlaşma servisi

Mobil mesaj gönderme ve almadaki en son gelişmelerden biri multimedya mesajlaşma servisi (MMS-Multimedia Message Service) olarak bilinmektedir. Geleneksel kısa mesaj servisi (SMS) gibi, multimedya mesajlaşma, kişisel mesajların otomatik ve anında teslimatını sağlamaktadır. Ancak SMS'ten farklı olarak, MMS, cep telefonu kullanıcılarının mesajlarına ses, görüntü ve diğer zengin içeriği katarak, mesajlarını kişiselleştirilmiş bir görsel ve sesli mesaj haline getirmelerine imkan vermektedir.

Multimedya kısa mesajları ancak MMS uyumlu cep telefonları veya e-mail olarak bilgisayarlardan alınabilmektedir. MMS mesajının gönderilme ücreti normal SMS mesajı gönderme ücretinden daha yüksektir. MMS olarak gönderilecek dosya ne kadar büyük olursa aktarım süresi ve ücreti de o kadar artmaktadır.

Şekil 2.6'da GSM işletmecilerinin toplam MMS sayılarındaki değişime yer verilmektedir. Gönderilen MMS sayısının henüz düşük seviyelerde olduğu görülmektedir. MMS sayısı, 2010'da yaklaşık 120 milyon olmuştur [18].



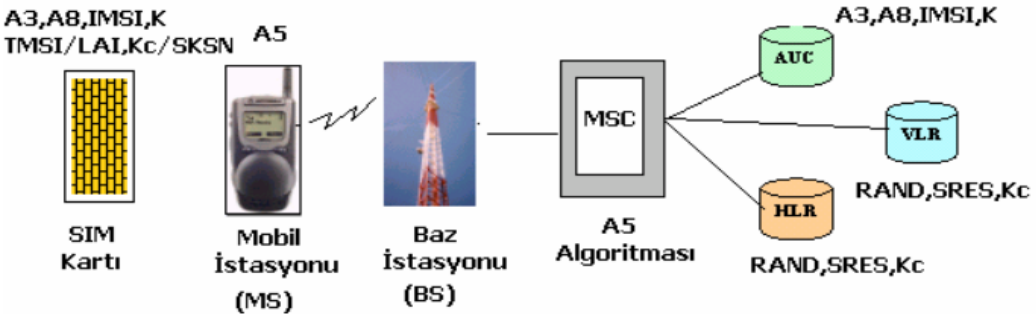
Şekil 2.6. Yıllara göre MMS miktarı [18]

2.3. Cep Telefonlarında Güvenlik

Cep telefonlarında güvenlik GSM operatörleri tarafından ve gsm güvenlik mekanizmaları tarafından sağlanabildiği gibi GSM şifreleme algoritmaları kullanılarakta sağlanabilmektedir.

2.3.1. GSM operatörleri tarafından sağlanan güvenlik hizmetleri

GSM'in güvenlik mekanizmaları üç farklı sistem elemanında gerçekleşmektedir; Abone Kimlik Modülü (SIM-Subscriber Identity Module), GSM el cihazı veya MS (Mobile Station) ve GSM ağı. SIM kartı, uluslararası mobil kullanıcı kimliği (IMSI-International Mobile Subscriber Identity), bireysel abone doğrulama anahtarı (Ki), şifreleme anahtarı üretim algoritması (A8), doğrulama algoritması (A3) ve kişisel kimlik numarası (PIN-Personal Identification Number) gibi kısımlardan oluşur.



Şekil 2.7. GSM ağında güvenlik özelliklerinin dağılımı [25]

Şekil 2.7'de güvenlik bilgisinin üç sistem arasındaki dağılımını göstermektedir; SIM, MS ve GSM ağı. GSM ağında güvenlik bilgileri doğrulama merkezi (AUC-Authentication Center), esas bölge kayıtçısı (HLR-Home LocationRegister) ve ziyaretçi bölge kayıtçısı (VLR- Visitor Location Register) arasında dağıtılır. AUC, RAND, SRES (Signed Response) ve Kc kümelerinin üretiminden sorumludur. RAND, SRES ve Kc doğrulama ve şifreleme işlemleri yerine getirmek için HLR ve VLR'de depolanırlar [26,27].

Her operatörün sağlamış olduğu ortak güvenlik hizmetleri vardır.

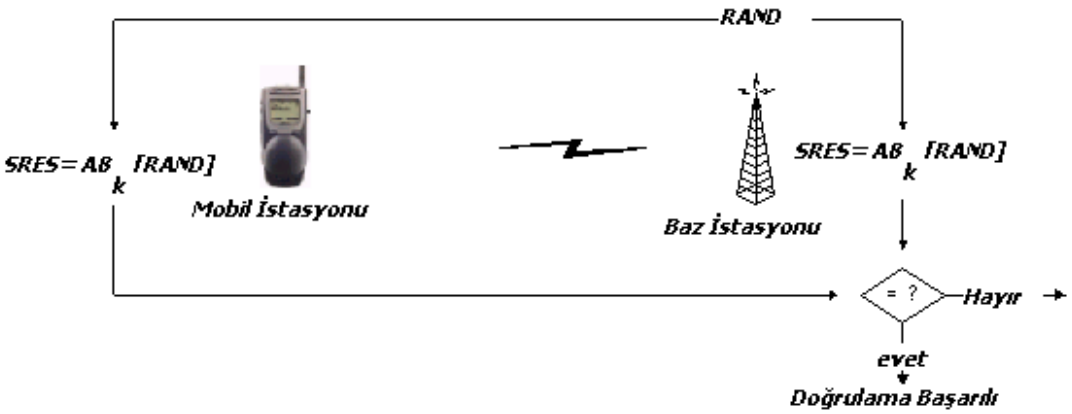
- Abone Kimlik Doğrulanması: Operatör faturalandırma amaçlı sistemi kimin kullanıyor olduğunu bilir.
- Sinyal halinde giden verinin güvenliği: Telefon numaraları gibi sinyal kanalında, hassas bilgilerin radyo kanalı üzerinde korunmasıdır.
- Kullanıcı veri güvenliği: Radyo kanalı üzerinden geçen kullanıcı verilerinin korunmasıdır.
- Abone Kimlik Gizliliği: Abonenin konumu saptanamamalı ve ona yapılan veya onun yaptığı çağrılar dinlenememelidir [28,29].

Abone kimlik doğrulanması

GSM ağında parola sorma-cevap verme mekanizmasının kullanımı ile abonenin (kullanıcının) kimliği doğrulanır. 128 bitlik rastgele bir sayı (RAND) MS'ye

gönderilir. MS, rastgele sayının şifrelenmesine bağlı olarak A3 ve kişisel abone doğrulama anahtarı (Ki) ile 32 bitlik imzalı mesaj üretir. Kullanıcıdan imzalı mesajın alınması üzerine GSM ağı kullanıcının kimliğini doğrulamak için tekrar hesaplama yapar. Buradaki önemli nokta, kişisel kullanıcı anahtarının (Ki) radyo kanalı üzerinden gönderilmemesidir. Bu anahtar, kullanıcının SIM kartındakine benzer olarak AUC, HLR ve VLR veritabanlarında daha önceden vardır. Eğer kullanıcıdan gelen SRES ile hesaplanan değer uyuşursa, MS'nin kimliği başarılı bir şekilde doğrulanmıştır. Eğer hesaplanan değerle uyuşmazsa bağlantı sonlandırılır ve MS'ye doğrulamanın başarısız olduğu belirtilir. Şekil 2.8'de doğrulama işlemi görülmektedir [25].

İmzalı cevabın (SRES) hesaplanması SIM kartın içinde yapılır. Bu işlem güvenliği artırır. Çünkü güvenli kullanıcı bilgisinin örneğin IMSI veya kişisel kullanıcı doğrulama anahtarının (Ki) doğrulama işlemi süresince görülmesi engellenmiş olmaktadır [25].

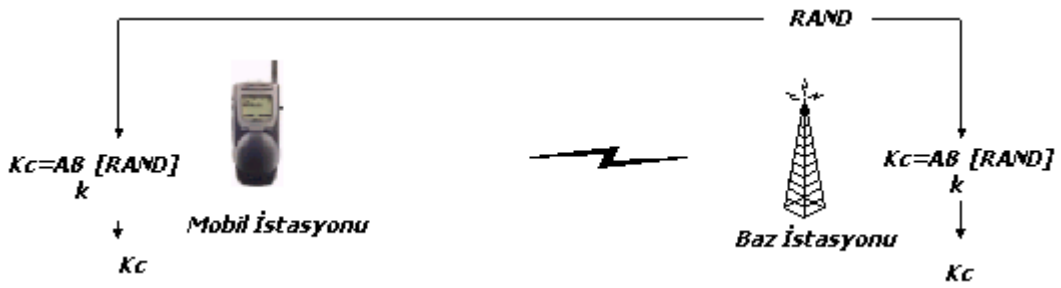


Şekil 2.8. GSM doğrulama mekanizması [25]

Sinyal halinde giden verinin güvenliği ve kullanıcı veri güvenliği

SIM, 64 bit şifreleme anahtarı olan Kc'nin üretilmesinde kullanılan şifreleme anahtarı üretim algoritması (A8)'i içerir. Şifreleme anahtarı doğrulama işleminde kullanılan aynı rastgele sayı (RAND) ile bireysel kullanıcı doğrulama anahtarı (Ki),

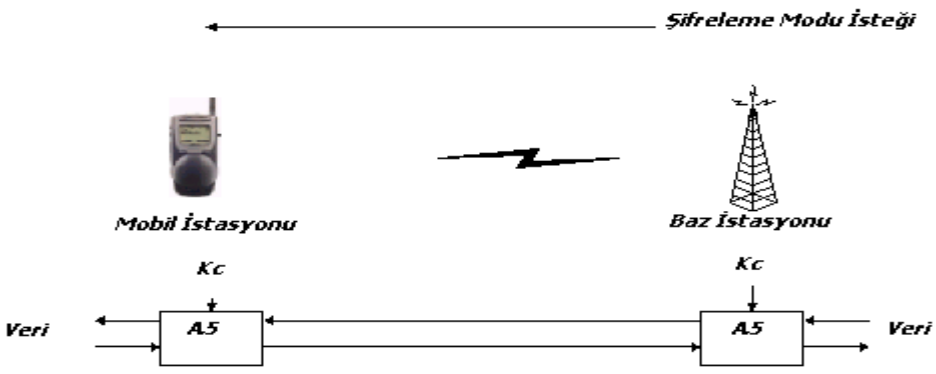
anahtar üretim algoritması A8'e uygulanarak şifreleme anahtarı hesaplanır. Şifreleme anahtarı MS ve BS arasında veri şifreleme ve deşifreleşmede kullanılır [29].



Şekil 2.9. Şifreleme anahtarı üretim mekanizması [25]

Bir ek güvenlik katmanı da, şifreleme anahtarının değiştirilmesi ile dinlemeye karşı direnç sağlanmasıdır. Şifreleme anahtarı, ağ tasarımına ve güvenlik gereklerine göre düzenli aralıklarla değiştirilir. Şekil 2.9'da şifreleme anahtarı Kc'nin hesaplanması gösterilmektedir [29].

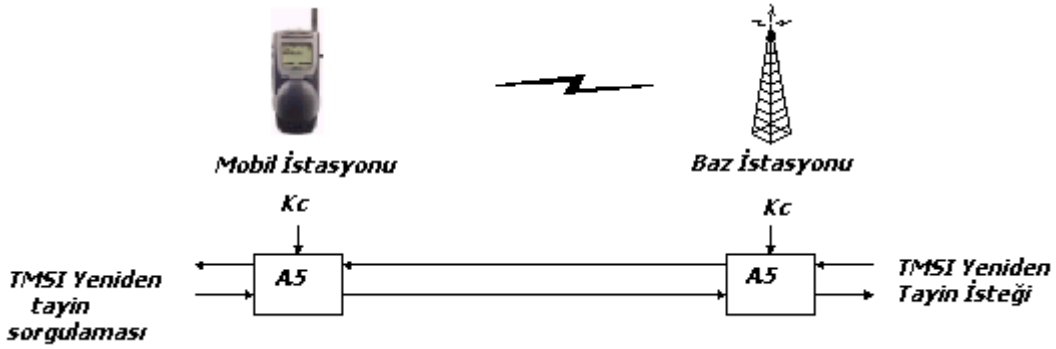
Mobil İstasyonu (MS) ve ağ arasındaki ses ve veri haberleşmesinin şifrelenmesi A5 şifreleme algoritması kullanılarak gerçekleştirilir. Şifrelenen iletim, GSM ağından şifreleme modu isteği komutuyla başlatılır. Bu komutun alınması üzerine, mobil istasyonu, A5 şifreleme algoritmasını ve Kc şifreleme anahtarını kullanarak şifreleme ve deşifreleme işlemini başlatır. Şekil 2.10'da şifreleme mekanizması gösterilmektedir [25].



Şekil 2.10. Şifreleme modu başlatma mekanizması [25]

Abone kimlik gizliliği

Kullanıcı, kimlik güvenliğini sağlamak için Geçici Mobil Kullanıcı Kimliği (TMSI-Temporary Mobile Subscriber Identity) kullanır. TMSI, doğrulama ve şifreleme prosedürlerinden sonra, mobil istasyona gönderilir. Mobil istasyonu TMSI'nin alınıp alınmadığına dair bir cevap üretir. TMSI dağıtıldığı yerel bölgede geçerlidir. Yerel bölgenin dışındaki haberleşme için TMSI'ye ek olarak Yerel Bölge Tanımlaması (LAI-Location Area Identifier) gereklidir. Şekil 2.11'de TMSI tayin/ yeniden tayin mekanizması gösterilmektedir [25].



Şekil 2.11. TMSI tayin mekanizması [25]

2.3.2. Telefon bazlı GSM güvenlik mekanizmaları

SIM, cihazın içine takılan, kullanıcıyı tanımlayan ve kullanıcının erişebileceği/kullanabileceği hizmetler hakkında bilgi veren elektronik bir karttır. Her cep telefonunun kendine ait IMEI (International Mobile Station Equipment Identity), yani uluslar arası mobil istasyon tanıtım kodu vardır.

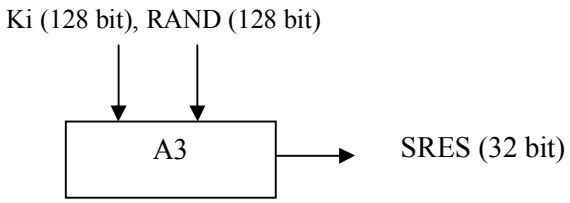
IMSI (International Mobile Subscriber Identity), SIM kartta kalıcıdır ve GSM sistemde aboneyi tanımlayan önemli bilgilerden biridir. IMSI' nin ilk üç basamağı mobil ülke kodunu (MCC - Mobile Country Code), daha sonraki iki basamak mobil şebeke kodunu (MNC - Mobile Network Code) , kalan on basamak mobil abone kimlik numarasını (MSIC- Mobile SubscriberIdentificationNumber) tanımlamaktadır.

2.3.3. GSM şifreleme algoritmaları

GSM'de güvenlik uygulanan üç algoritma sayesinde yerine getirilmektedir. Bualgoritmalar Mobil İstasyonu Doğrulama Algoritması, Anahtar Üretme Algoritmasıve Şifreleme Algoritması olarak tanımlanır.

Mobil istasyonu doğrulama algoritması A3

A3 bir doğrulama algoritmasıdır. Fonksiyonu, MSC(Mobile Switching Center-Mobil Bağlantı Merkezi)'nin rastgele gönderisi olan RAND'e SRES imzalı cevabını üretmektir. RAND, MSC tarafından HLR'den alınır. Şekil 2.12'de görüldüğü gibi, A3 algoritması MSC'den RAND'ı ve SIM'den Ki'yi alarak 32 bit SRES cevabı üretir. RAND ve Ki'nin ikisi de 128 bit uzunluğundadır [25].



Şekil 2.12. A3 algoritmasının çalışması

Şifreleme algoritması A5

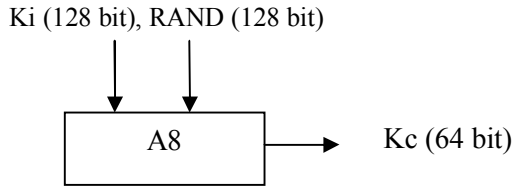
GSM sisteminde şifreleme için kullanılan A5 algoritmasının A5/1 ve A5/2 olarak isimlendirilen çeşitli varyasyonları vardır. A5/1 hava kanalı üzerinden ses şifrelemesinde kullanılan en güçlü şifreleme algoritması olarak bilinmektedir. A5/2 gibi daha zayıf versiyonları Avrupa dışında kullanılmaktadır. A5/1 hava kanalı iletimini şifrelemede stream (akış) şifreleme kullanılmaktadır.

Saldırılar söz konusu olduğunda, A5/1 algoritması A5/2'ye göre daha güçlüdür. Diğer bir versiyon olan A5/0 algoritması ise tümünde şifreleme yapılmadığından zayıf bir algoritmadır.

Hava aktarma kanalının üzerinde şifrelemek için kullanılan A5 algoritması, Bilinen Açık Metin Saldırısı, Kaba Kuvvet Saldırısı, Böl ve Fethet Saldırısına karşı korunmasızdır [25].

A8 anahtar üretme algoritması

A8, GSM modelde ses verisini şifrelemekte kullanılacak anahtarı üretme algoritmasıdır. A8, gizli anahtar Ki'yi ve MSC'denRAND'ı alarak oturum anahtarı Kc'yi üretir. A8 algoritması 128 bitlik iki giriş alır ve bunlardan 64 bit çıkış üretir. Bu çıkış 64 bit oturum anahtarı Kc'dir. BS(Base Station) aynı Kc'yiMSC'den alır. HLR'de aynı şekilde Kc'yi üretebilir. Çünkü HLR'deRAND ve Ki değerleri bulunmaktadır. Oturum anahtarı (Kc), MSC tarafından MS'nin doğruluğu tekrar onaylanmaya karar verilene kadar kullanılır. Bu bazen birkaç gün alabilir.



Şekil 2.13. A8 anahtar üretme algoritmasının çalışması

A3 ve A8 algoritmalarının ikisi de SIM kartta saklanır böylece anahtarların saldırganların bunları bozması önlemiş olur. Böylece GSM operatörünün donanım üreticilerinden bağımsız olarak hangi algoritmayı seçeceğine kendisi karar verebilir [25]. Şekil 2.13'de A8 anahtar üretme algoritmasının çalışması görülmektedir.

COMP 128 algoritması

A3 ve A8 algoritmalarının ikisi de tek yönlü fonksiyonlardır. COMP128 ise çoğu GSM ağında A3 ve A8 algoritmalarının ikisi için de kullanılır. COMP128, SRES cevabını ve oturum anahtarı Kc'yi üretir. COMP128 algoritmasının son 54 biti Kc'dir ve bu MS tarafından tekrar doğrulanana kadar kullanılır. Anahtar uzunluğu 64

bit yerine 54 bittir. Elde edilen bu anahtar uzunluğu A5 algoritmasına giriş olarak verilir. COMP128 algoritması tarafından anahtarın son 10 bitine sıfır eklenerek anahtar 64 bite çıkarılır. Bu işlem anahtar uzayını 64 bitten 54 bite düşürmektedir. COMP128 çıkışının 32 önemli biti ise A3 algoritmasının çıkış (SRES) değeridir [25]. Daha sonra, COMP 128 fonksiyonunda olan güvenlik açığını gidermek için A3 ve A8 algoritmalarını referans alarak COMP 128-2-3 hash fonksiyonları geliştirilmiştir [30].

2.4. Cep Telefonlarında Güvenlik Açıkları

Hayatın her alanında mobil telefonların yaygın kullanımı, dünyanın dört bir yanında bilgiye erişmeyi kolaylaştırırken, bilginin korunması ve güvenli bir şekilde taşınması çok önemli bir sorun haline gelmiştir. Bu kullanım sıklığı güvenlik açıklarını da beraberinde getirmektedir. Başlıca güvenlik açıkları;

- IMEI Klonlama
- Yasal ve Yasal Olmayan Dinlemeler
- Spam yazılımlarla mesajların başka bir telefona yönlendirilmesi olarak listelenmektedir.

2.4.1. IMEI klonlama

Ülkemizde çalıntı, kaçak veya kopyalanmış cihazların GSM işletmelerinden hizmet alımlarının durdurulması, kopyalanmış veya bilgileri değiştirilmiş cihazların kullanımının engellenmesi amacıyla Mobil Cihaz Kayıt (MCK) Sistemi kurulmuştur ve 14.12.2005 tarihinden itibaren ülke genelinde çalıntı veya kayıp olarak rapor edilen tüm cihazların hizmet dışı kalması sağlanmıştır. Böylece tüketicilerin mağdur olması, piyasada haksız rekabetin oluşması ve ülke ekonomisinin zarar görmesi engellenmiştir. Ancak günümüzde piyasada yer alan bir çok cihazın değişik yöntemlerle klonlanması MCK Sistemi'nin görevini yerine getirmesini engellemekte ve sistemin getirdiği tüm üstünlükleri ortadan kaldırmaktadır. Günümüzde bir sektör haline gelen IMEI klonlama ülkemiz telekomünikasyon piyasasına ciddi manada

zarar veren ve tüm sektör aktörlerinin işbirliği içerisinde mücadele etmesi gereken bir sorundur [31].

Aynı IMEI numarasının birkaç telefona kopyalanması haksız rekabete ve kazanca sebep olmaktadır.

2.4.2. Yasal ve yasal olmayan dinlemeler

Telefonda gerçekleştirilen haberleşmenin kayda alınmasının en önemli amacı suçla mücadeledir. Ancak, bu yapılırken 1982 Anayasa'sında da yer alan "özel yaşamın gizliliği" hakkına ve onun önemli bir unsuru olan "haberleşme özgürlüğüne" gereksiz ve hukuka aykırı müdahalelerden kaçınmak gerekir. Özel yaşamın gizliliği hakkı, önemi nedeniyle Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) de düzenlenmiştir [32].

Farklı dinlemelerin farklı yasal gereksinimleri vardır. En bağlayıcı yasal standartlar iletişimin içeriğinin dinlendiği durumlarda (telefon çağrı sesi, metin mesajı vb.) uygulanır. Bu dinlemeler ancak yeterince sebep olduğu ve araştırma için büyük önem teşkil ettiği hakkında mahkemenin ikna edilmesiyle, izin alınarak yapılabilir. Sadece metaveri ya da çağrı tanımlama bilgisini gösteren (kimin kimle ne zaman konuştuğunu gösteren liste) kalem kaydı (penregister) dinlemeleri daha düşük yasal standartta olabilir. Bu tip dinlemeler için genelde gerekli olan sadece belirli kayıtların araştırma ile ilintili olduğuna dair bir iddiada bulunmaktır ve kalem kayıtları çoğu zaman mahkemenin onayını gerektirmez. Çoğu yasal dinleme bu kategoridedir fakat aslında kalem kaydından elde edilen bilginin de içerik dinlemesi talebi için bir kanıt olarak kullanılması sıklıkla görülür [33].

Amerika'da, el altından üçüncü kişilerce yapılan telefon ve ağ iletişimi engellemeleri, kriminal araştırmalar ve benzeri durumlar haricinde, kişilerce de hükümet tarafından da yapılsa hukuka aykırıdır. İzin verilse dahi, yasal telefon dinlemeleri mahkeme gözetiminde, toplanacak bilginin çeşidine göre farklı

gereksinimlerle ve standartlarla yapılmalıdır. Birçok devlet de benzer kurallara sahiptir [34].

Yasal olmayan dinlemeleri yapmak günümüzde artık çok büyük bir maliyet gerekmemektedir. Bu da kişi ya da özel kuruluşların çıkar sağlamak için bu yollara başvurmasını kolaylaştırmaktadır.

2.4.3. Spam yazılımlarla mesajların başka bir telefona yönlendirilmesi

GSM SMS yönlendirme mesaj bildirim yazılımını hedef telefona yüklendikten sonra bu telefona gelen ve bu telefondan gönderilen tüm SMS'leri sizin belirlediğiniz numaraya gerçek zamanlı olarak gizlice gönderir. Hedef telefona yüklenen yazılım, uzaktan görünmez mesaj göndererek açılıp kapatılabilir. Ayrıca belirlenen numara istenilen zamanda hedef telefona görünmez bir mesaj gönderilerek değiştirebilir. Spam yazılımlarla mesajın başka bir telefona yönlendirilmesiyle telefon sahibinin kişisel bilgileri kişinin haberi olmadan kopyalanmakta ve bilgi gizliliğinin ihlali söz konusu olmaktadır.

2.5. Cep Telefonu Kullanımının Bağımlılık Boyutu

Yeni nesil cep telefonları, Üçüncü nesil (3G) kablosuz sistemleri, sadece konuşma için kullanılmamaktadır. 3G genellikle geleneksel sesli iletişim hizmetlerine ek olarak, multimedya mesajlaşma ve doğrudan internet erişimi için kullanılmaktadır. Cep telefonu ile kullanıcılar, telefon posta, sesli posta, hisse senedi fiyatları, maç skorları, restoran değerlendirmeleri, film kılavuzları ve benzeri şeylere erişebilmektedir [35]. Günümüzdeki kullanım amaçları ele alındığında cep telefonları son yıllarda bireysel iletişimin ve bilgi edinmenin en önemli aracı haline gelmiştir.

Ayrıca cep telefonu doğrudan veya dolaylı olarak insan ilişkileri ve insan etkileşiminin çok yönden etkilemektedir [36].

Cep telefonu ile ilgili yapılan ilk çalışmalarda, cep telefonunun güvenliği ve erişilebilirliğinin insanların iletişim teknolojisini kabul için önemli sebeplerinden olduğunu göstermektedir [37]. Rahatlık, mobilite, güvenlik ve ağ gibi çeşitli nedenler, cep telefonu kullanıcıları tarafından tercih nedeni olarak bulunmuştur [2,37]. Yapılan çalışmalarda cep telefonu kullanıcılarının bu iletişim aracına güvenmesinin dayandığı temel nedenin ağ (networking) olduğu görülmektedir [38].

Yapılan bir başka araştırma ise, mobil telefon kullanıcılarının %92'sinin kullanıcıların günlük yaşamlarında cep telefonuna sahip olmaya ihtiyaç duyduğunu hissettiğini göstermektedir [39].

Bazı bilim adamları cep telefonunun ebeveynler ve çocuklar, kullanıcılar ve yakın dostları arasında doğrudan ve özel iletişim kanalı sağladığını savunmaktadır. Bu yüzden, cep telefonu orijinal olarak, profesyonel ve ticari amaçlar için tasarlanmış olmasına rağmen, özellikle kullanıcıların aile üyeleri ve arkadaş ilişkilerinde sosyal sermaye artırmak için kullanılmaktadır [36,40].

Çalışmalarda cep telefonu kullanımının sosyalleşme, moda/statü sembolü, güvende hissetme, alışkanlık, ekonomik oluşu, iletişim sağlama boyutları olduğu belirlenmiştir [41-43].

Cep telefonu kullanımının en önemli ve temel özelliği; bireylerin nerede olurlarsa olsunlar iletişimi sağlamasıdır. Bu özellik ile bireyler yalnızlık endişelerini gidermektedirler [44].

Bireylerin yalnızlıklarını hafifletmek ya da azaltmak amacıyla cep telefonu kullanımları kabul görülebilmektedir, ancak, bireyler karşılanmayan sosyal ihtiyaçlarını cep telefonu ile gidermeye başladıkları noktadan itibaren cep telefonu kullanımının bağımlılık boyutundan söz edilmektedir. Duygusal hazzın devreye girdiği andan itibaren cep telefonu kullanımı iletişimi sağlayan bir araç olmaktan çıkmaktadır [45,46].

Ling'in Kore'de üniversite öğrencileri ile gerçekleştirdiği çalışmada, bireyler cep telefonlarını zaman geçirme ve alışkanlık edinilmiş bir araç olarak görmektedirler. Bireyler cep telefonu konuşmaları neticesinde gelecek olan yüksek faturanın bilincinde olmalarına karşın, cep telefonları ile sık sık arama yaptıkları ve kısa mesaj gönderdikleri görülmüştür. Cep telefonları olamadığı zamanlarda, cep telefonunun yokluğu nedeniyle yüksek endişe ve rahatsızlık duyduklarını bildirmişlerdir. Cep telefonu bağımlısı olarak tanımlanan bireyler eğlence ve bilgi alışverişi özellikleri yerine, cep telefonunu sadece iletişim aracı olarak görmektedirler [47].

Cep telefonlarının birçok olumlu sonucunun yanında olumsuz etkileri de mevcuttur. Bu etkiler ile ilgili çalışmalar bireylerin fiziksel sağlığı üzerine olabilecek zararlarına odaklanmaktadır. Cep telefonu kullanımının bilinen olumsuz etkilerinden biri olarak, araba kullanırken cep telefonu kullanmanın yarattığı tehlikelerden söz edilmektedir [48]. Ayrıca cep telefonu kullanımı sırasında yayılan radyasyonun zararlı etkilerine maruz kalmaları da olumsuz etkilerden birisidir [49].

Bireyler istedikleri her yerde ve zamanda cep telefonlarını kullanarak iletişime geçebilmektedirler. Bu durum, bireylere cep telefonsuz olamayacaklarını hissettirmeye neden olmaktadır [47].

Özellikle Asya'da cep telefonu kullanımının yaygınlığı neticesinde; Kore'de cep telefonu bağımlılığı ile ilgili çalışmalar geçekleştirilmiştir [50]. Yapılan bir çalışmada üniversite öğrencilerinin % 75'i cep telefonları yanlarında olmadığında kendilerini rahatsız ve tedirgin hissettiklerini bildirmektedirler. Bu durum bağımlılık belirtilerine işaret etmektedir. Aynı biçimde, Amerika'da yapılan çalışmalarda da bireylerin cep telefonlarını saplantı (obsession) halinde her yere taşıdıkları belirlenmiştir [41-43].

2.6. Cep Telefonu Kullanımı ve Bireysel Güvenlik

Cep telefonunun bireylerin algıladıkları güvenlik duygusuna etkisi olduğu görülmüştür [51].Bireylerin cep telefonlarını yanlarında bulundurmaları, bireylerin kendilerini daha güvende hissetmelerini sağlamaktadır [52-58].

Katz ve Aakhus'un yaptığı çalışmada katılımcıların acil durumlarda kullanmak üzere iletişim aracı olarak cep telefonu bulundurduğu saptanmaktadır. Katılımcılar geceleri sokağa çıktıklarında yanlarında cep telefonu bulundurduklarında kendilerini psikolojik olarak güvende hissettiklerini belirtmişlerdir [36].

Cep telefonu bireyleri riskli davranışlara yönlendirmektedir. Cep telefonu bireylerde bulundukları durumun farkındalığı ile ilgili algılarını etkilemektedir. Çalışmalarda, cep telefonu ile konuşmanın kullanıcıların dikkatini dağıttığını ve reaksiyonlarını yavaşlatarak, herhangi bir kazanın gerçekleşme olasılığını artırdığı görülmektedir [52-58].

2.7. Kamusal Alanlarda Cep Telefonu Kullanımı

Günümüzde mobil cihazlar hayatımızın bir parçası olmuştur. Neredeyse her zaman yanımızda bulundurduğumuz mobil cihazların yeteneklerinin artması yaşamımızda bu cihazlara olan istek ve beklentilerin de artmasına sebep olmaktadır.

Visa, Master-Card, Card Plus, American Express gibi kart tabanlı elektronik ödeme (e-ödeme)yöntemlerinin ödeme araçları olarak kullanılması, çalıntı, kayıp ve hasarlı olabilmeleri ihtimallerinden dolayı her yıl büyük ölçüde maddi zararlara yol açmaktadır [59]. Bu yöntemleri daha güvenli hale getirmek için geliştirilen, ödeme sırasında POS cihazlarına girilecek ve elektronik imza gibi düşünülebilecek kişisel kimlik numarası (PIN) da bazı güvenlik problemleri taşımaktadır. Cep telefonları, bu tür elektronik ödeme araçlarının yerini tutacak basit, kullanımı kolay ve çok yönlü bir araç olarak kullanılabilir.

Cep telefonu Kısa Mesaj Servisi (SMS), Kızıl ötesi (IrDa), BlueTooth, RFID gibi araçlar yardımıyla elektronik ödemelerde kullanılma imkanlarına sahiptirler [3,40]. Bu yöntemlerin tümü yapılan ödemeyi cep telefonu görüşmeleri için gelen faturaya ekleyebilme özelliklerine de sahiptirler [60].

Önerilen bu ödeme yönteminde cep telefonlarının kredi kartlarından daha yaygın kullanıldığı ortamlarda kullanılabilme şansına sahiptir. Gelişmemiş ve gelişmekte olan ülkelerde cep telefonu kullanımı kredi kartı kullanımından daha yaygındır. Bu ülkelerde, mobil ödemenin yaygınlaşması için cep telefonları kredi kartı yerine kullanılabilmektedir.

Cep telefonlarının ve kısa mesaj servisinin kullanıldığı diğer bir alan ise mobil bankacılıktır. Mobil bankacılık deyimi; bankaların müşterilerine, hesaplarına bir mobil teknoloji cihazı kullanarak herhangi bir yer ve zamanda hesaplarına ulaşarak istedikleri uygulamaları online ve iki yönlü olarak anında yapabilmeleri olarak ifade edilmektedir [61]. Mobil bankacılığın en basit ve en kolay uygulanabilir biçimi müşterilerin telefon ile arama yapmaları ya da yazılı mesaj göndermeleridir. Mobil aygıtların bankacılık sistemleri gibi alanlarda kullanılması durumunda sistem güvenlik açısından çeşitli tehlike ve saldırılara maruz kalabilmektedir.

Bu tehlikeler ikiye ayrılmaktadır: Transfer edilen gizli bilgilerin dinlenilmesi ve transfer sırasında bilginin ya da verinin değiştirilmesidir [62]. Gelişmiş şifreleme yöntemleri kullanılarak bu tehditlerin önüne geçilebilmektedir.

3. KRİPTOLOJİ

Matematiksel olarak gizli karakterleri oluşturma, çözme ve bu karakterlerin iletilmesini de içeren bilimsel çalışma, kriptoloji olarak ifade edilmektedir. Gizlilik sistemlerinin tasarımı ve uygulaması ile kriptografi bilimi ilgilenmektedir. Özellikle internet teknolojisinin yaygınlaşmasıyla adını sıkça duymaya başladığımız kriptoloji, kriptografik metotların matematiksel temelleriyle ilgilenen bir matematik dalıdır [63]. Böylece hassas bilgilerin saklanması ya da güvensiz ağlar üzerinden güvenli bir şekilde aktarılması sağlanır. Bir bilim olarak ortaya çıkışından beri güvenli iletişimi analiz etme ve kırma bilimi olarak ortaya çıkmıştır. Klasik kriptoanaliz, analitik sebeplerin matematiksel uygulamaların, iz bulma işlemi sabrın ve şansın bir birleşimidir [64].

Kriptoloji esas olarak kriptografi ve kriptoanaliz olmak üzere iki bölüme ayrılır.

3.1.Kriptografi

Kriptografi, metin şifrelemekte kullanılan tekniklerin tümünü inceleyen bilim dalıdır. Kriptografik algoritma şifreleme ve şifre çözme işlemini gerçekleştirmek için kullanılan matematiksel bir fonksiyondur ve veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılır. Kripto algoritmasının çalışması için bir anahtar (key) ve şifrelenecek bir ifade gerekir. Farklı anahtarlar kullanıldığında aynı şifrelenmemiş metinden farklı şifrelenmiş metinler üretilebilir. Şifrelenmiş bilginin güvenliği iki şeye bağlıdır;

- Algoritmanın Güçlülüğüne
- Anahtarın Gizliliğine

İki kişi arasında iletilen herhangi bir iletiye “mesaj”(message)denir. Bu mesajlar genellikle bazı bilgileri içermektedir. Bir mesajı gönderen kişiye “gönderici” (sender), gönderilen mesajı alan kişiye “alıcı” (recipient) denir. Bir mesajın orijinal

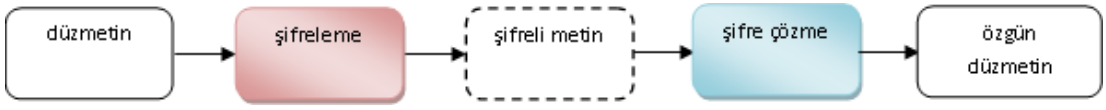
haline, yani herkes tarafından anlaşılabilen haline ise “açık metin” (plaintext), bir mesajın şeklini değiştirerek kimsenin anlayamayacağı hale sokma işlemi “şifreleme” (encryption) olarak adlandırılmaktadır. Şifrelenmiş mesaja, “şifreli metin” (ciphertext),şifreli metnin herkesin anlayabileceği şekle dönüştürülmesine, yani şifreli metnin açık metin haline getirilmesi işlemi “şifre çözme” (decryption) denilmektedir.

Şifreleme ve şifre çözme işlemleri belirli adımlardan oluşmaktadır. Bu adımların bütününe “şifreleme algoritması” denmektedir. “Anahtar”, şifreleme algoritmasının kullandığı bazı özel bilgilerdir. Bunlar genelde rastgele sayı dizileri olurlar. Bir şifreleme algoritmasında kullanılabilecek anahtarların tümünün kümesine “anahtar uzayı” denilmektedir [65].

Şifreleme ve çözme genelde bir anahtar (key) kullanılarak yapılır ve şifreleme algoritması çözme işlemi ancak doğru anahtarın bilinmesiyle gerçekleştirilebilmektedir [66].

Anahtar**,** bir metni şifrelemekte veya açmakta kullanılan veri parçasına (sayı, kelime veya herhangi bir sayısal veri parçası) verilen isimdir. Anahtar uzunluğu ne kadar büyük olursa şifrenin kırılması o kadar zorlaşır.

Kriptografik algoritmalar adı da verilen şifreleme algoritmaları, şifreleme ve şifre çözümü için kullanılan matematiksel işlemlerdir. Şekil 3.1’de Şifreleme ve şifre çözme işlemi görülmektedir.



Şekil 3.1. Şifreleme ve şifre çözme

3.1.1. Kriptografinin uygulama alanları

Şifreleme askeri ve diplomatik iletişimde (haberleşmede) güvenliği sağlamakiçin yüz yıllardır kullanılmaktadır. Günümüzde şifreleme uygulamalarına özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında işlemlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır.

Kriptografinin uygulama alanları olarak;

•kablolu ve kablosuz ağlarda ses ve/veya veri aktarımının istenmeyen kişilerce izlenmesinin önlenmesi,
• bilgisayar sistemlerinde bulunan verilere yetkisiz erişimlerin engellenmesi,
• güvenli bir şekilde e-ticaret işlemlerinin yapılabilmesi örneklenebilir [67].

Kimlik belirleme, birinin ya da bir şeyin kimliğinin doğrulanmasıdır. Her ATM kartının, kart sahibiyle, dolayısıyla hesapla ilişkilendiren bir PIN numarası vardır. Kimlik denetimi de kişilerin kaynaklara erişimini sağlaması bakımından kimlik belirlemeye benzer. Ancak kimlik denetiminde asıl yapılan; ilgili kişinin ilgili işlemi yapmaya yetkisi olup olmadığının tespitidir. Kimlik belirleme ve kimlik denetimi; kriptografinin en yaygın kullanım alanlarından birisidir [68].

E-ticaret, çevrimiçi bankacılık, internet üzerinden alışveriş, gibi başlıkları içerir. Kullanıcıların E-ticarete güven duyabilmesinin önündeki en önemli teknik sorun, Internet üzerindeki bilgi güvenliğinin sağlanması ve güvenli ödeme yapılabilmesidir. Ancak internet üzerinden kredi kartı numarasını göndermek gibi bir işlem, kişiyi dolandırılmaya açık hale getirir. Bu soruna kriptografik bir çözüm, çevrimiçi girildiği durumlarda kredi kartı numarasını (veya diğer gizli bilgileri) şifrelemektir veya sadece kredi kartı numarasını şifrelemek yerine tüm oturum güvenli hale getirilebilir. Bir bilgisayar bilgiyi şifreleyip internet üzerinden gönderdiği zaman, şifreli bilgi, onu elde eden üçüncü kişilere anlamsız gelir. Sunucu (internet üzerindeki alışveriş

merkezi), şifreli bilgiyi alarak şifreyi çözer ve kredi kartı numarasının başkalarının eline geçmiş olabileceği konusunda kaygı duymadan satışa devam eder. İnternet üzerinden iş yapmak yaygınlaştıkça, sahtekârlıklara karşı korunma ihtiyacı da artmaktadır.

Sertifika (E-kimlik) Dağıtımı; Kriptografinin diğer bir uygulaması sertifika dağıtımıdır. Sertifika dağıtımı, sertifika hizmet sağlayıcıları gibi güvenilir kurumlar tarafından, kişilere elektronik ortamlarda kimliklerini doğrulamasını amaçlı kimlik dağıtımı sağlayan bir yapıdır [69].

Uzaktan erişim; Temel "anahtar kelime" (şifre sorma) sistemleri belli bir seviyede güvenlik sağlar.

Mobil elektronik imza; Günümüzde elektronik ortamlar yaygınlaştıkça, iş ve işlemler elektronik ortamlara kaymakta, bu ortamlarda yüksek seviyede bir bilgi güvenliğinin sağlanması ise zorunluluk arz etmektedir. Ülkemizde 5070 sayılı Elektronik İmza (e-İmza) Kanunu ve Düzenlemeleri, yüksek seviyede bilgi güvenliği ve hukuksal olarak da geçerliliği olan altyapıyı oluşturmuştur. Dünyada ve ülkemizde elektronik imza uygulamalarına yönelik birçok proje hayata geçirilmektedir. İletişim ve bilişim teknolojilerindeki gelişmeler ve mobil cihaz penetrasyonunun artması elektronik ortamda yapılan iş ve işlemlerin mobil ortamlara kaymasına sebep olmaktadır. Mobil ortamlarda yapılan iş ve işlemlerin güvenli olarak yapılmasının yanında ise yapılan işlemlerin hukuken geçerliğinin de sağlanması sorununu gündeme taşımaktadır [70]. Günümüzde e-ticaret işlem hacminin artışı ile gündeme gelen elektronik ödeme çözümleri içinde kabul edilebilirliği yüksek olan ve maliyet üstünlüğü sağlayan e-çek sistemi, diğer ödeme araçlarının olumsuzluklarını bertaraf etmektedir. Bir anlamda kağıt çek sisteminin teknolojik versiyonu olarak tanımlayabileceğimiz e-çek sisteminin işletme dünyasında tüm taraflara hitap etmesi kabul edilebilirliğini artırmaktadır. Ayrıca güvenlik sisteminin çok iyi olması nedeniylede KOBİ' ler başta olmak üzere geleneksel ödeme araçlarından vazgeçmeyenler içinde alternatif bir ödeme aracı olarak karşımıza çıkmaktadır.

E-çek Güvenliği (eCheck Security): E-çek güvenliği, e-çekler üzerindeki sahtekarlıkları önleyen kurulu iş teamülleri ile en son teknolojinin kombinasyonudur. Eçek, sistem güvenliğinin sağlanması için, sıkı bankacılık ile devlet iş standartları ve uygulamalarına tabidir. Ek olarak, e-çek, teknoloji araçlarının, verilerin şifrelenmesinin, sayısal imzaların, sertifikaların, güvenli email ve akıllı kart teknolojisinin kombinasyonu ile sistem güvenliğinin tehlikede olmasını önler [71].

3.1.2. Kriptografinin önemi

Günümüzde iletişimin hızla gelişmesiyle internet hayatımızın vazgeçilmezlerinden biri olmuştur. Bu gelişimle birlikte insanlar, ağ aracılığıyla bilgi paylaşma yolunu kullanmaya başlamışlardır. Bunun yanında, internet üzerinden yaptığımız bilgi alış verişleri esnasında, ağların dinlenmesi, gelen verinin değiştirilmesi, bir başkası gibi davranarak yanlış bilgi gönderilmeye çalışılması, başkasına ait bilgilerin öğrenilmeye çalışılması gibi tehditler oluşmaya başlamıştır. Bütün bu tehditleri önlemek amacıyla internet üzerinde ki iletişimde güvenlik büyük önem kazanmıştır.

Finansal, kişisel ve iş hayatındaki bilgilerin paylaşımında kiminle haberleştiğimizin bilinmesi, gönderdiğimiz bilginin karşı tarafa doğru olarak iletilmesi ve bilgi transferi sırasında bilgilerin başkaları tarafından izlenememesi güvenliğin sağlanması açısından gerekmektedir. Bu gereksinimleri yerine getirebilmek amacıyla iletişimde anahtarlama yöntemleri kullanılmaya ve geliştirilmeye başlanmıştır.
Kriptografi, fiziksel dünyada sahip olunan güvenli ortamın elektronik dünyaya taşınmasına izin verir. Böylece insanların sahtekârlık ve aldatılma kaygısı duymadan elektronik ortamda iş yapabilmesini sağlar [68].

Kriptografi aşağıdaki alanlarda sıklıkla kullanılmaktadır.

- Sanal Bankacılık
- Elektronik Ticaret
- Askeri iletişim
- E-Devlet uygulamaları

- Ticari Sırlar
- Kişisel hayatın gizliliği

E-posta, günlük kişisel veya iş yazışmalarında vazgeçilmez bir yere sahiptir. Ancak herhangi bir önlem alınmadığında istenen kişilerce ele geçirilebilir ve değiştirilebilir. Şifreleme, mektupların istenmeyen kişilerce okunabilmesini veya değiştirilmesini engeller. Ayrıca, gönderilen mesajın kaynağının doğrulanması veya mesaj içeriğinin değişmediğinin güvencesinin verilebilmesi amacıyla sayısal imza kullanılabilir [68].

Bazı durumlarda kriptografi elektronik ortamda, fiziksel dünyadaki işlemlerde sahip olduğumuzdan daha fazla güven sağlar. İmzanız taklit edilebilir veya imzaladığınız bir belge değiştirilebilir. Ancak, elektronik imzanız gizli anahtarınız bilinmediği sürece taklit edilemez ve elektronik olarak imzaladığınız bir belge, imzanız belgenin içeriğine de bağlı olduğu için asla değiştirilemez [68].

Kriptografi sadece internet üzerinde değil, telefonlarda, televizyonlarda ve günlük hayatın birçok alanında kullanılmaktadır [68]. Güvenliği sağlamak amacıyla çeşitli kriptolu telefonlar geliştirilmiştir. Buna rağmen sadece devlet kurumları kriptolu telefon sahibi olabilmektedir. Herhangi bir sivil şahsın kriptolu telefon kullanması suç teşkil etmektedir. Bu durumun açığa çıkması halinde kişi yargılanmakta ve ceza almaktadır.

3.2. Kriptoanaliz

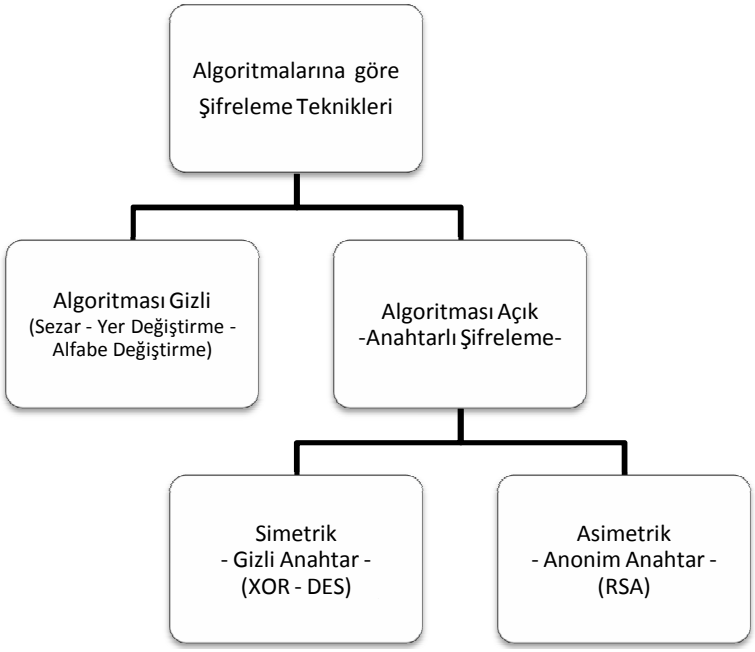
Kriptoanaliz (Şifre çözümü) ise şifrelenmiş bir metnin şifrelenmemiş düz metin haline getirebilmek için yapılabilecek her türlü saldırıları ve türlerini inceleyen bilim dalıdır.

3.3. Şifreleme Algoritmaları

Şifreleme teknikleri algoritmalarına, anahtar sayısına ve şifrelenecek mesajın tipine göre sınıflandırılmıştır.

3.3.1. Algoritmalara göre şifreleme teknikleri

Tarihi sürece bakıldığında şifreleme teknikleri önce açık ya da gizli algoritma kullanmalarına göre ikiye ayrılırlar. Şekil 3.2'de Algoritmalarına göre şifreleme teknikleri gruplandırılmıştır.



Şekil 3.2. Algoritmalarına göre şifreleme teknikleri [73]

Algoritması gizli olan şifreleme teknikleri

Bir algoritmanın güvenliği, bu algoritmanın çalışma biçimini gizlemeye dayalıysa, bu bir gizli algoritmadır (private key encryption). Geçmişte ilgilenilen kriptografi algoritmaları algoritmanın gizliliğine dayanmaktaydı. Gizli algoritmalar günümüzün şartlarına pek uymamaktadır. Bir gruptan her kullanıcı çıkışında, birisi yanlışlıkla ya da bilinçli olarak kullanılan algoritmayı açığa vurduğunda, geri kalan herkesin başka bir algoritmaya geçmesi gerekmektedir. Daha da kötüsü, gizli algoritmalar kalite kontrolüne ve standardizasyona olanak tanımamaktadır. Ciddi eksiklikleri olmasına rağmen, gizli algoritmalar düşük güvenlik gerektiren uygulamalarda sık sık kullanılmaktadır [68].

Literatürde bulunan en ilkel şifreleme algoritmaları sadece alıcı ile gönderen arasında bilinen ve birbirinin tersi olan gizli bir algoritmaya dayanmaktadır. Bu tip algoritma ilk defa Sezar tarafından generallerine mesaj göndermek için kullanılmıştır. Her bir karakteri belirli bir miktar kaydırma prensibine dayanmaktadır. Bu şifreleme türünün diğer örnekleri ise Yer değiştirme ve Alfabe değiştirme şifreleridir [73].

Algoritması açık olan şifreleme teknikleri

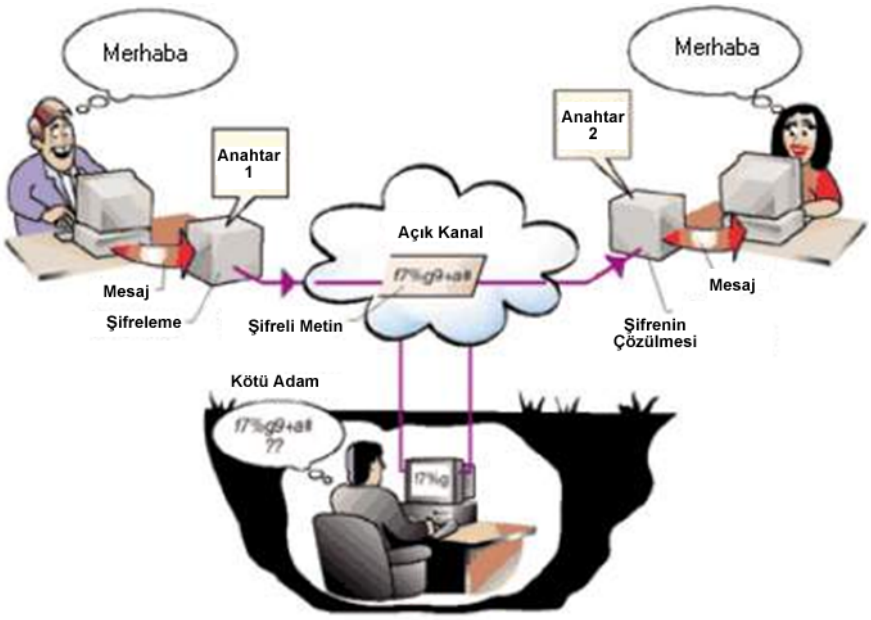
Şifreleme algoritmalarının geniş bir kullanım alanına sahip olabilmesi için standart hale getirilmesi gerekir. Gizli algoritmaya dayalı şifreleme sistemleri, algoritmanın gizliliğinin sağlanması zorunluluğu nedeniyle sadece sınırlı bir kullanım alanına sahiptir ve standart hale getirilmesi mümkün değildir. Özellikle, bankalar ve elektronik ticaret siteleri gibi yaygın iletişim ağlarına sahip kuruluşlar için gizli algoritmaya dayalı şifreleme sistemleri uygun değildir. Ayrıca, şifreleme sisteminin güncellenmesi gerektiğinde gizli algoritmaya dayalı şifreleme sistemleri esnek bir yapıya sahip olmadıklarından eski sistemin tamamen kaldırılıp yerine yenisinin kurulması gerekir. İşte bu standart hale getirme ve güncelleme gereksinimini karşılamak için algoritması herkes tarafından bilinen şifreleme sistemleri tasarlanmıştır(public key encryption). Bu tip şifreleme sistemlerine, açık metin sadece gönderen ile alıcı tarafından bilinen bir anahtarla şifrelendiği için bir anahtara dayalı şifreleme sistemi denilir. Modern şifreleme tekniklerinin büyük bir çoğunluğu açık algoritmaya sahip teknikler kullanırlar [73].

3.3.2. Anahtar sayısına göre şifreleme teknikleri

Bu algoritmalar güvenliklerini kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlarlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanır [72].

Bu algoritma türünde anahtarların hiçbiri algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenebildiği anlamına gelmektedir. Bu

algoritmayı kullanan ürünler seri üretilmektedir. Günümüzde kullanılmakta olan modern ve güçlü şifreleme algoritmaları artık gizli değildir. Bu algoritmalar güvenliklerini kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlamaktadırlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanmaktadır. Bir anahtar ile şifrelenmiş bilgi, kullanılan algoritmaya bağlı olarak, ilgili anahtar ile çözülebilir [73]. Genel olarak anahtarın kullanımı şu şekildedir (Şekil 3.3.):



Şekil 3.3. Bir mesajın dinlenmesini önlemek için anahtar ile şifreleme [74]

Kullanıcı bir mesajı "Merhaba" göndermeden önce bir anahtar (Anahtar1) kullanarak şifrelemektedir. Şifreli metin yasadışı dinleyicilere açık olan bir kanaldan gönderilmektedir. Mesajı okumak için alıcı bir anahtar (Anahtar2) kullanarak şifreyi çözmekte ve "Merhaba" mesajını elde etmektedir. Aktif düşmanlar araya girip iletişimi dinleyebilir.

Eğer Anahtar1 ve Anahtar2 eşitse, sistem simetriktir. Aksi takdirde bu sistem asimetrik olarak nitelenir. Güvenliğin garantilenmesi için Anahtar2 her zaman gizli olmalıdır, ancak Anahtar1'i kullanarak Anahtar2'yi elde etmek mümkün olmadığı

sürece Anahtar1 açıklanabilir. Bu durumda sisteme açık anahtarlı sistem (public key system) adı verilir [72].

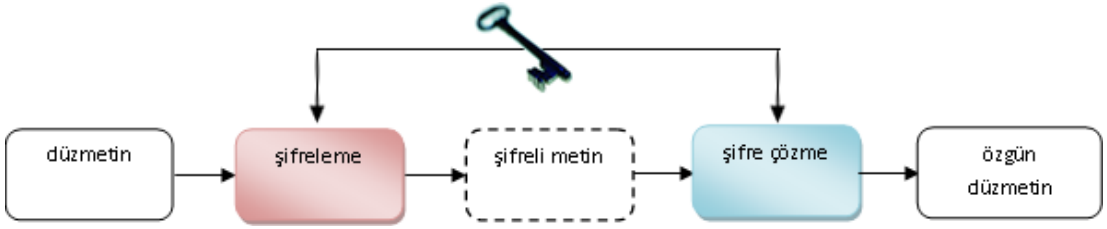
Anahtara dayalı şifreleme sistemleri anahtar sayısına göre simetrik ve asimetrik şifreleme teknikleri olarak ikiye ayrılır.

Simetrik şifreleme teknikleri

Anahtara dayalı simetrik şifreleme tekniğinde, hem şifreleme hem de çözme işlemi için tek bir anahtar kullanılır. Aynı zamanda bu teknik; şifreleme işleminde kullanılan anahtarı, gönderen ve alıcıdan başka kimsenin bilmemesi gerektiği için, gizli anahtar anonim anahtar ya da özel anahtar şifreleme olarak da adlandırılır. Ayrıca şifreleme ve çözme işlemlerinde tek bir anahtarla birbirinin simetriği olan algoritmalar kullanarak gerçekleştirildiğinden simetrik şifreleme teknikleri olarak da bilinirler [73].

Simetrik algoritmalar asimetrik algoritmalara nazaran daha hızlı çalışırlar. Bununla beraber, asimetrik algoritmalara nazaran saldırıya karşı daha az dirençlidirler. Simetrik algoritmalara örnek olarak AES, DES, 3DES, Blowfish, IDEA ve RC4 algoritmaları verilebilir [75-77]. Şekil 3.4'de simetrik şifrelemenin genel işleyişi görülmektedir.

Bu sistemlerin üstünlüğü hızı, zayıflığı ise ortak anahtarların belirlenmesi ve taraflara iletilmesinde karşılaşılan problemlerdir [72].



Şekil 3.4. Simetrik şifreleme

Örneğin; Gizli Anahtarlı Kriptografi ile haberleşmenin nasıl olduğunu inceleyelim:

X ve Y mektuplarını diğerleri için anlaşılmaz kılacak bir yöntem üzerine gizlice anlaşırlar. Örneğin, bütün kelimelerin tersten yazılacağına (AYŞE yerine EŞYA), veya her harften sonra rasgele bir harf konulacağı kararlaştırılabilir (AYŞE yerine AFYTŞMEN). Yöntemin bulunması durumunda bütün iletişimler çözülecektir. Farklı kişilerle iletişim kurmak istenirse, her kişi ile farklı yöntemler üzerinde anlaşılması gerekir. Birçok kişinin şifreyi bilmesi gerekiyorsa, güvenlik için sık sık yöntemin değiştirilmesi gerekebilir. Yeni yöntemler bulmak ise sanıldığından daha zordur.

Bu aşamada, temel işleyişi sabit olan ama parametrelenebilir bir yöntem gerekir. Artık birden fazla kişi ile temel mekanizma üzerinde, gizliliğe gerek duymadan anlaşabilirsiniz; gizli olarak anlaşmanız gereken tek kısım, şifreleme yönteminin değişken (şifreleme anahtarı) kısmıdır. Bu anahtar ile şifrelenmiş bir verinin güvenliği kullanılan anahtarın gizliliği ile doğrudan ilişkilidir.

Düşünülebilinecek en basit simetrik şifrelerden biri Sezar Şifresidir. Eski Roma İmparatoru Sezar'ın kullandığı bu şifre bütün kriptolojiye giriş yazılarının standart örneğidir. Sezar Şifresini kullanmanın basit bir yolu, alfabenin bütün harflerini bir kâğıt şeridi üzerine yazıp, şeridin başını sonuna yapıştırmaktır. Gizli Anahtar olarak (veya şifrenin değişkeni) olarak, bir ile alfabemizdeki harf sayısı eksi bir arasında bir *n* sayısı seçilir. Metinimizi şifrelemek için, harfleri teker teker alırız; şeritin üzerinde o harfin yerini bulup, sağa doğru *n* tane harf atlarız; şifreli metinimizde ise o harfin yerine bulduğumuz yeni harfi buluruz. Şifreyi çözmek için, aynı işlemi, şeriti aksi yönde çevirerek gerçekleştiririz. Tabi şifreyi çözebilmek için, haberleşen kişilerin birbirine gizlice *n* sayısını iletmeleri gerekir.

Türk alfabesi kullanarak n=10 için Sezar Şifresine bir örnek verelim;

Çözüm Şeridi : A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z
Şifreleme Şeridi: N O Ö P R S Ş T U Ü V Y Z A B C Ç D E F G Ğ H I İ J K L M

Açık Metin : BUGÜNHAVAÇOKGÜNEŞLİ
Şifreli Metin : İEOFVPIGIKYTOFVMÇUS şeklinde olacaktır.

Sezar Şifresi tek alfabeli yer değiştirme veya permütasyon şifreleri arasında değerlendirilir. Kullanılan simetrik şifrelerin çoğu parametrelenebilir bir permütasyon olarak değerlendirilebilir.

Simetrik tekniğini kullanan algoritmalara örnek olarak XOR Şifreleme, DES, 3DES, IDEA, RC2, RC4, RC5, AES algoritmaları verilebilir. Bunların en meşhuru Veri Şifreleme algoritması (Data Encryption Algorithm) olarak da bilinen DES'tir [73].

XOR Şifreleme: Akan şifre sistemleri, mesajın her karakterini (bitini) ayrı ayrı şifreler. Şifreleme işlemi mesaj uzunluğunda bir anahtar kullanılarak yapılır. Anahtarın her biti mesajın her bitiyle mod 2'de karşılıklı toplanır. Bu işleme XOR işlemi denir.

DES (Data EncryptionStandard): En çok kullanılan şifreleme tekniği 1977'de şimdiki adı Ulusal Standart ve Teknolojiler Enstitüsü olan Ulusal Standartlar Bürosunda ortaya atılan Veri Şifreleme Standardıdır (DES).Askeri amaçlı olmayan çalışmalarının ilki ve şifreleme algoritmalarının yeni bir boyut kazanmaya başladığı nokta olarak kabul edilen DES (Data Encryption Standard) bir veri şifreleme standardıdır. Kriptolojinin ve kriptoanalizin askeri olmayan çalışmalarının başlangıcı olarak kabul edilmektedir.

DES' de veri, 56-bitlik bir anahtar kullanılarak 64-bitlik bloklar halindeşifrelenir. Algoritma, 64-bitlik bir girişi bazı aşamalar sonucu 64-bitlik bir çıktı oluşturacak şekilde dönüştürür. Şifrelemeyi geri almak için aynı adımlar, aynı anahtar kullanılarak işlenir. DES' in çok geniş bir kullanım sahası vardır [78].

3DES algoritması: 3DES (Üçlü DES), 1978 yılında IBM tarafından geliştirilmiş olan bir şifreleme algoritmasıdır. Brute Force saldırılara karşı koymakta zorlanan DES (Data Encryption Standard-Veri Şifreleme Standardı) algoritmasının üzerine

geliştirilmiştir. Üç anahtarlı üçlü DES, 168 (3x56) bitlik bir etkin anahtar uzunluğuna sahiptir.Bankacılık sistemi, Ciddi güvenlik programları, Elektronik ödeme sistemlerinde(kredi kartıyla internetten alışveriş yapma gibi) kullanılmaktadır.

IDEA (International Data EncryptionAlgorithm): Şifreleme yapısı hem donanım hem de yazılım uygulamalarında kullanılabilecek şekilde tasarlanmıştır. IDEA, 128 bit uzunluklu bir anahtar ve her biri 16 bit uzunluğunda 52 alt-anahtar kullanmaktadır. Bualt-anahtarlar, her bir aşamada iki tane, her bir aşamadan önce ve son aşamadan sonra dört taneolmak üzere kullanılır. Toplam sekiz aşama bulunmaktadır [69].

RC5 (RivestCipherVersion 5): RSA grubu tarafından geliştirilmiş anahtar uzunluğu değişken bir yöntemdir. Anahtar uzunluğu 56, 64 veya 128 bit olabilir.

Simetrik şifreleme tekniğinde gizli anahtarın taraflar arasında iletilmesi problemi bulunmaktadır. Bu gizli anahtar taraflar arasında iletilirken istenmeyen kişiler tarafından ele geçirilebilir.

Polybius Algoritması: Antik yunanda, Polybius ismindeki kişi tarafından bulunan iki boyutlu bir tahtaya dayalı şifreleme sistemidir.

Bu sistemin özelliği, alfabedeki harflerin, iki boyutlu bir tabloya yerleştirilmesi ve ardından bu tablodaki satır ve sütun numaralarına göre okunmasıdır. Çizelge 3.1'de İngiliz alfabesindeki harfler için aşağıdaki gibi bir tablo gösterilmiştir.

Çizelge 3.1. İngiliz alfabesindeki harfler

	1	**2**	**3**	**4**	**5**
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I/J**	**K**
3	**L**	**M**	**N**	**O**	**P**
4	**Q**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Görüldüğü üzere, İngilizcede bulunan 26 harf, 5×5 = 25 boyutlarında bir tabloya yerleştirilmiş, dolayısıyla da bir hücreye iki harf I/J yerleştirilmesi gerekmiştir. Polybius şifrelemede kullanılan ızgara yukarıda ifade edildiği gibi 5 × 5 birimlik değil, kullanılan alfabe hatta şifrelenecek metnin içerdiği alfabe harfleri sayısına bağlı olarak istenen boyutta (n × m) tasarlanabilir [79].
Aynı tabloyu, örneğin Türkçe için uyarlarsak, çizelge 3.2'deki gibi bir tablo olabilir:

Çizelge 3.2. Türk alfabesindeki harfler

	1	**2**	**3**	**4**	**5**
1	**A**	**B**	**C/Ç**	**D**	**E**
2	**F**	**G/Ğ**	**H**	**I/İ**	**J**
3	**K**	**L**	**M**	**N**	**O/Ö**
4	**P**	**R**	**S**	**Ş**	**T**
5	**U**	**Ü**	**V**	**Y**	**Z**

Bu tablolardaki hücrelerin, hangilerinde çift harf olacağı tamamen rast gele seçilmiştir.

Şifreleme sisteminin çalışması

Şifreleme sırasında, sistem, basitçe her harf için iki sayıdan oluşan bir sonuç üretmektedir. Örneğin "gazi" kelimesini şifrelemek için her harfin satır ve sütun numaraları kullanılarak,
g harfi için, 2 satır ve 2 sütun – 22

a harfi için, 1 satır ve 1 sütun – 11

z harfi için, 5 satır ve 5 sütun – 55

i harfi için, 2 satır ve 4 sütun – 24

değerleri elde edilmektedir. Sonuçta bu değerler birleştirildiğinde şifreli mesaj elde edilmiş olacaktır.

gazi – 22115524

Bazı kaynaklarda, şifreli mesaj 22-11-55-24 şeklinde – işareti ile ayrılarak gösterilmektedir. Bunun tek amacı okumayı kolaylaştırmaktır.

Sistemin şifreyi açması

Şifrelenmiş mesaj açılırken tablo, tersten kullanılmaktadır.
Açmak istenen mesaj 22115524 ise,

İlk sayı 2, (2. satır), ikinci sayı 2 (2. sütun) – g

Üçüncü sayı 1, (1. satır) bakıyoruz, dördüncü sayı 1 (1. sütun) – a

Beşinci sayı 5, (5. satır), altıncı sayı 5 (5. sütun) – z

Yedinci sayı 2 (2. satır), sekizinci sayı 4 (4. sütun) – i

Sonuç olarak açık mesaj "gazi" olarak elde edilmektedir

Polybius şifrelemesine saldırı

Sistemin çalışması bir yerine koyma (substitution cipher) özelliği göstermektedir. Her harf, bir (iki basamaklı) sayı ile değiştirilmektedir. Dolayısıyla yerine koyma için geçerli olan bütün saldırı yöntemleri, bu sisteme karşı da kullanılabilmektedir [80].

Sonuç olarak, simetrik anahtarlı sistemlerin üstünlükleri ve zayıflıkları şöyle sıralanabilmektedir;

Üstünlükleri;

- Çok hızlıdır. Şifrelenmiş verinin bir yere gönderilmediği durumlarda kullanışlıdır. Mesaj şifreleme hızının araştırıldığı bir çalışmada simetrik şifreleme algoritmalarından AES algoritması kullanılmıştır [81].
- Şifrelenmiş verinin gönderilmesi sırasında şifrenin gizli tutulması maliyeti artıran bir uygulamadır.
- Bu tasarımda gönderici ve alıcı bir anahtar üzerinde anlaşmalı ve bu anahtar aralarında gizli kalmalıdır [64].

Zayıflıkları;

- Eğer kullanıcılar farklı yerlerde ise gizli anahtarın gönderilmesi sırasında hatların güvenliğinden emin olunmalıdır.
- Herhangi birisi anahtar değerini dinleyebilir ya da değiştirebilir.
- Burada ana problem anahtar dağıtma problemidir [64].

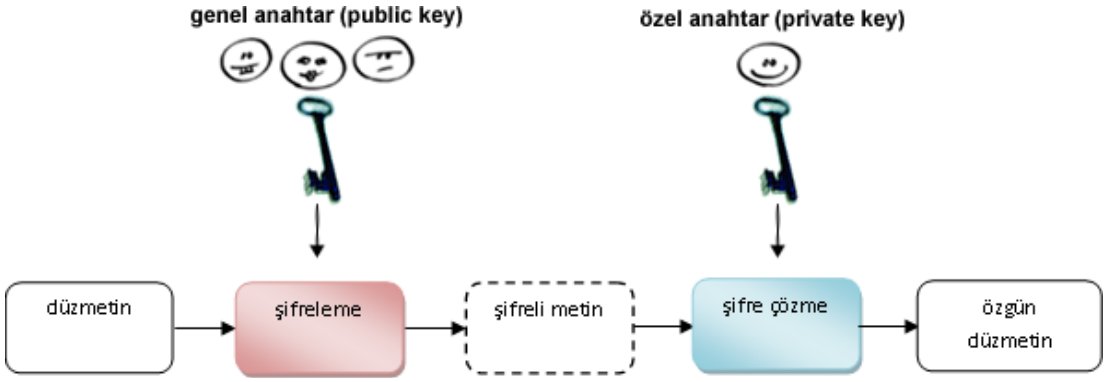
Simetrik şifreleme yöntemleri kullanılırken ortaya çıkan anahtar dağıtım problemine çözüm olarak bir şema geliştirilmiştir. Bu şemada kullanıcı kimlik doğrulamasına eş zamanlı olarak anahtar dağıtımı sağlanmaktadır. Bu şema yapılabilecek saldırılara karşı korunmaktadır. Böylece anahtar dağıtım problemi ortadan kalkmakta ve simetrik anahtar şifreleme yöntemleri asimetrik anahtar şifreleme yöntemlerine göre sınırlı donanıma sahip terminallerde kolayca uygulanabilmektedir [82].

Asimetrik şifreleme teknikleri

Asimetrik şifreleme, simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi olarak geliştirilmiştir. Asimetrik Anahtarlı Kriptografi Açık Anahtarlı Kriptografi olarak da adlandırılmaktadır.

Şifreleme ve çözme işlemi birbirinin simetriği olmayan (yani aynısı olmayan) algoritmalarla gerçekleştirildiğinden dolayı da asimetrik şifreleme sistemi olarak bilinir [83].

Açık Anahtarlı Kriptografi tek anahtar kullanan simetrik şifreleme algoritmalarının yerine iki ayrı anahtarın asimetrik kullanımını öngörür. Bu sistemde her bir kişi iki ayrı anahtar edinir. Bu anahtarlardan biri kamusal anahtar (public key), diğeri ise özel anahtar (private key) olarak adlandırılır. Açık anahtar kişinin şifreli iletişim kuracağı kişilere iletilir yani herkesin erişimine açıktır, gizli anahtar ise sadece sahibinin erişebileceği şekilde saklanmalıdır. Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır, fakat anahtarlardan birini kullanarak diğerini bulmak çok zor hatta imkânsızdır. Şekil 3.5'te asimetrik şifrelemenin genel işleyişi görülmektedir.



Şekil 3.5. Asimetrik şifreleme

Asimetrik kriptografinin iki temel kullanımı vardır, şifreleme ve sayısal imza. Bu sistemde her kişi biri açık, diğeri gizli olmak üzere bir çift anahtar edinir. Açık anahtar herkesin erişimine açıktır, gizli anahtar ise sadece sahibinin erişebileceği şekilde saklanmalıdır. Burada gönderenin ve alıcının aynı gizli bilgiyi tutma durumu ortadan kalkmıştır. Bütün iletişim sadece açık anahtarları gerektirir, gizli anahtarlar ne iletilir ne de paylaşılır. Bu sistemde, kaygı duyulacak tek nokta açık anahtar ve anahtar sahibinin güvenilir ve doğru şekilde eşleştirilmesidir. Açık anahtarı kullanarak herhangi bir kişi şifreli mesaj gönderebilir, ancak gönderilen şifreli mesajı sadece kullanılan açık anahtarın eşi olan gizli anahtar açabilir. Bundan başka,

asimetrik kriptografi sadece gizliliği (şifreleme) sağlamak amacıyla değil, kimlik denetimi (sayısal imza) ve daha birçok teknik için kullanılır [57].

Asimetrik sistemler pek çok ilginç olanaklar sunar; örneğin herkes online bir mağazaya mağazanın açık anahtarını kullanarak şifrelenmiş bir kredi kartı numarası gönderebilir. Özel anahtarı sadece mağaza bildiği için, kartın numarasını sadece mağaza öğrenebilir. Eğer simetrik sistem kullanılsaydı, mağaza potansiyel müşterilerinin her biriyle önceden ve gizlice ayrı ayrı anahtarlar belirlemek zorunda kalırdı [84].

Örneğin, Ayşe'nin Ahmet'e m mesajını göndermek istediğini farz edelim. Ayşe, m mesajının üssünü alarak, $c=m^e \pmod n$, c şifreli mesajını elde eder. Burada kullanılan (n,e) Ahmet'in açık anahtarıdır. Bu işlemleri yaptıktan sonra Ayşe şifreli c mesajını Ahmet'e gönderir. Ayşe aynı şekilde gelen şifreli mesaj c'nin üssünü alır. $m=c^d \pmod n$ Ancak bu sefer kendi gizli anahtarını kullanır. e ve d arasındaki bağlantı Ahmet'in doğru mesajı elde ettiğinin kanıtıdır. Ahmet'in gizli anahtarını sadece Ahmet bildiği için, gelen şifreli mesajı da sadece Ahmet okuyabilir.

Asimetrik şifreleme algoritmalarına örnek olarak RSA, DSA, Diffie-Helman, El Gamal verilebilir. Bunlardan en yaygın olarak kullanılanı RSA dır.

RSA şifreleme sistemi: Bir genel anahtarlı şifreleme tekniği olan RSA, ismini mucitlerinin baş harflerinden(Ronald L.Rivest, Adi Shamir ve Leonard Adleman) almıştır.

RSA, çok büyük tamsayıları oluşturma ve bu sayıları işlemenin zorluğu üzerine kurulmuş bir yapıdır. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. RSA'nın güvenliği çarpanlara ayırma probleminin zorluğuna dayanır. RSA en çok test edilen algoritmalardan biridir. Kullanılan anahtarlar yeteri kadar uzun olduğunda güvenli olduğu düşünülür [67].

Bu algoritma genel anahtarlı şifreleme ve dijital imza işlemlerinde güvenli bir şekilde kullanılır. Bu algoritma aynı zamanda Netscape Navigator ve Microsoft Internet Explorer web browser programlarının uygulamaları olan Secure Socket Layer (SSL) ve kredi kartı işlemleri için Secure Electronic Transaction (SET) protokolü ile Mastercard ve VISA uygulamalarında kullanılmaktadır. Ayrıca S/MIME, PEM, MOSS ve PGP gibi gizli haberleşme protokolleri temel olarak RSA kullanır.

DSA: NIST (National Institute of Standardsand Technology) tarafından sayısal imza standardı (Digital Signature Standard) olarak yayınlanmıştır. DSA "discrete logarithm (ayrık logaritma)" problemine dayanır. DSA algoritması da, RSA gibi asimetrik bir kriptografik algoritmadır. RSA'dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır.

Diffie-Helman algoritması: İnsanlığa ilk duyurulan açık anahtar algoritması, Diffie ve Hellman`ın açık anahtarlı kriptografi olarak tanımladıkları 1976 yılında yayımlanmış "New Directions in Cryptography" isimli makalelerinde yer almıştır. Birçok ticari uygulama bu anahtar değişimini kullanmıştır fakat günümüzde çok sık kullanılmamaktadır.

Diffie-Hellman ortak gizli anahtar oluşturma sistemi ayrık logaritma problemini üzerine kurulmuş ve güvenirliği çok büyük asal sayıları seçmeye dayanmaktadır [85].
Algoritmanın amacı, iki kullanıcının bir anahtarı güvenli şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Algoritma anahtar değişimi ile sınırlıdır.

*ElGamal algoritması***:** El Gamal yöntemi hem sayısal imza hem de şifreleme için kullanılmaktadır. Sistemin güvenliği ayrık logaritmaların hesaplanması probleminin zorluğuna dayanmaktadır.

Açık anahtar şifrelemesi Diffie-Hellman'ın paylaşılmış gizli bilgi üretimi üzerindeki orijinal fikrin geliştirilmiş halidir. Esasen, ortak bir gizli bilgi üretmekte ve bir blok veriyi şifrelemek için bunu tek-zamanlı bir pad gibi kullanmaktadır.“

Mobil telefonlarda asimetrik şifreleme algoritmalarının güvenlik gücü, şifreleme ve deşifreleme hızını kıyaslamak ve en verimli algoritmayı bulmak amacıyla birçok çalışma yapılmıştır.

Yapılan bir çalışmada RSA, Elgamal ve Eliptik eğri şifreleme teknikleri karşılaştırılmıştır. Deneysel sonuçlar her algoritmanın etkinliğini göstermek ve SMS şifreleme için en uygun algoritmayı seçmek için sunulmaktadır. Algoritmaların güvenlik gücü karşılaştırıldığında, RSA ve ELGamal eşit iken Eliptik eğri ise benzer güvenlik gücünü daha kısa anahtar uzunluğu ile sağlamıştır. Eliptik eğrilerin güvenlik gücü daha yüksek olmasına rağmen şifreleme ve deşifreleme hızına bakıldığında en yavaş olduğu görülmektedir. Uzun anahtar boyutlu algoritmalar SMS şifrelemede kısıtlı hafızadan dolayı SMS şifreleme için kullanışlı değildir. Eliptik eğrinin, küçük anahtar uzunluğu ile daha yüksek güvenilirlik sağlaması RSA ve ELGamal’a göre üstünlüğüdür. Bizim çalışmamızda özel anahtar kullanılmıştır ve anahtar uzunluğu arttıkça güvenilirlik artmaktadır [86].

Asimetrik şifreleme yöntemlerinin kıyaslandığı bir başka çalışmada çok uzun anahtar kullanılmadığı sürece RSA ve DSA kripto sistemlerinin ECDSA’dan daha iyi performans gösterdiği saptanmıştır. ECDSA’nın ise RSA’dan daha hızlı olduğu görülmüştür. Sonuç olarak güvenlik gücü ile hızın doğru orantılı olmadığı saptanmıştır [87].

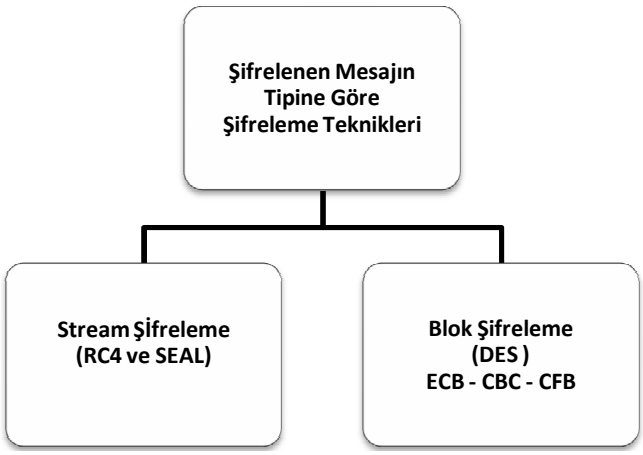
İşlemcisi ARM9 mimarisine sahip, 209 Mhz işlemci hızına sahip, Nokia N80 mobil telefonda bir çalışma gerçekleştirilmiştir. Çalışma platformu olarak Symbian OS seçilmiştir. Bu çalışmada asimetrik şifreleme yöntemlerinden RSA kullanılarak, SMS şifreleme uygulaması geliştirilmiştir. Bu program ek şifreleme cihazlarına ihtiyaç duymadan, mobil telefonlarda çalışabilmektedir. Gelecekte, şifrelemenin

MMS güvenliği için geliştirilebileceği ve kullanıcılar arasında daha büyük dağıtımlar için uygulamanın diğer platformlara taşınabileceği belirtilmiştir [88].

Birbirlerine göre çeşitli üstünlükleri olmakla birlikte simetrik şifreleme ile asimetrik şifreleme yöntemlerinin bir arada kullanıldığı protokoller de geliştirilmiştir. SMS'in iletişim güvenliğini sağlamak için Java programlama dili kullanılarak SMSSec olarak adlandırılan bir protokol önerilmektedir. SMSSec iki aşamalı bir protokoldür ve bu protokol içerisinde hem asimetrik hem de simetrik şifreleme kullanılmaktadır [89].

3.3.3. Şifrelenecek mesajın tipine göre algoritmalar

Şifreleme sistemlerinde, algoritmanın gizliliği ve anahtar kullanımından başka mesajın hangi biçimde şifreleneceği de önemlidir ve bu kritere göre şifreleme teknikleri iki kısma ayrılmaktadır. Şekil 3.6'da şifrelenecek mesajın tipine gör algoritmalar gruplandırılmıştır.



Şekil 3.6. Şifrelenecek mesajın tipine göre algoritmalar [63]

Akan şifre algoritmaları (Streamcipher)

Düz metin üzerinden tek bit olarak çalışır yani; belli bir anda bir bitlik (veya bazen sekiz bit) düz-metni şifreleyebilir. Bu algoritmalar mesajı bit bit ya da bayt-bayt ele alıp şifrelemektedirler. Yani arka arkaya gelen bir veriyi şifreleme işlemi bir

periyotta akan arka arkaya gelen girdi veriler için bir eleman üreten işlemdir. Bu algoritmaların en önemlileri RC4 ve SEAL algoritmalarıdır.

Blok algoritmalar (BlockCipher)

Blok şifreleme algoritmaları veriyi bloklar halinde işlemektedir. Pek çok biti alıp (tipik olarak modern cipher'larda 64 bit), bunları tek bir birim olarak şifreler. Yani bir blok şifreleme işlemi, bir periyotta bir girdi bloğu için bir çıktı bloğu üreten işlemdir. Bit gruplarına bloklar denir. Algoritmaların büyük çoğunluğu blok şifreleme kullanmaktadır.

Blok şifreleme stream şifrelemeye göre daha güvenlidir. Çünkü blok halinde şifrelenen verilerin içerisinden karakterleri tahmin etmek mümkün değildir.

3.3.4. Kullanım alanına göre şifreleme uygulama çeşitleri

Şifreleme uygulamaları, aşağıdaki gibi gruplandırılabilir:

1. *Gizliliği Sağlayan Şifreleme Uygulamaları:* Bu tip uygulamalar gönderilen verinin içeriğine yetkisiz kişiler tarafından erişilmesine karşı korunmasını sağlarlar. Buna örnek olarak gizli mesajlaşmayı ve şifreli e-mail göndermeyi sağlayan PGP yazılımı verilebilir.

Ayrıca elektronik alış verişte kullanıcı, web server, banka arasındaki iletişimin gizliliğini sağlayan SSL ve SET güvenlik protokolleri kullanılmaktadır. Bu tip verilerin şifrelenerek iletişimini sağlayan uygulamalarda şifreleme ve çözme işlemlerinin harcadığı zaman önemli olduğu için simetrik şifreleme algoritmaları kullanılır. Bu uygulamalarda asimetrik şifreleme algoritmaları daha fazla güvenlik sağlasa da işlem zamanının büyüklüğünden dolayı tercih edilmemektedir.

2.Veri Bütünlüğünü Sağlayan Uygulamalar: Bu uygulamalar gönderilen verinin yetkisiz kişiler tarafından değiştirilmesini veya iletim sırasında bozulmasını tespit etmeye yönelik alınmış önlemlerdir. Bunlara dijital imza kullanarak imzalı mesaj gönderen uygulamaları (örneğin PGP) verebiliriz. Dijital imzalar mesaj ya da dökümlerin içeriğinin değişip değişmediğini sorgulamayı mümkün kılar.

3. İnkar Edememeyi Sağlayan Uygulamalar: Bu uygulamalar verinin gönderen tarafından daha sonra gönderdiğini inkar edememesini sağlarlar. İnkar edememeyi sağlayan uygulamalar dijital sertifika ve dijital imza sistemini kullanırlar. Örneğin SSL ve SET ile iletişimi sağlayan bir web sitesinden yapılan alış veriş dijital sertifikaya dayalı olarak gerçekleştiğinden dolayı inkar edilemez. Özel anahtar tabanlı sistemlerin inkar edememeyi sağlaması ortak anahtar kavramından dolayı imkansızdır. Çünkü gönderici gönderdiği bir mesajın alıcı tarafından uydurulduğunu iddia edebilir, alıcı da aynı anahtarı bildiği için bu durumun aksini ispatlayamaz. Açık anahtar tabanlı sistemlerde ise şifreleme anahtarı ile şifreyi çözme anahtarı farklı anahtarlar olduğundan inkar edememe sağlanabilir. Bunun en güzel örneği dijital imzalardır.

4. *Doğrulama Uygulamaları*: Bu uygulamalar verinin yetkisiz veya tanınmayan bir kişiden gönderilmesini tespit etmeye yönelik alınmış önlemleri kapsamaktadır. Bunlara kredi kartı bilgilerinin doğruluğunu sağlamada ve bir sisteme girişi denetlemede kullanılan asıllama sistemleri verebiliriz. Bunlar da dijital sertifika sistemlerini kullanırlar. Dijital imza ve dijital sertifika sistemleri ancak asimetrik şifreleme algoritmaları ile gerçekleştirilebilmektedir [55].

3.3.5. Şifreleme algoritmalarının performans kriterleri

Bir şifreleme algoritmasının performansı aşağıdaki kriterlere göre belirlenmektedir.

- Kırılabilme süresinin uzunluğu.
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı).

- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı).
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesi.
- Algoritmanın kurulacak sisteme uygunluğu.

Teorik olarak, simetrik anahtar kullanan şifreleme algoritmaları, olası bütün anahtarları sırasıyla denemek yoluyla kırılabilir. Olası anahtarların denenmesi işlemi de, anahtarın uzunluğu arttıkça güçleşecektir [66].

Çizelge3.3'de belirli anahtar uzunluklarına göre şifreyi deneyerek bulma zamanları verilmiştir.

Çizelge 3.3. Anahtar uzunluğuna göre şifreyi deneyerek bulma zamanları [66]

Anahtar Uzunluğu	**n**	**10^6 şifre/s hızında ortalama çözme süresi**	**10^9 şifre/s hızında**	**10^{12} şifre/s hızında**
32 bit	$4x10^9$	36 dak	2.16 s	2.16 ms
40 bit	10^{12}	6 gün	9 dak	1 s
56 bit	$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128 bit	$.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

3.3.6. Şifreleme algoritmaları seçim kriterleri

Şifreleme algoritması seçilirken aşağıdaki kriterlerden biri ya da her ikisine dikkat edilmelidir

- Şifrenin kırılmasının maliyeti şifrelenmiş bilginin değerinden fazla olmalıdır.
- Şifreyi kırmak için gereken zaman, bilginin yararlı ömründen fazla olmalıdır.

Eğer şifreleme yöntemi yukarıda sözü edilen iki kriteri karşılıyorsa bu yöntem hesaplama yönünden güvenilir olarak kabul edilmektedir.

3.4. Şifreli Metine Yönelik Gerçekleştirilen Bazı Saldırı Teknikleri

En önemli saldırı tekniklerinden bazıları aşağıda verilmiştir:

1. *Sadece şifreli metin saldırısı: Bu* saldırı tipinde, saldırıyı yapan kişinin elinde sadece şifreli metin vardır, mesajın içeriği hakkında hiç bir şey bilmemektedir. Amaç sadece şifreli metni kullanarak, düz metin ve anahtarı bulmaktır. Uygulamada düz metine (pek çok mesaj türü sabit başlık formatlarına sahip olduğundan) ilişkin tahminler yapmak genelde olasıdır. Sıradan mektuplar ve belgeler bile kestirilebilir bir şekilde başlamaktadır. Örneğin, pek çok klasik saldırıda şifreli metinin frekans analizi kullanılmaktadır, ancak modern şifreleme yöntemlerine karşı bu yöntem iyi çalışmamaktadır.

2. *Bilinen düz metin saldırısı:* Saldırganın elinde bir ya da daha çok sayıda şifreli metin ve bu metinlerin karşılığı olan düz metin vardır. Amaç bu mesajları şifreleyen anahtarı ya da anahtarları kullanarak oluşturulacak yeni mesajları çözebilmektir.En sık kullanılan Bilinen Düz Metin Saldırısı, blok şifrelemeye karşı lineer kriptanaliz saldırısıdır.

3. *Seçilmiş düz metin saldırısı:* Saldırgan bazı düz mesajları seçebilir ve bunların şifrelenmiş hallerini elde etmeye çalışır. Amaç diğer mesajları şifrelemede kullanılan anahtarı anlamak ve anahtarı kullanan yeni şifrelenmiş düz metinleri çözümlemektir. Bu saldırı için iyi bir örnek, blok cipherlara karşı (ve bazı durumlarda hash fonksiyonlarına karşı) uygulanabilen diferensiyel kriptanalizdir.Bazı kripto sistemler, özellikle RSA, seçilmiş-düz metin saldırılarına karşı açıktır. Bu tip algoritmalar

kullanıldığında, uygulama öyle tasarlanmalıdır ki saldırgan istediği düz metni şifrelenmiş olarak elde etmemelidir.

4. *Ortadaki adam saldırısı:* Bu saldırı, kriptografik iletişim ve anahtar değişimi protokolleri ile ilgilidir. Fikir şudur; iki kişi güvenli iletişim için anahtarlarını değiş-tokuş ederken (örneğin Diffie-hellman kullanarak), bir düşman kendisini iletişim hattındaki iki kişi arasına yerleştirir. Sonra bu düşman her iki kişi ile ayrı bir anahtar değiş tokuşu gerçekleştirir. Her iki kişi farklı bir anahtar kullanarak işlerini tamamlayacaklardır ki bu anahtarlar düşman tarafından bilinmektedirler. Bu noktadan sonra saldırgan uygun anahtar ile herhangi bir iletişimi deşifre edebilecek ve bunları diğer kişiye iletmek için diğer anahtar ile şifreleyecektir. Her iki tarafta güvenli bir şekilde konuştuklarını sanacaklardır, ancak gerçekte saldırgan konuşulan her şeyi duymaktadır.

Kullanılan şifreleme algoritması bilinmese bile genellikle saldırganın şifreleme algoritmasını bildiği kabul edilmelidir. Bu özelliğe dayanarak muhtemel saldırılardan biri, olası tüm anahtarları denemek olan '*Brute force*' yaklaşımıdır. Bu yüzden saldırgan değişik istatistiksel uygulamalar, çeşitli testler yapmak zorundadır.

4. MOBİL TELEFONLAR İÇİN POLYBIUS ALGORİTMASI İLE ŞİFRELİ MESAJLAŞMA UYGULAMASI

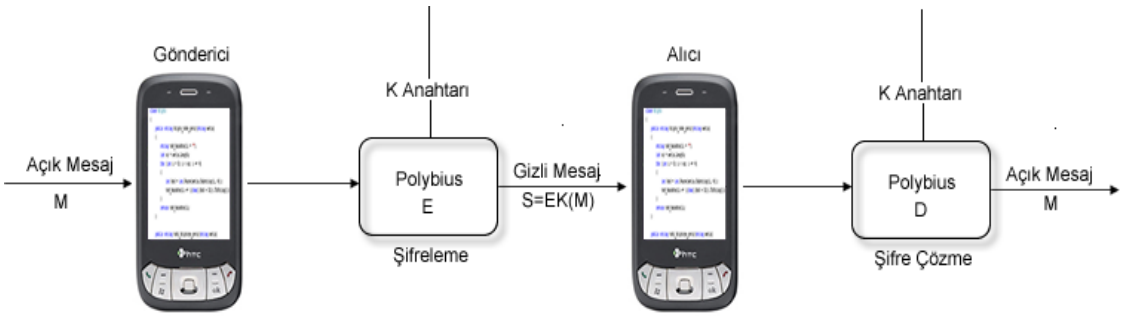
Bu çalışma ile cep telefonları için geliştirilen şifreli mesajlaşma uygulamasında, gönderilen mesajın güvenliğini arttırmak amacıyla şifreleme işlemi gerçekleştirilmiştir. Uygulama gerçekleştirilirken, simetrik şifreleme yöntemlerinden Polybius algoritması kullanılmıştır. Polybius algoritmasına ek olarak güvenliği arttırmak amacıyla yalnızca mesajı gönderen ve mesajı alan kullanıcının bildiği anahtar bilgisi eklenmiştir. Polybius algoritmasında 15x15'lik bir tablo kullanılmıştır. Kullanıcının girdiği anahtar bilgisi matematiksel işlemlere tabi tutularak, tablonun hangi satır ve sütununa karakterin yerleştirileceği belirlenmektedir. Bu yöntem ile tablo sürekli dinamik olmaktadır. Şifreleme algoritması ve anahtar sayesinde iki kişi arasında güvenli bir şekilde mesajlaşma gerçekleşmektedir. Üçüncü bir şahıs mesajı ele geçirse bile bu programı elde etmeden mesajı çözememektedir. Programı elde etse dahi anahtar bilgisi olmadan yine mesajı çözmesi mümkün olamamaktadır.

Bu çalışmada, yazılım geliştirme aracı olarak Visual Studio 2008 platformu ve c#.NET programlama dili kullanılmıştır.Programa AltugSec adı verilmiştir. Telefon olarak Windows Mobile 6.5 Professional işletim sistemi olan HTC telefon kullanılmıştır.

Şifreleme için gerekli Polybius algoritması c#.NET programlama dili ile yazılarak bağlantı kablosu ile uygulamanın geliştirileceği telefona yüklenmektedir. Hazırlanan program Windows Mobile İşletim sistemi olan cihaza yüklendikten sonra telefon klavyesinden girilen şifresiz(düz) mesaj ve şifreleme anahtarı Polybius algoritmasına gönderilmekte ve şifreleme işlemi gerçekleştirilmektedir. Şifreli mesaj göndericinin mesajın şifreli halini görebilmesi için ekranda görüntülenmektedir.

Göndericiden gelen şifreli mesaj alıcının program ekranında görüntülenmektedir. Alıcının şifre çözme anahtarını girmesinden sonra şifreli mesaj ve şifre çözme anahtarı Polybius şifre çözme algoritmasına gönderilmektedir. Şifresi çözülen mesaj

alıcının ekranında görüntülenmektedir. Şekil 4.1'de şifreli mesajlaşma uygulama blok şeması görülmektedir.



Şekil 4.1. Şifreli mesajlaşma uygulama blok şeması

Açık mesaj, verinin orijinal biçimdeki halidir. Dönüştürülmüş biçimine ise şifrelenmiş mesaj veya gizli mesaj denilmektedir. M açık mesajı, E ve D simgeleri de kriptolama ve kripto çözme işlemlerini, her iki ifadede kullanılan K ise, kripto anahtarını temsil etmektedir. Gönderici açık mesajı simetrik şifreleme yöntemlerinden Polybius algoritmasını ve kendi belirlediği K anahtarını kullanarak Eşitlik 4.1.'de ifade edilen gizli mesajı (S) elde etmektedir. Şekil 4.2'de açık mesajın gizli mesaj haline getirilmesi ile ilgili akış şeması görülmektedir.

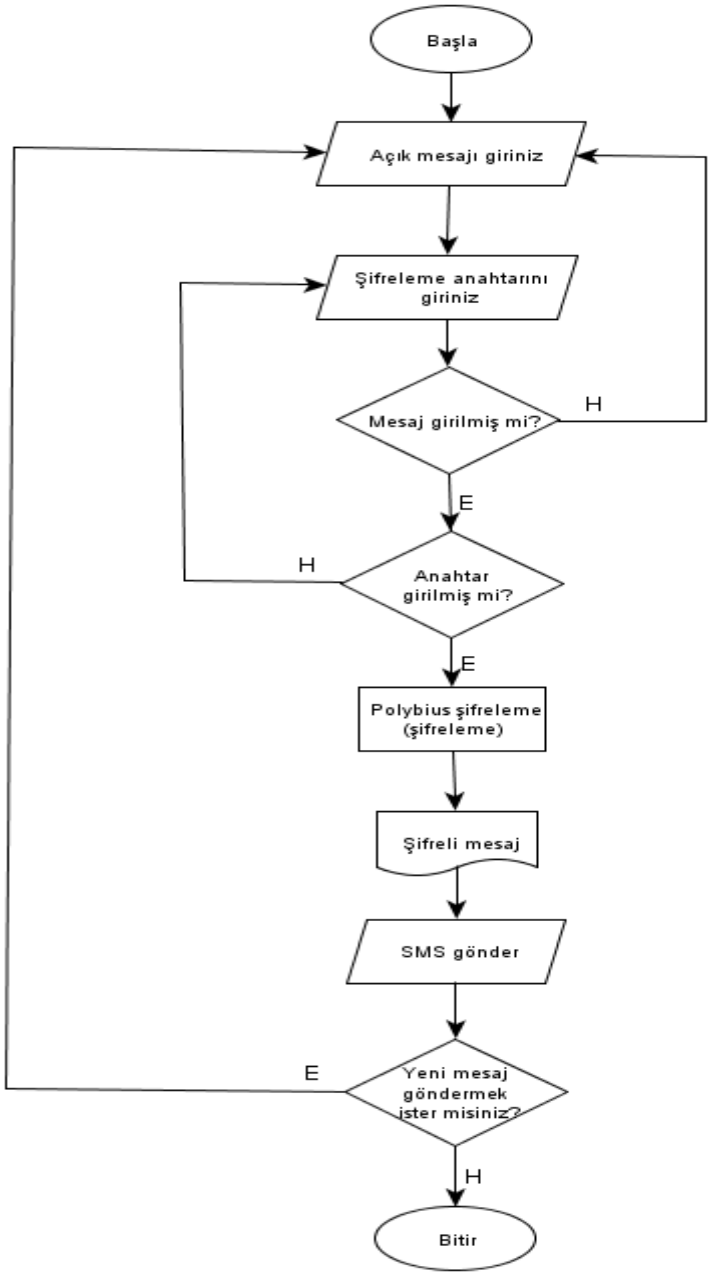
$$S = E_K(M) \tag{4.1}$$

Gizli mesajı alan alıcı yine simetrik şifreleme yöntemlerinden Polybius algoritmasını ve göndericinin kullandığı ve alıcının da bildiği K anahtarını kullanarak Eşitlik 4.2'deki açık mesajı (M) elde etmektedir. Gizli mesajın açık mesaj haline getirilmesi Şekil4.3'de gösterilmektedir.

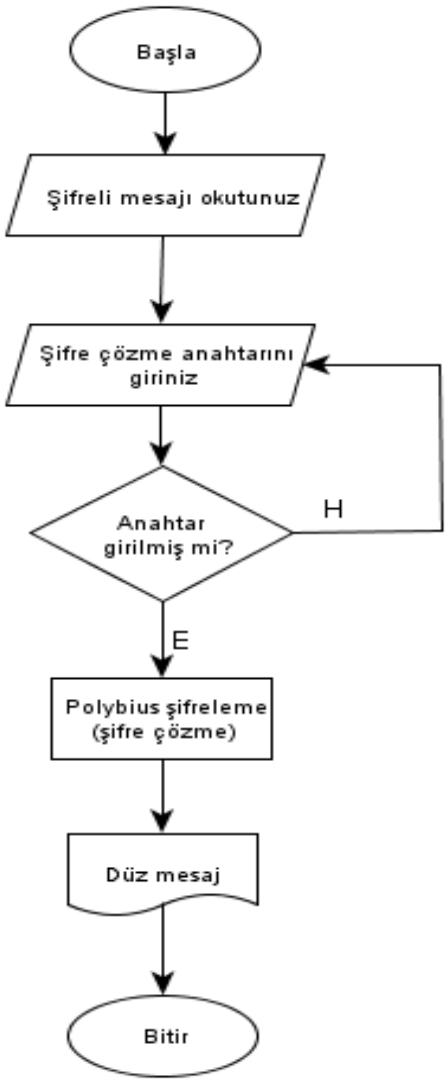
$$M = D_K (S)) \tag{4.2}$$

Burada K anahtarını kullanmanın amacı, eğer M açık metni sadece E kripto işlevi ile şifrelenirse gizliliği sağlayacak olan tek parametrenin kripto algoritması olmasıdır. Ayrıca iletişim güvenliğini arttırmak amacıyla alıcı tarafın her yeni kripto işlevi için farklı bir kripto algoritmasını bilmesinin gerekmesidir. Eğer mesajın şifrelendiği E

işlevi kaybolacak olursa yeni bir algoritma tasarlanmak durumundadır. Bu durumda zaman kaybı da göz önüne alınacak olursa bu oldukça pahalı bir yöntemdir. Bunun yanı sıra K anahtarı mesajın kripto algoritması bilinse de ikinci bir güvenlik parametresi olduğundan iletişim güvenliğini arttırmaktadır [83,90].



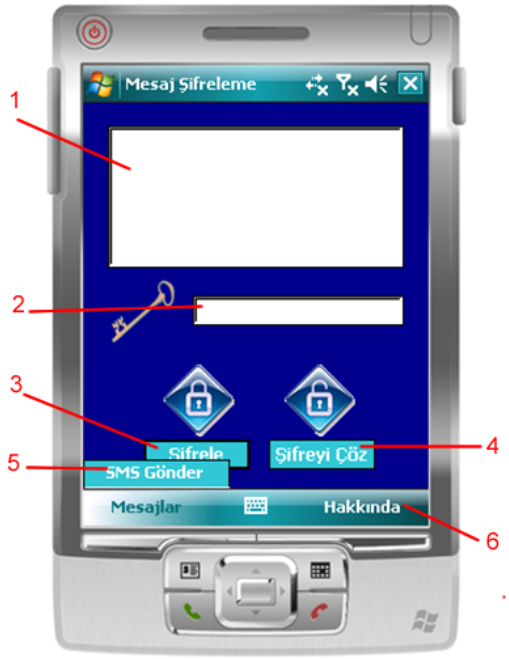
Şekil 4.2. Şifreleme işlemi akış şeması



Şekil 4.3. Şifre açma akış şeması

4.1. Şifreli Mesajlaşma Arayüzü

Windows Mobile CE işletim sistemine sahip cep telefonları için Visual C# ortamında geliştirilen şifreli mesajlaşma programında yer alan bileşenler Şekil 4.4'te görüldüğü gibi mesajın yazıldığı metin kutusu, şifreleme anahtarının girildiği metin kutusu, şifrelemeyi sağlayan buton, şifre çözmeyi sağlayan buton, sms gönder butonu ve hakkında ekranlardan oluşmaktadır.



Şekil 4.4. Arayüz bileşenleri

1- Mesajın yazıldığı metin kutusudur.
2- Şifreleme anahtarının girildiği metin kutusudur.
3- Şifreleme yapılmasını sağlayan butondur.
4- Şifre çözümünün yapılmasını sağlayan butondur.
5- SMS göndermek için kullanılan butondur.
6- Program hakkında bilgi alma butonudur.

Uygulama öncelikle emülatörde gerçekleştirilmiştir. Şekil 4.5.(a)'da uygulamanın ilk arayüzü ve Şekil 4.5.(b)'de ise düz mesajın ve şifreleme anahtarının girildiği arayüz görülmektedir.

(a) Uygulama arayüzü

(b) Düz mesajın ve şifreleme anahtarının girilmesi

Şekil 4.5. Şifreli Mesajlaşma uygulamasına ait benzetim ekranı

Benzetim uygulaması ilk açıldığında mesaj yazılacak text kutusu, anahtar (parola) girilecek text kutusu, şifrele ve şifreyi çöz butonları Şekil 4.5.(a)'da görülmektedir. Açık mesaj birinci text kutusuna, anahtar ise ikinci text kutusuna yazılmaktadır (Şekil 4.5.(b)).

Şekil 4.6. Şifrelenmiş mesaj ekranı benzetimi

Yazılan açık mesaj ve anahtar Polybius algoritmasıyla şifrelenmektedir. Anlaşılamayan şifreli mesaj elde edilerek, gönderilmeye hazırlanmıştır. Şekil 4.6'da şifrelenmiş mesaj görülmektedir.

(a) SMS gönderme işlemi (b) Telefon numarasının girilmesi

Şekil 4.7.Şifreli Mesajlaşma uygulaması benzetiminde mesaj gönderme ekranı

Şekil 4.7.(a)'da olduğu gibi SMS Gönder seçeneği seçilerek telefon numarasının yazılacağı ekrana ulaşılmaktadır. Alıcının telefon numarası girilerek ve Ok tuşuna basılarak şifreli mesaj gönderme işlemi gerçekleştirilir (Şekil 4.7.(b)).

Şekil 4.8. Şifreli Mesajlaşma uygulaması benzetiminde hakkında ekranı

Şekil 4.8'deki hakkında ekranı ile programın kullanımı hakkında kullanıcılara sistemin nasıl çalıştığı ile ilgili bilgi verilmektedir.

4.2. Gerçekleştirilen AltugSec Programı

Günümüzde telefon yoluyla karşılıklı gönderilen kısa mesaj servisleri çeşitli yöntemler kullanılarak ele geçirilebilmektedir. Buna önlem olarak tasarlamış olduğumuz AltugSec programını her iki cep telefonuna yüklemek güvenli veri iletişimi için bir çözüm önerisidir. Cep telefonuna yüklenilen bu yazılım sayesinde, yapılan görüşmelerin 3. kişiler tarafından elde edilmesi neredeyse imkânsız hale getirilmektedir.

Bu sistemde, her telefona yüklenen şifre sabit değil, değişkendir. Telefon kullanıcısı, her kısa mesaj göndermesinde, farklı bir şifre üzerinden mesaj gönderebilmektedir. Telefon kullanıcısının gönderdiği kriptolu gizli mesajlar, sadece yine bu programın yüklendiği başka telefonlarla ve yine aynı şifre ile çözülebilmektedir. AltugSec'in menü görüntüsü Şekil 4.9'da görülmektedir.

Şekil 4.9. AltugSec'in menü görüntüsü

(a) Uygulama arayüzü

(b) Düz mesajın ve şifreleme anahtarının girilmesi

Şekil 4.10. AltugSec programı çalışma ekranı

AltugSec uygulaması ilk açıldığında mesaj yazılacak text kutusu, anahtar (parola) girilecek text kutusu, şifrele ve şifreyi çöz butonları Şekil 4.10.(a)'da görülmektedir. Açık mesaj birinci text kutusuna, anahtar ise ikinci text kutusuna yazılmaktadır.(Şekil 4.10.(b))

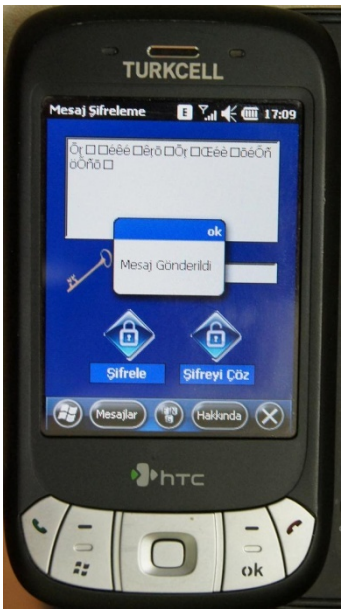
Şekil 4.11. AltugSec'de şifrelenmiş mesaj ekranı

Yazılan açık mesaj ve anahtar Polybius algoritmasıyla şifrelenmektedir. Anlaşılamayan şifreli mesaj elde edilerek, gönderilmeye hazırlanmıştır. Şekil 4.11'de şifrelenmiş mesaj görülmektedir.

(a) Sms gönderme işlemi (b) Telefon numarasının girilmesi

Şekil 4.12. AltugSec programı mesaj gönderme ekranı

Şekil 4.12.(a)'da olduğu gibi SMS Gönder seçeneği seçilerek telefon numarasının yazılacağı ekrana ulaşılmaktadır. Alıcının telefon numarası girilerek ve Tamam tuşuna basılarak şifreli mesaj gönderme işlemi gerçekleştirilir (Şekil 4.12.(b)).



Şekil 4.13. AltugSec mesaj gönderildi iletisi

Mesajın alıcıya iletildiğine dair mesaj Şekil 4.13'de görülmektedir.

Şekil 4.14. AltugSec hakkında ekranı

Şekil 4.14'deki hakkında ekranı ile programın kullanımı hakkında kullanıcılara sistemin nasıl çalıştığı ile ilgili bilgi verilmektedir.

(a) Şifreli mesajın görüntülenmesi (b) Açık mesajın alıcı tarafından görüntülenmesi

Şekil 4.15.AltugSec şifreli mesaj çözme ekranı

Şekil 4.15.(a)'da alıcı ekranında şifreli mesajın görüntülenmesi, Şekil 4.15.(b)'de ise alıcı ekranında şifreli mesajın çözülmüş hali gözükmektedir.

4.3. AltugSec'in Sistem Gereksinimleri

AltugSec programı düşük sistem gereksinimlerine ihtiyaç duymaktadır. AltugSec'i kullanmak istemeniz durumunda telefonunuzda bulunması gereken özellikler aşağıda belirtilmiştir:

- Windows Mobile 6.0 Professional işletim sistemi
- 856K hafıza alanı.
- 201 MHz işlemci hızı.
- 748K Ram.

5. SONUÇ VE ÖNERİLER

Bu çalışmada cep telefonları için gerçekleştirilen AltugSec adını taşıyan uygulamada, gönderici tarafından anlamlı halde yazılan mesaj anlamsız hale getirilerek alıcıya gönderilmektedir. Telefonunda AltugSec programı kurulu olan alıcı anlamsız halde gelen mesajı AltugSec programı sayesinde açık mesaj haline çevirebilmektedir. Bu şifreleme işleminde simetrik şifreleme yöntemlerinden Polybius algoritması kullanılmıştır.

Güvenliğe ikinci bir kademe getirebilmek, güvenliği daha da arttırmak amacıyla Polybius algoritmasına ek olarak güvenliğin kişiselleştirilmesi sağlanarak, kullanıcının kendisi tarafından belirlenen yalnızca mesajı gönderen ve mesajı alan kullanıcının bildiği anahtar bilgisi eklenmiştir. Anahtarlama türü olarak özel anahtar (privatekey) kullanılmıştır. Bu şifreleme algoritması ve anahtar sayesinde iki kişi arasında güvenli bir şekilde mesajlaşma gerçekleşmektedir. Programa sahip olmayan üçüncü bir şahıs mesajı anlamlı hale getirememektedir. Programı elde etse dahi kullanıcı tarafından belirlenen anahtar bilgisi olmadan yine mesajı çözmesi neredeyse imkansız hale gelmektedir. Böylelikle yetkisiz kişilerin korunmuş verilere erişimi zor hale getirilmektedir.

Birbirleri ile mesajlaşma yoluyla iletişim kurmak isteyen kişilerin mesajlarının, başka kişiler tarafından okunmadan, güvenilir bir şekilde iletilmesi için AltugSec programı kullanılabilir. Ayrıca kişinin telefonu çalındığında veya kaybolduğunda mesaj olarak kaydettiği önemli bilgilerin istenmeyen şahısların eline geçmesi AltugSec ile önlenebilmektedir. Bunlara ek olarak günümüzde mobil bankacılık kavramı oldukça önemli bir yere sahiptir. Mobil bankacılık müşterinin bankaya mesaj yollaması ile de mümkün olabilmektedir. Banka ile müşteri arasında mesaj yolu ile güvenli iletişim kurulabilmesi için AltugSec programı tercih edilebilir.

Mathkour ve arkadaşlarının simetrik şifreleme yöntemlerinden AES kullanarak yaptıkları bir çalışmada Nokia N73 telefonda algoritmanın çalışabilmesi için

330MHz işlemci hızı ve 26MB RAM'e ihtiyaç duyulmaktadır. AltugSec programının HTC telefonda çalışabilmesi için ise 201 MHz işlemci hızına ve 748K RAM'e gereksinim vardır. AltugSec programı AES algoritmasının gereksinimlerinden daha düşük işlemci hızı ve RAM'e ihtiyaç duymaktadır.

AES algoritmasının Nokia N73 telefonda 128 karakter mesajı şifreleme hızı 263 ms iken Polybius algoritmasının HTC telefonda 160 karakter mesajı şifreleme hızı 10 ms'dir. Sonuç olarak AltugSec programında daha fazla karakterde mesaj daha kısa sürede şifrelenebilmektedir.

Bunlara ek olarak, yapılan bu uygulamada RAM 1MB'ın altındayken ve karakter uzunluğu 256'nın üzerindeyken şifreleme ve deşifreleme gerçekleştirilememektedir. AltugSec programında ise RAM 1MB'ın altındayken 256 karakterden daha uzun mesajlarda şifrelenebilmektedir.

Özel anahtar yaklaşımında özel anahtarların kullanıcılara nasıl dağıtılacağı konusu gündeme gelmektedir. Çünkü bu dağıtım işlemi esnasında da anahtarlar istenmeyen ellere geçebilir. Bu iş için e-mail'den yararlanılabileceği gibi (gerekli güvenlik önlemleri alınmak kaydıyla), telefonla da bu anahtarlar sahiplerine aktarılabilir. Bu işlemler gerçekleştirilirken güvenliğe azami derecede dikkat etmek gerekmektedir. Şifreleri kişilere atamanın bir başka yolu da, bir sunucu vasıtasıyla dağıtma işlemini yapmaktır. Bu durumda, şifreleri ele geçirmek isteyenlere direkt bir hedef sunulmakta, burada sağlanacak yeterli bir güvenlik mekanizması ile, bu tehlike de önlenebilmektedir.

Genel anahtar (publickey) kullanılması daha üstün gibi görülmekle birlikte, bazı zayıflıkları da mevcuttur. Bunların başında da, birbirlerine şifrelenmiş veri gönderecek bilgisayarların her defa yürütmeleri gereken el sıkışma protokolleri, ilgili anahtarları kullanarak bilgileri çözme işlemlerinin CPU zamanından çok fazla almasıdır. Bu işlemler, hesap yoğunluğu olan işlemler olduğundan sistemi oldukça yavaşlatacak, ağ performansının azalmasına sebep olmaktadır. Genel anahtar yöntemi, yavaş olması nedeniyle sistemin performansının yavaşlamasına neden

olabileceği için tercih edilmemiştir. Anahtarın sabit olmamasının yanı sıra anahtar uzunluğunun da sabit olmaması yani kullanıcı tarafından belirleniyor olması geliştirilen uygulamanın üstünlüğüdür. Anahtar uzunluğu arttıkça şifrenin kırılması güçleşmektedir.

Simetrik şifreleme yöntemlerinden Polybius algoritması kullanarak geliştirdiğimiz AltugSec Programı mobil cihazların kısıtlı hafıza, işlemci hızı, görselleştirme yeteneklerini çok az kullanmaktadır. AltugSec programı gelişmiş bir şifreleme yapmış olmasına rağmen oldukça sade bir arayüze sahiptir. Şifreleme işlemi en düşük gereksinimleri karşılayan bir cep telefonunda 201 MHz işlemci hızı ve 748K ram 0.01 sn. gibi kısa bir sürede geliştirilmekte ve mesaj alıcıya iletilmektedir.

Bu çalışma gerçekleştirilirken algoritma seçimi ve seçilen algoritmanın cep telefonunda uygulanması zaman almıştır. Daha sonraki çalışmalarda Private key'in anahtar dağıtım problemi üzerine geliştirilmiş olan public key kullanılarak şifreleme işlemi gerçekleştirilebilir. Public key ile anahtar dağıtımı daha güvenli olduğu için geliştirilen uygulama mobil bankacılık alanında da rahatlıkla kullanılabilir. AltugSec ile kısa mesaj servisleri şifrelenmektedir. Bundan sonra yapılacak olan çalışmalarda multi medya mesajların şifrelenmesi sağlanabilir.

KAYNAKLAR

1. Gülmez, M., "Üniversite öğrencilerinin cep telefonu satın alma ve kullanımını etkileyen faktörler: Sivas Cumhuriyet Üniversitesi ile Tokat Gaziosmanpaşa Üniversitelerinde bir uygulama", ***Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi***, 24: 37-62 (2005).

2. Ling, R., "The Mobile Connection: the Cell Phone's Impact on Society", ***Morgan Kaufmann Publishers***, San Francisco, CA (2004).

3. Özcan, Y. Z., Koçak, A., "Research Note: A Need or a Status Symbol? Use of Cellular Telephones in Turkey", ***European Journal of Communication***, 18, 241–254 (2003).

4. Bilgi Teknolojileri ve Elektronik Araştırma Enstitüsü, "Bilgi Teknolojileri Yaygınlık ve Kullanım Araştırması", ***TÜBİTAK-BİLTEN***, **Ankara**, (2001).

5. Rose, G., "Authentication and Security in Mobile Phones", ***AUUGN***, Australia (1999).

6. Canbek, G., Sağıroğlu, Ş., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme***", Politeknik Dergisi Journal of Polytechnic***, 9(3), 165-174 (2006).

7. Canbek, G., Sağıroğlu, Ş., "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir inceleme", ***Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi***, 23(1-2), 1-12 (2007).

8. İnternet: Tüketiciler Birliği, " Telefon kopyalama (klonlama) nedir?", http://www.tuketiciler.org/?com=news.read&ID=1348 (2011).

9. İnternet: C5 Electronics "Tam Güvenli GSM İletişimi", http://www.systemtechnic.com.tr/sistemteknik.swf, (2011).

10. İnternet: Reyhaber "ASELSAN'dan Yerli ve Kriptolu Cep Telefonu", http://www.reyhaber.com/index.php?option=com_content&view=article&id=23343&catid=12&Itemid=4 (2011).

11. İnternet: Nokia "Mobil Cipher", http://store.ovi.com/content/50365 (2011).

12. Anonim, "Universal Mobile Telecommunications System (UMTS) Protocols and Protocol Testing", 1-4, (2003).

13. Öztürk, A, "Mobil Telekomünikasyon Lisans Rejimi: Dünya Örnekleri ve Türkiye Analizi", Uzmanlık Tezi, ***Telekomünikasyon Kurumu***, Ankara, (2002).

14. Bilim, M., Develi, İ., Kabalcı, Y.,"Gsm 900 Mhz Frekans Bandındaki Elektromanyetik Yoğunluğun Günün Farklı Zaman Dilimleri İçin Ölçülmesi Ve Değerlendirilmesi", ***Elektrik-Elektronik ve Bilgisayar Sempozyumu***, Elazığ, (2011).

15. Leggett, R., Boer, W., Janousek, S., "Flash Applications for Mobile Devices. ApressInc", Berkeley, 514 (2006).

16. Aksu, M., "3. Nesil Cep Telefonları İçin Symbian İşletim Sistemi Üzerinde Çalışabilen C++ Tabanlı Uygulama Geliştirilmesi", Yüksek Lisans Tezi, ***K.S.Ü.***, Kahramanmaraş, (2004).

17. Andrade R., Wangenheim A., Bortoluzzi M., "Wireless and PDA: a novel strategy to Access DICOM-compliant medical data on mobile devices", ***International Journal of Medical Informatics***, 71, 157-163 (2003).

18. Bilgi Teknolojileri ve İletişim Kurumu, "Faaliyet Raporu 2010", ***BTK***, Ankara, (2011).

19. Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma Ve Stratejiler Dairesi Başkanlığı, "İstatistiki Veriler Işığında Dünyada ve Türkiye'de Elektronik Haberleşme Sektörü", ***BTK***, Ankara, (2010).

20. İnternet: wikipedia.org, "Cep Telefonu", http://tr.wikipedia.org/wiki/Cep_telefonu (2011).

21. İnternet: linux.org, "Mobil İstemcilere Yönelik Güvenlik Tehditleri ve Özgür Uygulamalarla Savunma", http://seminer.linux.org.tr/wp-content/uploads/MobileSecurity.pdf (2011).

22. İnternet: milinic.blogspot "SMSC", http://milinic.blogspot.com/2010/10/smsc.html (2011).

23. Yüksel, M. E., Zaim, A. H., "GSM/GPRS Aygıtları Üzerinden Çok Dilli SMS Gönderme", ***Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri***, Şanlıurfa, 229-238 (2009).

24. Hossain, A., Jahan, S., Hussain, M.M., Amin, M.R., Shah Newaz, S.H., "A proposal for enhancing the security system of short message service in GSM**",** ***2nd International Conference on Anti-counterfeiting, Security and Identification (ASID)***, Guiyang, 235-240 (2008).

25. İnternet: ab.org.tr "GSM Güvenliğinde Son Durumlar" , http://ab.org.tr/ab05/tammetin/160.doc (2011).

26. İnternet: gsm-security.net "GSM Security and Encryption", http://www.gsm-security.net/gsm-security-papers.shtml (2011).

27. İnternet: elektrik.gen.tr "GSM Sistemlerine Genel Bakış", http://www.elektrik.gen.tr/icerik/gsm-sistemlerine-genel-bak%C4%B1%C5%9F (2011).

28. İnternet: gsm-security.net "The Clone, RT, The GSM Security Technical Whitepaper for 2002", http://www.gsm-security.net/gsm-security-papers.shtml (2011).

29. İnternet: brookson.com "Gsm Security (and PCN) and Encryption", http://www.brookson.com/gsm/gsmdoc.pdf (2011).

30. İnternet: theukwebdesigncompany.com "Security of GSM System", http://www.theukwebdesigncompany.com/articles/article.php?article=1191 (2011).

31. Güneş, M., Olcay, E., Gülersoy, Y. E., "IMEI Klonlama; Ekonomik Sosyal ve Hukuksal Boyutları", ***Haberleşme Teknolojileri ve Uygulama Sempozyumu***, İstanbul, (2007).

32. İnternet: Yaşayan Anayasa "Yargıdan Telefon Dinlemeye Yeni Bir Yorum", http://www.yasayananayasa.ankara.edu.tr/belgeler/analizler/telefon_dinleme.pdf (2011).

33. Şen, Ş., "İndirgenmiş SPN(Substitution Permutatin Network) Algoritması için Lineer Kriptanaliz Uygulaması", Yüksek Lisans Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, (2006).

34. İnternet: dunyateknolojisi.com "Beni Duyabiliyorlar mı? Yasal Telefon Dinlemelerinin Güvenlik Analizi", http://www.dunyateknolojisi.com/Uploads/alpoges/Yasal_Telefon_Dinlemelerinin_Guvenlik_Analizi.pdf (2011).

35. Aoki, K., Downes E., "An analysis of young people's use of and attitudes toward cell phones", ***Telematics and Informatics,*** 20: 349-364 (2003).

36. Katz, J.E., Aakhus, M.A., "Perpetual contact: Mobile communication, private talk, public performance 1 edition", ***Cambridge University Press***, Cambridge, , UK, 193–205 (2002).

37. Palen, L., Salzman, M., Youngs, E., "Goingwireless: behavior&practice of new mobile phoneusers", ***Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work***, Philadelphia, PA, 201–210 (2000).

38. Ling, R., "New Tech, New Ties: How Mobile Communication is ReshapingSocialCohesion", ***MIT Press***, Cambridge, MA (2008).

39. İnternet: The Carphone Warehouse "The Mobile Life Report 2006: How Mobile Phones Change The Way We Live", http://www.mobilelife2008.co.uk/mobilelife2007/PDF/Mobile%20Life%20Report%202006%20Black%20&%20White%20Version.pdf (2011).

40. De Vries, I., "Mobile telephone: realising the dream of ideal communication", Mobile World: Past, Present and Future, L. Hamill, A. Lasen, Editors, ***Springer***, London, UK, 42–62 (2005).

41. Wikle, T.A., "America's Cellular Telephone Obsession : new geographies or personal communication", ***Journal of American and Comparative Cultures***, 24 (12): 123-128 (2001).

42. Licoppe, C. ve Heurtin J-P., "Managing One's Availability to Telephone Communication through Mobile Phones: A French Case Study of the Development Dynamics of Mobile Phone Use", ***Personal and Ubiquitous Computing***, 5(2): 99-108 (2001).

43. Wooldridge, A., "The downside of the Mobile", ***The Economist***, 353: 29 -35 (1999).

44. Townsend, A. M., "Life in the Real Time City : mobile telephones and urban metabolism", ***Journal of Urban Technology***, 7 : 85-104 (2000).

45. Griffiths, M. D. ve Dancaster, I., "TheEffect of Type A Personality on Pyschological Arousal while Playing computer games", ***Adictive Behaviors***, 20(4) : 543-548 (1995).

46. Finn, S., "Origins of Media Exposure", ***Addictive Behaviors***, 19 : 545-553 (1997).

47. Ling, R., ve Pedersen P., "Thesocio-linguistics of SMS: An analysis of SMS use by a random sample of Norwegians", Mobile Communications: Renegotiation of the Social Sphere, ***Springer***, London, 335- 349 (2005).

48. Green, N., "Who's watching whom? Monitoring and accountability in mobile relations", Wireless World: Social and Interactional Aspects of the Mobile Age, B. Brown, N. Green, R. Harper, Editors , ***Springer***, London, UK, 32–45 (2001).

49. Sandstrom, M., Wilen, J., Oftedal, G., Hansson-Mild, K., "Mobile phone use and subjective symptoms. Comparison of symptoms experienced by users of analogue and digital mobile phones", ***Occup Med (London)***, 51(1): 25-35 (2001).

50. Lee, D. J., "College Students Hand Phone Usage Culture Survey", ***University Culture Newspaper***, 18-25 (2002).

51. Nasar, J.,Hecht, P., Wener, R., "Call If You Have Trouble : mobile phones and safety among college students", ***Internatinal Journal of Urban and Regional Research***, 31(4): 863-873 (2007).

52. McKnight, A.J., McKnight A.S., "Theeffect of cellular phone use upon driver attention", ***Accident Analysis and Prevention***, 25(3): 259–65 (1993).

53. Violanti, J.M., "Cellular phones and traffic accidents", ***Public Health***, 111(6): 423–28 (1997).

54. Violanti, J.M., "Cellular phones and fatal traffic collisions", ***Accident Analysis and Prevention***, 30(4): 519–24 (1998).

55. Lamble, D., Kauranen T., Laakso M., Summala H., "Cognitive load and detection thresholds in car following situations: safety implications forusing

mobile (cellular) telephones while driving", ***Accident Analysis and Prevention***, 31(6): 617–23 (1999).

56. İnternet: nrd.nhtsa.dot.gov "The Influence of The Use of Mobile Phones on Driver Situation Awareness", http://www-nrd.nhtsa.dot.gov/departments/Human%20Factors/driver-distraction/PDF/2.PDF (2011)

57. Royal, D., "Findings national survey of distracted and drowsy driving attitudes and behaviours:2002", ***The Gallup Organization, Report number 809 566***, National Highway Traffic Safety Administration, Washington, DC, 33 (2003).

58. Klauer, S.G., Dingus, T.A., Neale, V.L., Sudweeks, J.D. and Ramsey D.J., "The impact of driver inattention on near-crash/crash risk: an analysis using the 100-car naturalistic driving study data", ***Virginia Tech Transportation Institute, Report number DOTHS 810-594***, National Highway Traffic Safety Administration, Washington, DC, 152 (2006).

59. İnternet : ecommerce-guide.com, "Eliminating Some Credit Card Risk for E-Business", http://www.ecommerce-guide.com/solutions/building/article.php/6321_569741 (2001).

60. Schwiderski-Grosche, S. ve Knospe, H., "Secure Mobile Commerce", ***Special issue of the IEE Electronics and Communication Engineering Journal on Security for Mobility***, 14(5): 228-238 (2002).

61. İnternet : Chip "Mobil Bankacılık", http://chip.com.tr/mobil bankacılık (2004).

62. Şahin, A. B., Selçuk, G., "İletişim Ağ Güvenliğinde Son Aşama: Kuantum Kriptografi ve Fiber Optik Ortamda Kuantum Temelli Rastsal Sayı Üretimi", ***ISCTURKEY 2006 Sözlü Bildirileri***, Ankara, (2006).

63. Şen,Ş., "İndirgenmiş SPN(Substitution Permutatin Network) Algoritması için Lineer Kriptanaliz Uygulaması", Yüksek Lisans Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, (2006).

64. Yıldırım, K., "Veri şifrelemesinde simetrik ve asimetrik anahtarlama algoritmalarının uygulanması (hybrid şifreleme)", Yüksek lisans tezi, ***Kocaeli Üniversitesi Fen Bilimleri Enstitüsü,*** Kocaeli, (2006).

65. Akleylek, S., Nuriyev, U.G., "Steganografi ve Steganografinin Yeni Bir Uygulaması", ***IEEE 13. Sinyal İşleme ve İletişim Uygulamaları Kurultayı***, Kayseri, (2005).

66. Tektaş, M., Baba F., Çalışkan M., "Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması", ***3RD International Advanced Technologies Symposium***, Ankara, (2003).

67. Yerlikaya, T., Buluş, E., Buluş, H. N., "RSA Şifreleme Algoritmasının Pollard RHO Yöntemi ile Kriptanalizi", ***Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı Bildirileri***, Kütahya , 79-86 (2007).

68. Yılmaz, R., "Kriptolojik uygulamalarda bazı istatistik testler", Yüksek Lisans Tezi, ***Selçuk Üniversitesi Fen Bilimleri Enstitüsü***, Konya, (2010).

69. İnternet: savaskartal.com, "Kriptografide Kullanılan Teknikler ve Kriptografik Uygulamalar", http://www.savaskartal.com/2010/04/12/kriptografide-kullanilan-teknikler-ve-kriptografik-uygulamalar/ (2011).

70. Sağıroğlu, Ş., Kabasakal, D., Alkan M., "Elektronik İmzadan Mobil Elektronik İmzaya Geçiş Sürecinde Türkiye", ***I. Ulusal Elektronik İmza Sempozyumu***, Ankara, 21-27 (2006).

71. Karabıyık, A., "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)", ***Muhasebe ve Finansman Dergisi***, (39): 155-166 (2008).

72. İnternet: tektasi.net, "Şifreleme Algoritmalarının Sınıflandırılması ve Algoritmalara Saldırı Teknikleri", http://tektasi.net/attachments/article/4/sifreleme-algoritmalarinin-siniflandirilmasi.pdf(2011).

73. İnternet: cyber-warrior.org, "PublicKeyEncription", http://www.cyber-warrior.org/forum/public-key encryption_307186,0.cwx (2011).

74. Fındık, O., "Şifrelemede Kaotik Sistemin Kullanılması", Yüksek Lisans Tezi, ***Selçuk Üniversitesi Fen Bilimleri Enstitüsü***, Konya, 10-11 (2011).

75. Schneier, B., "AppliedCryptology, Second Edition: Protocols, Algorithms,and Source Code in C", ***Wiley Publishing***, Canada, (1996).

76. Stalings, W., "Crytography and Network Security Second Edition", ***Prentice Hall***, (1998).

77. Salomaa, A., "Public-Key Cryptography", ***Springer Verlag***, New York, (1990).

78. Koblitz, N., "A Course in Number Teory and Cryptography", ***Springer Verlag***, New York, (1994).

79. İnternet: kriptoloji.net, "Polybius Şifrelemesi", http://kriptoloji.net/polybius-sifrelemesi (2011).

80. İnternet: bilgisayarkavramlari.com, "Polybius Şifrelemesi", http://www.bilgisayarkavramlari.com/2010/07/07/polybius-sifrelemesi/ (2011).

81. Mathkour, H., Assassa, G., Al-Muharib, A., Juma'h, A., "A Secured Cryptographic Messaging System", ***International Conference on Machine Learning and Computing***, (2009).

82. Hwang, T., "Scheme for secure digital mobile communications based on symmetric key cryptography", ***Information Processing Letters***, 48(1): 35-37 (1993).

83. Yerlikaya, T., Buluş, E., Arda, D., "Asimetrik Kripto Sistemler Ve Uygulamaları", ***II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi-MBGAK***, İstanbul (2005).

84. Yılmaz,T., "Akıllı kartlarda güvenlik problemleri çözümü", Yüksek Lisans Tezi, ***Selçuk Üniversitesi Fen Bilimleri Enstitüsü***, Konya, (2004).

85. Diffie, W.,Hellman, M.E., "New directions in cryptography", ***IEEE Trans***, 22(6): 644-654 (1976).

86. Agoyi, M., Seral, D., "SMS Security: An Asymmetric Encryption Approach", ***6th International Conference on Wireless and Mobile Communications (ICWMC)***, Valencia, 448-452 (2010).

87. De Santis, A., Castiglione, A., Cattaneo, G., Cembalo, M., Petagna, F., Petrillo, U.F., "An Extensible Framework for Efficient Secure SMS", ***International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)***, Krakow, 843-850 (2010).

88. Lisonek, D., Drahansky, M., "SMS Encryption for Mobile Communication", ***International Conference on Security Technology (SECTECH '08)***, Hainan Island, 198-201 (2008).

89. Li-Chang Lo, J., Bishop, J., Eloff, J.H.P., "SMSSec: An end-to-end protocol for secure SMS", ***Computers & Security***, 27(5-6): 154-167 (2008).

90. İnternet: certicom "Current Public-Key Cryptographic Systems", http://amadousarr.free.fr/crypto/ECDSAECC/EccWhite2.pdf (2011).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: ALTUĞ, Mehtap
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 05.02.1984 ŞEREFLİKOÇHİSAR
Medeni hali	: Bekar
Telefon	: 0 (312) 250 38 81
E-mail	: mehtapaltug@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Mersin Üniversitesi/Elektronik Bilgisayar Eğitimi	2006
Lise	Şerefli Koçhisar Yab. Dil. Ağır. Lise	2001

İş Deneyimi

Yıl	Yer	Görev
2006-2010	Beypazarı K.T. M. L. ANKARA	Öğretmen
2010-	Etimesgut K.T. M. L. ANKARA	Öğretmen

Yabancı Dil

İngilizce

Hobiler

Tiyatro, Sinema, Müzik