T.C.

BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

AKILLI KARTLAR VE ŞİFRELEME YAPILARI

(Yüksek Lisans Tezi)

Tezi Hazırlayan: **Mehmet ÖZDOĞAN**

İstanbul, 2010

T.C.

BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

AKILLI KARTLAR VE ŞİFRELEME YAPILARI

(Yüksek Lisans Tezi)

Tez Hazırlayan:

Mehmet ÖZDOĞAN

Öğrenci No:
070820005

Danışman:

PROF. DR. M. Yahya KARSLIGİL

İstanbul, 2010

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum "Akıllı Kartlar ve Şifreleme Yapıları" başlıklı bu çalışmamın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıklarını her yerde bunlara atıf yapıldıklarını belirtir ve bunu onurumla doğrularım. 14/09/2010

Aday: Mehmet ÖZDOĞAN

AKILLI KARTLAR VE ŞİFRELEME YAPILARI

Tezi Hazırlayan: Mehmet ÖZDOĞAN

Özet

Bu tez çalışmasında akıllı kartların tanımı yapılıp onlar için uygulanan şifreleme yapıları ele alınmıştır. Knapsack algoritması ile güçlendirilmiş ECC yeni bir şifreleme sisteminin kullanımının akıllı kartlarda uygulanmasıyla ne gibi avantajlar ve dezavantajlar sağlayacağı belirtilmiştir. Gelecekte akıllı kartların bilgisayarlara daha çok yaklaşacağı hatta kendi üzerlerinde biyometrik okuyucularını barındıracağı söylenebilir. Geleceğe dönük uygulamalarla ilgili günümüzde yapılan çalışmalar analiz edilip öngörülerde bulunulmaktadır.

Anahtar Kelimeler: Akıllı Kartlar, Manyetik Şeritli Kartlar, RSA, Knapsack, DES, AES, ECC

SMARTCARDS AND CRYPTOLOGIC STRUCTURES

Presented by: Mehmet OZDOGAN

Abstract

In this thesis, we describe smartcards and told applied cryptographic structures. We try to explain disadvantages and advantages of a new cryptographic technique, knapsack based EEC algorithm, when it use on smartcards. We can say smartcards will hold bometric readers on their own in the near future. We analyzed nowadays works on smartcards and in the light of this information we predict on future of smartcards.

Key Words: Smart Cards, Magnetic Stripe Cards, RSA, Knapsack, DES, AES, ECC

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

AES	:Advanced Encryption Standard
CDMA	:Code Division Multiple Access
CPU	:Central Processing Unit
CVV	:Card Verification Value
DES	:Data Encryption Standard
EC	:Elliptic Curve
ECC	:Elliptic Curve Cryptography
EMV	:Europay, Mastercard, Visa
EEPROM	:Electrically Erasable Programmable Read-Only Memory
FDMA	:Frequency Division Multiple Access
GSM	:Global System for Mobile Communications
ICC	:Integrated Circuit Chip
ISO	:International of Organization Of Standartization
PVV	:Pin Verification Value
ROM	:Read-Only Memory
RSA	:Rivest, Shamir, & Adleman
SDMA	:Space Division Multi Access
TDMA	:Time Division Multiple Access
VCC	:Supply Voltage

1.GİRİŞ

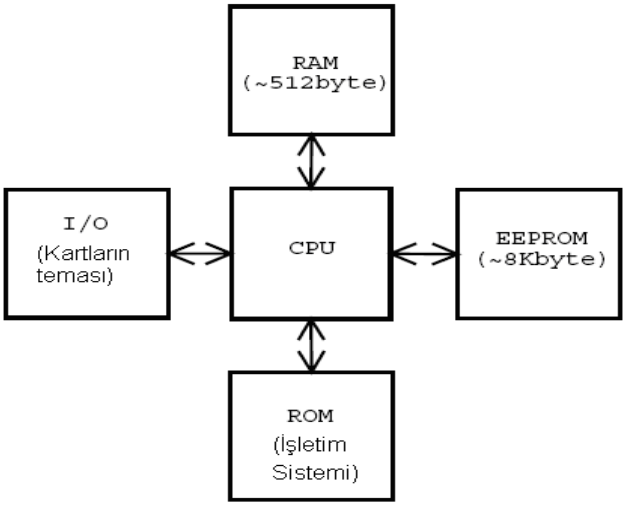
Akıllı kartlar için çağımızda kullandığımız ‘en küçük bilgisayarlardır’ denilebilir. Boyutları bir kredi kartı kadar olup akıllı diye çağrılmalarının nedeni içinde bir çip barındırmasından dolayıdır. Klavye, ekran gibi genel çıkış birimlerine sahip olmamakla birlikte temel bilgisayar birimlerine sahiptir. Akıllı kartlar, içinde bir işlemci ve çeşitli hafıza tipleri barındırır. Bu işlemci 8-bit bir mikro denetleyici içerir. Bir bilgisayardan hız, hafıza ve giriş çıkış birimleri konusunda daha geri olup esas amaçları olan kendilerine özgü özelliklerinin sağladığı güvenlik bakımından üstündürler.

Kartın üzerindeki yazılım, güvenlik konusu üzerine uzmanlaşmıştır ve karttaki çeşitli alanlara giriş yetkilerinin onayı, reddi ve hem işlemler öncesi hem de sonrası işlem sonucunun görüntülenmesi gibi görevleri bulunur. Kartın giriş kontrol yazılımı ROM ve EEPROM’da yer alması sebebiyle korumalıdır, çünkü bu alanlara sadece okuma yetkisi verilmiştir.

Güçlü güvenlik yapıları kişisel bilgisayarlara da uygulanabilmektedir. Fakat hassas verilerin mantık kontrol girişinin birbirinden ayrı olmasından dolayı bir güvenlik açığı oluşturmaktadır. Kartta ise bu veriler aynı mikroçip üzerine gömülü olarak yer almaktadır.

Şekil 1’de bir akıllı kartın mimarisi görülüyor.[10] Burada görüldüğü üzere mimari olarak von Neumann yapısı bilgisayarlara benzemektedir. Fakat Neumann yapısından ana farkı, akıllı kartların iç yolları I/O birimleri tarafından direk olarak kullanılamaz. Bu sayede dış etkinliklerin kartın yapısına doğrudan etkileri engellenerek güvenlikten emin olunur.

Akıllı kartlar, çağın gerekliliklerine uygun olara gittikçe hareketli hale gelen dünyamızda insanların en büyük yardımcılarından biri olarak birçok fırsatın ve yeniliğin kapılarını açmaktadır. Akıllı kartların gittikçe yaygınlaşmasının en önemli nedeni ucuz bir çözüm sunması, kolayca kopyalanamaması, iyi bir güvenlik sağlaması olarak sayılabilir.



Şekil 1. Akıllı Kartın İçindeki Fiziksel Birimler

1.1. Tarihçe

İlk plastik kart 1950'lerin başında Amerika'da kullanılmaya başlanmıştır. İlk akıllı kartlar 1968 yılında 2 alman mühendisi, Jürgen Dethloff ve Helmut Gröttrupp, tarafından keşfedilmiştir. Benzer bir kart patenti de 1970'te Japonya'da Kunitaka Arimura tarafından alınmış[1] olmasına rağmen esas gelişme 1974'te Fransa'da Roland Moreno'nun aldığı patentler üzerinden olmuştur. Bu tip kartların ilk uygulama alanı Fransız posta teşkilatı telefon kartları olmuştur. Bu yıllarda Almanya'da da telefon kartlarıyla ilgili pilot bir proje uygulanmaya konulmuştur. Bu projenin amacı manyetik, holografik ve akıllı kartlardan hangisinin daha uygun olduğunu görmeye yönelikti ve yüksek güvenilirliği ve hileye karşı koruması sayesinde kazanan akıllı kartlar olmuştur. Akıllı kartların esas çıkışları Avrupa'da GSM şebekesinde kullanılmak için tanıtımı yapılan SIM kartlar vasıtasıyla olmuştur.

Bankacılık sistemini incelendiğinde yine Fransızlar ile karşılaşılır. 1982–1983 yıllarında ilk çipli kart uygulaması denemelerini yapmışlardır. Ancak tüm Fransız bankalarının çipli kartlara geçmesi 10 sene sürmüştür. Akıllı kartların bankalarda gittikçe kullanımının artmasıyla 1993 yılında Mastercard, Visa ve Europay(EMV) akıllı kartlar olarak kullanılan ödeme ve kredi kartlarının özelliklerinin geliştirilmesi için birlikte çalışma konusunda anlaşmaya vardılar. Böyle bir anlaşmanın amacı kartlar arasında genel bir uyumluluk sağlayıp akıllı kartlara bir standart getirme arayışıdır. İlk EMV sistemi versiyonu

1994'te tanıtıldı. İlk EMV standardı 1996'da EMV'96 Sürüm 3.1.1 adıyla getirildi. Şu an kullanılan Sürüm 4.1 olup 2007'de kabul edilip kullanılmaya başlanmıştır.

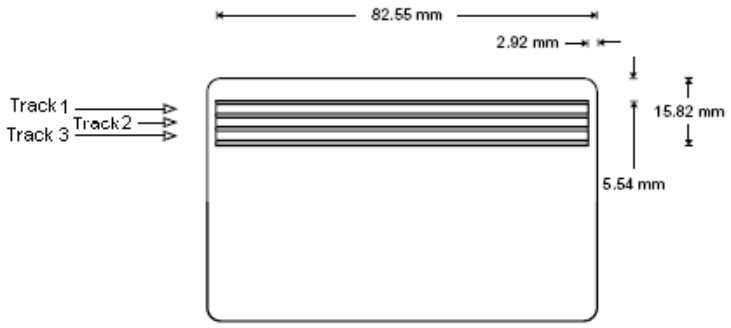
Günümüzde akıllı kartların uygulama alanları çok genişlemiştir. Ehliyetler, kimlik kartları, alışveriş kartları, toplu taşıma kartları gibi hayatımızın her alanını işgal etmeye, gittikçe önem kazanmaya başlamıştır.

1.2. Kart Çeşitleri

Yıllar boyunca teknolojinin gelişmesi sebebiyle akıllı kart sistemlerinin de buna paralel olarak benzer bir gelişim içinde bulunması kaçınılmaz bir olgudur. Bu gelişme, bazen tüm kart teknolojisinin değişmesi anlamına geldiği gibi bazen de sadece kart okuma tekniklerinin değiştirilmesi şeklinde olabilmektedir. Kart türleri esas olarak iki başlık altında sınıflandırılabilir. Bunlar manyetik şeritli kartlar ve akıllı kartlardır.

1.2.1. Manyetik Şeritli Kartlar

Manyetik şeritli kartlar, üzerinde manyetik bir bant bulunan ve bu bant üzerinde kullanım amacına uygun veriyi tutan kart çeşididir. Bu kartlar, düşük maliyetleri ve kolayca okuma ve yazma yapılabilmesi sayesinde hızla yaygınlaşmışlardır. İlk çıkışlarını yaptıkları telefon kartı uygulamalarından sonra, bankacılık uygulamalarında da yıllarca kullanılmış olup artık yerini EMV kartlara bırakmaya başlamıştır. Günümüzde halen bilet sistemlerinde, giriş sistemlerinde yaygın olarak kullanılıyor.



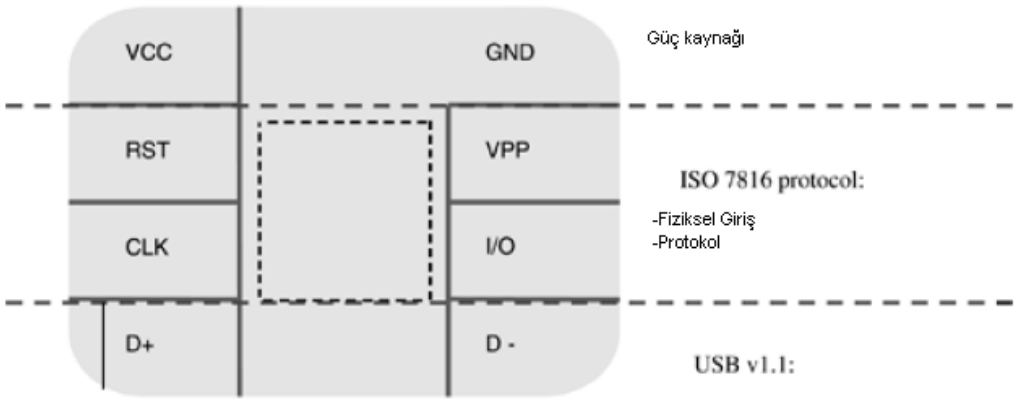
Şekil 2. Bir manyetik kartın arkadan görünüşü

Şekil 2'de gösterildiği üzere arkasında manyetik bir şerit bulunup veri bu şerit üzerine yazılmaktadır. Bu şeritte Track1,Track2 ve Track3 olarak sınıflandırılan 3 tane kısım vardır. Bu veriler kullanıcının adresini, ismini, CVV(Card Verification Value), PVV(Pin Verification Value), kartın son kullanma tarihi gibi bilgileri barındırmaktadır.

Manyetik şeritli kartlar ile ilgili en önemli problem, herhangi bir şifreleme mekanizmasının olmamasından dolayı oluşan güvenlik açığıdır. Kartın verisinin okunmasının ve okunan bu verinin başka karta yazılmasının herhangi bir okuma yazma cihazıyla gerçekleştirilebiliyor olması da güvenlik açığı oluşturan başka bir etmendir. Bu yolla bir kartın kopyalandığını anlamak çok zor olacağından artık bankaların öncülük etmesiyle başlayan bir süreçte yerini çipli kartlara bırakmaya başlamıştır. Bu konuda bankaların öncülüğü çok anlamlı görülebilir çünkü en ufak bir hatanın bile çok büyük maddi kayıplara yol açabildiği bir sektör olan bankacılık sektörünün bu şekildeki güvenlik zaaflarına karşı çok hassas davranması gerekmektedir.

1.2.2. Akıllı Kartlar

Temelinde bir plastik kart üzerinde haberleşme, depolama veya veri işlemek için kullanılan bir çipin gömülü olduğu karttır. Şekil 3'de çipin yapısı gösterilmektedir.



Şekil 3. Bir çipin üzerindeki bölümler

Buradaki kısımları tanımlamamız gerekirse;

VCC: Güç kaynağı girişi

RST: Sıfırlama.

CLK: Zamanlama sinyali

GND: Topraklama.

VPP: Programlama voltaj girişi

I/O: Kartın içindeki çipe giriş çıkış birimi.

NOT - Kalan 2 alan daha sonra kullanılmak için ayrılmış olup özel uygulamalar için kullanılabilir durumdaki yedek alanlardır.

Bu kartların en önemli avantajları olarak verilerin izinsiz girişlere ve veri değişikliklerine karşı korumalı olması gösterebilir. Bu kartın, okunması kartın bir temaslı kart okuyucuya sokulup üzerindeki çipin yüzeyine elektrik verilmesi sayesinde içindeki işlemcinin çalışmaya başlayıp iletişim için hazır hale gelmesiyle olmaktadır. Veri sadece bir işletim sistemi ve çipe yazılmış güvenilir verinin dışarıdan okunmasının engellendiği bir güvenlik mantığıyla okunmaktadır. Temelde hem yazılım yönüyle olsun hem donanım olsun özel durumlara bağlı olan sınırlandırılmış bir yazma, okuma ve silme yetkisi mevcuttur. Ayrıca bu kartlar manyetik şeritli kartlarla karşılaştırıldığında üzerindeki okunma yapıları (çip ve şerit) daha iyi dayanıklılık ve daha uzun ömür sunmaktadır. Akıllı kartlar

Artık akıllı kartlardan veri okumanın tek yolu temaslı kartlar kullanmak değildir. Akıllı kartlarda gelişen teknolojiyle birlikte yeniliklere açık bir duruma gelmiştir. Aşağıda akıllı kart tiplerinin ayrımlarını görmektesiniz. [2]

Şekil 4. Akıllı kart çeşitleri

1.2.2.1. Temaslı Kartlar

Bu tip kartların çipinin içinde şekil 1.'de de görüldüğü üzere 4 tane fonksiyon bloğuyla çevrilmiş olan, bunlar bir EEPROM(Electronically Eraseble Programmable Read Only Memory), RAM(Random Access Memory), ROM(Read Only Memory) ve I/O çıkışı, bir işlemci bulunmaktadır. ROM çipin işletim sistemini barındıran kısmını oluşturmaktadır. Bu kısım değiştirilemez. EEPROM çipin sabit hafızası görevini görüyor. Bilgiler ve program kodları işletim sisteminin denetiminde yazılıp okunabiliyor. RAM işlemcinin hafızası işlevi görmektedir fakat EEPROM'dan farklı olarak elektriksel temas kesildiğinde içindeki tüm datalar kaybolmaktadır. I/O kısmı ise data transferinde kullanılmaktadır.

Şekil 5. Bir çipli akıllı kart

Çağımızın sistemlerinde içerisinde birden çok uygulamanın çalıştığı kartlar kullanılmaya başlanmıştır. Bu kartlarda sadece işletim sistemi ROM'da tutulmaktadır. Diğer uygulamaya özel kısımlar EEPROM'da tutulmaktadır.

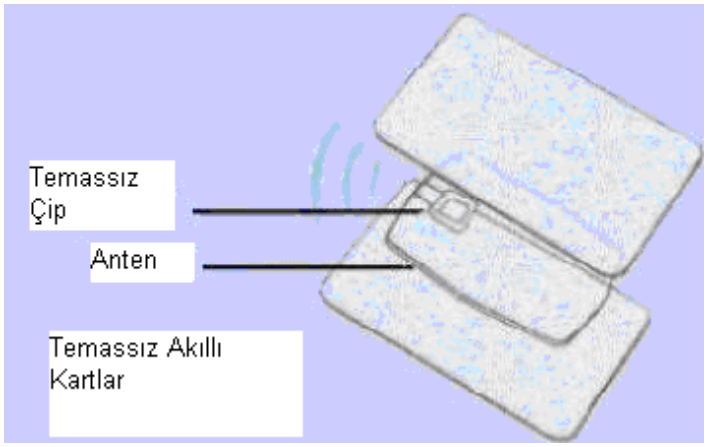
Artık flash hafızalar yavaş yavaş EEPROM'ların yerini almaktadır. Çünkü karşılaştırıldığında göz ardı edilemez avantajları vardır. İlki EEPROM'un üzerine yazma sayısı birkaç yüz bin ile sınırlıdır, bu da kartın yaşam süresini etkiler. Flash hafızada böyle bir sorun yoktur ve yazma konusunda da çok daha hızlıdır. RAM ile kıyaslandığında ise üretimin süresini uzatması ve sürenin uzamasının da ekstra maliyet getirmesi açısından pek olumlu bakılmamaktadır. Ayrıca flash hafızanın güvenliği konusundaki endişeler kullanılmasını engellemektedir. Buna karşın mikro işlemcili kartların gün geçtikçe kapasiteleri ve güçleri artmakta olup her gün yeni özelikler eklenmiş bir halde karşımıza çıkacaklardır.

Tablo 1. EEPROM ve Flash Bellek Kullanımı Arasındaki Farklar

	Flash	EEPROM
Yazma Sayısı	Sınırsız	100.000
Hız	Hızlı	Yavaş
Üretim Süresi	Uzun	Kısa
Maliyet	Yüksek	Düşük

1.2.2.2. Temassız Kartlar

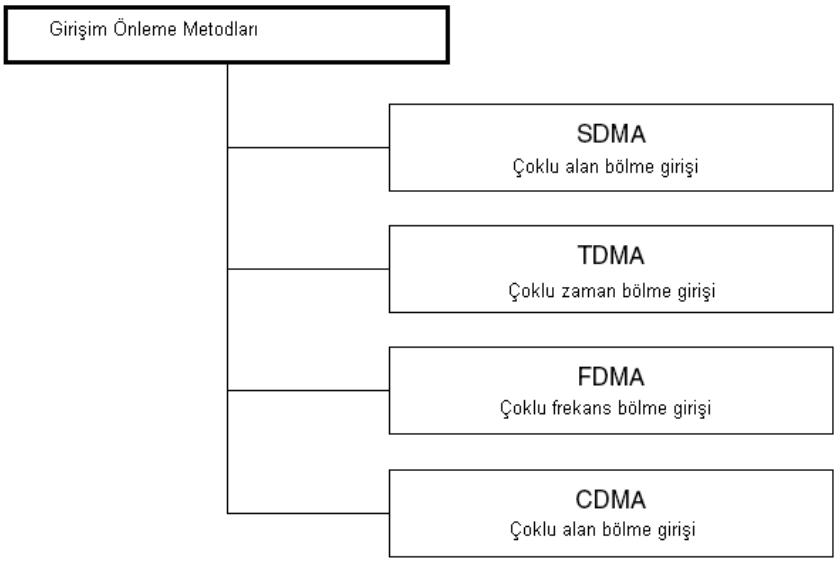
Çipli kartlardaki kontak yerleri en çok arızalanan yerlerin başında gelmektedir. Aşınma, aşırı elektrik yüklenmesi gibi sebeplerden dolayı arızalanan kart sayısı azımsanmayacak seviyededir. Bunu aşmanın en iyi çözüm yolu olarak temassız kartlar gösterilebilir. Temassız kartların çalışma mantığı radyo frekansı sinyalleri vasıtasıyla okuyucu ile kartın haberleşmesi temeline dayanmaktadır. Kart için gerekli olan enerji mikrodalga frekanslarıyla iletilmektedir. Bu kartın menzili 1 metreye kadar etkili olmaktadır ancak karta yazma için azami etkili menzil 10 cm ile sınırlıdır. Bunun sebebi kartın yazma için gereken güç ihtiyacının önemli ölçüde artmasından kaynaklanmaktadır. Temassız kartların terminalle haberleşmesi esnasında terminalden karta enerji, saat sinyali ve veri iletimi olur, karttan ise sadece veri transferi gerçekleşmektedir.



Şekil 6. Bir temassız kartın yapısı

Şekil 6'te görüldüğü üzere kartın tüm çevresini saran bir anten görev yapmaktadır. Bu antenin görevi kartın okuyucuyla haberleşmesini sağlamak ve veri iletimini kolaylaştırmaktır. Bu kartlardaki çipler normalde pasif halde bulunurlar. Çipin çalışması için gereken enerji okuyucudan alınır. Kart yaklaştırıldığında okuyucunun oluşturduğu manyetik alanla çip etkileşime girerek etkin hale geçer.

Kart okuyucunun menzilinde iki kart varsa ne olur buna bakmak gerekirse bunun için kullanılan çeşitli girişim önleme algoritmaları mevcuttur. Şekil 7'de görmektesiniz.



Şekil 7. Temassız kartların çakışma önleme algoritmaları

Bu yöntemleri açıklamak gerekirse SDMA(space division multiple access) okuyucunun sorgulama alanını (interrogation zone) belirli parçalara bölerek çoklu erişimi olanaklı hale getirmektedir. Bunun için elektronik olarak kontrol edilen doğrusal bir anten kullanılabilir, böylece bir etikete doğrudan ulaşılabilecektir. Sorgulama alanında farklı pozisyonlara sahip etiketler bulundukları konumdan dolayı ayrıştırılabileceklerdir. SDMA tekniğinin dezavantajı ise karmaşık bir anten sistemine ihtiyaç duymasından kaynaklanan maliyetlidir. FDMA(frequency division multiple access) çoklu iletişim kanalları için çoklu taşıyıcı frekanslar yoluyla iletim kurmaya dayanır. Her kullanıcı için bir frekans ayrılır ve kullanıcı veri göndermese de bekleme pozisyonunda bekler. TDMA(time division multiple access) ise FDMA ile büyük benzerlik gösterir. Farklı yanı belli bir süre için frekansı o kullanıcıya ayırmasıdır. Girişim önleme algoritmaları arasında en son çıkanı CDMA(code division multiple access)'dır. Burada herhangi bir zaman veya frekansta herhangi bir kullanıcı tarafından veri gönderilebilir. Bunlar arasında en sık kullanılanı TDMA'dir.

1.2.3. Çift Arayüzlü Kartlar

Çift arayüzlü kartların özelliği hem temassız kartların hem de temaslı kartların özelliklerini içinde barındırmasından gelmektedir. Normal kartlar gibi üzerinde altın renginde plakalı bir çip bulundurur. Kart okuyucuya takıldığında işlem normal bir şekilde gerçekleştirilir.

Bunun yanında aynı zamanda temassız kartlardaki gibi bir alıcı bulunur. İstenirse de bu alıcı sayesinde temassız okuyucularla kart iletişime geçip işlem gerçekleştirilebilir. Böylece eldeki bir kartla birden fazla durum için pratik bir kullanım olanağı sunulmuş olur.

1.3. Manyetik Ve Akıllı Kartlar Arasındaki Farklar

Akıllı kartlar manyetik kartlardan getirdiği fiyat yükü açısından daha yüksek bir maliyete sahip olup buna karşın bilgi güvenliği konusunda daha uygun bir çözüm sunmaktadırlar. Birden fazla kartı tek bir kartın içinde sunabilirler. Manyetik kartlar, sadece şerit kısmındaki verinin kopyalanması ile kırılabilirken akıllı kartlar, içlerinde yer alan güçlü şifreleme mekanizmaları sayesinde, verinin güvenli bir şekilde taşınmasını ve kullanılmasını

sağlar. Manyetik şeritli kartların şeritleri çok kolay bozulabilirler, manyetik alanlardan etkilenirler veya kolayca zarar görebilirler ve bu da şeritteki veriye erişimi imkansız hale getirir. Fakat akıllı kartlar çipli yapılarından dolayı ve datayı tutan mikroişlemcinin konumu itibariyle kolay kolay bozulmazlar.

Tablo 2'te birbirlerine karşı avantajlarının daha iyi anlaşılabilmesi için örnek bir gösterim yapılmıştır.

Tablo 2. Manyetik ve Akıllı Kartlar Arasındaki Farklar

	Akıllı Kart	Manyetik Şeritli Kart
Maliyet	Yüksek	Düşük
Bilgi Güvenliği	Yüksek	Düşük
Veri Şifreleme	Var	Yok
Sağlamlık	Sağlam	Sağlam değil

1.4. Akıllı Kart Tipleri Arasındaki Farklar

Bu iki kart tipi arasındaki temel fark, kartın üzerinde yer alan çipin kart okuyucuyla fiziksel olarak temas etmesi gösterilebilir. Maliyetleri yüzünden temassız kartlar geniş çaplı kullanım olanağı bulamamışlardır. Günümüzde bankacılıkta sadece düşük limitli işlem yapma izni verildiği için temaslı kartlara göre nispeten daha kullanışsızdırlar. Temaslı kartlar ayrıca hem hafıza hem de şifreleme gücü olarak daha güçlüdür.

Temassız kartlar kullanım alanları itibariyle çok hızlı veri aktarımı yapmaya gereksinim duyarlar bu yüzden hesaplamaların minimum düzeyde tutulması gerekmektedir. Bunun sonucu olarak güvenlik açısından daha düşük güvenlikli olduğu söylenebilir.

Tablo 3. Akıllı Kart Tipleri Arasındaki Farklar

	Temassız Kart	Temaslı Kart
Maliyet	Yüksek	Düşük
Bilgi Güvenliği	Düşük	Yüksek
Hafıza Miktarı	Düşük	Yüksek

Yukarıda görünen tabloda genel itibariyle akıllı kart tipleri için anlatılan farkların özeti bulunmaktadır.

2. AKILLI KARTLARIN ÖZELLİKLERİ VE YAPISI

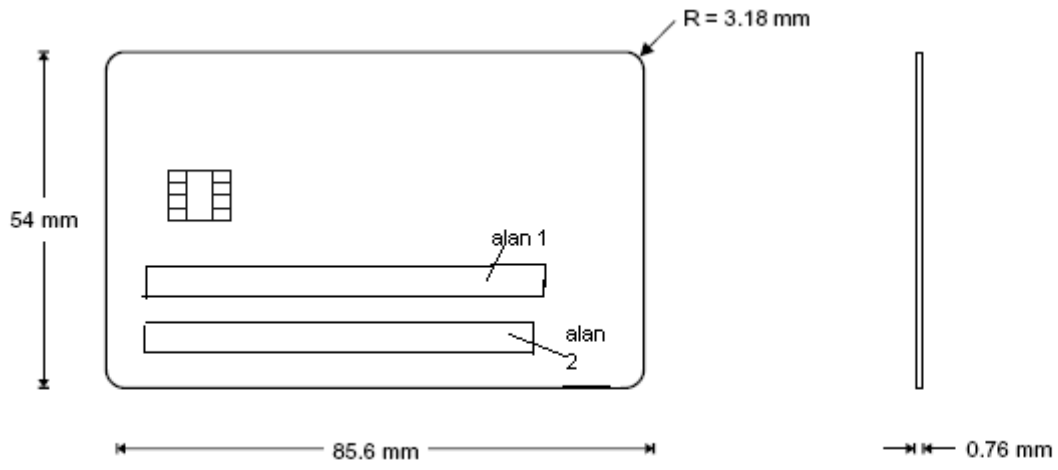
Akıllı kartlar yapıları itibariyle bir bilgisayarı andırırlar ve fiziksel özellikleri ISO standartlarıyla korunmuştur. Her kart üreticisinin uyması gereken bu standartlar okuyucularla akıllı kartlar arasında genel bir uyumluluk kurulmasını sağlar.

2.1. Fiziksel Özellikleri

Akıllı kartlardaki bilgisayar, bir CPU, hafıza sistemi ve genel amaçlı bulunan giriş çıkış hatlarına sahiptir. Tek çipli dizayndan bilgisayara doğru olan bilgi akışına engel olmak daha zorken birden fazla çip sayısına sahip sistemlerde çipler arasındaki bağlantılar saldırılara açık vaziyettedir.

2.1.1. Boyutları

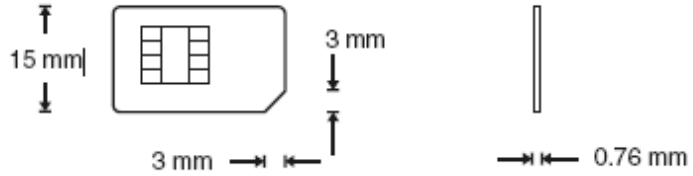
Temel kart biçimi ve boyutu 1985 yılında kabul edilmiş olan ISO 7810 standardında tanımlanan ID-1'dir. Bu manyetik ve çipli tüm kredi kartlarının uyduğu ortak boyut olup, aşağıdaki özellikleri taşımaktadır;



Şekil 8. Bir akıllı kartın yerleşimi

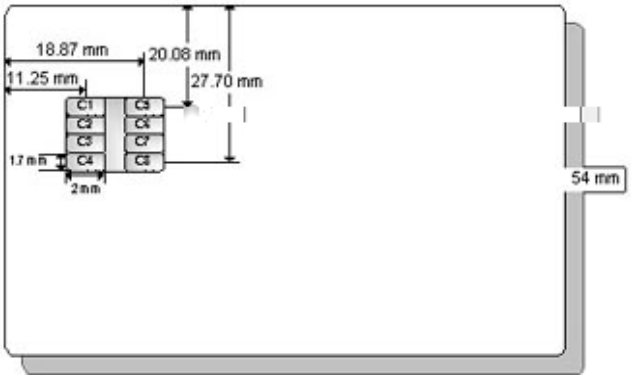
Kartların ön yüzünde 2 tane kabartmalı yazılmış alan bulunur. Resimde görülen bu alanlardan birincisi kart numarası için ayrılmıştır. İkinci alan ise kartın sahibinin ismini belirtir. Çipli kartlarda bu alanlardan ayrı olarak bir tane yonga bulunmaktadır. Kartın arka yüzünde daha önce manyetik şeritli kartlarda da anlatılan şekilde 3 kısımlı alan bulunmaktadır.

Cep telefonlarına baktığımızda ise ID-1 standartının boyutlarının büyüklüğünden dolayı normal akıllı kartları bu alanda kullanmanın imkânsızlığı göze çarpmaktadır. Cep telefonları için kullanmak üzere daha sonradan getirilmiş olan ID-000 formatı uygulanmaktadır. Bu formata göre boyutlandırmak gerekirse;



Şekil 9. ID-000 standartı kart boyutları

Akıllı kartların üzerindeki çiplerin yerleşimi ise 1988'de kabul edilmiş olan ISO(International Organization for Standardization) 7816-2 standartlarına göre olmaktadır.



Şekil 10. Bir akıllı kartın boyutları

Kartların sağlamlığı ile ilgili standartlar ISO 7810, 7813 ve 7816'a göre belirlenmiştir. Buradaki belirtilen standartlarda kartın UV ışınlarına, X-ray ışınları, kartın yüzey profili, kartın ve temas kontaklarının mekanik dayanıklılığı, elektromanyetik duyarlılık, akımlar, ısı dayanıklılığı gibi alanlardaki ölçülerini gösterir.

2.1.2. Akıllı Kart Hafıza Sistemi

Akıllı kartların hafıza sistemi çipin ufak yapısından dolayı oldukça sınırlıdır.3 çeşit hafıza yer alır. ROM genel amaçlı kartlarda genellikle 8 KB ile 96 KB arasında değişir. Bu kısımda işletim sistemi tutulur. Şifreleme veya özel aritmetiksel yapıların yanında iletişim ve bakım için de gerekli kısımları içermekte ve bu alanlar kart üretildiği zaman yerleştirilmektedirler. Daha sonrasında da değiştirilememektedirler.

Elektronik programlanabilir silinebilir ROM(EEPROM) hafıza ise çeşitli kart bilgilerini içerir. Örneğin hesap bilgileri, loyalty diye tabir edilen kart sahibinin puan durumu, elektronik para miktarı vb. Bu kısım uygulama programlarıyla yazılıp okunabilir. RAM'den farkı elektrik akımı olmadığında da içindeki bilgileri saklayabilmesinde yatmaktadır. Bunlarda en çok iki problem tipi görülebilir;

- Yavaşlık: EEPROM'a yazmak genelde 3 ile 10 ms arasında sürmektedir.
- Data Kaybı:100000 kez yazıldıktan sonra işlevini yitirmektedir.

Akıllı kartlarda RAM(Random Access Memory) adlı bir hafıza modülü de bulunmaktadır. Bu hafıza genelde 2000 bytedan daha küçüktür. Elektriksel teması kesildiğinde içindeki veriler kaybolmaktadır. Üzerine yazma limiti bulunmamakla beraber EEPROM'lardan 10000 kez daha hızlı yazılabilmektedir.

2.1.3. Akıllı Kart İşlemcisi

Çağımızda akıllı kart teknolojisinde kullanılan işlemciler basit 8 bit mikrokontrolörlerden 32 bit yapılara kadar değişmektedir. Bu seçim genelde kod yoğunluğu, güç ihtiyacı, ataklara karşı olan dayanıklılık ihtiyacına göre yapılmaktadır. 32 bit işlemcili kartlar 8 bit işlemcilere göre daha iyi bir veriyolu, daha yüksek bir işlem hızı sağlamakta olup, buna karşın daha büyük entegre devre boyutundan dolayı daha yüksek maliyet ve daha fazla güç ihtiyacı gibi dezavantajlara sahiptir. Genellikle Motorola 6805 veya Intel 8051 işlem setleri kullanılmakta ve saniyede 1 milyon işlem yapabilme hızına sahiptirler.

Bir akıllı kartın yaptığı işlem 1 ile 3 saniye arasında değişmektedir. Bu süre 1024 bitlik bir RSA şifreleme işleminde 10 saniye veya daha fazla olabilmektedir. Bu yüzden bu işlem yükünü hafifletmek amacıyla yardımcı bir işlemci yerleştirilmiştir. Çoğu işlemci

RAM'in içindeki kodları çalıştırmayacak şekilde üretilir. 64 KB ile sınırlandırılmış adreslendirme hakkına sahiptir. Entegre devre boyutu ne kadar büyürse çipin kırılganlığı da o ölçüde artar, o yüzden genellikle $23mm^2$'den büyük üretilmezler. Ayrıca mikrokontrolörler herkese satılmaz böylece bulunabilirlikleri az olacağı için bir saldırganın analiz etmesi zorlaşır.

2.1.4. Akıllı Kartların Giriş Çıkış Yapıları

Kartlardaki giriş çıkış yapılarının çalışması tek yönlü seri kanalla sağlanır. Yani bir veri bir anda bir yönde akar. Veri transfer hızı olarak en fazla 115200 bps olabilmektedir. Host bir karta veri gönderdiğinde bir cevap için dinlemeye başlar. Host mesaj göndermeden kart gönderemez. Ayrıca çip içindeki işletim sistemi de bu giriş çıkış verilerini bloklama ve bunun gibi işlevleri düzenleme hakkına da sahiptir.

2.2. Akıllı Kartların Yazılımsal Yapısı

Akıllı kartlarda yer alan işletim sistemleri, her kart üreticinin ürününe özel bir yazılımdır. Bu yazılım, kartın ROM'una yüklenmiş ve korumalı olarak tutulmaktadır. Bunun yanında özel amaçlı uygulamalar ise EEPROM'da yer almaktadır.

İşletim sisteminin görevleri arasında dosya yönetimi, güvenlik, I\O yönetimi, komutların kontrolü, uygulamalar vb sayabiliriz. Akıllı kartlardaki bu yazılım PC'deki işletim sistemlerine benzemektedir. Farklı olarak daha az hafızaya sahiptir, daha güvenlidir ve kullanıcı arayüzü bulunmamaktadır.

İlk zamanlarda ortaya çıkan işletim sistemi yapılarından gelişmiş diye söz etmek mümkün değildi. İlk çıkan işletim sistemi diyebileceğimiz yapı STARCOS'tu. STARCOS ile birlikte Gemplus'tan MPCOS, Siemens'ten CardOS, GIS'ten OSCAR ortaya çıkmıştır.[3] STARCOS birkaç uygulamanın depolanıp yönetilmesine izin veriyordu. Ancak günümüzde akıllı kartlarda kullanılan işletim sistemlerinin yapısı ve sayısı oldukça arttı. Aşağıdaki tabloda en popüler işletim sistemleri görülmektedir;

Tablo 4. Akıllı kartlarda işletim sistemleri

İşletim Sistemi	Üretici	Maksimum Hafıza Boyutu	Uzantısal
Cryptoflex™	Schlumberger	32 KB	Evet
MPCOS-EMV 128k™	Gemplus	16 KB	Evet
Cyberflex Access™	Schlumberger	32 KB	Evet
GemXpresso211/V2	Gemplus	32 KB	Evet
SIMphonIC™	Oberthur	32 KB	Evet
SIMtelligence 32/J Java™	Orga	32 KB	Evet

Bu işletim sistemleri bildiğimiz klasik işletim sistemi mantığıyla geliştirilmektedir. Terminalle kart arasında PC'dekine benzer bir yapı kurulmuştur. Sunucu komut üretir sonra bu karta iletilir. Kart bu komutu çalıştırır ve sonucu sunucuya bildirir. Sonra da yeni komutu beklemeye başlar. Burada ana amaç problemsiz bir şekilde istikrarlı bir ortamda karttaki uygulamaların çalıştırılabilmesidir. Akıllı kartlardaki işletim sistemlerinin en büyük engeli olarak bir kart için onun işlemcisine uygun üretilmiş işletim sisteminin başka kart için çalıştırılamaması gösterilebilir.

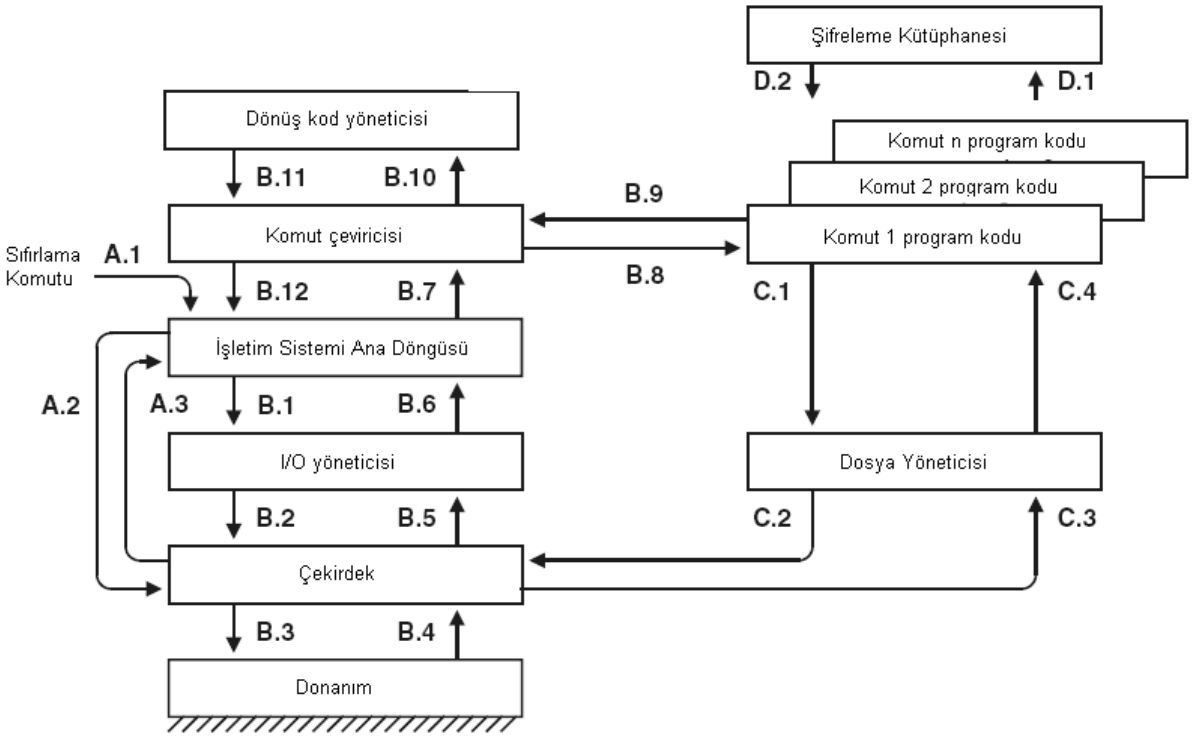
Mevcut GSM kartların işletim sistemlerinde artık hafıza yönetimi, çoklu dosya sistemi gibi uygulamalarla çoklu uygulamalı işletim sistemi yapısına yaklaşmışlardır. Bunların üretildiği komut standartları ISO 7816 ve CEN 726'da tanımlanmıştır. Çoğu kart üreticisi bu standartlardaki komutların yanı sıra kendi özel komutlarını da karta eklemektedir.

İşletim sisteminin I/O yöneticisi hata denetimi yapma ve süreçleri düzeltme gibi bir işleve sahiptir. Eğer bir mesaj hatasız olarak alınırsa şifre çözülür, eğer şifre çözme başarısız olursa mesaj geri gönderilir. Eğer başarılı olursa hangi kanal uygunsa o kanaldan durum makinesine gidilip mesajın durumuna bakılır. Yasaklanmamış ve parametre değerleri izin veriliyorsa dosya yöneticisi tüm mantıksal adresleri fiziksel adreslere çevirir ve fiziksel adresli EEPROM için gerekli olan tüm yönetimsel fonksiyonları gerçekleştirir.

Akıllı kart dosya sistemi, klasör tabanlı, hiyerarşik, tek köklü, uzun sayısal dosya isimlerine sahip olabilecek şekildedir. DOS veya UNIX dosya sistemiyle benzerlikler gösterir.

En bariz fark, akıllı kartların uygulamaya özel dosya içermemesidir. Akıllı kart işletim sistemleri yazma, silme, değiştirme gibi dosya komutlarını destekler.

Bir komutun işlenmesi önce akıllı kartın I/O girişinden komutu almasıyla başlar. I/O yöneticisi hata kontrol mekanizmasını çalıştırır. Komutun hatasız olduğu kontrol edildikten sonra güvenli mesaj yöneticisi(secure messaging manager) şifresini çözer ve doğruluğunu kontrol eder. Bundan sonra komut yorumlayıcısı(command interpreter) mesajı deşifre eder. Eğer deşifre etme sırasında bir hata oluşursa o zaman cevap kodu yöneticisi çağrılır(return code manager). Deşifre edilme tamamlandıktan sonra mantık kanalı yöneticisi(logical channel manager) hangi kanalın seçildiğini anlar ve durum makinesini çağırır(state machine).



Şekil 11. Akıllı Kart İşletim Sisteminin Çalışma Şekli

Durum makinelerinin görevi, komut dizilerini tanımlamaktır. Bir dizinin ilk komutu karta gönderildiğinde aktif hale geçmektedir. Durum makinesi, komut ve komuta eşlik eden parametrelere akıllı kartın o an izin verilip verilmediğini kontrol eder ve izin verilmişse; komutu çalıştırır. İzin verilmemişse terminal cevap kodu yöneticisinden ve I/O yöneticisinden hata mesajını alır.

Komut çalıştırılırken bir dosyaya erişilmeye ihtiyaç varsa dosya yöneticisi çağrılır. Dosya yöneticisi, bir dosyanın mantıksal adresini onun çip üzerindeki fiziksel adresine çevirir. Gerekli görüldüğünde dosyaya erişim durumlarını test eder.

Cevap kodu yöneticisi, bir durum için gerekli olduğunda cevap dönüşü yapmaktadır. Çağıran program kısmı için bir cevap üretir ve bu cevabı I/O yöneticisi üzerinden terminale iletir.[18]

Şekil 11'de bir işletim sisteminin çalışma şekli gözükmektedir. A kısmında işletim sisteminin açıldığı anda kullandığı çağrılar yer almaktadır. B kısmında bir komut çağrıldığında işletim sisteminin nasıl davranacağını göstermektedir. C kısmında bu komut çağrıldığında bir dosyaya erişim sağlanması gerektiğinde işletim sisteminin nasıl davranacağını anlatmaktadır. D kısmında ise işletim sisteminin şifreleme algoritmalarını çağırma şekli yer almaktadır.

2.3. Akıllı Kart Okuyucular

Akıllı kart okuyucuları, kart üzerinde yer alan yongaya okuma ve yazma işlemi yapan cihazlardır. Bu okuyucular çok çeşitli şekillerde ve arayüzlerde bağlantı sağlayabilir. Örneğin; RS232 seri portlarından, USB portlarından, PCMCIA slotlarından, disket slotlarından, paralel portlardan, kızılötesi portlardan ve klavyelerden bağlanabilir.

Kart okuyucu sunucu ile kart arasındaki fiziksel bağlantıyı sağlamaktadır. Buradaki sunucudan kastedilen bir PC olabileceği gibi tek başına çalışan başka bir cihazda olabilmektedir. Okuyucu elektrik akımını karta verir, kartı tanımlar ve sunucu ile kart arasında aracı gibi çalışır. [19]

2.4. Akıllı Kart Uygulamaları Arasındaki Farklar

Tek uygulamalı kartların çiplerinde tek bir program için yer vardır. Bu da maliyeti düşürmesine karşın kullanılan az sayıdaki uygulamanın sunduğu sınırlı özelliklere mahkum

ettiği için pazarlama değeri açısından büyük problem teşkil eder. Kullanıcı tek bir uygulamanın sağladığı faydalardan yararlanır.

Çok uygulamalı akıllı kartlar ise birden çok özelliği aynı anda destekler. Böylece daha esnek, daha kullanıcı dostu uygulamaların kart içinde kullanımının önü açılmaktadır. Örneğin, bir kart tek uygulamalı olduğunda sadece kimlik kartı olarak kullanılabilecek iken çok uygulamalı olduğunda aynı anda kimlik kartı, toplu taşıma kartı, kredi kartı olarak uygulanabilir. Bu sayede kullanıcı birden fazla kart taşıma zahmetinden kurtulmasının yanı sıra iki kartın maliyetinden daha düşük bir fiyata aynı özelliklere sahip olmuş olur.

Tablo 5. Kartların Uygulamalarına Göre Karşılaştırılması

	Tek Uygulamalı Kartlar	Çok Uygulamalı Kartlar
Maliyet	Düşük	Daha Yüksek
Esneklik	Düşük	Yüksek
Pazarlama Değeri	Düşük	Yüksek

Tablo 5'de çok uygulamalı kartlar ve tek uygulamalı kartların karşılaştırılmasının özet şeklinde gösterimi mevcuttur. Bu tabloda üç ölçüte göre karşılaştırma yapılmıştır. Bunlar maliyet, esneklik, pazarlama değeridir.

3. AKILLI KARTLARDA ŞİFRELEME TEKNİKLERİ

Bilindiği üzere akıllı kartların en önemli özelliklerinden birisi şifreleme işlemleri için içinde işlemci bulundurmasıdır. Hatta bu işlemcinin yetersiz görüldüğü durumlar için içine yardımcı bir işlemci daha yerleştirilebilmektedir. Bu kartların özel anahtarları güvenli depolayabilme özelliği ve modern algoritmaları çalıştırabilme yetenekleri onları güvenilir çevrimdışı ödeme sistemi haline getirmiştir. Ama önce genel anlamda şifreleme sistemlerinden bahsetmek gerekir. Daha sonra bu konuyu açmak maksadıyla kartlardaki kullanımına bakabiliriz. Şifrelemenin temeli iki kısımdan meydana gelmektedir.

- Encrytion

Temel olarak bir bilgiye ulaşmasını istemediğimiz bir kişi tarafından erişilse bile okunmasını engellemek amacıyla bir anahtar vasıtasıyla şifreli hale getirilmesi olayıdır.

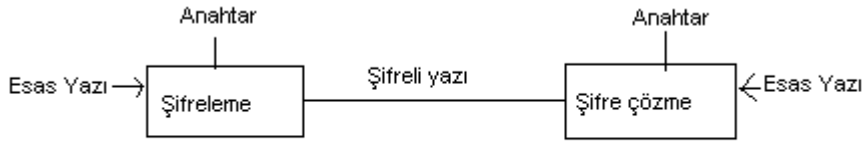
E(P) => C şeklinde ifade edilebilir. Buradaki P şifrelenmesini istediğimiz yazı, E şifreleme fonksiyonu ve C'de yazının şifrelenmiş halini temsil etmektedir.

- Decryption

Şifrelenmiş bir bilginin okunabilmesi amacıyla bir anahtar vasıtasıyla normal haline dönüştürülmesi işlemidir.

D(C) => P şeklinde ifade edilebilir. Buradaki P esas yazımız, C şifreli hali ve D ise decryption fonksiyonunu göstermektedir.

Burada anahtar diye tabir edilen kısımlar şifreleme ve şifreyi çözmek için gerekli olan matematiksel karakterlerdir.



Şekil 12.Şifreleme ve şifre çözme mantığı

Birkaç çeşit şifre kırma yöntemi ile saldırgan kırmayı deneyebilir. Bunlar;

A-Sadece şifreli yazıyı bilerek(*Ciphertext-only attack*): Veri güvenliği konusundaki saldırının sadece şifreli mesaj üzerinden yapılması (Ciphertext only attack, COA) durumudur. Basitçe saldırganın elindeki tek bilgi şifrelemede kullanılan method ve şifreli mesajın kendisidir. Şayet saldırgan açık mesajın alabileceği değerleri azaltmayı başarır ya da daha büyük bir başarıyla anahtarı veya açık mesajın kendisini bulabilirse başarılı sayılır.

Gelişmiş bütün şifreleme yöntemleri bu konuda saldırıya karşı dayanıklı olarak tasarlanmakta ve sadece şifreli mesajdan yapılan saldırılarla anahtarın ve açık mesajın alabileceği değerlerin azaltılması engellenmektedir.

B- Bilinen şifrelenmemiş yazıyla(*Known-plaintext attack*):Saldırgan bir verinin hem şifreli hem de şifresiz halini bilir ve bunları kullanarak anahtar fonksiyonu elde etmeye çalışır. Daha sonra bu anahtar fonksiyonuyla diğer şifreli mesajları ele geçirir.

C-Seçilmiş şifreli veri veya seçilmiş esas yazıyla(Chosen-plaintext attack): Veri güvenliğinde bir şifreleme yöntemine saldırı yapılırken saldırganın istediği bir mesajı şifrelemesi ve bu istenen açık mesajın şifreli haliyle birlikte ele geçirmesi durumudur. Genellikle asimetrik şifreleme yöntemlerinde (açık anahtar şifrelemesinde), açık anahtarın (public key) kullanılarak mesajın şifrelenmesi ve şifreli mesajın ele geçirilmesi için kullanılır. Bu saldırı yöntemine dayanıklı olan bir şifreleme yöntemi aynı zamanda bilinen açık mesaj saldırısına (known plain text attack) ve sadece şifreli mesaj saldırısına (cipher text only attack) dayanıklı olmak zorundadır.

Şifreleme sistemleri anahtar yapısına göre ikiye ayrılır. Şifreleme ve şifre çözme anahtarının aynı olduğu sistemler simetrik veya gizli anahtarlı şifreleme sistemleri, şifreleme

ve şifre çözme anahtarlarının farklı olduğu sistemler ise asimetrik veya açık anahtarlı şifreleme sistemleri diye adlandırılır.

Açık anahtarlı sistemlerin avantajları ve dezavantajları yıllardır çeşitli konulara malzeme olmuştur. Akıllı kartlarda kullanılırken bu tip kartların işlemcilerine özgü çeşitli sınırlandırmalarla karşılaşmıştır. Bunlar arasında en önemli problem olarak limitli işlem yapma gücü gösterilebilir. Fakat son zamanlarda açık anahtarlı sistemlerin performansını önemli ölçüde arttıracak hem donanımsal hem yazılımsal olarak gelişmeler yaşanmıştır. [5]

Akıllı kartlarda günümüzde en sık olarak kullanılan şifreleme yöntemleri 3-DES ve RSA'dır. Bu yöntemlerin anahtarları RSA için oluşturulur veya DES için önceden yüklenir.

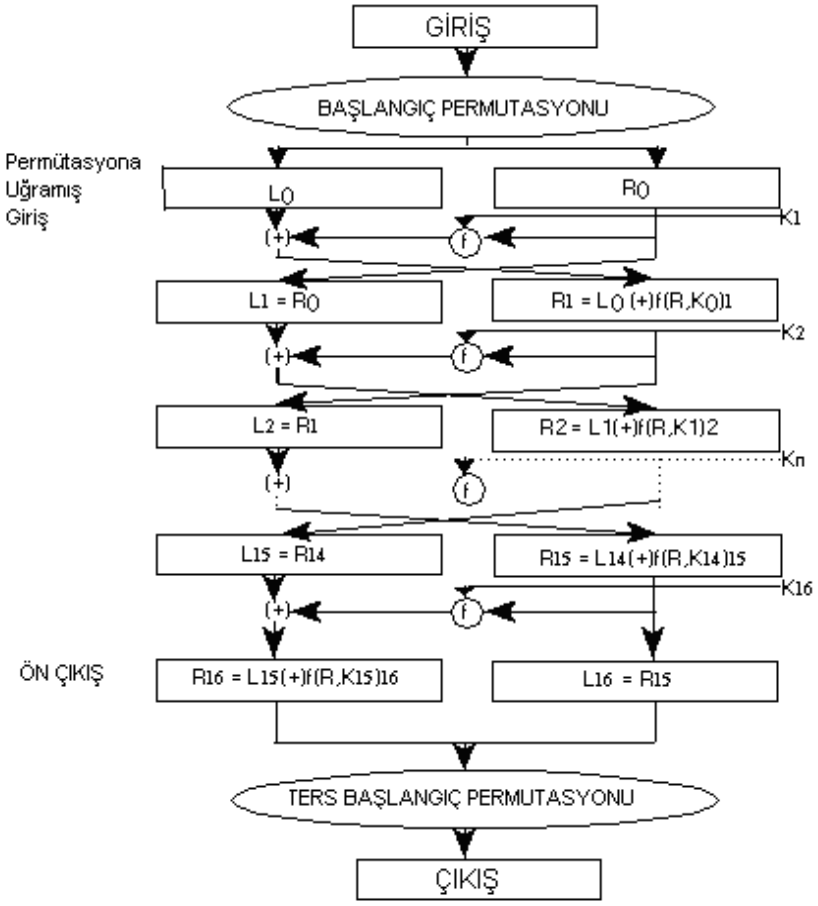
3.1. Simetrik Şifreleme

Simetrik şifreleme ya da diğer adıyla gizli anahtarlı şifreleme sistemleri, şifrelemek ve şifreyi çözmek için kullanılan anahtarların aynı olduğu şifreleme sistemidir.

3.1.1. Data Encryption Standard (DES)

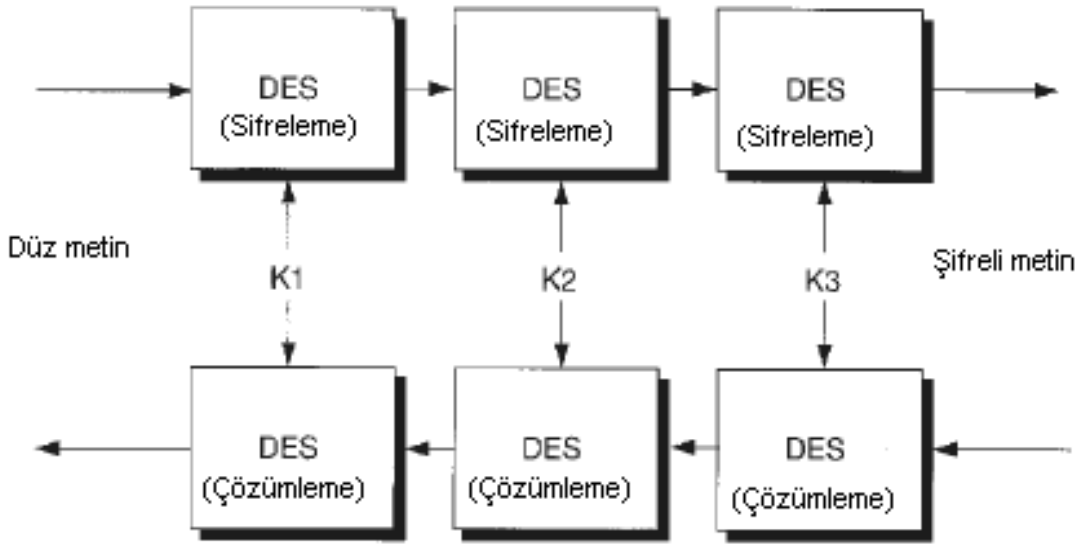
Akıllı kartlarda kullanılan şifreleme yöntemlerinden bir tanesi DES'tir. ISO 8731-1 ve ISO 8372 ile standartları belirlenen DES akıllı kartlar için uygulama şifresi oluşturma, kullanıcı doğrulama ve güvenli mesajlaşma için kullanılmaktadır.[11]

DES algoritması temel olarak basit mantıksal (lojik) işlemler kullanmaktadır. Yöntem, 64-bitlik veri bloklarını, 64-bitlik bir anahtarın 8. bitlerini kullanmadan 56-bitlik anahtar kullanılarak şifreler. Yani kullanılabilecek anahtar sayısı 2^{56} = 72.057.594.037.927.936'dır (yaklaşık 72 katrilyon). Bu anahtarlardan çok az bir kısmı kullanılarak şifrelenen metinler kolayca çözülebilir. Bunlar zayıf anahtar (weak key) olarak adlandırılır. DES algoritmasının detayları [2] ve [3] kaynaklarından edinilebilir.



Şekil 13. DES algoritmasının çalışma şekli

DES algoritmasının güvenli olmadığı ve anahtar boyutunun artırılması gerektiği Bruce Schneier tarafından daha önce dile getirilmişti [4]. DES ile şifrelenmiş verinin ikinci bir anahtarla şifre çözme işlemine tabi tutulması ve elde edilen bu verinin farklı bir anahtarla tekrar şifrelenmesi ile oluşan 3-DES (triple-DES, üçlü-DES) algoritması, DES algoritmasından 2^{56} kat daha güçlüdür.[7] Başka bir deyişle kaba kuvvet atağı ile DES algoritmasını 1 saniyede kırılabilen bir sistemin 3-DES algoritmasını kırması 2 milyar yıldan fazla sürer. Bruce Schneier bu durumu "Bu galakside 3-DES'i kaba kuvvet atağı ile kırabilecek kadar silikon veya güneş yok olmadan önce kırabilecek kadar zaman yok" sözü vurgulamıştır. Bu şifreleme yöntemi günümüzde bütün bilinen saldırılara karşı iyi bir güvenlik sağlamaktadır.



Şekil 14. 3DES algoritmasının çalışma şekli

Dezavantajlarına gelince her simetrik şifreleme yönteminde olduğu gibi aynı anahtarın hem mesajı şifreli hale getirme hem de şifre çözme için kullanılıyor olmasından kaynaklanan sorunlar problem oluşturmaktadır.

3.1.2. AES

AES (**A**dvanced **E**ncryption **S**tandard; Gelişmiş Şifreleme Standardı), uluslararası olarak kullanılan bir şifreleme (kripto) sistemidir. Belçikalı Vincent Rijmen ve Joan Daemen tarafından geliştirilmiş, DES'in ve diğer olası algoritmaların zayıf ve paranoyak yönlerini tamamen temizleyerek, matematikle oluşturulmuş algoritmadır. Bruce Schneier'in twofish'ini ve RSA'in RC6'sini eleyerek 1997'de NIST'in yarışmasını kazanmış ve yeni şifreleme standardı olmuştur. DES'in linear ve differential cryptoanalysis karşısında yenik düştüğü durumlara düşmemesi için özel önlemler alınmış, round içerisindeki xor'lamaların birbirine yakın bitlerdeki probabilistic bias'larının takip edilememesi için, des'te yer almayan mixcolomn ve shiftrow türü işlemlerle 128 bitlik 8 bitlik 4 satır ve 4 sütüna ayrılmış plaintexti çorbaya döndürmektedir. Bugün bilinen tüm akademik ve pratik saldırılara, bruteforce'lara karşı dayanıklı olduğu düşünülmektedir. 128, 256 ve 512 bitlik key'leri destekleyebilmekte, 8

bitlik akıllı card işlemcilerinden 128 bitlik olası fütüristik çiplere kadar destekleyebilecek şekilde tasarlanmıştır.

AES algoritmasının akıllı kartlarda uygulanma alanları ise 3G mobil uygulamaların güvenliğini sağlamak için kullanılan ana temellerden bir tanesi olarak yer almaktadır. Mobil iletişim işlemlerinin güvenilirliği, onaylanması ve bütünlüğünü sağlama amacıyla kullanılır. Temel olarak akıllı kartların yapısından dolayı 3 faktör gözetilerek uygulanır.

- Mümkün olduğunca az RAM kullanmak
- Uygulamayı mümkün olduğunca hızlı yapmak.
- Uygulama side-channel attacks diye tabir edilen saldırıları hesaba katmalı.

3.2. Açık Anahtar Şifrelemesi

Akıllı kartlarda dijital imza oluşturmada kullanılan algoritmalardan açık anahtar şifreleme algoritması RSA en sık kullanılan algoritmadır. Bunun temel sebebi mevcut tüm sistemin zamanında RSA'ı temel olarak alıp daha sonra bunu değiştirilmesinin maliyetinin büyüklüğü karşısında mevcut yapının uygulanmaya devam etmesidir.

The EMVCo Security Working Group (SWG) şu anda ki bankacılık sisteminde kullanılan akıllı kartlardaki mevcut şifreleme sistemi yerine geçecek yeni bir şifreleme sistemi arayışındadır. Çünkü 1984-bitlik mevcut sistem ömrünü doldurmaya başlamıştır. US National Institute of Standards & Technology (NIST) günümüzdeki RSA anahtarları yapısının ömrünü 2025 ve 2030 yıllarında dolduracağını öngörüyor. EMVCo kalan mevcut süremiz içerisinde yeni bir şifreleme yapısı için gereken süreyi 12 ile 15 yıl olarak hesaplamıştır.

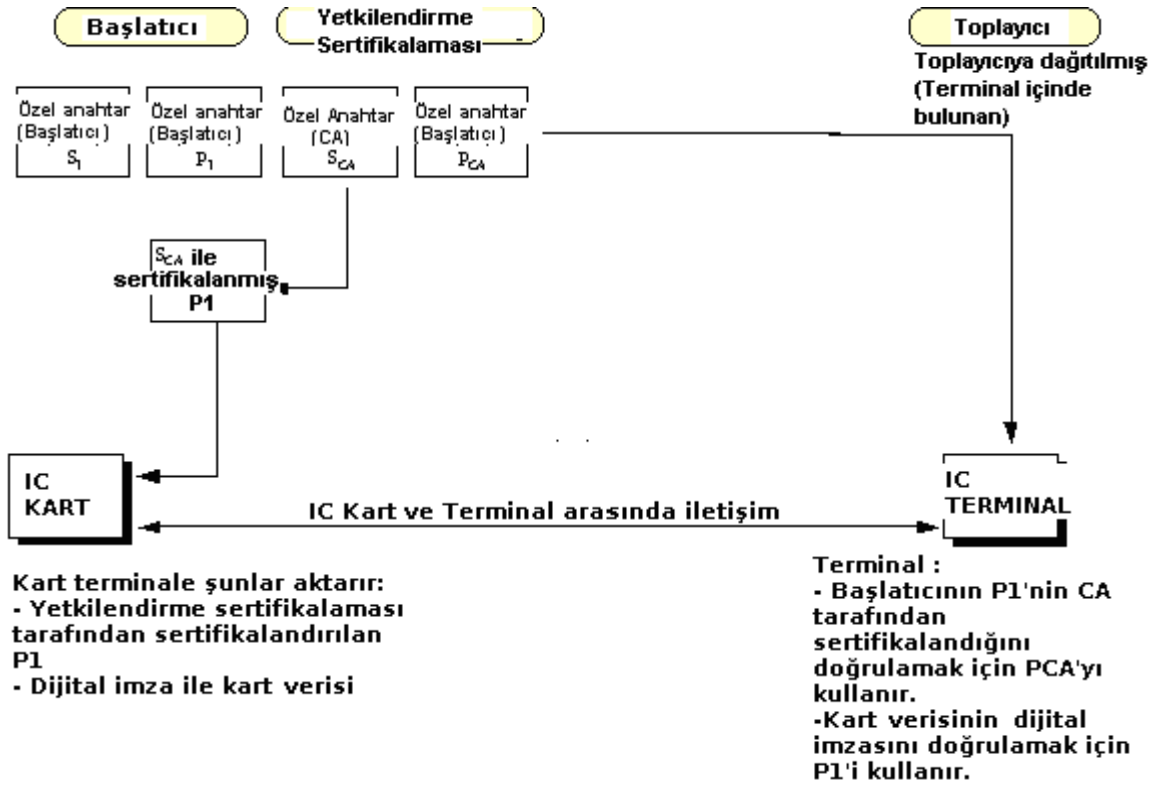
Bunun akabinde The SWG'nin yaptığı çalışmalarda 3 seçenek üzerinde durulmuştur.

- RSA algoritmasının kullanılmaya devam etmesi-Kart anahtarları hariç mevcut anahtar boylarının iki katına çıkartılması.
- RSA algoritmasının kullanılmaya devam etmesi-Kart anahtarları dâhil tüm anahtar boylarının iki katına çıkartılması
- Eliptik Eğri Şifrelemesi kullanılması [13], [14],[15]

Akıllı kartların en önemli kullanım yeri olan bankacılıkta açık anahtar şifrelemesinin kullanıldığı veri onaylama türleri iki çeşittir; Statik veri onaylama ve dinamik veri onaylama.

3.2.1. Statik Veri Doğruluğunu Onaylama(SDA)

SDA işleyişi tamamıyla bir sertifika otoritesi üzerine kurulmuştur. Banka(Issuer) bir açık ve bir tanede gizli anahtar çifti oluşturur. Sertifika otoritesi çok güvenli bir yapı olup o da kendi açık ve gizli anahtarına sahiptir ve sertifika otoritesinin açık anahtarı daha önceden EMV kart destekleyen bir terminale yüklenmiştir. Issuer kartın içindeki finansal bilgiyi kendi gizli anahtarıyla imzalar oluşan imzayı karta yerleştirir. Bir kart terminale yerleştirildiğinde ve SDA seçilmişse terminal sertifika kurumunun açık anahtarını issuerın açık anahtarının doğruluğunu onaylamak için kullanır. Sonra issuerın açık anahtarını kartta bulunan finansal verideki imzayı doğrulamak için kullanır ve bu işlem tamamlandığında terminal bu datanın değiştirilmemiş olduğundan emin olmuş olur.



Şekil 15. SDA işleyişi

3.2.2. Dinamik Veri Doğruluğunu Onaylama (DDA)

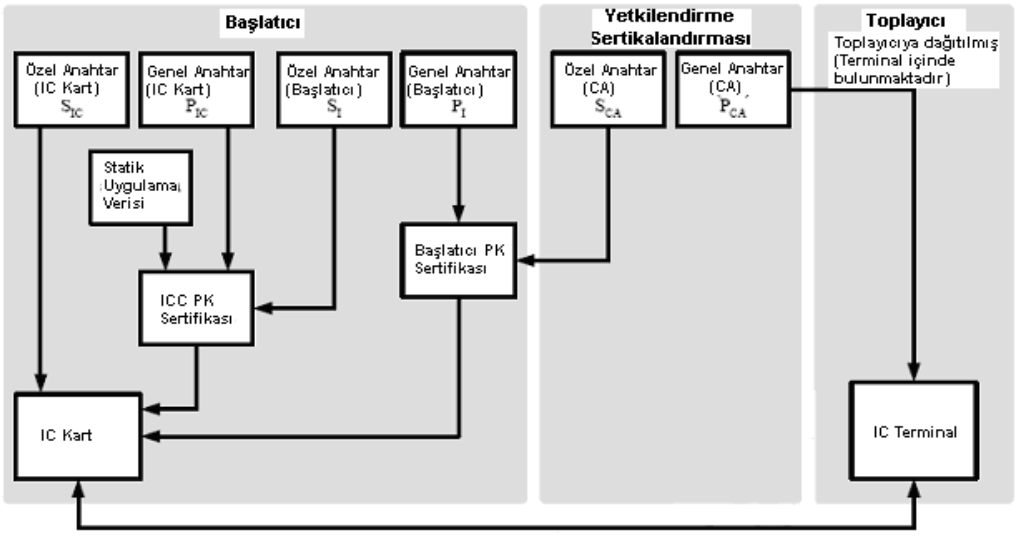
DDA'da SSAD(signed static application data) issuer tarafından imzalanmış bir ICC açık anahtar sertifikası tarafından yerleştirilir. İşlem esnasında, ICC dinamik işlem verisi üzerinde bir açık anahtar dijital imzası oluşturur.

Terminale işlem sırasında çipli kartın açık anahtar sertifikası ve issuer sertifikası gönderilir. Bu terminale SDA'deki gibi onaylanmış issuer açık anahtar kopyasını elde etmesini sağlar. Aynı şekilde daha sonra bu kart açık anahtar sertifikasının doğruladığı anahtarı kullanarak çipli kart açık anahtar sertifikasını elde eder.

Çipli kart üzerindeki gizli anahtarı kullanarak bazı işlem datalarını imzalar. Dijital imzanın sonucu olarak Signed Dynamic Application Data (SDAD) terminale sağlanır. Daha önceden alınmış çipli kart açık anahtarı kullanılarak terminal bu verinin doğruluğunu onaylar.[12]

DDA ile SDA'in temel farkı DDA kendi anahtar çiftine sahip olduğu için bağlantısız (offline) PIN onaylama yapabilir. Kart aynı zamanda kendi hesaplama yeteneğine sahiptir. [8]

Aşağıdaki şekilde bu olayın ayrıntısı görülmektedir;



Şekil 16. DDA İşleyişi

Karttan terminale geçenler:

- Issuer PK sertifikası
- ICC PK sertifikası
- Kart tarafından imzalanmış kart ve terminal dinamik verileri

Terminal'de:

- Pca Sertifika otoritesi tarafından sertifikalanmış issuer'ın public keyini doğrulamak için kullanılır.
- Pı issuer tarafından sertifikalanmış Pıc ve statik uygulama verisini doğrulamak için kullanılır.
- Pıc, kart tarafından imzalanmış veriyi doğrulamak için kullanılır.

RSA ile eliptik eğrinin matematiksel işlev türlerinin farklılıkları akıllı kartlardaki kullanım kolaylığı bakımından da büyük bir fark oluşmasını sağlamaktadır.

3.2.3. RSA

Açık anahtar şifrelemesinde hem metni şifreli hale getirmede hem de onaylamada uygulanan standart algoritma RSA algoritmasıdır. RSA algoritmasının ismi 1978 yılında MIT'de çalışırken onu bulan kişilerin baş harflerinin (Rivest, Shamir, Adleman) birleşmesinden oluşmuştur. Bu algoritmanın güvenliğinin, kırılmasının zorluğunun temelinde çarpanlara ayrılacak sayının çok büyük alınması yatmaktadır.

RSA algoritması üç kısımdan oluşur.

A)Anahtar Oluşturma

Anahtar oluşturma işlemi için asal sayılar kullanır. Bu sayede daha güvenli bir yapı oluşturulmuş olur.

-İki tane asal p ve q sayısı seçilir.

-N=p*q hesaplanır.

- φ(N) = (p − 1)(q − 1) hesaplanır. (φ Euler'in totient fonsiyonu)

-Bir tane e tamsayısı seçilir. Bu seçilen e tamsayısı 1'den büyük ve φ(N)'den küçük olmalıdır. Aynı zamanda φ(N) ile aralarında asal olma şartı taşımalıdır.

-e tamsayısının mod(φ(N))'e göre tersi alınır. Bu tamsayı d gibi bir harfle gösterilir.

- e ve N sayıları özel anahtarı, d ve N özel anahtarı oluşturur.

B)Şifreleme

Şifrelenecek mesaj m olsun. m'nin e 'ninci kuvveti alınır. Bu sayının Mod N karşılığı bize şifreli mesajı verir.

C)Şifre Çözme

Şifreli mesajın d'ninci kuvveti alınır ve elde edilen sayının Mod N'deki karşılığı bize bizim esas mesajımızı verir.[21]

RSA ile ilgili örnek bir uygulama EK-A'da yeralmaktadır.

3.2.4. Eliptik Eğri Şifrelemesi

1985 yılında Neal Koblitz ve Victor Miller birbirinden bağımsız olarak eliptik bir eğri üzerindeki noktalar grubunu kullanarak yeni bir asimetrik şifreleme sistemi geliştirmişlerdir. Bugün daha hızlı ve daha küçük bir şifreleme sistemi arayanlar için en sınırlı ortamlarda bile çalışabilecek bir açık anahtar şifreleme sistemi sunmaktadır.

Öncelikle eliptik eğri algoritması neden diğer algoritmalara göre daha güçlüdür bunu açmamız gerekmektedir. Bunun başlıca sebebi, eliptik eğri, temeli olan problemin çözümünün

zorluğundan dolayı bit başına en güçlü korumayı sağlar. Problem zorlaştıkça aynı oranda güvenlik daha küçük anahtarla elde edilir. Aşağıdaki tabloda da eliptik eğrinin RSA ve DSA'ya karşı anahtar uzunluğu bakımından gücü görülmektedir. [16] Bir anahtarı elde etmek için gerekli olan kaç MIPS yılı gerektiği ve ortalama olarak birbirlerinin anahtar uzunluğu oranlarının karşılaştırılması da ayrıca verilmiştir. Bu tablodan anahtar uzunluğundan ziyade bir anahtarın kırılması için gerekli olan algoritmanın zorluğunun aslında daha önemli olduğu açıkça görülmektedir.

Tablo 6. RSA ve ECC anahtar boyu karşılaştırması

Kırmak için gereken MIPS yılı	RSA / DSA Anahtar Boyutu	ECC Anahtar Boyutu	RSA/ECC Anahtar Boyutu Oranı
10^{4}	512	106	5 : 1
10^{8}	768	132	6 : 1
10^{11}	1,024	160	7 : 1
10^{20}	2,048	210	10 : 1
10^{78}	21,000	600	35 : 1

Bu algoritma akıllı kartlara uygulandığında bize getirisi çok büyük olmaktadır. Hep bahsettiğimiz üzere akıllı kartlar boyutları itibariyle çok sınırlı kaynaklarla üzerinde çalışılabilen bilgisayarlardır. Eliptik eğri şifreleme algoritmasının bize en büyük getirileri olan daha küçük anahtar kullanımıyla daha güçlü bir güvenlik elde edilebilmesidir. Daha küçük anahtar kullanmak demek anahtarları ve sertifikaları depolamak için daha az EEPROM kullanımı ve bunun yanında daha az veri alışverişi neticesinde uygulamaların iletişim zamanlarının kısalması anlamına gelmektedir.

Akıllı kartların kaynak kullanımı ve bu kaynaklar için üreticiye belli bir maliyet yükünün binmesi kaçınılmazdır. Eliptik eğri kullanılması durumunda daha az kaynak harcanması gerekeceğinden dolayı bu maliyetlerde azalacaktır veya maliyet miktarı artmadan daha yüksek seviyede güvenlik için kullanılacaktır.

Diğer şifreleme sistemleri için gerek RSA olsun, gerek 3-DES olsun yoğun işlem gerektiren şifreleme sistemlerinde bir yardımcı işlemci kullanımından bahsedilmiştir. Bu işlemcinin maliyeti kartın maliyetinin %20 ile % 30 arasında olabilmektedir. Eliptik eğri algoritması kullandığımızda ise algoritma ROM'un içinde işlenebilmektedir. Bu da ekstra bir donanıma ihtiyaç duymadan hızlı ve güvenli onaylama işlemleri yapabilmemize olanak sağlar.

Akıllı kartlarda eliptik eğri kullanılması bize ne yarar sağlar bunu göstermemiz gerekirse;

A-Daha az hafıza ve daha kısa iletişim süresi

ECDLP algoritması küçük anahtarlarla çok güçlü bir güvenlik sağlar. Anahtar küçük olunca onu depolamak için gereken hafızada küçülmektedir, bunun sonucunda da kart ile uygulama arasındaki veri iletişimi de azalmaktadır. Bu nedenle iletişim süresi kısalır.[6]

B-Ölçekleme

Akıllı kart uygulamaları her zaman daha uzun anahtarlarla başarılabilen daha güçlü güvenlik gerektirir. Eliptik eğri şifrelemesi, aynı kaynakla daha iyi güvenliği sağlayabilmektedir. Bunun anlamı maliyet artışı olmadan daha yüksek bir güvenlik demektir.

C-Yardımcı işlemci gereksinimi

EEC kendi içinde kullanılan hesaplamalardan dolayı işlem zamanını büyük miktarda düşürür. (Özellikle de modüler işlem gerektirmeyen $GF(2^n)$ kullanıldığında) Diğer şifreleme sistemleri hesaplamaları için özelleştirilmiş şifreleme yardımcı işlemcileri kullanırlar. Bu işlemcilerin kullanımı da hem alan kullanımını hem de maliyeti arttırmaktadır. EEC ise ekstra bir yardımcı işlemciye ihtiyaç duyulmadan bu işi CPU yeterli bir hızda yapabilmektedir.

D-Kartta anahtar oluşturulması

Güvenlik için gizli(private) anahtarlar saklı kalmalı ve kimse tarafında ulaşılamamalıdır. Mevcut asimetrik şifreleme yöntemlerinde kartlar bu kriter göz önünde bulunarak anahtarlar güvenli bir ortamda karta yüklenir. İşlemlerin karmaşıklığından dolayı kartta anahtar oluşturmak pratik olmayan ve etkisiz bir yöntemdir. Ancak eliptik eğri

şifrelemesi sayesinde kartta anahtar oluşturmak için gereken süre çok kısadır ve az bir işlem gücü gerektirdiğinden dolayı bu işlem gerçekleştirilebilmektedir.

Yukarıda bahsedilen özellikler aşağıda bir tablo olarak verilmiştir.

Tablo 7. ECC ve RSA Algoritmalarının Karşılaştırılması

	ECC	RSA
Kullanılan Hafıza Miktarı	Az	Çok
İletişim Miktarı	Az	Çok
Kart Üzerinde Anahtar Oluşturma	Uygun	Uygun Değil
Anahtar Boyuna göre işlem süresi	Kısa	Uzun

Akıllı kartlar için hangi eliptik eğri şifrelemesi oluşturma yöntemi daha uygundur buna bakarsak genelde $GF(2^n)$'nın kullanımı $GF(p)$'ye nispeten önemli bir performans artışı sağlar. Bunun sebebi $GF(p)$'de kullanılan modular işlemlerdir. Aradaki bu performans farkını kapatmak için yardımcı işlemci kullanılması gerekmektedir. Bu da kartın maliyetini %20-%30 arttıracağı için tercih sebebi olmamaktadır. Oysa $GF(2^n)$ ile bir yardımcı işlemciye gerek olmadığından daha ucuza mal olmaktadır. Maliyetin gözardı edilebildiği ve bir aritmetik işlemcinin olduğu durumlarda $GF(p)$ performans açısından özel bir aritmetik işlemci barındırmayan $GF(2^n)$'yı geçmektedir. Ayrıca nokta sıkıştırması eliptik eğri üzerindeki noktaların daha az veri ile gösterilmelerini sağlamaktadır. Akıllı kart uygulamalarında nokta sıkıştırması hayati önem taşımaktadır, çünkü kart üzerindeki anahtarlar için kullanılan alanı düşürmenin yanında karta giren ve çıkan veri miktarını da azaltacağından iletişim süresini kısaltır.

Bu kadar çok avantajına rağmen ECC'nin RSA'a göre yaygınlaşamamasının en önemli nedeni olarak güvenli eğrilerin kurulması için güvenlikten sorumlu IT uzmanlarının bile kolayca anlayamadığı karmaşık bir matematik kullanmaktadır.[17]

3.2.5. Knapsack ve Knapsack Tabanlı ECC Algoritması Kullanımı

Merkle-Hellman kriptosistemi 1978 yılında Ralph Merkle and Martin Hellman tarafından bulunmuştur. Bu kriptosisteminin temelinde bir mesajın ikilik düzene çevrilip

sonra bu ikilik düzendeki karşılığının bir vektör üzerinde toplanması yoluyla şifreli mesajın büyültülmesi yatar.

Merkle-Hellman algoritması üç kısımdan oluşur. İlki anahtar oluşturmadır.

- Anahtar oluşturma işlemi için öncelikle süper skalar bir vektör seçilir. Bu vektörlerin özelliği her eleman kendinden önceki elemanların toplamından daha büyük olmak zorundadır.

$$w_{i+1} > \sum_{i=1}^{n-1} w_i$$

- w vektörünün tüm elemanlarından büyük bir q sayısı seçilir.

$$q > \sum_{i=1}^{n} w_i$$

- Bir tane r sayısı alınır. Bu sayı 1<r<q ve gcd(r,q)=olmalıdır.
- r sayısı ile w vektörünün tüm elemanları çarpılıp q'ya göre modu alınarak yeni bir B vektörü oluşturulur.

$b_i = rw_i \bmod q$

İkinci kısım şifrelemedir. Şifrelenecek mesaj ikilik düzene çevrilip B vektörüne konur ve vektör elemanlarıyla çarpılır. Bu çarpımın sonucunda bir y sayısı elde edilir. Bu elde edilmesi istenen şifreli mesajı verir.

$y= b_1x_1 + b_2x_2 + \ldots + b_nx_n$

Üçüncü kısım şifre çözme kısmıdır. Şifre çözmek için öncelikle r sayısının mod q'ya göre tersi bulunur.

$r.r^{-1}=1(\text{Mod } q)$

Şifreli mesajımızla r'nin mod q 'ya göre tersini çarpıp mod q'ya göre değerini alırız.

$y.r^{-1}(\text{Mod } q)=y'$

Daha sonra w vektörünü taramaya sondan başlayarak toplam >= w(i) ise toplam=toplam-w(i) ve wi) nin üstüne 1 koyulmaktadır. toplam < w(i) ise 0 koyarız. Elde edilen 1 ve 0'lar harf dizisine dönüştürüldüğünde kelimeyi vermektedir. Bu algoritma ile ilgili hazırlanmış bir program EK-B'de bulunabilir.

Knapsack algoritması 1982'de kırılmış bir algoritmadır. Fakat diğer mevcut şifreleme sistemlerini kuvvetlendirerek kullanılması mümkündür. Örneğin knapsack tabanlı bir eliptik eğri şifrelemesi kullanılabilmektedir.

Normal eliptik eğriden farkı şifreleme ve çözümlemede mesajı oluşturan karakterlerin ASCII değerleri alınıp bu değerler knapsack algoritmasına bağlanır. RSA algoritmasıyla karşılaştırdığımızda karmaşıklık açısından daha iyi sonuçlar vermektedir. Ayrıca brute force ataklara karşı çok iyi bir koruma sağlamaktadır. [21]'de bu konu ile ilgili yapılmış bir çalışma bulunmaktadır.

Bu çalışmanın amacı eğer G noktası, gizli sayı k ve dönüştürme noktası P_m bilinse bile şifrenin çözülmesini imkansız hale getirmektir. Sadece A_i knapsack vektörünün gizli tutulması yeterlidir.

Alice Bob'a bir şifreli karakter göndermek istesin. Önce gönderilecek karakterin ASCII değeri alınıp P_m noktası ile dönüştürülür.

$$P'_m = SP_m$$

Bu nokta esas kimliklerini gizlemek için temel noktası G'den farklı seçilir. Yeni bulunan noktada eliptik eğri üzerinde bulunmaktadır. Bu işlem iki sebepten dolayı yapılır. Birincisi ASCII değerini eliptik eğrinin x-y koordinat düzlemine yerleştirmek için. İkincisi ise hackerlara karşı kamufle etmek için. Sonraki aşamada ise kP_B oluşturulur. Buradaki P_B

Bob'un açık anahtarıdır. Bu çarpma işlemi k'nın değerine bağlı olarak toplama ve çiftleme işlemleri gerektirir. Örneğin k=386 olsun.

P	2P	3P	6P	12P	24P	48P	96P	192P	193P	386P
-	İkileme	Ekleme	İkileme	İkileme	İkileme	İkileme	İkileme	İkileme	Ekleme	İkileme

Şifreli mesajı oluşturmak için P'_m ile kP_B toplanır. Bir x_2,y_2 seti elde edilir. Daha sonra kG den x_1,y_1 seti elde edilir. Daha sonra bu elde ettiğimiz saylar daha yüksek bir güvenlik için knapsack algoritmasıyla şifrelenir. Elde ettiğimiz sayı Alice'in şifreli mesajıdır.

$$C_m = ((\mathrm{S}[x_1], \mathrm{S}[y_1]), (\mathrm{S}[x_2], \mathrm{S}[y_2]))$$

Buradaki iki sayı mesajdaki bir harfi oluşturmaktadır. Daha uzun bir mesaj için elimizde daha fazla sayı çiftleri olacaktır. Aşağıdaki tabloda knapsack şifrelemesi öncesi ve sonrası elde edilen koordinat çiftleri görülmektedir.

Tablo 8. Knapsack algoritması öncesi ve sonrası oluşan koordinat çiftleri

Karakter	Knapsack algoritmasından önce şifreleme $kG,\ P'_m+kP_B$	Knapsack algoritmasından sonra şifreleme
S=83	(99,253),(51,58)	(18756,82031),(3756,656)
A=65	(99,253),(116,280)	(18756,82031),(656,3751)
V=86	(99,253),(427,287)	(18756,82031),(472006,488126)
E=69	(99,253),(135,341)	(18756,82031),(96876,406901)

Knapsack algoritmasının gücü a_i vektörünün seçiminde yatmaktadır. Sonsuz şekilde seçilme şansı olduğu için kırılmasını imkânsız hale getirmektedir.

RSA ve Knapsack tabanlı bir ECC algoritmasının karşılaştırılması ile ilgili bir çalışmada 'SAVE'mesajının RSA ile şifrelenip çözülmesi 36.26 ms almıştır. Aynı mesajın Knapsack tabanlı ECC'de çözülmesi ise 60,9 ms almıştır. Ayrıca ECC uygulamasının

sonuçlarının depolanması için gereken yer miktarı RSA'ınkinin iki katından daha fazla kaplamaktadır.

Tablo 9. Knapsackli ve Knapsacksiz ECC algoritmasının şifreleme süreleri

	Yürütme Zamanı (Şifreleme ve çözümleme)
Knapsack ile	~ 60.9 ms
Knapsack sız	~ 55.6 ms

Bu görünen dezavantajlarına rağmen sadece gizli kalması gereken verinin a_i vektörü olması ve RSA'ın yüzlerce haneli sayılar kullanmayı gerektirmesi Knapsack tabanlı ECC algoritmasının RSA karşısında avantajları olarak göze çarpmaktadır.

3.3. Gizli Anahtar Şifreleme Algoritmaları İçin Kullanılan Yardımcı İşlemciler

Şimdiye kadar DES finansal işlemlerde ve telekomünikasyon işlemlerin standart şifreleme algoritması olarak kullanıldı. Bu geniş pazar potansiyelinden dolayı yarı iletken üreticileri, kendi DES hesaplama birimlerini kartın mikroişlemcisinin içine gömmeleri gayet karlı bir iş olarak görmüşlerdir.

DES hesaplama ünitesinin avantajları, aşağıda verilen örnekte anlatıldığı üzere hız olarak incelendiğinde gayet net olarak görülebilmektedir. Örneğin 3.5 MHZ hızında hesaplama yapabilen bir işlemcimiz olduğunu varsayalım. Bunda bir basit DES operasyonunun süreceği zaman 75 nanosaniye ve 2 anahtarlı bir 3-DES işlemi için öngörülen hesaplama süresi ise 150 nanosaniyedir. Saat hızı arttıkça hesaplama süresi çizgisel bir şekilde düşmektedir. Bunun yanında yazılımsal destekli bir DES uygulamasının ROM kodunun kapladığı alandan daha fazla bir alan kaplamamaktadır. Yani donanım olarak desteklemek entegre devre boyutunu arttırmaz. Bu da aynı entegre devre boyutuyla bize iyi bir güvenlik sağlar.

Gelecekte DES işlemcisinin yanında 128, 196, 256 baytlık 3 anahtarı da destekleyen AES yardımcı işlemcilerini mikroişlemcilerin içinde görmemiz şaşırtıcı olmayacaktır. AES algoritmasının donanımda görece daha kolay uygulanabilir olmasından dolayı teknik olarak

DES yardımcı işlemcisinin kullanımı kadar akıllı kartlara yerleştirilmesi uygulanabilir olmaktadır.

3.4. Açık Anahtarlı Şifreleme İşlemleri İçin Yardımcı İşlemciler

Eliptik eğri ve RSA gibi public key algoritmalarında da işlemler için özel olarak geliştirilmiş, bir akıllı kart mikroişlemcisinin standart fonksiyonel işlem birimleriyle birlikte silikonun içine yerleştirilmiş aritmetik hesaplama birimleri mevcuttur. Bu hesaplama birimleri bu tip algoritmalarda kullanılması gerekli olan ve büyük sayılarla hesaplanması gereken modül işlemleri veya exponentiation türü basit hesaplamaları yapması için konulmuşlardır. Bu tip aritmetik birimlerin hızları bu tür hesaplamalar için özelleştiğinden dolayı hızlı olabilir. Hatta kendi özel uygulama alanlarında güçlü bir PC'yi alt edebilecek hızlara ulaşabilirler.

Genelde bu yardımcı işlemciler, RSA algoritması için mevcut veriyi 1024 bitlik anahtar uzunluğuna kadar ve hatta ileri yıllarda uzun vadede bu 2048 bite kadar çıkaracaktır. Eliptik eğriler için ise genellikle bu kapasite 160 bit kadardır. Gelecekte bu 210 bite kadar çıkacaktır.

4. BAZI ÖNEMLİ UYGULAMA ALANLARI

Akıllı kart sistemleri her gün gitgide daha fazla hayatımıza girmektedir. Bunun sonucu olarak uygulama alanlarını genişletmektedirler. Bu uygulama alanları taşımacılıkta dahil olmak üzere bankacılığa kadar geniş ve birbirinden farklı alanları kapsamaktadır.

İlk akıllı kartların ortaya çıkması daha önceden de bahsettiğim üzere iletişim sektöründe olmuştur. Ancak daha sonraları diğer sektörlerde de kullanılmaya başlanmıştır. Ancak kartların yapısı gereği güvenilir bir ortam sağladığı için esas yaygınlaşmasını bankacılık sistemi sağlamıştır.

Bazı uygulama alanları aşağıda sıralanmıştır.

- Cep Telefonu SIM Kartı
- Kredi kartı, e-cüzdan
- Ankesörlü Telefon Kartı
- Toplu Ulaşım Kartı
- Sağlık Sigortası Kartı
- Elektronik (Sayısal) İmza Kartı
- Kimlik Kartı
- Ödeme Sistemlerinde Akıllı Kart
- Otomatik Geçiş Sistemi

4.1.Ödeme Sistemleri

Ödeme sistemleri alanında akıllı kartların kullanımı 3 şekilde olmaktadır. Bunlar kredi kartları, banka kartları ve elektronik cüzdan olarak kullanılan kartlardır.

Şekil 17. Ödeme kartı çeşitleri

4.1.1. Kredi Kartları

Kredi kartları bir hizmet aldıktan sonra ödemesinin yapıldığı kartlardır. Yani hizmetin önce alındığı ödemesinin ise belli bir süre sonunda tamamının tek seferde veya taksitlendirilerek ödendiği bir ödeme sistemi aracıdır. Daha sonra bu aldığınız hizmet hesabınızdan düşmektedir. Bu arada bu hizmet karşılığında malı veya hizmeti satın aldığınız kişi bankaya bir komisyon ödemektedir.

Şekil 18. Kredi kartları ödeme yapısı

Şekil 18'de gösterilen ödeme yapısını açıklamak gerekirse ilk önce kart sahibi müşteri alışverişini yapmakta ve bu alışverişin karşılığı olarak kartla ödemeyi seçmektedir. Kredi kartıyla ödemeyi seçtiğinde dükkân sahibinin ondan kimliğini tanımlamasını istemesi gerekir. Bunun için iki tane yöntem vardır. Birincisi ve öncelikli tercih edileni PIN girişidir. Karta atanmış olan ve sadece kart sahibinin bildiği bir PIN numarası ile onaylama işlemi gerçekleştirilebilmektedir. İkinci yöntem ise imzalama yoluyla kimliğini onaylamaktır. Eğer kart sahibi PIN kodunu unutmuşsa yine PIN bypass yapılarak imzayla kimlik onaylaması gerçekleştirilebilir.

Kimlik onayından sonra kartın geçirildiği POS makinesi vasıtasıyla veriler onaylanmak için POS'un sahibi olan bankaya gönderilir. Oradan da önce aracı kuruluşa (genelde VISA, Mastercard) sonrasında da kart sahibinin hesabının bulunduğu kartı vermiş olan bankaya gider(2a,2b,2c). Eğer kartın limiti alınan hizmetin bedelini ödemek için

yeterliyse onay mesajı geldiği yolu takip ederekten satıcının POS'una iletilir. Ürün satışı gerçekleşmiş olur. Daha sonrasında hesap kesim tarihine göre o ay içinde alınan hizmetlerin toplam bedeli bir hesap belgesi halinde kart sahibine iletilir. Kart sahibi ödemeyi yapsa da yapmasa da ücret satıcıya ödenir. Bu işlemin gerçekleştirilmesi karşılığında satıcı POS'u aldığı bankaya belli bir komisyon öder. Bu komisyon miktarı yine banka tarafından belirlenmiş bir ücret olmaktadır.

Kartların çeşidi yapılabilecek işlemlerin tipini belirlemektedir. Mesela manyetik tabanlı kartlarda sadece imza ile işlem yapılabilmektedir. Sadece imzalı olması önemli güvenlik açıklarını da beraberinde getirmektedir. Çipli kartlarda ise hem imzalı hem de PIN'li işlem geçmektedir. Bu bankanın sisteminin destekleyip desteklememesiyle ilgili olarak düzenlenen bir konudur.

4.1.2. Banka Kartları

Bu kartlar mevcut banka sisteminde hesabınızdan para çekmek için kullanılmaktadır. Ayrıca internet alışverişi yaparken veya telefonla alışverişlerde de aynı şekilde kullanılabilmektedir.

Kredi kartından farkı kendi hesabınızda para olması gerekliliğidir. Kredi kartında alışveriş yaptığınızda bankaya borçlanmaktasınız ve bu borcunuzu belli bir süre sonra ödemektesiniz. Banka kartında ise doğrudan sizin hesabınızdan para satıcının hesabına geçmektedir.

4.1.3. E-Cüzdan Uygulamaları

Bu kartların limiti çipin içinde belirlidir. Bir işlem yapıldığında para bu çipten düşer ve yeni kalan miktar tekrar çipi içine yazılır. Günümüzde Avusturya ve Almanya'da kullanılan bir sistemdir.

4.2. GSM Şebekelerinde Akıllı Kartlar

Akıllı kartların GSM şebekelerinde kullanılan şekline subscriber identity module (SIM) denmektedir. Bu modülün görevi, kullanıcının detayları (IMSI yani International Mobile Subscriber Identity), güvenlik verisini ve kişisel telefon numaralarını saklamaktır. GSM, şebeke sağlayıcısının arayanı tanımlayabilmesi için gereken bilgileri depolar. Bu kart çıkartılabilir bir yapıda olup başka bir telefonda kullanıldığında yine aynı verileri diğerine de taşımaktadır. Bu bakımdan daha çok taşınabilir hafıza kartı gibi çalışmaktadır. Kart bir telefona takıldığında o telefon hangi şebekeyi ve hesabı kullanması gerektiğini öğrenir. Sim kartın şifreleme ve onaylama özellikleri telefonun çalınması veya konuşmaların dinlenmesinin önüne geçer.

4.3. Diğer Kullanım Alanları

Toplu taşıma araçlarında yüklenmiş kredi miktarından düşecek şekilde kullanılmaktadır. Kullanıcı belli aralıklarla karta kredi yüklemesi yapmak zorundadır.

Elektronik kimlik sistemi olaraktan kullanılmaktadır. Böylece bir kişinin tüm bilgileri istendiği takdirde ulaşılabilir hale gelmektedir. Her bir bilgi için ayrı kartın taşınması zorunluluğu ortadan kalkmakta olup hem de daha güvenli bir ortamda verilerin taşınabilmesine olanak sağlanmaktadır.

Elektronik telefon kartı uygulaması akıllı kartların ortaya çıkışına sebebiyet vermiştir. Günümüzde de bu şekilde kullanılmaya devam etmektedir. Sistem olarak toplu taşımada kullanılana benzer bir şekilde çalışmaktadır. Kullanıcı kontör yüklettiği kart ile konuşmasını yapmakta olup bittiğinde tekrar doldurtabilmektedir.

5. AKILLI KARTLARA AİT GELECEK ÖNGÖRÜLERİ

Mini web-sunucu kartlardan temassız mobile telefon ve pasaportlara akıllı kart teknolojisi, internet ve mobil ağlar üzerinde anahtar bir rol oynamak için dönüşüm geçirmektedir. Şimdiye kadar akıllı kart teknolojisi gittikçe büyüyen ağ yapılarına karşın kendi soyut sistemini korumayı başarmıştı. Ağ yapılarına göre yavaş okuma veri okuma hızlarına sahip olması ve bilginin alınabilmesi için özel cihazlar gerektirmesi bunun temel sebebiydi. Bilgisayar teknolojileri gün geçtikçe değişirken akıllı kartlar buna uyum sağlayamamaktadır. Geleceğe yönelik olarak uygulanmaya konmaya çalışılan planların başında bu gelmektedir.

İleriki zamanlarda akıllı kartlarla ilgili yeni özellikler eklenecektir. Her akıllı kart kendi IP adresine sahip olması planlanmaktadır. Bunun avantajı bir taşıyıcıdan kendi iletişimini kontrol eden bir istemciye dönüşecektir. Böylece iletişimi başlatıp proaktif olarak veri araması yapabilecektir. [20]

Gelecekte akıllı kartlar PC ve mobil cihazlarla aynı protokolleri ve arayüzleri kullanacaktır. Bu da direkt iletişim kurabilmelerine imkân sağlayacaktır. Şu an bunun önündeki en önemli sorun olarak yüksek hızlı ve yüksek hafızalı kartların yüksek maliyetleri gözükmektedir. PC'ler üzerlerinde akıllı kart okuyucularla gelecektir. Böylece internet alışverişlerini kullanıcı en güvenli şekilde oturduğu yerden yapabilecektir. Böylece küçük değerli işlemlerinde önü açılmış olacaktır, örneğin bir ürünün tanıtımı için bile çok küçük bir meblağ talep edilebilecektir veya bir kitap için sayfa başına ödeme yapılıp sadece o kişinin ihtiyacı olan sayfayı alması sağlanabilir.[9]

Japonya'da günümüzde mobil iletişimde ödeme ve bilet alma gibi işlemler için temassız çipler kullanılmaktadır. Avrupa'da da bununla ilgili çalışmalar yapılmaktadır. Örneğin bir kullanıcı bir telefon ağından bir müzik indirdiğinde aynı zamanda aynı sanatçının biletini de indirecek ve bundan sonra tek yapması gereken konsere girerken kapıdaki okuyucuya cep telefonunu tutmak olacak.

Ayrıca gelecekte akıllı kartlara daha ileri bir kişi tanımlama güvenliği için biyometrik okuyucuların eklenmesi mümkün olacaktır. Bir işlem yapılmadan önce okuyucu, parmak izi

okuyucu veya ses tanıma gibi çeşitli tanımlamalar isteyerek kart sahibi dışındaki kişilerin işlem yapmasının önüne geçebilir. Günümüzde bunun uygulamaları görülmektedir. Hollanda'daki Schiphol Havaalanında uygulanmakta olan "registered traveler" programına kayıtlı yolculara verilen akıllı kartın içinde kendi iris taraması mevcuttur. Fakat yine bu tip uygulamalarda şu an için yüksek olan maliyetlerinden dolayı yaygın hale gelebilmesi pek mümkün gözükmemektedir.

Artık yavaş yavaş içinde birden fazla uygulamanın çalıştığı akıllı kartlar çoğalmaktadır.

6. SONUÇ

Bu araştırmada amaçlanan güvenliğin büyük önem teşkil ettiği akıllı kartlar için çeşitli şifreleme sistemleri arasında hangisinin daha uygun bir çözüm sunduğunu bulmaya yöneliktir. Akıllı kartların kaynakları(hafıza, işlemci hızı) sınırlı olması sebebiyle şifreleme işlemlerinde bazı matematiksel işlemler üzerine uzmanlaşmış ek bir işlemci gereksinimi ortaya çıkmıştır.

Mevcut bankacılık sisteminde yakın gelecekte anahtarların yetersiz hale geleceğinin öngörülmesi üzerine mevut RSA tabanlı dijital imza uygulamalarının anahtar boylarının arttırılması konusunda çalışmalar başlatılmıştır. Eliptik eğri şifrelemesi akıllı kart sistemlerinde kullanımı artmaya başlamıştır.

Araştırmada şu anda kullanılan mevcut şifreleme sistemlerinin yanında biraz hızdan ödün verilerek knapsack tabanlı eliptik eğri şifrelemesi kullanımının bize sağlayacağı faydalar ortaya konulmuştur.

Mevcut sistemlerde kullanılan manyetik ve akıllı kartlar arasındaki farklar manyetik kartlar daha az maliyetli bunun yanında içinde şifreleme tabanlı bir güvenlik mekanizması bulundurmamaktadır. Bunun yanında karmaşık yapılı akıllı kartlar ise sundukları güvenlik özellikleri, tutulabilen veri boyları ve içlerinde bulundurdukları işlemciyle insanlara yeni dünyaların kapılarını açmaktadır.

Yeni özellikler eklemek için hafızaları arttırılarak, işlemci hızları yükseltilerek gerek güvenlik olsun gerek hız olsun kullanıcıların ihtiyaçlarını tatmin etmek için maksimum seviyede kendilerini geliştirmektedirler.

Üçüncü bölümde açıklanan şekilde akıllı kartlar üzerinde yeni şifreleme yapıları denenerek çok daha uygun ve güvenli hale getirilebilir. Knapsack tabanlı EEC algoritması için yapılan analizlerde görülmüştür ki akıllı kartlar için daha çok veri depolaması gerektiğinden ve işlem süresini uzattığından dolayı her ne kadar bize daha iyi bir güvenlik sağlasa da sınırlı bir alana sahip olan akıllı kartlarda kullanılması için uygun görülmemektedir. Fakat ileride akıllı kartların işlem yapma güçleri ve bellek miktarları arttırıldığında kullanılabilir.

Çoklu uygulamalı kartlar içlerinde barındırdıkları birden çok uygulama ile kullanıcılarına kolaylıklar sağlamaktadırlar. Bu uygulamalar sayesinde para çekilen bir kart aynı zamanda toplu taşıma kartı olarak tanımlanabilmektedir. Bu da sınırsız bir kullanım olanağı sunmaktadır.

Dünyada her yıl milyonlarca yeni akıllı kart yeni kullanıcılarıyla buluşmaktadır. Bu sayının her geçen gün artması akıllı kartların gün geçtikçe yeni kullanım alanları bulmasından ve belirli aralıklarla bu kartların yenilenme gereksiniminden kaynaklanmaktadır.

Bugün için pahalılığından dolayı hayata geçirilemeyen birçok proje akıllı kartlar alanında meydana gelen gelişmelerle birlikte geleceğin dünyasına bir adım daha yaklaştığımızı ispatlayacak şekilde ucuzlamaktadır.

KAYNAKLAR

[1] Jurgensen, Timothy M. ve Guthery, Scott B. , "Smart Cards: The Developer's Toolkit",Ch 1,P.2, 2002

[2] Rankl, Wolfgang ve Effing, Wolfgang, "Smartcard Handbook",Ch. 2,P.18,2003

[3] Mayes, Keith ve Markantonakis, Konstantinos, "Smart Cards, Tokens, Security and Applications",Ch. 3,P.53,2008

[4] O'Mahony, Donal, Pierce, Mchael A., Tewari, Hitesh, "Electronic Payment Systems for E-Commerce", Ch 3,P.20,2001

[5] Markantonakis, Konstantinos, Mayes, Keith, "A Secure Channel protocol for multi-application smart cards based on public key cryptography",P.3

[6] Khaled M. A-Kayalı," Elliptic Curve Cryptography and Smart Cards",Ch. 2,P. 3,2004

[7] Urhan, Oğuzhan, Zengin, Fevzi ve Şanlı, Musa, "DES ALGORİTMASI KULLANILAN AKILLI KART İLE GÜVENLİK SİSTEMİ TASARIMI ve UYGULAMASI",P.4

[8] Smartcards Manufacturer, http://www.paymentscardsandmobile.com/buyersguide/articles/smartcard_manufacturers.html

[9] Smart Cards, www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm

[10] BERTA, István Zsolt ve MANN, Zoltán Ádám,"Implementing Elliptic Curve Cryptoghraphy On PC And Smartcard",Ch.3,P.57,2002

[11] Mastercard International," MX-Entire_Manual Security & Key Management",Ch. Appendix B Cryptographic Algorithms, P.B-1,2002

[12] VISA International,"EMV-SWG-N232"

[13] EMV ICC Specifications for Payment Systems v4.1x RSA+ Book, http://www.emvco.com/download_agreement.aspx?id=414

[14] EMV ICC Specifications for Payment Systems v4.1y RSA++ Book 2, http://www.emvco.com/download_agreement.aspx?id=415

[15] EMV ICC Specifications for Payment Systems v4.1z ECC Book 2, http://www.emvco.com/download_agreement.aspx?id=416

[16] Randall K. Nichols, “ICSA Guide to Cryptography”, Computing McGraw-Hill, First edition, December 1999

[17] Henna Pietilainen,”Elliptic Curve Cryptography On Smart Cards”,2000

[18] Gemplus, “Smartcards Operating Systems”, 2002

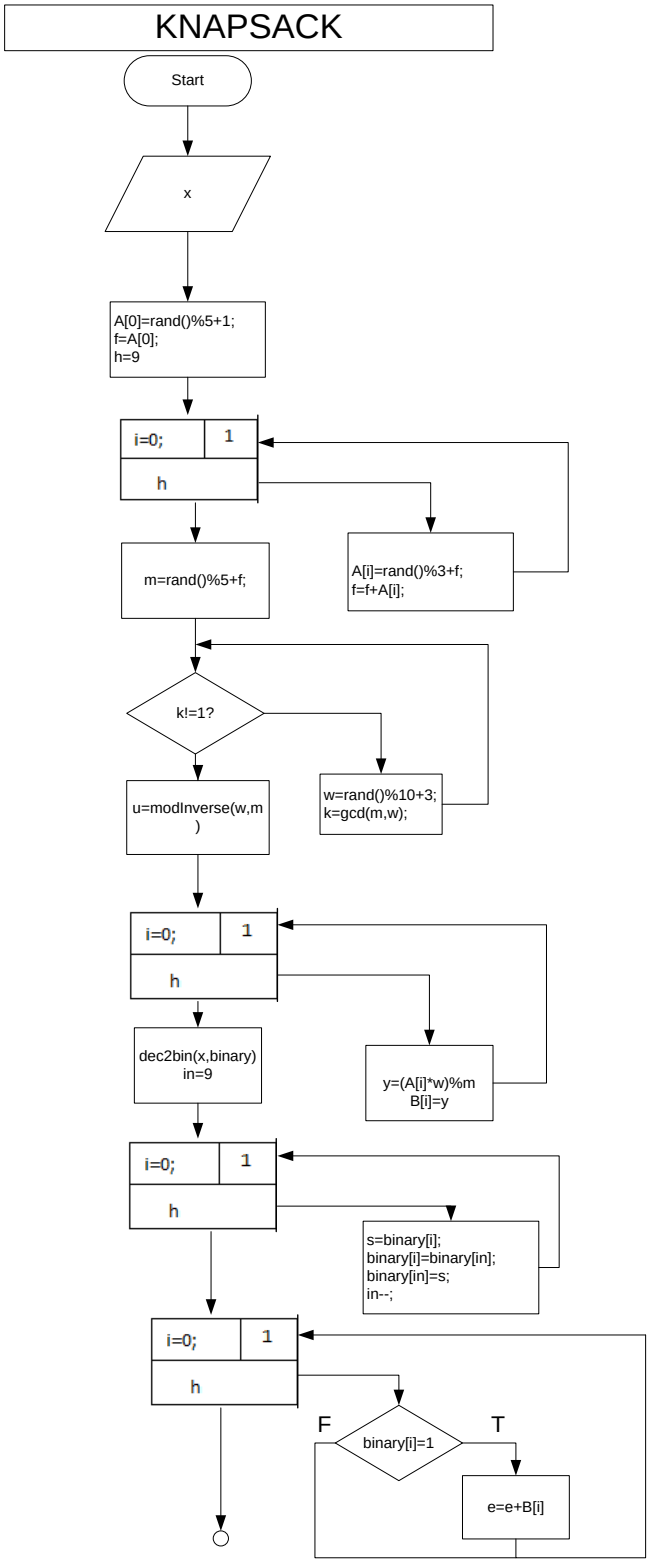
[19] Fernando Ferreira, “Smart Card Evolution”, 2003

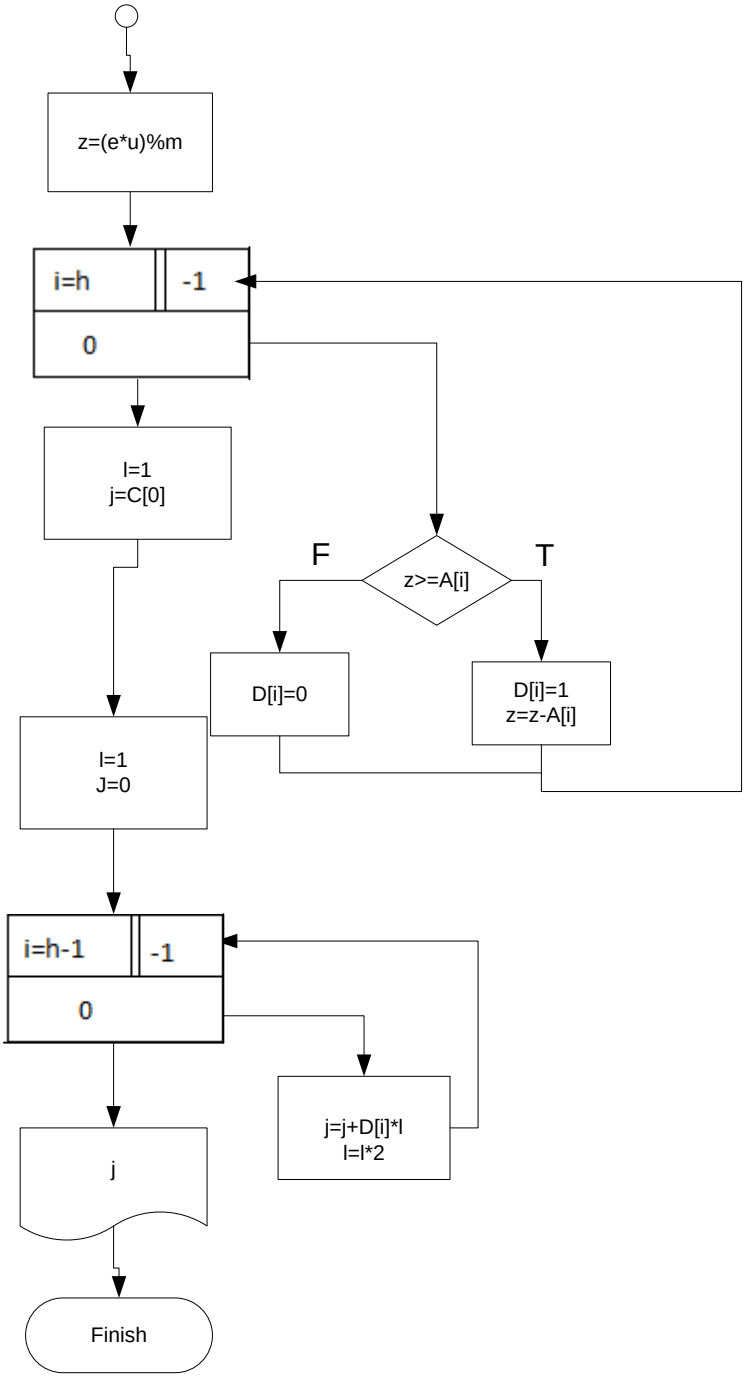
[20] MIPS Technologies, “Smart Card: The Computer in Your Wallet”,2001

[21] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone “Handbook of Applied Cryptography”,Ch11,P.434,1997

EKLER

EK-A. Knapsack Algoritması Akış Diyagramı ve Kaynak Kodları




z=(e*u)%m
i=h
-1
0
l=1
j=C[0]
F
z>=A[i]
T
D[i]=0
D[i]=1
z=z-A[i]
l=1
J=0
i=h-1
-1
0
j=j+D[i]*l
l=l*2
j
Finish

```
////////////////////////////////////////////////
//// Author:Mehmet ÖZDOGAN                  ////
//// Knapsack Simulation Program            ////
////////////////////////////////////////////////

#include "stdafx.h"
#include "math.h"
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <conio.h>
#include <string.h>



unsigned long dec2bin(unsigned long x, unsigned long binary[]);
long long unsigned int gcd(long long unsigned int a,long long unsigned int
b);
unsigned long int modInverse(unsigned long int a,unsigned long int b);

int _tmain(int argc, _TCHAR* argv[])
{
unsigned long int B[10],i,top,n,m,w,e,z,l,in;
unsigned long int A[9];
unsigned long int x,k,j,f;
unsigned int y;
unsigned long binary[10], D[10];
unsigned long u;

n=0;
top=1;
e=0;
u=0;

//creating a random array//
srand ((unsigned int) time(NULL) );
A[0]=rand()%100+1;
f=A[0];
for(i=1;i<=9;i++)
{
      A[i]=rand()%3+f;
      f=f+A[i];
}
for(i=1;i<11;i++)
{
      printf("%ld\t",i);
}
printf("\n=============================================================
============\n");
for(i=1;i<11;i++)
{
      printf("%ld\t",A[i-1]);
}
//M value bigger than last member of A array//
m=rand()%1000+f;
```

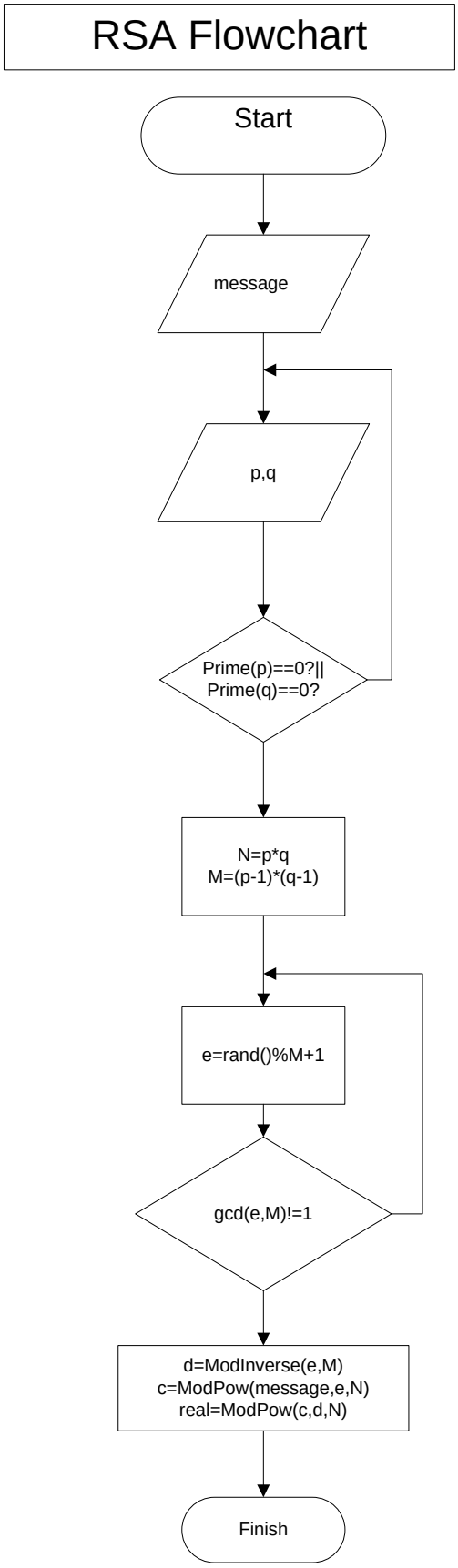
```
printf("\nm=%lu\n",m);
//W value is smaller than M value and coprime with M//
do{
	w=rand()%10+3;
	k=gcd(m,w);
}while(k!=1);
printf("w=%lu\n",w);
u = modInverse(w,m);
printf("inverse of w is %lu\n",u);
for(i=0;i<=9;i++)
{
	binary[i]=0;
	y=(A[i]*w)%m;
	B[i]=y;
}
//Entering message//
printf("\n\nEnter an integer value : ");
scanf_s("%d",&x);
dec2bin(x,binary);
in=9;

int av=in/2;
for(i=0;i<=av;i++)
{
	int s=binary[i];
	binary[i]=binary[in];
	binary[in]=s;
	in--;
}
for(i=0;i<10;i++)
{
	printf("%ld\t",B[i]);
}
printf("\n=========================================================================
============\n");

for(i=1;i<11;i++)
{
	printf("%ld\t",binary[i-1]);
}
//Encryption//
for(i=0;i<=10;i++)
{

	if(binary[i]==1)
	e=e+B[i];
}
printf("\n encrypted message=%lu\n",e);
z=(e*u)%m;
printf("x=%lu\n",z);
//decryption//
for(int i=9;i>=0;i--)
{
	if(z>=A[i])
	{
		D[i]=1;
		z=z-A[i];
	}
	else
	{
```

```
            D[i]=0;
      }
}
l=1;
j=0;
for(int i=9;i>0;i--)
{
      j=j+D[i]*l;
      l=l*2;
}
printf("Plain message=%lu\n",j);
getchar();
getchar();
return 0;
}

unsigned long int dec2bin(unsigned long int x, unsigned long int binary[])
{
int i=0;
while(x>0)
{
binary[i] = x%2;
x = x/2;
i++;
}
return i;
}



unsigned long int modInverse(unsigned long int a,unsigned long int b)
{
unsigned long int x[3];
int i,k,l,m,t;
int quotient = a / b;
int remainder = a % b;

x[0] = 0;
x[1] = 1;



for (i=2; (b % (a%b)) != 0; i++)
{
k=i%3;
l=(i - 1) % 3;
m=(i - 2) % 3;

a = b;
b = remainder;
quotient = a / b;
remainder = a % b;
int z=b % (a%b);
x[k] = (-quotient * x[l]) + x[m];
printf(" a=%d,b=%d,i=%d,Sonuc:%d\n" ,a,b,i,z);
}
t=(i-1)%3;
return x[t];
}
```

```
long long unsigned int gcd(long long unsigned int a,long long unsigned int
b) {

while(a!=b){
if(a>b)
a=a-b;
else
b=b-a;
}
return a;
}
```

```
1       2       3       4       5       6       7       8       9       10

================================================================================
56      58      114     229     457     914     1829    3658    7316    14633

m=29299
w=10
inverse of w is 2930


Enter an integer value : 23
560     580     1140    2290    4570    9140    18290   7281    14562   29134

================================================================================
0       0       0       0       0       1       0       1       1       1

 encrypted message=60117
x=26521
Plain message=23
```

EK-B. RSA Algoritması Akış Diyagramı ve Kaynak Kodları



```
//////////////////////////////////////////////
//// Author:Mehmet ÖZDOĐAN                  ///
//// RSA Simulation Program                 ///
//////////////////////////////////////////////

#include "stdafx.h"
#include "Rsa1.h"
#include "stdafx.h"
#include "math.h"
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <conio.h>
#include <string.h>

long long unsigned int real;
long long unsigned int p,q,b,M,i,d,t,N,e,c,message;
bool g;

int _tmain(int argc, _TCHAR* argv[])
{
	srand ((unsigned int) time(NULL) );
	//creating randomly of p and q values
	do{
		printf("Please enter a p value=");
		scanf("%llu",&p);
		printf("Please enter a q value=");
		scanf("%llu",&q);
	}while(Prime(p)==0||Prime(q)==0);
	printf("\n\n\tP=%llu Q=%llu\n\n",p,q);
	printf("\n\n\tEnter Message= ");
	scanf_s("%llu",&message);
	//N and Phi calculation
	N=p*q;
	M=(p-1)*(q-1);
	//creating random encryptor value
	do{
		e=rand()%M+3;
	}while(gcd(e,M)!=1);
	printf("\n\n\tN=%llu M=%llu e=%llu\n\n",N,M,e);
	//inverse of e for Mod Phi(N)
	d = modInverse(e,M);
	printf("\n\n\td=%llu\n\n",d);
	//creating ciphertext
	c = ModPow(message,e,N);
	printf("\n\n\tciphertext= %llu\n\n",c);
	//creating plaintext from ciphertext
	real = ModPow(c,d,N);
	printf("\n\n\tplain message= %llu\n\n",real);

	getchar();
	getchar();
	return 0;
}
```

```
long long unsigned int gcd(long long unsigned int a,long long unsigned int b) {

        while(a!=b){
                if(a>b)
                        a=a-b;
                else
                        b=b-a;
        }
return a;
}



unsigned long int modInverse(unsigned long int a,unsigned long int b)
{
unsigned long int x[3];
int i,k,l,m,t;
int quotient = a / b;
int remainder = a % b;

x[0] = 0;
x[1] = 1;



for (i=2; (b % (a%b)) != 0; i++)
{
k=i%3;
l=(i - 1) % 3;
m=(i - 2) % 3;

a = b;
b = remainder;
quotient = a / b;
remainder = a % b;
x[k] = (-quotient * x[l]) + x[m];
}
t=(i-1)%3;
return x[t];
}



long long unsigned int ModPow(long long unsigned int x,long long unsigned int y,long long unsigned
int n)
{
long long unsigned t=1;
for(long long unsigned i=1;i<=y;i++)
{ t=t*x;
  t=t%n;
}
return t;}

long long unsigned Prime(long long unsigned int j)
{
        long long unsigned a=3,s=1;
        for(long long unsigned i=1;i<j;i++)
```

```
        {
                s=s*a;
        }
        if(s%j==1)
                return 1;
        else
                return 0;
}
```

```
Please enter a p value=11
Please enter a q value=13

        P=11 Q=13


        Enter Message= 5

        N=143 M=120 e=103


        d=7


        ciphertext= 125


        plain message= 5
```

ÖZGEÇMİŞ

20 Mart 1980 yılında İstanbul doğumluyum. İlkokulu Bahçelievler İlkokulu'nda, ortaokulu 50. Yıl Avcılar İNSA Lisesi'nde, liseyi ise Fatih Koleji'nde okudum. Üniversite eğitimimi 1998-2004 yılları arasında Fatih Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde aldım. Askerliğimi Erzurum'da hava savunma takım komutanı olarak tamamladım. 2006 yılından beri bir özel şirkette yazılım uzmanı olarak çalışmaktayım. 2007 yılında Beykent Üniversite'nde Bilgisayar Mühendisliği Bölümünde yüksek lisans eğitimime başladım.

Aday: Mehmet ÖZDOĞAN