T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ELİPTİK EĞRİ ŞİFRELEME ALGORİTMASININ UYGULAMASI VE ANALİZİ

Meltem KURT

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

Yrd. Doç. Dr. Tarık YERLİKAYA

EDİRNE 2012

ELİPTİK EĞRİ ŞİFRELEME ALGORİTMASININ UYGULAMASI VE ANALİZİ

Meltem KURT

Yüksek Lisans Tezi

Bilgisayar Mühendisliği Anabilim Dalı

2012

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

T.Ü. Fen Bilimleri Enstitüsü onayı

……

Doç. Dr. Mustafa ÖZCAN
Fen Bilimleri Enstitüsü Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

……

Yrd. Doç. Dr. M. Tolga SAKALLI
Ana Bilim Dalı Başkanı

Bu tez tarafımca okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

……

Yrd. Doç. Dr. Tarık YERLİKAYA
Tez Danışmanı

Bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir Yüksek lisans tezi olarak oy birliği/oy çokluğu ile kabul edilmiştir.

Jüri Üyeleri:	İmza
Yrd. Doç Dr. Tarık YERLİKAYA	……
Yrd. Doç Dr. Deniz TAŞKIN	……
Yrd. Doç Dr. Ercan BULUŞ	……

Tarih: ...../……/……

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

İlgili tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin kaynak gösterilerek ilgili tezde yer aldığını beyan ederim.

.... /..../ 2012
Meltem KURT
İmza

Yüksek Lisans Tezi

Eliptik Eğri Şifreleme Algoritmasının Uygulaması Ve Analizi

T.Ü. Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

1980'li yılların ortalarında, Miller ve Koblitz eliptik eğrilerin kriptolojide kullanılabileceğini ortaya koydu. Lenstra, eliptik eğrileri, tamsayıları çarpanlarına ayırmak için kullandıktan sonra, eliptik eğriler güvenliğin ve gizliliğin gerekli olduğu durumlarda önemli bir rol oynadı. Eliptik eğrilerin kriptolojide kullanılmasının diğer bir nedeni, büyük anahtar uzunluklarıyla sağlanan güvenlik seviyesinin, eliptik eğrilerin kullanılmasıyla geliştirilen; eliptik eğri şifreleme algoritmasının kullandığı daha küçük anahtar uzunluklarıyla sağlanabilmesidir. Daha küçük anahtar uzunluğu kullanımı, işlem gücü, saklama kapasitesi, bant genişliği ve güç tüketimi gibi kaynakların sınırlı olduğu ortamlarda önemlidir.

Bu tez çalışmasının amacı güvenli bir iletişim kanalı oluşturmak için kullanılan eliptik eğrilerin matematiksel temelini incelemek ve elde edilen bilgiler doğrultusunda eliptik eğri şifreleme sisteminin matematiksel modellemesini gerçekleştirmektir.

İkinci bölümde şifreleme algoritmalarının alt yapısını oluşturan matematiksel kavramlar yer alırken, üçüncü bölümde kriptografik sistemler incelenmiş, eliptik eğri kriptosisteminin özellikleri açıklanmıştır. Dördüncü bölümde ise Menezes Vanstone Eliptik Eğri Kriptografisinin kullandığı şifreleme yöntemine birtakım özellikler eklenerek, değişikliğe uğratılmış sistem Dev C++ 4.9.9.2 ile geliştirilen programla modellenmiştir.

Yıl : 2012

Sayfa Sayısı : 81

Anahtar Kelimeler : Kriptografi, Eliptik Eğriler, Eliptik Eğri Şifreleme Algoritması, Asimetrik Şifreleme Algoritmaları, Simetrik Şifreleme Algoritmaları, Menezes Vanstone Eliptik Eğri Kriptosistemi, RSA

MS (MASTER) Thesis

Application and Analysis of Elliptic Curve Cryptography Algorithm

Trakya University Institute of Natural Sciences

Computer Engineering Department

ABSTRACT

In the mid-1980s Miller and Koblitz introduced elliptic curves into cryptography. After Lenstra showed how to use elliptic curves to factor integers, elliptic curves played an increasingly important role in many cryptographic situations are required security and privacy. Another reason of using elliptic curves in cryptography is that they seem to offer a level security needs comparable to classical cryptosystems that use much larger key sizes. Using of smaller key sizes is important in the environments where resources like processing power, storage bandwidth and power consumption are limited.

The aim of this thesis is to examine the basis of elliptic curves that used to create a secure communication channel and simulate the elliptic curve cryptography system in line with this obtained information.

The mathematical concepts underlying cryptographic algorithms are given in the second chapter and the third chapter includes cryptographic systems' properties especially elliptic curve cryptosystem. The fourth chapter involves information about developed program that was modeled Menezes Vanstone Elliptic Curve Cryptosystem using a number of additional features its encryption method and the program is written in Dev C ++ 4.9.9.2.

Year : 2012

Number of Pages : 81

Keywords : Cryptography, Elliptic Curves, Elliptic Curve Cryptography Algorithm, Asymmetric Encryption Algorithms, Symmetric Encryption Algorithms, Menezes Vanstone Elliptic Curve Cryptosystem, RSA

TEŞEKKÜR

Çalışmalarım boyunca karşılaştığım zorluklarda yardım ve desteğini esirgemeyen, pozitif yaklaşımlarıyla beni her zaman motive eden, değerli yardım ve katkılarıyla beni yönlendiren Danışman Hocam Sayın Yrd. Doç. Dr. Tarık YERLİKAYA'ya içtenlikle teşekkür ederim.

Ayrıca yaşamım boyunca benden sevgi ve desteğini asla esirgemeyen annem Hatice KURT, babam İbrahim KURT ve kardeşim Görkem Mert KURT'a teşekkürü bir borç bilirim.

Akademik çalışmalarımda benimle değerli bilgi birikimlerini paylaşan ve manevi desteklerini esirgemeyen Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'ne ve tüm iş arkadaşlarıma teşekkürlerimi sunarım.

İÇİNDEKİLER

1. GİRİŞ 1
2. MATEMATİKSEL KAVRAMLAR 3
2.1. Gruplar 3
2.2. Halka ve Cisimler 3
2.3. Tamsayılar ve Tamsayılarda Aritmetik 5
2.3.1. Bölünebilme 5
2.3.2. Euclid Algoritması 6
2.3.3. Aritmetiğin Temel Teoremi 7
2.3.4. Euler Fonksiyonu 8
2.3.5. Modüler Aritmetik 8
2.3.6. Euler Teoremi 11
2.4. Abelyen Gruplar 15
2.5. Sonlu Cisimler 15
2.5.1. Cisim İşlemleri 15
2.6. Asal Cisimler 16
2.7. Asal Sayılar 16
2.7.1. Mersenne Sayıları 16
2.8. Asal Sayı Üretimi 17
2.8.1. Fermat Asallık Testi 17
2.8.2. Rabin - Miller Asallık Testi 18
2.8.3. Lucas - Lehmer Asallık Testi 18
2.8.4. Diğer Testler ve Asal Sayı Üretme Yöntemleri 19
3. KRİPTOGRAFİK SİSTEMLER 20
3.1. Kriptoloji 20
3.1.1. Kriptografi ve Kriptanaliz 21

3.2. Kripto Algoritmaları 23
3.2.1. Simetrik Şifreleme Algoritmaları 24
3.2.2. Asimetrik Şifreleme Algoritmaları 26
3.3. Anahtar Yönetimi 28
3.4. RSA Kriptosistemi 28
3.5. ECC Şifreleme Algoritması 33
3.5.1. Eliptik Eğri Teorisi 34
3.5.2. Projektif Uzaylar 35
3.5.3. Eliptik Eğriler 36
3.5.4. Sonlu Cisimlerdeki Eliptik Eğriler 39
3.5.5. Eliptik Eğri Aritmetiği 42
3.5.6. Eliptik Eğrilerde Şifreleme Sistemleri, Problem Çözüm Yöntemleri ve Yaklaşımları 45
3.6. Eliptik Eğri Kriptosistemleri 52
3.6.1. Eliptik Eğri ElGamal Kriptosistemi 56
3.6.2. Menezes Vanstone Eliptik Eğri Kriptosistemi 59
3.6.3. Koyama – Maurer – Okamoto - Vanstone (KMOV) Kriptosistemi 61
3.6.4. Ertaul Kriptosistemi 61
3.6.5. Massey Omura Kriptosistemi 62
4. UYGULAMA 63
5. SONUÇ 73
KAYNAKLAR 75
ÖZGEÇMİŞ 80
TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER 81

TABLOLAR DİZİNİ

Tablo 3.1. Bazı Simetrik Şifreleme Algoritmaları Bilgileri 25

Tablo 3.2. $E_{23}(3, 5)$ Eliptik Eğrisi Üzerindeki Noktalar 40

Tablo 3.3. Pollard ρ Yöntemi Kullanılarak EEALP Çözümü İçin Gereken İşlem Gücü 50

Tablo 3.4. Eşit Güvenlik Seviyeleri İçin ECC ve RSA Algoritmalarının Anahtar Uzunlukları 52

ŞEKİLLER DİZİNİ

Şekil 2.1. Toplama (a) ve Çarpma (b) İşlemleri ile Tanımlı Yapı 4
Şekil 3.1. Güvensiz Ortamda Şifreli Haberleşme 20
Şekil 3.2. Temel Kriptografi Mekanizması 21
Şekil 3.3. Şifrelenen Mesaja Karşı Yapılan Atak Tipleri 23
Şekil 3.4. Simetrik Şifreleme Algoritmalarının Yapıları 24
Şekil 3.5. Asimetrik Şifreleme Algoritmalarının Yapıları 26
Şekil 3.6. RSA Şifreleme Algoritması 29
Şekil 3.7. RSA Şifreleme Algoritmasının Sayısal Örneği 32
Şekil 3.8. Kriptografi İçin Uygun Olmayan Eliptik Eğriler (a) Düğüm Durumu, (b) Çıkıntı Durumu 37
Şekil 3.9. $y^2 = x^3 - 3x + 3$ Eliptik Eğrisinin Grafiği 37
Şekil 3.10. $y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$ Eliptik Eğrisinin Grafiği 38
Şekil 3.11. $E_{23}(3, 5)$ Eliptik Eğrisi Üzerindeki Noktalar 40
Şekil 3.12. Eliptik Eğri Üzerindeki P Noktasının Tersi 41
Şekil 3.13. $y^2 = x^3 - x$ Eliptik Eğrisi Üzerinde P + Q = R Toplama İşlemi 43
Şekil 3.14. $y^2 = x^3 - x$ Eliptik Eğrisi Üzerinde P + P = 2P = R P Noktasının Çiftlenmesi 44
Şekil 3.15. $y^2 = x^3 - 6x + 6$ Eliptik Eğrisi Üzerinde Aynı Noktanın Tersi İle Toplanması 45
Şekil 3.16. ECC Kriptosisteminin Yapısı 53
Şekil 3.17. ECC Kriptosisteminde Şifreleme 54
Şekil 3.18. ECC Kriptosisteminde Kimlik Doğrulama 56
Şekil 4.1. Karakterlerin Hexadecimal Tabandaki Karşılıkları 63
Şekil 4.2. Modellenen Kriptosistemin Akış Diyagramı 68
Şekil 4.3. Eliptik Eğri Üzerindeki Noktaların Bulunması 69
Şekil 4.4. E: $y^2 = x^3 + x + 4 \bmod 23$ Eliptik Eğrisi Üzerindeki Noktalar 70
Şekil 4.5. E: $y^2 = x^3 + x + 4 \bmod 23$ Eliptik Eğrisi Üzerindeki (9, 1) Noktasının Şifrelenmesi ve Deşifrelenmesi 71
Şekil 4.6. E: $y^2 = x^3 + 7x + 40 \bmod 101$ Eliptik Eğrisi Üzerindeki Noktalar 71

Şekil 4.7. E: $y^2 = x^3 + 7x + 40$ mod 101 Eliptik Eğrisi Üzerinde "SIFRE:" Mesajının Şifrelenmesi ve Deşifrelenmesi 72

SİMGELER DİZİNİ

Kısaltmalar

AES	Advanced Encryption Standard
ALP	Ayrık Logaritma Problemi
ANSI	American National Standards Institute
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEALP	Eliptik Eğri Ayrık Logaritma Problemi
EEDH	Eliptik Eğri Diffie - Helman
EEK	Eliptik Eğri Kriptosistemi
FEAL	Fast Data Encipherment Algorithm
IDEA	International Data Encryption Algorithm
KMOV	Koyama – Maurer – Okamoto – Vanstone
NESSIE	New European Schemes for Signature Integrity and Encryption
RC2	Rivest's Chipher Ron's Code2
RC5	Rivest's Chipher Ron's Code5
RSA	Rivest - Shamir - Adleman

BÖLÜM 1

GİRİŞ

Uygarlığın başlangıcından bu yana, kullanılan iletişim teknikleriyle birlikte aktarılan verilerin güvenliği ile ilgili kaygılarda başlamıştır. Özellikle askeri bilgilerin güvenliğini sağlama çabaları ile Sezar şifresinden Enigma'ya uzanan; ardından iletişimin her alanında kullanılmaya başlanan şifreleme yöntemleri tarihte kayda değer bir aşama kaydetmiştir.

1970'lere kadar şifreleme yöntemleri neredeyse sadece askeri, diplomatik ve hükümet uygulamalarında kullanılmaktayken, 1980'li yıllarda finans ve telekomünikasyon endüstrileri şifreleme tekniklerinin donanımsal uygulamasını gerçekleştirmiş, bu uygulamanın ilk kitlesel-pazar örneği olan dijital mobil telefon sistemlerini geliştirmişlerdir. Günümüzde insanlar birçok işlemde şifreleme biliminin uygulamalarını kullanırlar. Örneğin uzaktan kumanda cihazı ile araç ya da garaj kapısını açma, yazılım güncelleştirmesi yükleme, IP (internet protocol - internet protokolü) üzerinden ses iletimi ile telefon konuşması yapma, internet üzerinden bankamatik ya da kredi kartı ile ürün satın alma, kablosuz ağa bağlanma [1].

Özellikle, bilgisayar ve internet tabanlı haberleşme sistemlerinde bilgi güvenliğini sağlamada şifreleme, şifre çözme, bilgi kaynağının doğrulanması ve bu gibi birçok konu üzerinde çeşitli çalışmalar yapılmış ve yapılmaya devam edilmektedir. Gereksinimler sonucu ortaya çıkmış olan şifreleme sistemleri Simetrik (Gizli Anahtarlı) ve Asimetrik (Açık Anahtarlı) Şifreleme Sistemleri'dir [2]. Günümüzde en sık kullanılan şifreleme sistemlerinden Rivest Shamir Adleman (RSA) Şifreleme Sistemi [3] ve Elliptic Curve Cryptography (ECC) Sistemi [4,5] de birer Asimetrik Şifreleme Sistemi'dir.

Daha önce yapılan çalışmalar, kaynakların sınırlı olduğu ortamlarda eliptik eğrileri kullanarak geliştirilmiş olan ECC algoritmasının kullanılmasıyla, diğer şifreleme algoritmalarına oranla daha hızlı ve daha verimli sonuçlar elde edildiğini göstermiştir. Bu tez kapsamında Asimetrik Şifreleme Sistemleri, özellikle ECC Algoritması ve temelde ECC algoritmasını kullanarak geliştirilmiş olan eliptik eğri kriptosistemleri incelenmiştir.

Gerekli olan matematiksel temel konulara değinilmiş, elde edilen bilgiler doğrultusunda Menezes Vanstone Eliptik Eğri Kriptosistemi temel alınıp şifreleme adımında bir takım değişiklikler yapılarak, kriptosistem değişikliğe uğratılmış ve bu kriptosistemin matematiksel modellemesi yapılmıştır.

BÖLÜM 2

MATEMATİKSEL KAVRAMLAR

Günümüzde birçok haberleşme ortamında kullanılan asimetrik şifreleme algoritmalarının alt yapısını matematiksel teoremler oluşturmaktadır. Asimetrik şifreleme algoritmaları zor matematiksel problemler üzerine oturtulmuş şifreleme algoritmalardır. Bu algoritmaların daha iyi anlaşılması ve analizlerinin gerçekleştirilebilmesi için bu bölümde aritmetik ile ilgili temel kavramlar açıklanmış olup özellikle de sayılar ve sayılar üzerinde ortaya konulmuş olan çeşitli teoremlere ve tanımlara değinilmiştir.

2.1. Gruplar

Tanım (Grup)

Üzerinde tersi alınabilir ve birleşme özelliğine sahip iki değişkenli bir operasyonun tanımlı olduğu kümeler *grup* olarak adlandırılır. Grup, boş olmayan bir G kümesi ve onun üzerinde tanımlı bir $\cdot$ işleminden oluşur. Bu operasyonun aşağıdaki şartları sağlaması gereklidir;

- $\cdot$ işlemi, G'de kapalıdır.
- $\cdot$ işlemi, "$a, b, c \in G$ için *birleşme özelliğini* sağlar.

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- $\cdot$ işleminin $e \in G$ şeklinde bir *birim elemanı* vardır.

$$a \cdot e = e \cdot a = a$$

- $\cdot$ işlemine göre G'deki her elemanın *tersi* vardır.

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

$(G, \cdot)$ yapısı sadece 1. ve 2. aksiyomlarını sağlıyorsa bir *yarı grup* denir.

$(G, \cdot)$ yapısı bir grupsa ve $\cdot$ işleminin değişme özelliği de varsa bir *değişmeli grup* denir.

2.2. Halka ve Cisimler

Tanım (Halka)

R boş olmayan bir küme olsun. + ve · ikili işlemleri bu küme üzerinde tanımlı olsunlar. Eğer (R, +, ·) cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa bu cebirsel yapıya *halka* adı verilir.

- (R, +) değişmeli gruptur.
- · işleminin R'de birleşme özelliği vardır.
- · işleminin + işlemi üzerine sağdan ve soldan dağılma özelliği vardır.

Bir halkanın + (toplama) işlemine göre etkisiz elemanına *sıfır eleman* denir. Halkanın · (çarpma) işlemine göre etkisiz elemanı varsa bu halkaya *birimli halka* denir. Ayrıca · işlemine göre değişmeli ise bu halkaya *birimli ve değişmeli halka* denir.

Tanım (Cisim)

R, birimli ve değişmeli bir halka ve $R' = R - \{O_R\}$ ikinci işlem · 'a göre bir grup ise

R'ye *cisim* denir. Bir cisimde sıfırdan farklı her elemanın çarpımsal tersi vardır ve tektir.

Örnek

{0, 1, 2, 3} elemanları ile tanımlı Şekil 2.1'de verilen farklı toplama ve çarpma işlemleri ile tanımlı yapı cisim oluşturur.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

(a)

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

(b)

Şekil 2.1. Toplama (a) ve Çarpma (b) İşlemleri ile Tanımlı Yapı

Şekil 2.1 (a) ve (b)'den de anlaşılacağı gibi 0 elemanı hariç tüm elemanların tersi olduğu için bu elemanlar için tanımlı yapı cisim oluşturur.

2.3. Tamsayılar ve Tamsayılarda Aritmetik

...,-2, -1, 0, 1, 2, ... sayılarına *tamsayılar*, 0, 1, 2, ... sayılarına *negatif olmayan tamsayılar* ve 1, 2, 3, 4, ... sayılarına da *pozitif tamsayılar* denir. Tamsayıların oluşturduğu kümeye *tamsayılar kümesi* denir ve Z ile gösterilir.

Tamsayıların şu özellikleri vardır; ($a, b, c \in Z$ için)

- Kapalılık özelliği: $a + b \in Z$ ve $a \cdot b \in Z$
- Değişme özelliği: $a + b = b + a$ ve $a \cdot b = b \cdot a$
- Birleşme özelliği: $a + (b + c) = (a + b) + c$ ve $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Dağılma özelliği: $a \cdot (b + c) = a \cdot b + a \cdot c$ ve $(b + c) \cdot a = b \cdot a + c \cdot a$
- Kısaltma özelliği: $a + c = b + c$ ise $a = b$ ve $a \cdot c = b \cdot c$ ise $a = b$ $(c \neq 0)$
- Üç hal kuralı: $a = b$, $a < b$,$a > b$ ifadelerinden yalnızca biri doğrudur.

2.3.1. Bölünebilme

Tanım

$a, b \in Z$ için $b = a \cdot c$ olacak şekilde bir $c \in Z$ bulunabilirse, a, b 'yi *böler* denir ve $a \mid b$ ile gösterilir. Bu c tamsayısını bulmaya b'yi a *ile bölme islemi* denir. b'ye *bölünen*, a'ya *bölen* ve c'ye *bölüm* denir. a ve c'ye b'nin *bölenleri* denir.

$a, b, c, d, m, n \in Z$ olmak üzere bölünebilmenin aşağıdaki özellikleri vardır:

- Yansıma özelliği: $a \mid a$
- Geçişme özelliği: $a \mid b$ ve $b \mid c$ ise $a \mid c$
- Doğrusallık özelliği: $a \mid b$ ve $a \mid c$ ise $x, y \in Z$ olmak üzere $a \mid b \cdot x + c \cdot y$
- $a \mid b$ ise $a \mid b \cdot c$
- $m \neq 0$ ve $a \mid b \Leftrightarrow m \cdot a \mid m \cdot b$
- $1 \mid a$
- $a \mid 0$
- $0 \mid n$ ise $n = 0$
- $a \mid b$ ve $b \mid a$ ise $a = \pm b$
- $a \mid b$ ve $a > 0, b > 0$ $a \leq b$

- $a \mid b$ ve $a \neq 0$ ise $\frac{b}{a} \mid b$

Teorem (Kalanlı Bölme Teoremi)

Herhangi $a > 0$ ve b tamsayıları için $b = a \cdot q + r$ ve $0 \leq r < a$ olacak şekilde tek türlü belirli q ,r tamsayı çifti vardır. Eğer $a \mid b$ sağlanmıyor ise r tamsayısı daha kuvvetli olan $0 < r < a$ eşitsizliğini sağlar.

2.3.2. Euclid Algoritması

Teorem (Euclid Teoremi)

Asal sayılar sonsuz çokluktadır [21].

Teorem (Euclid Algoritması)

Ardı ardına yapılan kalanlı bölmeler arasında 0'dan farklı en son kalana m ve n'in en büyük ortak böleni denir ve *Obeb* (m,n) şeklinde gösterilir.

$$n = q_1 \cdot m + r_1, \qquad (0 \leq r_1 < m)$$

$$m = q_2 \cdot r_1 + r_2, \qquad (0 \leq r_2 < r_1)$$

$$r_1 = q_3 \cdot r_2 + r_3, \qquad (0 \leq r_3 < r_2)$$

$$\vdots$$

$$r_{k-1} = q_{k+1} \cdot r_k + r_{k+1}, \qquad (0 \leq r_{k+1} < r_k)$$

$$r_k = q_{k+2} \cdot r_{k+1} + 0$$

Yapılan işlemler sonucunda *Obeb* (m,n) = r_{k+1}'dir.

Örnek

99 ile 17'nin en büyük ortak böleni Euclid Algoritması ile hesaplanacak olursa;

$$\begin{aligned} 99 &= 17.5 + 14 \\ 17 &= 14.1 + 3 \\ 14 &= 3.4 + 2 \\ 3 &= 2.1 + 1 \end{aligned} \Rightarrow \begin{aligned} 1 &= 3 - 2.1 \\ 1 &= 3 - 1(14 - 3.4) \\ 1 &= 5.3 - 14 \\ 1 &= 5(17 - 14) - 14 \\ 1 &= 5.17 - 6.14 \\ 1 &= 5.17 - 6.(99 - 17.5) \\ 1 &= 35.17 - 6.99 \end{aligned} \Rightarrow d = 1,\ x = 35,\ y = -6$$

Yapılan işlemler sonucunda Obeb $(99,17) = 1$ olduğu görülür. Yukarıdaki yöntem kullanılarak $d = x.m + y.n$ olacak şekilde $x, y \in Z$ tam sayılarını elde ederiz.

2.3.3. Aritmetiğin Temel Teoremi

Her $a > 1$ tamsayısının asal çarpanlarına ayrılışı, sıra düşünmeksizin tek türlüdür.

Örnek

$600 = 2^3.3.5^2$

Tanım

m ve n sıfırdan farklı iki tamsayı olsun:

- $m \mid k$ ve $n \mid k$ olacak şekilde bir $k > 0$ tamsayısı varsa k'ya m ile n'in bir *ortak katı* denir.
- k, m ile n'in bir ortak katı olsun. Eğer m ile n' in her ortak katı için $k \mid t$ ise, k'ya m ile n'in *en küçük ortak katı* denir ve $k = [m, n]$ ile gösterilir.

$$a = p_1^{m_1} . p_2^{m_2} . \dots . p_r^{m_r}$$

$$b = p_1^{n_1} . p_2^{n_2} . \dots . p_r^{n_r}$$

olsun.

$$(a,b) = p_1^{\min(m_1,n_1)} . p_2^{\min(m_2,n_2)} . \dots . p_r^{\min(m_r,n_r)} \rightarrow \text{Obeb}$$

$$(a,b) = p_1^{\max(m_1,n_1)} . p_2^{\max(m_2,n_2)} . \dots . p_r^{\max(m_r,n_r)} \rightarrow \text{Okek}$$

Önerme

a ve b pozitif tamsayılar olsun. $(a,b) \cdot [a,b] = a \cdot b$

2.3.4. Euler Fonksiyonu

Tanım

Pozitif n tamsayısı için $1 \leq a \leq n$ ve $(n, a) = 1$ olan a tamsayılarının sayısı $\varphi(n)$ ile gösterilir ve *Euler Fonksiyonu* denir.

Euler Fonksiyonu'nun özelliklerine göz atılacak olursa;

- p asal sayı ise,

$$\varphi(p) = p-1 = p \cdot \left(1-\frac{1}{p}\right),\ \varphi(7) = 7-1 = 7 \cdot \left(1-\frac{1}{7}\right)$$

- p asal sayı ve $a \in N$ ise,

$$\varphi(p^a) = p^a - p^{a-1} = p^a \cdot \left(1-\frac{1}{p}\right),\ \varphi(8) = 2^3 - 2^2 = 4$$

- $(m,n) = 1$ ise,

$$\varphi(m,n) = \varphi(m) \cdot \varphi(n),\ \varphi(14) = \varphi(7) \cdot \varphi(2) = 6 \cdot 1 = 6$$

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

$$\varphi(m) = m \cdot \left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_r}\right)$$

$$\varphi(144) = \varphi\left(2^4 \cdot 3^2\right) = 2^4 \cdot 3^2 \cdot \left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{3}\right) = 48$$

2.3.5. Modüler Aritmetik

Tanım

$m \neq 0$ ve $m, a, b \in Z$ için;

$a \equiv b \pmod{m} \Rightarrow m \mid a-b$ ile tanımlanır.

Önerme

Yukarıda tanımlanan $\equiv$ bağıntısı bir *denklik bağıntısıdır*.

- Yansıma: $a \equiv a$
- Simetri: $a \equiv b$ ise $b \equiv a$
- Geçişme: $a \equiv b$, $b \equiv c$ ise $a \equiv c$

Tanım

Z'deki denklik bağıntısının belirttiği denklik sınıflarına, *m* modülüne göre (mod *m*) kalan sınıfları denir ve tüm kalan sınıfları kümesi Z_m ile gösterilir. $a \in Z$'nin denklik sınıfı;

$\bar{a} = \{x \in Z : m \mid a - x\}$

Tanım

Z'de her sınıftan bir ve yalnız bir eleman almakla elde edilen sisteme *tam temsilciler sistemi* denir. Z_m'nin bir tam temsilciler sistemi olarak {0, 1, 2, …} alınabilir.

Örnek

$\overline{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$11 \equiv 1 (\text{mod } 5),\ 11 \in \bar{1}$

$29 \equiv 4 (\text{mod } 5),\ 29 \in \bar{4}$

$\bar{0} = \{\ , -10, -5, 0, 5, 10, \}$

$\bar{1} = \{\ \ , -9, -4, 1, 6, 11, \}$

$\bar{2} = \{\ \ , -8, -3, 2, 7, 12, \}$

$\bar{3} = \{\ \ , -7, -2, 3, 8, 13, \}$

$\bar{4} = \{\ \ , -6, -1, 4, 9, 14, \}$

Önerme

$a \equiv a_1 \pmod m$ ve $b \equiv b_1 \pmod m$ ise $a + b \equiv a_1 + b_1 \pmod m$ olur.

Önerme

$a \equiv a_1 \pmod m$ ve $b \equiv b_1 \pmod m$ ise $a \cdot b \equiv a_1 \cdot b_1 \pmod m$ olur.

Örnek

Z_5' de $\bar{4} \oplus \bar{3} = \bar{7} \equiv \bar{1}$, $\bar{4} \otimes \bar{3} = \overline{12} \equiv \bar{2}$

Önerme

$\forall \bar{a}, \bar{b}, \bar{c} \in Z_m$ için Z_m'de $\oplus$ işleminin şu özellikleri vardır;

- Değişme: $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$
- Birleşme: $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$
- Etkisiz eleman: $\bar{a} \oplus \bar{0} = \bar{a}$

- Ters eleman: $\bar{a} \oplus \bar{x} = \bar{0}$ olacak şekilde $m \exists \bar{x} \in Z_m$ bulunabilir.

Önerme

$\forall \bar{a}, \bar{b}, \bar{c} \in Z_m$ için Z_m'de $\otimes$ işleminin şu özellikleri vardır;

- Değişme: $\bar{a} \otimes \bar{b} = \bar{b} \otimes \bar{a}$
- Birleşme: $\bar{a} \otimes (\bar{b} \otimes \bar{c}) = (\bar{a} \otimes \bar{b}) \otimes \bar{c}$
- Birim eleman: $\bar{a} \otimes \bar{1} = \bar{a}$
- Yutan eleman: $\bar{a} \oplus \bar{0} = \bar{0}$

Önerme

$\forall \bar{a}, \bar{b}, \bar{c} \in Z_m$ için;

$\otimes$'nın $\oplus$ üzerine dağılma özelliği; $\bar{a} \otimes (\bar{b} \oplus \bar{c}) = (\bar{a} \otimes \bar{b}) \oplus (\bar{a} \otimes \bar{c})$ şeklinde ifade edilir.

Tanım

$\bar{a}, \bar{b} \neq \bar{0}$ ancak $\bar{a} \otimes \bar{b} = \bar{0}$ olan sınıflara *sıfır bölen sınıflar* denir.

Örnek

Z_8 'de sıfır bölen sınıflar $\bar{2}, \bar{4}, \bar{6}$'dır. ($\bar{2} \otimes \bar{4} \equiv \bar{0}, \bar{4} \otimes \bar{6} \equiv \bar{0}$)

Önerme

$\bar{a} \equiv \bar{b} \pmod{m} \Rightarrow (a, m) = (b, m)$ olur.

Tanım

$\bar{a} \in Z_m$ için $(a, m) = 1$. $\bar{a}$ sınıfına bir *asal kalan sınıfı* denir. Z_m'in bütün asal kalan sınıfları Z_m^* ile gösterilir.

Örnek

$\varphi(14) = \varphi(7).\ \varphi(2) = 6.1 = 6,\ Z_6^* = \{\bar{1}, \bar{5}\}$

Z_m^* kümesinin eleman sayısı $\varphi(m)$ Euler Fonksiyonu ile verilir. m modülü asal ise $Z_m^* = Z_m - \{0\}$ olur.

Önerme

İki asal kalan sınıfının çarpımı da bir asal kalan sınıfıdır.

Önerme

Z_m'deki $\overline{0}$'dan farklı bir kalan sınıfının sıfır bölen olması için gerek ve yeter koşul asal kalan sınıfı olmamasıdır.

Tanım

$\overline{a} \in Z_m$ olsun. $\overline{a} \cdot \overline{c} = 1$ olacak şekilde $\exists \overline{c} \in Z_m$ varsa, $\overline{c}$ 'ye $\overline{a}$'nın tersi denir.

Önerme

Z_m'deki bir kalan sınıfının tersinin olması için gerek ve yeter koşul bir asal kalan sınıfı olmasıdır.

Sonuç

m asal tamsayı ise, Z_m'deki sıfırdan farklı her kalan sınıfının tersi mevcuttur.

Örnek

$\overline{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$

$\overline{1} \cdot \overline{1} \equiv \overline{1}$

$\overline{3} \cdot \overline{3} \equiv \overline{1}$

$\overline{5} \cdot \overline{5} \equiv \overline{1}$

$\overline{7} \cdot \overline{7} \equiv \overline{1}$

Örnek

Z_{12}'deki asal kalan sınıfları veya tersi mevcut sınıflar $\varphi(12) = \varphi(3).\varphi(4) = 2.2 = 4$ tane olup;

$\overline{1} \cdot \overline{1} \equiv \overline{1}$

$\overline{5} \cdot \overline{5} \equiv \overline{1}$ $\Rightarrow Z_{12}^{*} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$'dir.

$\overline{7} \cdot \overline{7} \equiv \overline{1}$

$\overline{11} \cdot \overline{11} \equiv \overline{1}$

Z_{12}'deki asal bölenlerde $\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}$ 'dir. ($\overline{3} \cdot \overline{4} \equiv \overline{0}$, $\overline{4} \cdot \overline{6} \equiv \overline{0}$)

2.3.6. Euler Teoremi

Teorem

$m \in Z$ ve $(a, m) = 1$ olsun. $\forall a \in Z$ için;

$a^{\varphi(m)} \equiv 1(modm)\ veya\ \bar{a}^{\varphi(m)} \equiv \bar{1}$

İspat

Z_m^* asal kalan sınıflar kümesini düşünecek olursak;

$Z_m^* = \{a \in Z: 1 \leq a \leq m\ ve\ (a, m) = 1\}$

$Z_m^{12} = \{1,5,7,11\}$

$Z_m^8 = \{1,3,5,7\}$

$\varphi(m)$: Z_m^* kümesinin eleman sayısı

$a \in Z_m^*$ sabit bir asal kalan sınıfı alacak olursak $\forall \bar{b} \in Z^m$ için;

$f(\bar{b}) = \bar{a} \otimes \bar{b}$ ile $f: Z_m^* \to Z_m^*$ fonksiyonu tanımlansın. $\bar{a} \otimes \bar{b} \in Z_m^*$ olur. f' in bire bir olduğunu gösterelim;

$f(\bar{b}) = f(\bar{c}) \Rightarrow \bar{a} \otimes \bar{b} = \bar{a} \otimes \bar{c} \Rightarrow \bar{b} = \bar{c}$ elde edilir.

Z_m^* sonlu elemanlı bir küme olduğundan f'in bire bir olması, örten olmasını da gerektirir. Şu halde f, Z_m^*'in elemanlarını aralarında değiştirir. Buradan

$Z_m^* = \{\bar{a}_1, \bar{a}_2, \ldots \bar{a}_{\varphi(m)}\}$

$f(\bar{a}_1) \cdot f(\bar{a}_2) \cdot \ldots \cdot f(\bar{a}_{\varphi(m)}) = \bar{a}_1 \cdot \bar{a}_2 \cdot \ldots \cdot \bar{a}_{\varphi(m)}$

$f(\bar{b}) = \bar{a} \otimes \bar{b}$

$f(\bar{a}_1) = \bar{a} \otimes \bar{a}_1$

$f(\bar{a}_2) = \bar{a} \otimes \bar{a}_2$

.

.

$f(\bar{a}_{\varphi(n)}) = \bar{a} \otimes \bar{a}_{\varphi(m)}$

$f(\bar{a}_1 \cdot \bar{a}_2 \cdot \ldots \cdot \bar{a}_{\varphi(m)}) = \bar{a}_1 \cdot \bar{a}_2 \cdot \ldots \cdot \bar{a}_{\varphi(m)} = \bar{a} \cdot \bar{a}_1 \cdot \bar{a} \cdot \bar{a}_2 \cdot \ldots \cdot \bar{a} \cdot \bar{a}_{\varphi(m)} = (\bar{a})^{\varphi(m)} \cdot \bar{a}_1 \cdot \bar{a}_2 \cdot \ldots \cdot \bar{a}_{\varphi(m)}$

Örnek

$m = 250$ ve $a = 17$ ise

$(250,17) = 1$ $\varphi(250)=100.\ 1=100$

$a^{\varphi(m)}=17^{100} \pmod{250} \equiv 1$

Sonuç (Fermat Teoremi)

$m = p$ asal tamsayı ise $p \chi\ a$ olan $\forall a \in Z$ için $a^{p-1} \equiv 1 (mod\ p)$ olur.

Örnek

37^{49} sayısının 9 ile bölümünden kalan Fermat Teoremi kullanılarak bulunacak olursa;

$37^8 \pmod 9 \equiv 1 \quad 37^{49}=37^{48} \cdot 37=(37^8)^6 \cdot 37 \equiv 1 \pmod 9$

Tanım

$a \equiv b\ m$ seklinde bir denkleme *bir bilinmeyenli lineer kongrüans* denir. Bu denklemi sağlayan x tamsayılarının kümesine de *kongrüansın çözüm kümesi* denir.

Önerme

$a \cdot x \equiv b \pmod m$ 'in bir çözümü $x_0 \in Z_m$ ise x_0 sınıfındaki bütün tamsayılar da bir çözümdür.

Önerme

$a \cdot x \equiv b \pmod m$ 'in bir çözümünün olması için gerek ve yeter koşul $(a, m) \mid b$ olmasıdır.

Önerme

$(a, m) = 1$ ise $a \cdot x \equiv b \pmod m$ 'in bir çözümü vardır ve mod m tek bir sınıftır.

Sonuç 1

$a \cdot x \equiv b \pmod m$ kongrüansı verilsin. $d = (a, m) \mid b$ ise bu kongrüansın çözümleri mod m, d sınıftır.

Sonuç 2

$a \cdot x + b \cdot y = c$ Diophant Denklemi'nin bir çözümü olması için gerek ve yeter koşul

$(a, b) = d \mid c$ olmasıdır. Bu takdirde (x_0, y_0) bir çözüm ise $\forall k \in Z$ için $x = x_0 + \frac{b}{d} \cdot k$ ve $y = y_0 - \frac{a}{d} \cdot k$ da bir çözümdür.

Örnek

$17 \cdot x \equiv 12 (\text{mod } 99) \Leftrightarrow 17 \cdot x - 99y = 12$

- $(17, 99) = 1$ olduğundan çözüm vardır ve mod 99 tek sınıftır.

$$99 = 17.5 + 14$$
$$17 = 14.1 + 3$$
$$14 = 3.4 + 2$$
$$3 = 2.1 + 1$$

$$1 = 3 - 2.1$$
$$1 = 3 - 1(14 - 3.4)$$
$$1 = 5.3 - 14$$
$$1 = 5(17 - 14) - 14$$
$$1 = 5.17 - 6.14$$
$$1 = 5.17 - 6.(99 - 17.5)$$
$$1 = 35.17 - 6.99$$

$12 = (12 \cdot 35) \cdot 17 - (12 \cdot 6) \cdot 99$

$x = (12 \cdot 35)$, $y = (12 \cdot 6)$

Verilen kongrüansın çözümü $\bar{x} = 420 = 24$'tür.

Önerme (Çinlilerin Kalan Teoremi)

$m, n \in Z$ ve $d = (m, n)$ olsun.

$x \equiv a \text{ (mod } m)$

$x \equiv b \text{ (mod } n)$

denklem sisteminin çözümü vardır ve bu çözüm mod $m \cdot n$ tektir.

$x \equiv 1 \text{ (mod } 9)$

$x \equiv 4 \text{ (mod } 5)$

$x \equiv 1 \text{ (mod } 9) \Rightarrow x = 1 + 9 \cdot k, k \in Z$

$1 + 9 \cdot k \equiv 4 \text{ (mod } 5)$

$9 \cdot k \equiv 3 \pmod 5$

$k \equiv 2 \pmod 5$

$x = 1 + 9 \cdot 2 = 19$

$x \equiv 19 \pmod{45}$

2.4. Abelyen Gruplar

Grup tanımında verilen dört özelliğe ek olarak eğer;

- Her $a, b, c \in G$ için $a \cdot b = b \cdot a$ ise (Değişme Özelliği) bu gruba *Abelyen (Değişmeli) grup* denir [22].

2.5. Sonlu Cisimler

Cisim kavramı, bilinen sayı sistemlerinin soyutlaması ve bu sistemlerin temel özelliklerinin bir araya getirilmesi ile oluşan bir kavramdır. F grubu ile birlikte toplama (+ ile gösterilir) ve çarpma ($\cdot$ ile gösterilir) ön tanımlı iki aritmetik işlemi barındırırlar ve aşağıdaki aritmetik şartları sağlarlar [16].

- $(F, +)$ abelyen bir gruptur ve toplamsal özdeşlik o ile gösterilir.
- $(F \setminus \{0\}, \cdot)$ abelyen bir gruptur ve çarpımsal özdeşlik 1 ile gösterilir.
- Dağılma özelliğini sağlar $(a + b) \cdot c = a \cdot c + b \cdot c$

2.5.1. Cisim İşlemleri

Bir cisim toplama ve çarpma olmak üzere iki temel işlem içermektedir. $a, b \in F$ olmak üzere, çıkarma işlemi toplama işlemi kullanılarak;

$$a - b = a + (-b)$$

şeklinde ifade edilir.

Burada bulunan $-b$, F de tektir. $-b$, b'nin negatifi ya da toplamsal tersi olarak adlandırılır ve $b + (-b) = 0$'dır.

$a, b \in$ F ve b $\neq 0$ olmak üzere, bölme işlemi çarpma işlemi kullanılarak

$$\frac{a}{\mathrm{b}} = a \cdot \mathrm{b}^{-1}$$

şeklinde ifade edilir.

Burada bulunan b^{-1}, F de tektir. b^{-1}, b'nin çarpımsal tersi olarak adlandırılır ve $b \cdot b^{-1}=1$'dir.

2.6. Asal Cisimler

p'yi asal bir sayı olarak kabul ettiğimizde, $\{0, 1, 2, \ldots, p-1\}$ tamsayıları, toplama ve çarpma işleminin mod p'ye göre yapılacağı, p. dereceden bir sonlu cisim olacaktır. Bu cisim F_p olarak adlandırılır.

2.7. Asal Sayılar

Pozitif bölenleri yalnız 1 ve kendisi olan, 1'den büyük tamsayılara *asal sayı* (prime number) denir ve en küçük asal sayı 2'dir. Asal olmayan sayılar (örneğin 128, 1520 ve 4634) çarpanlarına ayrılabilirler. Asal olmayan sayılar asal çarpanlarının çarpımı olarak bir ve ancak bir yolla ifade edilebilirler.

Binyıllardır birçok matematikçi çeşitli fonksiyonlar bularak asal sayıları kendi nezdinde modellemişlerdir. Fakat genel bir seri henüz mevcut değildir. Günümüzde daha çok asal sayı üreteçleri adı verilen paralel işleme aracılığıyla büyük asal sayılar bulunmaya çalışılmaktadır. Asal sayıların sayısı sonsuzdur. Yani sonsuz sayıda asal sayı vardır [18].

2.7.1. Mersenne Sayıları

n bir asal sayı olmak üzere; 2^n-1 sayısı da eğer asal sayı ise bu tip sayılara *Mersenne sayıları* denir. Eski çağlardan beri matematikçiler n asal sayı olmak koşuluyla 2^n-1 asal sayılarını modellemeye çalıştılar [17,20].

$31 \Rightarrow 2^{31} - 1 = 2147483647$ sayısı Mersenne sayısıdır.

- 1644 yılında Fransız Matematikçi Mersenne n'in 257'e kadar sadece 11 sayıda diğerleri için olmadığını gösterdi.
- $2^{3\,021\,377} - 1$ (909526) 1998 (GIMPS)
- $2^{2\,976\,221} - 1$ (895932) 1997 Spence

2.8. Asal Sayı Üretimi

Kripto sistemin güvenliği asal sayının büyüklüğüne ve başka biri tarafından seçilme ihtimalinin düşük olmasına yani rastgele olmasına dayanır. Açık anahtarlı sistemlerde büyük asal sayıların hızla üretilmesi önemli bir rol oynar.

Bir sayının asal olup olmadığını anlamak için sayıların çarpanlara ayrılması oldukça uzun zaman aldığından çoğunlukla kullanılan bir yöntem değildir. Uygun büyüklükte bir *N* sayısı üretilir ve asal olup olmadığı test edilir. Bu test sayının asal olduğunu kanıtlayan (*kanıtlanmış asal*) ya da *büyük olasılıkla asal* denir. Sayı muhtemel asal çıkıyorsa bu tür testlere *olasılıklı asallık testleri*; eğer matematiksel olarak ispatlıyorsa buna da *gerçek asallık testleri* denir.

2.8.1. Fermat Asallık Testi

Fermatın küçük teoremi üzerine kuruludur [19].

p bir asal sayı a da bir tamsayı ve *obeb (a, p)* = 1 olmak üzere;

$\forall a \in Z$ için; $a^{p-1} \equiv 1 \pmod p$

$\forall a \in Z$ için; $a^{p} \equiv a \pmod p$

Algoritma

- sayac = 0
- while (1)
- a← rasgele bir sayı
- if obeb (a, p) ≠ 1 return asal = false; break; endif;
- if $a^{p-1} \pmod p \neq 1$ return asal = false; break; endif;
- sayac = sayac+1
- if (sayac = 100) return asal = true; break; endif;
- end while;

2.8.2. Rabin - Miller Asallık Testi

Bir sayının asal olup olmadığını test etmek için kullanılan en yaygın yöntemlerden biride Michael Rabin tarafından Gary Miller'ın fikirlerine dayanılarak geliştirilen Rabin-Miller Asallık Testidir [35]. Hata oranı oldukça düşüktür.

Algoritma

r: herhangi bir rassal sayı,

b: (r-1) değerini kalansız bölen 2^b değerindeki üs sayısı

m: $(r-1) / 2^b$

r sayısından küçük ikinci bir rassal a sayısı alınır,

- $j = 0$ ve $z = a^m \pmod r$ işlemleri yapılır,
- $z = 1$ veya $z = r-1$ ise; r testi geçer ve r asaldır.
- $j > 0$ ve $z = 1$ ise; r asal değildir.
- $j = j+1$ işlemi yapılır. $j < b$ ve $z \neq r-1$ ise; $z = z^2 \pmod r$ işlemi yapılır ve bu adım tekrarlanır. $z = r-1$ ise; r testi geçer ve asaldır.
- $j = b$ ve $z \neq r-1$ ise; r asal değildir.

2.8.3. Lucas - Lehmer Asallık Testi

Mersenne sayılarının asallığını test etmek için kullanılan asallık testidir. Lucas-Lehmer asallık testi [23], çok yoğun işlem ve buna bağlı olarak merkezi işlem birimi zamanı gerektiren bir yöntemdir.

Mersenne sayıları özel bir sayı grubunu oluşturduğundan, bu sayılarla yapılan işlemler tüm sayılar için genelleştirilemez. Bundan dolayı asal sayı elde etmek için yapılan işlemlerde, tüm asal sayıların, Mersenne sayı formatına uymadığının bilinmesi ve Mersenne sayı grubuna girmeyen asal sayıların tespiti için diğer yöntemlerin uygulanması gerekmektedir.

Algoritma

- $p > 2$ ve asal sayı olmak üzere; $s(0) = 4$,

- $s(n) = (s(n-1)^2-2) \pmod{(2^p-1)}$) şeklinde s( ) fonksiyonu tanımlanmış olsun,
- n = n+1 işlemi yapılır ve s(n) değeri hesaplanır,
- $n \neq p-2$ ise bir önceki basamağa geri dönülür. eğer n = p-2 ve s(n) = 0 2^p-1 değeri testi geçer ve asaldır aksi halde asal değildir.

2.8.4. Diğer Testler ve Asal Sayı Üretme Yöntemleri

Diğer bölümlerde (2.8.1, 2.8.2, 2.8.3) bahsedilen Fermat, Rabin-Miller ve Mersenne sayılarına uygulanan Lucas-Lehmer asallık testlerinin dışında Solovay-Strassen [24], Lehmann [25], Cohen-Lenstra [26], Gordon ve Maurer [27], çarpanlarına ayırma ve eliptik eğriler ile asallık testleri bulunmaktadır. Adı geçen asallık testleri asal sayı üretim yordamları daha fazla işlem gerektirmeleri ve daha az kesinlik içermelerinden dolayı yapılan tez çalışması kapsamında ayrıca ele alınmamıştır.

BÖLÜM 3

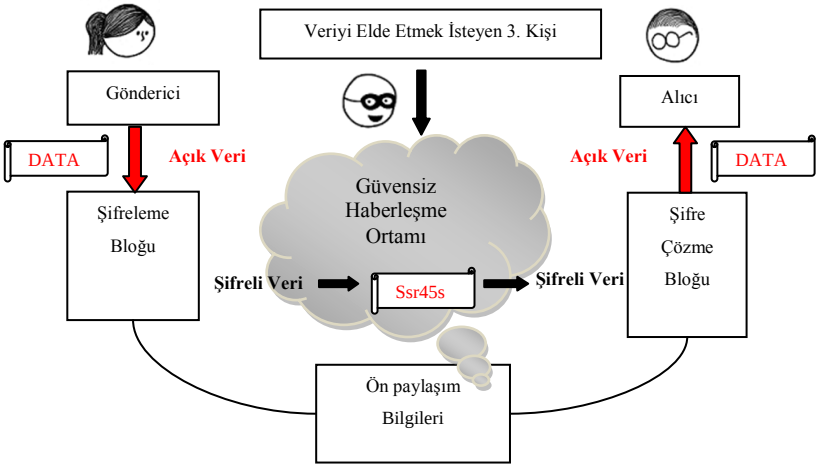
KRİPTOGRAFİK SİSTEMLER

Bu bölümde kriptoloji kavramı ve temel kriptografik sistemin özellikleri incelenmiştir.

3.1. Kriptoloji

Kriptoloji kelimesi, köken olarak eski Yunanca'da yer alan "kryptos logos" kelimelerinden gelmektedir. "kryptos" kelimesi "gizli dünya" anlamını, "logos" ise sebep-sonuç ilişkisi kurma, mantıksal çözümleme alanı anlamını taşımaktadır. Kelimenin birçok dünya dilindeki karşılığı da bu orijinal halini korumaktadır [6].

Kriptolojinin amacı, haberleşmek isteyen noktaların bulunduğu güvensiz ortam içerisinde, güvenli bir kanal oluşturarak iletişimin güvenliğini sağlamaktır. Oluşturulan bu kanal sayesinde ortamda bulunan üçüncü kişiler haberleşen iki nokta arasında gidip gelen verileri elde etseler bile anlamlandıramazlar (Şekil 3.1).



Şekil 3.1. Güvensiz Ortamda Şifreli Haberleşme

Haberleşme ortamları kullanılarak yapılan birçok işlemde güvenlik konusu yıllar ilerledikçe daha önemli hale gelmiş ve bu tarz problemlerin aşılmasına yönelik birçok yöntem ortaya koyulmuştur.

Kriptoloji esas olarak iki bölüme ayrılır, kriptografi (şifreleme) ve kriptoanaliz (şifre çözme). Gönderilmek istenen orijinal mesaj açık mesaj (plain text) ve bu mesajın şifrelenmiş hali şifreli mesaj (cipher text - cryptograph) olarak adlandırılır [7].

3.1.1. Kriptografi ve Kriptanaliz

Tanım

Kriptografi sistemi aşağıdaki koşulları sağlayan bir (P, C, K, E, D) beşlisidir:

- P, sonlu elemanlı düz metinler kümesidir.
- C, sonlu elemanlı şifreli metinler kümesidir.
- K, sonlu elemanlı anahtarlar kümesidir. (anahtar uzayı)
- Her k ∈ K için bir e_k ∈ E şifreleme kuralı ve buna karşılık gelen

d_k ∈ D şifre çözme kuralı vardır. Her X ∈ P düz metni için;

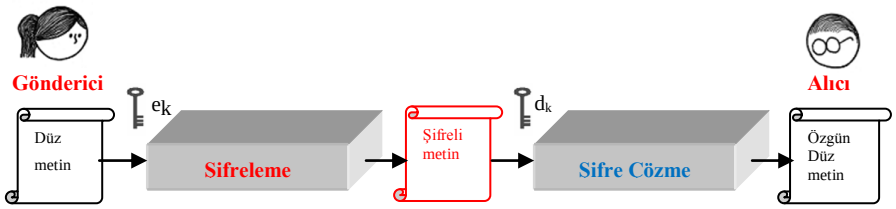
$d_k (e_k (X)) = X$

eşitliği sağlanır.

$e_k : P \rightarrow C$

$d_k : C \rightarrow P$

Bir X düz metni e_k ile şifrelendiğinde elde edilen şifreli metnin şifresi d_k ile çözülerek yine X düz metni elde edilir (Şekil 3.2).



Şekil 3.2. Temel Kriptografi Mekanizması

Kriptografi başka bir ifadeyle; gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür [8]. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi

dolayısıyla bilgi ile beraber bilginin göndericisini ve alıcısını da koruma amacı güderler. Yöntemlerden kısaca bahsetmek gerekirse [8]:

- Gizlilik: Bilgiyi görme yetkisi olanlar dışındaki herkesten gizli tutmaktır.
- Kimlik Denetimi: İletimi gerçekleştirilen bir mesajın göndericisinin gerçekten gönderen kişi olduğu garantisidir.
- Bütünlük: Bütünlük bir bağlantının tamamı ya da tek bir veri parçası için, mesajın gönderildiği gibi olduğuna, üzerinde hiçbir değişiklik, ekleme, yeniden düzenleme yapılmadığı garantisidir.
- Reddedilmezlik: Alıcının veya göndericinin iletilen mesajı inkar edememesidir. Böylece bir mesaj gönderildiğinde alıcı göndericinin mesajı gönderdiğini, benzeri biçimde gönderici de alıcının mesajı aldığını ispatlayabilir.
- Erişim Kontrolü: İzinsiz kişi ya da uygulamaların erişmemeleri gereken kaynaklara erişemeyecekleri garantisidir. Ağ güvenliği bağlamında, erişim kontrolü, ana bilgisayar sistemlerine erişimleri kontrol etme ve sınırlandırma yetisidir. Bu kontrolü başarmak için, erişimi kazanmaya çalışan her varlık ilk olarak tanımlanmalı veya doğrulanmalıdır. Erişim kontrolü servisleri kimlik denetimi yapılmış varlıkların kaynaklara ancak kendilerine izin verilen şekilde erişebilecekleri garantisini vermekle yükümlüdür.

Kriptanaliz, istenmeyen taraflarca okunmaması için şifrelenen bilginin çözülmesi, gizliliğinin ortadan kaldırılmasıdır.

Şifrelenen metnin ne kadar güvenli olduğu ve çözümlenmesi için yapılacak atak tiplerinin neler olduğunun bilinmesi önemlidir. Şekil 3.3'de şifrelenen mesajı çözmek için yapılan atak tipleri ve kriptoanalistin neler bildiği gösterilmiştir.

AtakTipi	Kriptoanalist'in bildiği
Sadece Şifreli Metin (ciphertext only)	Kriptolama algoritması Kodu çözülecek şifreli metin (istatistiksel atak, eksiksiz arama)
Bilinen Düz metin (known plaintext)	Kriptolama algoritması Kodu çözülecek şifreli metin Gizli anahtar ile şifrelenen bir veya daha fazla düz-şifreli metin çifti (Şifreye atak için kullanılır.)
Seçilen Düz metin (chosen plaintext)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen açık metin, bununla birlikte açık metnin gizli anahtar ile üretilen şifreli hali
Şeçilen Şifreli metin (chosen ciphertext)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen kuvvetle muhtemel şifreli metin ve karşılığı olan, gizli anahtar ile üretilen çözümlenmiş açık metin.
Şeçilen metin (chosen text)	Kriptolama algoritması Kodu çözülecek şifreli metin Kriptoanalist tarafından seçilen açık metin, bununla birlikte açık metnin gizli anahtar ile üretilen şifreli hali Kriptoanalist tarafından seçilen kuvvetle muhtemel şifreli metin ve karşılığı olan, gizli anahtar ile üretilen çözümlenmiş açık metin.

Şekil 3.3. Şifrelenen Mesaja Karşı Yapılan Atak Tipleri

İki farklı temel yöntem ile şifreler güvenli olabilir:

- Mutlak Güvenlik: Bilgisayar gücü ne kadar fazla olursa olsun şifre hiçbir şekilde kırılamaz.
- Hesaplamaya Bağlı Güvenlik: Verilen bilgisayar gücü sınırları içinde, hesaplama zamanının çok uzun olmasından dolayı şifre kırılamaz.

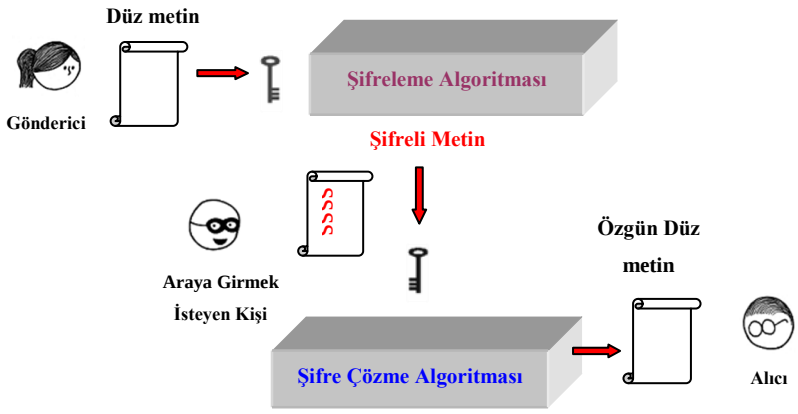
Hesaplamaya bağlı güvenlik için şifreleme algoritması ve kullanılan anahtar uzunluğu önemlidir. Çözümleme süresi için gerekli olacak zaman hesabı ortalama olarak alternatif şifre sayısının yarısı kadardır. Bilgisayar hesaplama gücünü ise paralel mimarili tasarım ile arttırmak mümkün olmaktadır.

3.2. Kripto Algoritmaları

Bahsettiğimiz tüm bu güvenlik sistemleri kriptografik algoritmalar ile sağlanmaktadır. Bu bölümde kriptografik algoritmaların özellikleri incelenmiştir. Temel olarak iki tip kriptografik algoritma vardır. Bunlar kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılırlar [2].

3.2.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve deşifreleme işlemleri için tek bir gizli anahtar kullanmaktadır (Şekil 3.4).



Şekil 3.4. Simetrik Şifreleme Algoritmalarının Yapıları

Bu durum veri şifreleme için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermesi gerekmektedir. Bu kriptosistemin güvenliği algoritmanın gizliliğinden değil, anahtarın gizliliğinden gelmektedir.

Blok şifreleyiciler ve dizi şifreleyiciler olmak üzere iki tür simetrik anahtarlı kriptosistem vardır [6]. Blok şifreleyicilerde şifrelenecek veri sabit bloklara ayrılıp her turda bir blok şifrelenir. En temel örnekler Veri Şifreleme Standardı (DES: Data Encryption Standard) ve Gelişmiş Kodlama Standardı (AES: Advanced Encryption Standard) şifreleme algoritmalarıdır [9,10,11].

Dizi şifreleyiciler şifrelenecek verinin her bir adımda sadece bir bitini şifreler [12]. Bazı durumlarda blok şifreleyicilerde blok uzunluğu bir seçilip dizi şifreleyicilerle aynı duruma gelebilmektedir. Bu şifreleyicilerde verinin her bir biti için farklı bir şifreleme metodu ya da anahtar kullanılabilmektedir. Ayrıca iletim sırasında hata oluşma olasılığı yüksek durumlarda kullanılabilmektedirler çünkü hata gecikmesi yoktur, şifre çözme sırasında hata oluştuğu anda başka herhangi bir bit işleme sokulmaz. Bunlara ek olarak

donanımsal yetersizlik nedeniyle düşük performanslı aynı anda çok fazla işlem yapamayan sistemlerde her bir turda bir sembol işlenmesi gerekiyorsa dizi şifreleme kullanılmalıdırlar.

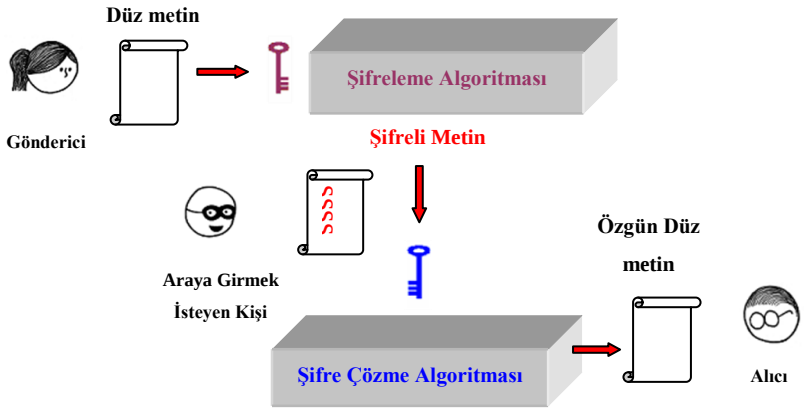
Tablo 3.1. Bazı Simetrik Şifreleme Algoritmaları Bilgileri

Algoritmanın Adı	Geliştiren	Tarihi	Tipi	Anahtar Uzunluğu	Döngü Sayısı	Çözülme Durumu	Kullanım Koşulları
Data Encryption Standard (DES)	IBM (ABD)	1977	Feistel Blok (64 bit)	56 bit (parity ile 64 bit)	16	Sağlam; 8 döngülü çeşidi çözülebiliyor; 16 zayıf anahtar	Serbest
International Data Encryption Algorithm (IDEA)	Lai-Massey, ETH Zurich (İsviçre)	1992	Blok (64 bit)	128 bit	8	Sağlam; 251 zayıf anahtar	Ticari faaliyetler hariç serbest
Rivest's Cipher veya Ron's Code2 (RC2)	Rivest, RSA Data Security (ABD)	1992	Katar	2048 bite kadar	Bilinmiyor	Zayıflık bulunmadı	Algoritma RSA tarafından saklı tutuluyor
Rivest's Cipher veya Ron's Code5 (RC5)	Rivest, RSA Data Security (ABD)	1995	Blok (32, 64 veya 128 bit)	2048 bite kadar	255'e kadar	64 bit blok ve 12 döngü ile diferansiyel ve doğrusal şifre çözüme dayanıklı	Serbest
Blowfish	Bruce Schneier, Counterpane Systems (ABD)	1993	Feistel Blok (64 bit)	448 bite kadar	16	3 döngülü çeşidi diferansiyel şifre çözüme hassas	Ticari faaliyetler hariç serbest
Fast Data Encipherment Algorithm (FEAL)	Shimizu ve Miyaguchi (Japonya)	1988	Blok	FEAL-4 64 bit; FEAL-N 128 bit	FEAL-4 4 döngü; FEAL-N 31 döngü	Güvensiz; çeşitleri başarıyla çözümlendi	-
Secure and Fast Encryption Routine (SAFER)	Massey, Cylink Corporation (ABD)	1993	Blok (64 bit)	64 bit; 128 bit	10 döngüye kadar	İlk sürümlerinin anahtar açılımında zayıflıklar vardı	-
Skipjack (Clipper Chip)	NSA (ABD)	1993	Blok (64 bit)	80 bit	32	Algoritma gizli	Sadece özel entegre devre olarak bulunuyor
Lucifer	IBM (ABD)	1970?	Feistel Blok (64 bit)	128 bit	16	DES'in prototipi olduğundan zayıflıklar içermesi olasıdır	-
GOST 28147-89	I.A.Zabotin, G.P.Glazkov, V.B.Isaeva (Sovyetler Birliği)	1989	Feistel Blok (64 bit)	256 bit; 512 bit tanımlanabilir sübsitüsyon; 610 bit etken gizli bilgi	32	SSCB tarafından bütün gizlilik derecelerindeki bilgiler için uygun görülmüştür	Serbest
ASEKAL-21	Aselsan (Türkiye)	-	Doğrusal olmayan katar	57 bit ?	-	Ulusal olarak onaylanmış algoritma	Aselsan 2101, 2010 veri ve ses şifreleme birimlerinde kullanılıyor
Advanced Encryption Standard (AES)	NSA (ABD)	2001	Blok	128 bitten 256 bite kadar	128 bit için 10, 192 bit için 12, 256 bit için 14	Atak biclique adı verilen yapılar kullanılarak anahtarlar elde edilmiştir.	Serbest

Simetrik anahtarlı şifrelemede en temel sorun hangi simetrik anahtarın kullanılacağı konusunda tarafların anlaşma yöntemidir. Tarafların birbiri ile anlaşması ve gizli anahtarı en etkili ve güvenli şekilde değişmesi gerekmektedir. Bu anahtar dağıtım problemi 1977 yılında Diffie ve Hellman EL-GAMAL şifreleme algoritması [13] tarafından önerilmiş olan yöntemle aşılmıştır. Diffie ve Hellman bu problemin çözümü için açık anahtar kriptosistemini önermiştir. Bazı simetrik şifreleme algoritmalarının özelikleri Tablo 3.1'de verilmiştir.

3.2.2. Asimetrik Şifreleme Algoritmaları

Asimetrik şifreleme algoritmaları, simetrik şifreleme algoritmalarından radikal bir farklılık göstermektedir. Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve çözme işlemlerinin her biri için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir (Şekil 3.5).



Şekil 3.5. Asimetrik Şifreleme Algoritmalarının Yapıları

Bu sistemde şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılır. Şifreleme ve çözme işlemi birbirinin simetriği olmayan (yani aynısı olan) algoritmalarla gerçekleştirildiğinden dolayı da asimetrik şifreleme sistemi olarak bilinir [12,14,15].

Her kullanıcının gizli ve açık olmak üzere iki anahtarı vardır. Bu anahtarlardan açık anahtar haberleşme ortamındaki herkes tarafından bilinmektedir. Gizli anahtar ise kişiye özel olup sadece ait olduğu kullanıcı tarafından bilinir. Anahtarlar özel seçilmiş olup kriptosisteme göre değişiklik boyutlardadır. Anahtarlar algoritma içinde yer alan çok özel işlevler tarafından kullanılmaktadır ve her kullanıcının açık ve gizli anahtarı bir çift

oluşturur. Herkes kendi açık ve gizli anahtar çifti ile diğer tüm kullanıcıların açık anahtarına sahiptir. Açık anahtar bilgisi alıcı tarafa herhangi bir koruma yapılmadan iletilir. Açık anahtarı alan taraf bu bilgiden şifreli veriyi çözmek amacı ile kullanacağı gizli anahtarı üretir. Açık anahtarın üçüncü bir kişinin eline geçmesi tek başına bir şey ifade etmez.

Asimetrik şifreleme algoritmalarının üç önemli sınıfı vardır:

- Açık anahtar Dağıtım Şeması (Public-Key Distribution Schemes): Bilginin bir kısmının güvenli olarak değiştirilmesi için kullanılır (değer iki tarafa bağlıdır). Bu değer gizli anahtar seması için bir oturum anahtarı olarak kullanılır.
- İmza Şeması (Signature Schemes): Sadece sayısal imza üretmek için kullanılır, burada gizli anahtar imzayı üretmekte, açık anahtar ise doğrulamakta kullanılır.
- Açık anahtar Şeması (Public Key Schemes): Şifrelemek için kullanılır, burada açık anahtar mesajları şifreler, gizli anahtar mesajların şifresini çözer.

Asimetrik şifreleme sistemleri, gizli anahtarın açık anahtar kullanılarak hesaplanmasının güçlüğüne dayanır. Buna dayanarak ve sayılar teorisinin de kullanılmasıyla ortaya çıkmış olan en önemli üç asimetrik şifreleme algoritması aşağıda verilmiştir:

- Bir Tamsayının Çarpanlarına Ayrılmasına Dayanan Algoritmalar: Verilen bir n pozitif tamsayının asal çarpanlarını bulmaya dayanmaktadır. n sayısı çok büyük ve özel seçilmektedir. RSA en çok kullanılan açık anahtar algoritması olup bu problemin çözümünün zorluğuna dayanmaktadır. Ayrıca Rabin-Willams [40] şifreleme yöntemi tamsayıların çarpanlarına ayrılması problemine dayanır.
- Ayrık Logaritma Problemine (ALP) Dayanan Algoritmalar: Verilen bir α , β ve p için öyle bir x değeri bulunmalıdır ki $\beta = \alpha_x \bmod p$ sağlamalıdır. Diffie - Hellman anahtar değişim protokolü, ElGamal Şifreleme ve İmza Yöntemleri [29], Schnorr İmza Yöntemi [41] ve Nyberg-Reuppel [42] algoritması bu probleme dayanmaktadır.
- Eliptik Eğri Ayrık Logaritma Problemine (EEALP) Dayanan Algoritmalar: Bu algoritmalar da ALP tabanlıdır ancak burada ALP bir eliptik eğri üzerinde tanımlıdır. Eliptik Eğri Diffie Helman (EEDH) protokolü ve Eliptik Eğri Sayısal İmza Algoritması (ECDSA) bu matematiksel temele dayanmaktadır. Diğer grupta

yer alan algoritmalarla 1024-2048 bit uzunluğunda sağlanan güvenlik seviyesi 160-256 bit uzunluğu ile sağlanabilmektedir. Sonlu alan aritmetiğine dayanmaktadır. EEDH ve EEALP hakkında ayrıntılı bilgi bölüm 3.5.6'da verilmiştir.

3.3. Anahtar Yönetimi

Hem simetrik hem de asimetrik algoritmaların temel özelliği yapılarının açık olarak bilinmesidir. Böylece kripto algoritmalarının tasarımında, şifrelenmiş verinin anahtar bilgisi olmadan şifrenin çözülememesi ilkesi göz önüne alındığından, iletişim güvenliği, kripto anahtarlarının güvenliği problemine indirgenmiştir. Kriptografik anahtarların üretilmelerinden dağıtılmalarına ve kullanılmalarına kadar olan sürecin sıkı bir denetim altına alınması kriptografik işlemlerin güvenilirliği açısından büyük öneme sahiptir. Bu işlemlerin tümüne anahtar yönetim denir. Anahtar yönetiminin en zayıf halkası, dış müdahalelere tümüyle açık olan anahtarların güvenli bir şekilde dağıtılması işlevidir.

Şifreleme algoritmalarının başarımı altı ana kritere göre belirlenir [4]:

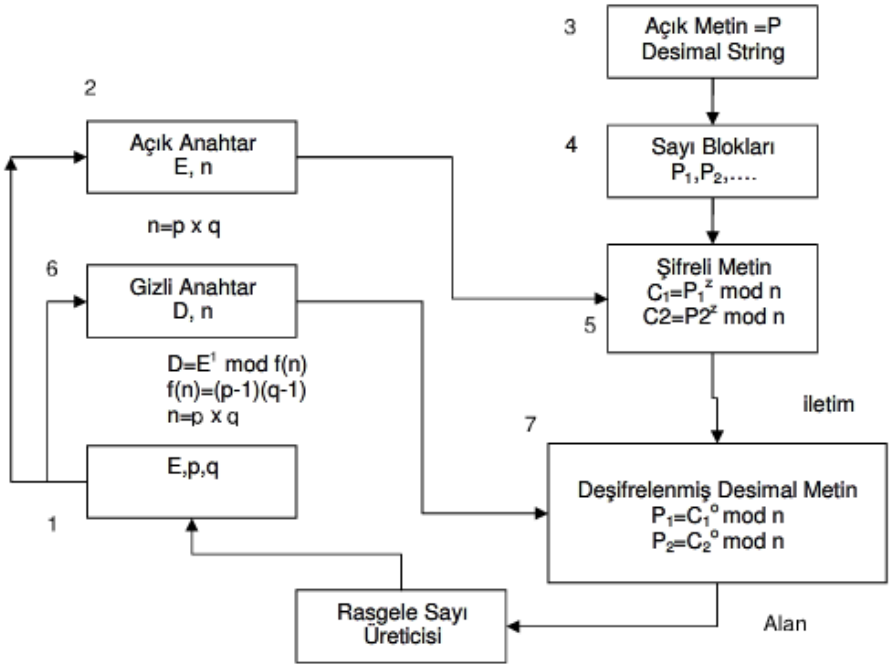
- Kırılabilme süresinin uzunluğu,
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı),
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı),
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği,
- Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların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

3.4. RSA Kriptosistemi

Whitfield Diffie ve Martin Hellman'ın, 1976 yılında asimetrik şifreleme sistemleri hakkında yayınladıkları makale [13] kriptoloji bilimine yeni bir yön sağladı. RSA kriptosistemi adını bu algoritmayı 1977 yılında uygulamaya sokan Ronald Rivest, Adi Shamir ve Leonard Adleman'dan alır. RSA sisteminin temelinde tamsayı çarpanlara ayırma problemi bulunmaktadır.

RSA Algoritması asimetrik şifreleme yönteminin temel bir uygulamasıdır. Bu şifreleme yönteminin diğer bir iyi tarafı ise önceden aralarında hiçbir görüşme yapmamış olan alıcı ve vericinin kendi aralarındaki iletişimin güvenli bir ortamda(güvenli gönderim ve mesajların doğrulanması) yapılmasıdır.

Daha önce hiç karşılaşmamış, birbirini tanımayan kişiler bile birbirlerine gizli mesajlar gönderebilir. Örneğin internet üzerinden alışveriş yapan birisi, kendisini hiçbir şekilde tanımayan bir web sitesine giderek, sitenin kamuya açık anahtarını alır, kart numarasını bu anahtarla şifreleyerek gönderir. Şifreli bilgiyi gönderen kişi de dahil olmak üzere, hiç kimse çözemez. Sadece web sitesinde bulunan gizli anahtarla gelen kart numarasını web sitesi çözebilir. Böylece kart hamili kart numarasının başkası tarafından okunmayacağından emin olacaktır. Bu noktada web sitesi gerçekten dürüst bir satıcı mı, yoksa sahte bir site mi sorusu akla gelir. Çözüm sadece sertifika yöntemiyle sağlanmaktadır [28].



Şekil 3.6. RSA Şifreleme Algoritması

RSA şifreleme algoritmasında şifrelenecek olan açık metni öncelikle [0, n-1] arasındaki pozitif tamsayı bloklar haline dönüştürülür. Şekil 3.6'da [29] ayrıntılı olarak matematiksel işlemler gösterilmektedir.

Bu sistem $n \in Z_n$'deki hesaplamalara dayanmaktadır. n sayısı iki farklı asal sayı olan p ve q'nun çarpımıyla elde edilmektedir.

Sistemin detayları su şekildedir: (P, C, K, E, D)

- p ve q asal sayılar olmak üzere, $n = p \cdot q$ hesaplanır.
- P, C = Z_n kabul edilir ve

$$K = \{(n, p, q, a, b) : a \cdot b \equiv 1 \pmod{\varphi(n)}\} \text{ alınır.}$$

- K={(n, p, q, a, b) ile

$$e_K(x) = x^b \pmod{n} \text{ ve } d_K(y) = y^a \pmod{n} \text{ tanımlanır. } (x, y \in Z_n)$$

Bu işlemler sonucunda elde edilen n ve b, *açık anahtarı* oluşturur. p, q ve a ise *gizli anahtar*lardır.

Şayet şifreleme ve deşifreleme işlemlerinin ters işlemler olduğunu göstermemiz gerekirse:

$a \cdot b \equiv 1 \pmod{\varphi(n)}$

$t \geq 1$ alınırsa;

$a \cdot b \equiv t \cdot \varphi(n)+1$

$x \in Z_n^*$ olduğundan;

$(x^b)^a \equiv x^{t \cdot \varphi(n)+1} \pmod{n}$

$\equiv (x^{\varphi(n)})^t \cdot x \pmod{n}$

$\equiv 1^t \cdot x \pmod{n}$

$\equiv x \pmod{n}$ elde edilir.

Örnek

$p = 2357$ ve $q = 2551$ alınarak açık ve gizli anahtarlar hesaplanacak olursa;

- $n = p \cdot q = 2357 \cdot 2551 = 6012707$,
- $\varphi(n) = (p-1) \cdot (q-1) = 6007800$,

- e = 3674911 seçilirse OBEB (e = 3674911, φ = 6007800)=1 ve 1< e < φ koşulunu sağlar,
- $e \cdot d \equiv 1 \pmod{\varphi}$ $3674911 \cdot d \equiv 1 \pmod{6007800}$ d = 422191 değeri hesaplanır.

Elde edilen e = 3674911 sayısı açık anahtar olarak kullanılabilir. d = 422191 sayısı ise gizli anahtardır.

Algoritma (RSA Anahtar Çiftinin Oluşturulması)

Girdi. Güvenlik parametresi, l. (l, rasgele pozitif çift tamsayı)
Çıktı. RSA açık anahtarı (n, e) ve gizli anahtar d.

- $l/2$ şartını sağlayan, eşit uzunlukta rasgele p ve q asal sayıları belirlenir.
- $n = p \cdot q$ ve $\varphi = (p-1) \cdot (q-1)$ hesaplanır,
- $1 < e < \varphi$ ve $(e, \varphi) = 1$ şartlarını sağlayan keyfi e sabiti belirlenir,
- $1 < d < \varphi$ ve $e \cdot d \equiv 1 \pmod{\varphi}$ şartlarını sağlayan d sayısı hesaplanır,
- (n, e, d) bulunmuş olur.

RSA şifreleme sistemi tüm m tamsayıları için;

$m^{e \cdot d} \equiv m \pmod{n}$ prensibine dayanmaktadır.

Algoritma (Temel RSA Şifrelenmesi)

Girdi. RSA açık anahtarı (n, e), düz metin $m \in [0, n-1]$.
Çıktı. Şifreli metin c.

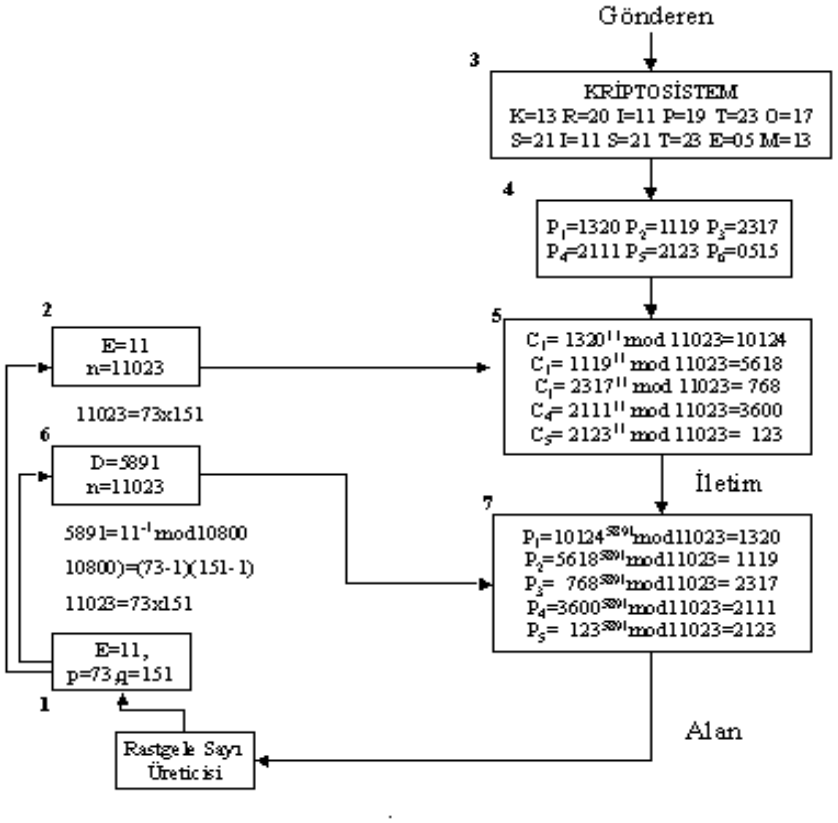
- $c \equiv m^e \pmod{n}$ hesaplanır.
- c bulunmuş olur.

Algoritma (Temel RSA Deşifrelenmesi)

Girdi. RSA açık anahtarı (n, e), RSA gizli anahtarı d, şifreli metin c.
Çıktı. Düz metin m.

- $m \equiv c^d \pmod{n}$ hesaplanır.
- m bulunmuş olur.

Şekil 3.7'de RSA şifreleme algoritmasının sayısal örneği verilmiştir [30].



Şekil 3.7. RSA Şifreleme Algoritmasının Sayısal Örneği

RSA kriptosistemin sayısal imzalar içinde kullanılır. Gönderici A'nın açık anahtarı (n, e), d gizli anahtarı olsun. Göndereceği mesaj x ve x'in {0, 1, 2, …., n-1} arasında olması gerekir.

İmzalama işleminde A kullanıcısı,

- $\sigma = x^d \bmod n$ hesaplayıp (x, σ) imzalı mesajını B kullanıcısına gönderir.

İmza doğrulama işleminde B alıcısı,

- $x = \sigma^e \bmod n$ ile mesajı elde edilir imza doğrulanmış olur.

Örnek

A kullanıcısı anahtar oluşturma işlemi için,

p= 7927, q = 6997, e = 5,

n= p · q = 7927 · 6997 = 55465219, φ = (p – 1) · (q – 1) = 7926 · 6996 = 5540296,

$e \cdot d = 1 \bmod \varphi = 5 \cdot d = 1 \bmod 5540296 = 44360237$,

Açık anahtar (55465219, 5), gizli anahtar d = 44360237 olur.

A kullanıcısı imzalama işlemi için,

x = 31229978 mesajını B kullanıcına göndermek istesin.

$\sigma = x^d \bmod n = 31229978^{44360237} \bmod 55465219 = 30729435$,

B kullanıcısına (31229978, 30729435) çiftini gönderir.

B kullanıcısı imza doğrulama işlemi için,

$x = \sigma^e \bmod n = 30729435^5 \bmod 55465219 = 31229978$ gönderilen mesaj elde edildiği için imza doğrulanmış olur [53].

RSA sisteminin kırılması birkaç değişik şekilde yorumlanabilir. Sisteme en çok zarar verecek saldırı bir kriptanalistin belli bir açık anahtara karşı gelen gizli anahtarı bulmasıdır. Bunu başarabilen bir kişi hem şifrelenen bütün mesajları okuyabilir hem de imzaları taklit edebilir. Bunu yapmanın en akla gelen yolu n'nin asal çarpanlara ayrılması yani p ve q'nun hesaplanmasıdır. p, q ve açık üs e kullanılarak d kolaylıkla hesaplanabilir. Ancak buradaki zorluk n modülünün çarpanlarına ayrılmasıdır. RSA sisteminin güvenliği çok büyük sayıların asal çarpanlarına ayrılmasının zorluğu varsayımına dayanır. Büyük sayıların çarpanlarına ayrılmasının zorluğu ispatlanmış değildir. Son üç yüzyıl içerisinde Fermat ve Legendre gibi ünlü matematikçiler bu konuda çalışmalar yapmışlardır [30,31].

3.5. ECC Şifreleme Algoritması

Eliptik Eğri Kriptosistemi (EEK) bir açık anahtar kriptosistemi olup RSA açık anahtar kriptosistemine alternatif olarak 1985 yılında öne sürülmüştür. RSA'nın güvenli kullanımı için, çalışılan bit uzunlukları zaman içerisinde büyümüş ve dolayısıyla RSA kullanan uygulamalar üzerine büyük bir hesapsal ağırlık getirmiştir. Özellikle büyük sayıların transferini güvenlik içinde gerçekleştirmesi gereken ticari siteler bundan çok fazla etkilenmişlerdir. RSA kriptosisteminin güvenliği, büyük tam sayıların asal çarpanlarına ayrılmasındaki matematiksel zorluğa dayanırken EEK güvenilirliği RSA'ya göre daha yeni

bir matematiksel problem olan ve günümüzde yarı üstel zamanda hala çözülemeyen ayrık logaritma problemine (ALP) dayanmaktadır.

NESSIE (New European Schemes for Signature, Integrity and Encryption) tarafından yayımlanan rapora [32] göre EEK daha kısa anahtar ile RSA kriptosistemi ile aynı güvenlik seviyesi sağlayabilmektedir. Örneğin 160-bitlik bir EEK ile 1536-bitlik bir RSA kriptosisteminin birbirine güvenlik seviyesi anlamında denktir. Ayrıca aynı anahtar uzunluğu için EEK, RSA kriptosisteminden daha hızlı şifreleme yapabilmektedir. Bu özellikleri ile EEK, RSA kriptosisteminin yerini almak için adaydır çünkü ihtiyaç duyulan güvenlik seviyesi EEK daha küçük anahtarlar ile karşılayabilecektir. Küçük anahtar uzunluğu ile gerçeklenen EEK, daha az işlem maliyeti ve daha az bellek tüketimi demektir ya da başka bir bakış açısıyla aynı anahtar uzunluğu kullanıldığında EEK daha hızlı bir kriptosistemdir.

3.5.1. Eliptik Eğri Teorisi

Eliptik eğriler elips değildirler. Bu şekilde adlandırılmalarının sebebi, bir elipsin çemberinin hesaplanması için kullanılan kübik denkliklere benzer ifadeler ile gösterilmeleridir. Bir *K* cismi ele alınırsa, *K* cismi, *R* Gerçel sayılar, *Q* Rasyonel sayılar, *C* Kompleks sayılar veya *p*'nin asal bir sayı olduğu kabul edilirse, $q = p^r$ elemanlarından oluşan F_q sonlu cismi olabilir. $GF(2^m)$ sonlu cisminin karakteristiği 2, gerçel ve kompleks sayıların karakteristiği ise sonsuzdur.

Bir cisimde 1 sayısına kendisi eklenir. Eğer 1 + 1 = 0 oluyorsa bu cismin karakteristiği " 2 " dir. Eğer 1+1+1 = 0 oluyorsa bu cismin karakteristiği " 3 " tür. Genel olarak 1 + 1 + 1 +…+ 1 = 0 oluyorsa cismin karakteristiği " n " dir. N Eğer cisimde 1 sayısına kendisi sonsuz defa eklenebiliyorsa cismin karakteristiği " 0 " dır. Herhangi bir *K* cismi için, eliptik eğrinin Weierstrass biçimdeki genel denklemi;

$$y^2+axy+by=x^3+cx^2+dx+e \text{ 'dir} \qquad (3.1)$$

Eğer *K* cisminin karakteristiği Char(*K*) = 2 ya da başka bir deyişle $GF(2^m)$ alanında tanımlı ise Eş. 3.1;

$$y^2+ay=x^3+bx+c$$

$y^2+xy=x^3+2ax+b$ denklemine dönüşür. (3.2)

Eğer *K* cisminin karakteristiği Char(*K*) = 3 ya da başka bir deyişle *GF(3^m)* alanında tanımlı ise Eş. 3.1;

$y^2=x^3+2ax+bx+c$ denklemine dönüşür. (3.3)

Eğer *K* cisminin karakteristiği Char(*K*)≠ 2 veya 3 ise Eş. 3.1;

$y^2=x^3+ax+b$ denklemine dönüşür. (3.4)

Her bir denklem için Affine Dönüşümleri kullanılır ve bu denklemde yer alan *x, y, a, b, c, d* ve *e* değerleri de *K* cisminin üstünde yer almaktadır. Yukarıda belirtilen herhangi bir şartı sağlayan, *K* alanında yer alan ve (x,y) noktalarının kümesinden oluşan denkleme *E eliptik eğri denklemi* diyebiliriz.

3.5.2. Projektif Uzaylar

Bir eliptik eğrinin noktalarını bir Abelian grup yapan toplama işleminin verilebilmesi için projektif uzayların kısa bir tarifinin verilmesi gerekir. Bu toplama işleminin tanımında, reel eksene dik olan, eliptik eğrinin noktaları üzerindeki toplamanın etkisiz elemanı olarak karsımıza çıkacak olan ve sonsuzdaki nokta olarak adlandırılan noktanın tanımına ihtiyaç duyulur. Grup aksiyomlarından birleşme özelliğinin anlaşılabilmesi için kübik eğrilerin kesişimlerinin iyi belirlenmesi gerekmektedir.

K^3-{(0, 0, 0)} kümesi üzerinde aşağıdaki şekilde tanımlanan bağıntı bir denklik bağıntısıdır.

$\forall(X_1, Y_1, Z_1),(X_2, Y_2, Z_2)\in K^3$-{(0, 0, 0)} için eğer $(X_1, Y_1, Z_1)=t\cdot(X_2, Y_2, Z_2)$ olacak şekilde bir $0\neq t\in K$ varsa (X_1, Y_1, Z_1) ve (X_2, Y_2, Z_2) noktalarına denktirler denir ve $(X_1, Y_1, Z_1)\equiv(X_2, Y_2, Z_2)$ ile gösterilir.

Bu denklik bağıntısından oluşan denklik sınıflarının kümesine iki boyutlu projektif uzay denir ve $\wp^2(K)$ ile gösterilir. $\wp^2(K)$'nın elemanlarına da projektif noktalar denir ve (X: Y: Z) ile gösterilir.

$\wp^2(K)$'dan herhangi bir (X: Y: Z) noktasını alalım:

Eğer $Z\neq 0$ ise $x:=\frac{X}{Z}$, $y:=\frac{Y}{Z}$ olmak üzere (X: Y: Z) = (x: y: 1)'dir. Bu durumda $\wp^2(K)$ 'nın (x: y: 1) şeklindeki elemanları K^2'nin elemanlarıyla eşlenebilir.

$\wp^2(K)$ 'nın (x: y: 0) şeklindeki elemanlarına *sonsuzdaki noktalar* denir. Böylece,

$$\wp^2(K)=K^2 \cup \{(x: y: 0) \mid x, y \in K\}$$

şeklinde düşünülebilir [2].

E eliptik eğrisinin sonsuzdaki noktaları belirlenirse;

$f(x, y)$, katsayıları K cisminden alınan iki değişkenli bir polinom olmak üzere afin düzlemdeki $f(x, y)=0$ eğrisine, $x:=\frac{X}{Z}$, $y:=\frac{Y}{Z}$ dönüşümlerini uygulayıp bu eğriyi Z'nin yeterince büyük bir kuvveti ile çarpınca $\wp^2(K)$ 'da bir eliptik eğri olarak düşünebiliriz. E.ş. 1.4'de $x:=\frac{X}{Z}$, $y:=\frac{Y}{Z}$ dönüşümlerini yapıp, denklemin her iki tarafını Z^3 ile çarparsak projektif düzlemde eliptik eğri:

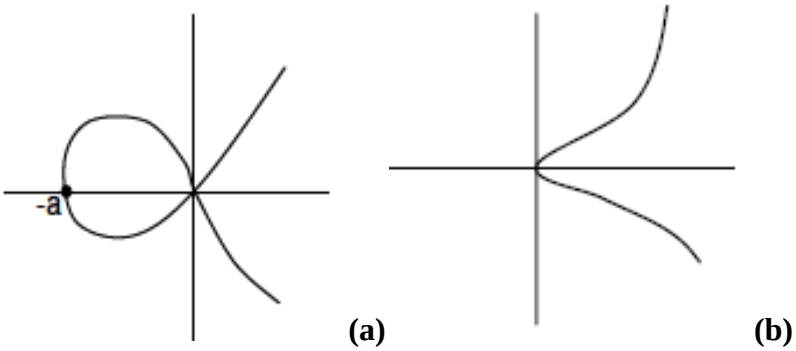
$$E^* := \{(X: Y: Z) \in \wp^2(K) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}\text{'dir.}$$

$(X: Y: Z) \in E^*$ olsun. $Z = 0$ ise $X = 0$ elde edilir. X, Y ve Z'nin üçü birden sıfır olamayacağından $Y = 1$ dir. Yani E^* daki sonsuzdaki nokta sadece (0: 1: 0) dır [2].

3.5.3. Eliptik Eğriler

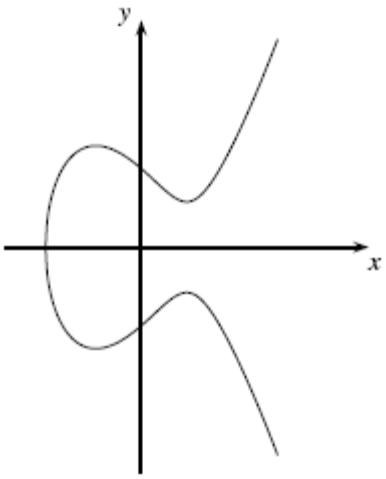
Eliptik eğrinin kriptosistemlerde kullanılabilmesi için grup olma özelliklerini sağlaması gerekir. Jacobi, 1835'de, kübik bir eğri üzerinde grup olma kurallarının sağlanabileceğini önermiştir [36]. Eliptik eğri üzerindeki iki noktadan geçen bir doğru, eliptiği üçüncü bir noktada keser kuralı "kiriş - teğet kuralı" (Chord - tangent rule) [37] olarak anılır ve kriptografiye uygun, cisim olma özelliklerini barındıran grubun oluşturulmasında kullanılır.

Genel olarak, bundan sonra incelenecek eliptik eğri denklemlerinde E.ş. 3.4 kullanılacaktır. $f := x^3+ax+b$ denklemdeki a ve b sayıları gerçel sayılardır ve x^3+ax+b denkleminin çoklu kökü olmaması için $\Delta(f)=4a^3 + 27b^2 \neq 0$ olmalıdır. Eğer bu koşulları sağlıyorsa $y^2 = x^3 + ax + b$ *eliptik eğridir* denilir. Böylece eliptik eğri tekil olmaz ve sonlu sayıda (x, y) nokta çifti ile çözümlenebilir. Şekil 3.8'de $\Delta(f)=4a^3 + 27b^2 \neq 0$ kuralına uymayan eğriler verilmiştir. Bu eğriler kriptografi için uygun değildir.

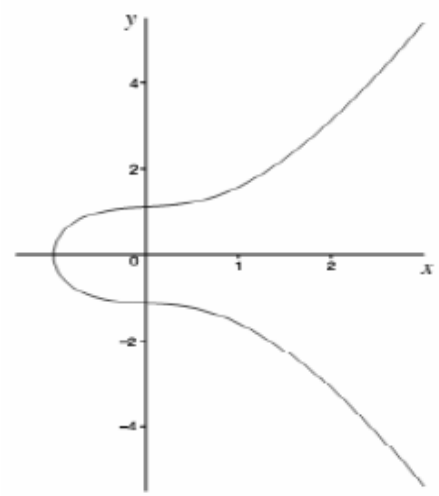


Şekil 3.8. Kriptografi İçin Uygun Olmayan Eliptik Eğriler (a) Düğüm Durumu, (b) Çıkıntı Durumu

Şekil 3.9'da $y^2 = x^3 - 3x + 3$ eliptik eğrisinin, Şekil 3.10'da ise $y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$ eliptik eğrisinin grafiği verilmiştir. En büyük dereceli üs 3 olduğundan bu denklemler kübik olarak adlandırılır. Ayrıca, eliptik eğrinin tanımlanmasında sonsuzluk ya da sıfır nokta adı verilen bir *O* notasyonu vardır.



Şekil 3.9. $y^2=x^3-3x+3$ Eliptik Eğrisinin Grafiği



Şekil 3.10. $y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$ Eliptik Eğrisinin Grafiği

Eğer bir eliptik eğrinin 3 noktası düz bir çizgi üzerinde bulunuyorsa, bunlar *O* olarak özetlenir. Bu açıklamadan yola çıkarak, bir eliptik eğri için şu kuralları tanımlayabiliriz [33]:

- Eliptik eğri üzerindeki herhangi bir *P* noktası için, $P + O = P$ olur.
- Bir dikey çizgi, aynı *x* değeri için eliptik eğriyi $P_1 = (x, y)$ ve $P_1 = (x,-y)$ gibi iki noktasında kesiyorsa, bu çizgi aynı zamanda eliptik eğriyi *sonsuzluk noktasında* da kesiyordur. Bu yüzden $P_1 + P_2 + O = O$ ve $P_1 = -P_2$ olur. Böylece bir noktanın negatifi, *x* ekseni üzerinde aynı değeri alacak şekilde bir noktadır ve bu noktanın *y* ekseni üzerindeki değeri ilk noktanın negatiflisidir.
- *x* koordinatı farklı olan *Q* ve *R* noktası seçip bu iki noktadan geçen düz bir çizgi çizdiğimizde kesişimin üçüncü noktası olan P_1 'i buluruz. Ve çok kolay bir şekilde görülebilir ki, P_1 noktası sadece bir tanedir (eğer çizdiğimiz doğru, *Q* veya *R* noktalarından birisinden teğet geçiyorsa bu durumda $P_1 = Q$ veya $P_2 = R$ alırız). Bu durumda $Q + R + P_1 = O$ ve dolayısıyla $Q + R = -P_1$ olacaktır.
- Bir *Q* noktasını çift katlı yapmak için, bir teğet çizgisi çizip eğriyi kestiği diğer noktayı buluruz. Eğer bu noktaya *S* diyecek olursak $Q + Q = 2Q = -S$ eşitliği sağlanır.

3.5.4. Sonlu Cisimlerdeki Eliptik Eğriler

ECC için, eliptik eğrilerin, "*sonlu alanlardaki eliptik eğriler*" olarak tanımlanan formu şu şekilde gösterilir [34]:

p bir asal sayı olsun ve *a* ve *b p*'den küçük negatif olmayan iki tamsayı olsun;

$$4a^3 + 27b^2 (\text{mod } p) \neq 0$$

Bu durumda $E_F(a,b)$, (x,y)'nin P'den küçük negatif olmayan tamsayılar olduğu durum için, O sonsuz noktası ile şu eşitliği ifade eder;

$$y^2 \equiv x^3 + ax + b \ (\text{mod } p)$$

Örnek

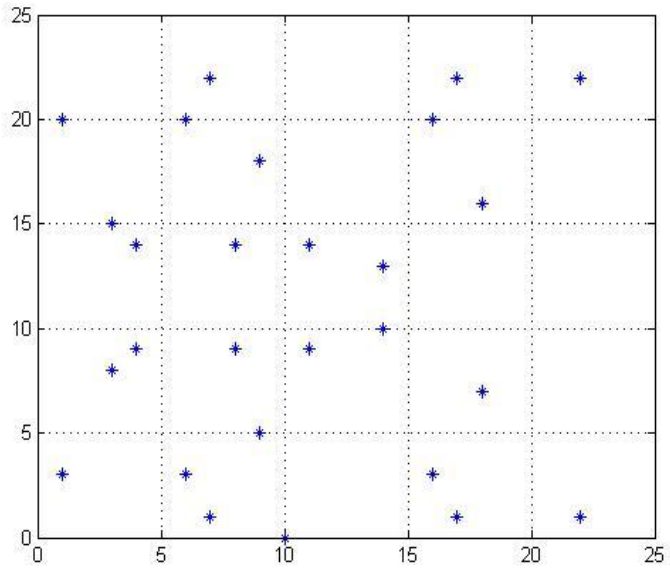
$p = 23$ ve eliptik eğrimiz de $y^2 = x^3 + 3x + 5$ olsun. Bu durumda $a = 3$, $b = 5$ olur. Bu durumda $4(3)^3 + 27(5)^2 \ (\text{mod } 23) = 1 \neq 0$, seçilen eliptik grubun mod 23 e göre durumunu gösterir.

Eliptik grup için sadece (mod *p*'den dolayı), (0, 0) - (*p, p*) aralığında olan pozitif tamsayılar ile denklem oluşturulur. Tablo 3.2 ve Şekil 3.10'da, E_{23} (3, 5) için O dışındaki noktaları listelenmiştir. Genel olarak liste aşağıdaki yolla oluşturulmuştur [34]:

- $0 \leq x < p$ koşulunu sağlayan her x değeri için $x^3 + ax + b \ (\text{mod } p)$ denklemi hesaplanmıştır.
- Önceki adımın her sonucu için, sonucun (mod *p*) 'ye göre çift katlı kökü olup olmadığına bakılır, eğer yoksa bu *x* değeri için, $E_F(a, b)$ 'nin bir değeri yoktur. Aksi takdirde, çift katlı kök koşulunu sağlayan iki adet *y* vardır (*y*'nin 0 olduğu durum haricinde). Bu (*x, y*) değerleri $E_F(a, b)$ 'nin noktalarıdır.

Tablo 3.2. E_{23} (3, 5) Eliptik Eğrisi Üzerindeki Noktalar

(1, 3)	(1, 20)	(3, 8)
(3, 15)	(4, 9)	(4, 14)
(6, 3)	(6, 20)	(7, 1)
(7, 22)	(8, 9)	(8, 14)
(9, 5)	(9, 18)	(10, 0)
(11, 9)	(11, 14)	(14, 10)
(14, 13)	(16, 3)	(16, 20)
(17, 1)	(17, 22)	(18, 7)
(18, 16)	(22, 1)	(22, 22)

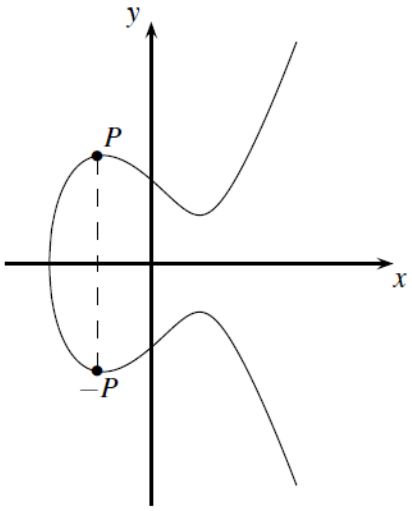


Şekil 3.11. E_{23} (3, 5) Eliptik Eğrisi Üzerindeki Noktalar

Her $P,Q \in E_F(a,b)$ olacak şekilde alınan noktalar için aşağıdaki gibi gösterilebilir:

- $P + O = P$.

- Eğer $P = (x, y)$ ise $P + (x, -y) = O$ olur. $(x,-y)$ noktası P'nin negatifidir (Şekil 3.12) ve $-P$ olarak gösterilir. $E_{23}(3, 5)$ 'de $P = (11, 14)$ noktasını ele alalım. Bu durumda $-P = (11, -14)$ olacaktır. Fakat -14 (mod 23) e göre 9'dur. $-P$ noktası aslında, yine $E_{23}(3, 5)$ 'de yer alan (11, 9) noktasıdır.



Şekil 3.12. Eliptik Eğri Üzerindeki P Noktasının Tersi

- Eğer $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ ise ve $P \neq -Q$ ise bu durumda, $P + Q=(x_3, y_3)$ şu kuralla hesaplanır:

$$x_3 \equiv \lambda^2 - x_1 - x_2 (\text{mod } p)$$

$$y_3 \equiv \lambda (x_1 - x_3) - y_1 (\text{mod } p)$$

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

Teorem (Hasse Teoremi)

E, F_q cismi üzerinde tanımlı bir eliptik eğri polinomudur ve $E(F_q)$ olarak gösterilir. $q = p^n$ olarak p asal sayısının n 'inci üstsel değerini tanımlar. E polinomunu sağlayan (x, y) nokta çiftlerinin sayısı; polinomun eğrisini sonsuzda kesen nokta O da dahil, eliptik eğrinin cisim üzerinde oluşturduğu grubun eleman sayısını verir ve $\#E(F_q)$ ile gösterilir. x'in her bir değeri için y'nin en çok iki değeri vardır. Sonsuzdaki O noktasıyla birlikte bu eğri üzerinde

en çok 2q + 1 tane nokta vardır. Fakat rasgele seçilen bir elemanın ikinci dereceden bir kalan olma şansı %50 olduğundan bu sayı yarı yarıya azalacak ve q + 1 olacaktır.

E. Artin 1926 yılında yayınladığı doktora tezinde bu teoremi konjektür olarak verdi. 1930' lu yıllarda ise bu teorem Hasse tarafından ispatlanmıştır [38].

Weierstrass eşitliğinde her $x \in F_q$ için x eksenine göre eliptik eğrinin simetrisinden dolayı iki çözüm vardır ve Hasse kuramı; Fq cismi üzerinde tanımlı E eliptik eğrisinin tanımladığı grubun eleman sayısının $\# E(F_q) = N$ ve $| q + 1 - N | \leq 2\sqrt{q}$ olacağını söyler. $q = p^n$ olarak bir p asal sayısının üssü olarak yazılabiliyorsa $N = q + 1 - a$ 'dır. Sadece ve sadece $|a| \leq 2\sqrt{q}$ olması ve a 'nın aşağıda verilen koşullardan birisini sağlaması durumunda, F_q cismi üzerinde $\# E(F_q) = N$ eşitliğini sağlayan bir E eliptik eğrisi bulunduğu söylenebilir [39]:

- $a \neq 0 \pmod p$ ve $a^2 \leq 4q$.
- n tek sayıysa;
  a. $a = 0$; veya
  b. $a^2 = 2q$ ve $p = 2$; veya
  c. $a^2 = 3q$ ve $p = 3$.
- n çift sayıysa;
  a. $a^2 = 4q$; veya
  $a^2 = q$ ve $p \neq 1 \pmod 3$; veya
  $a = 0$ ve $p \neq 1 \pmod 4$.

Yukarıdaki kuramdan, p asal sayısı ve a tamsayısı için $a \leq 2\ q$ koşulu sağlandığında F_q cismi üzerinde tanımlanan E eliptik eğrisinin oluşturacağı grupta $\# E(F_q) = q + 1 - a$ adet eleman olacağı sonucu çıkarılır [38,39].

3.5.5. Eliptik Eğri Aritmetiği

Eliptik eğri nokta toplama ile ilgili bir önceki bölümde yer alan geometrik yaklaşım eliptik eğri aritmetiğinin ortaya koyulması açısından oldukça yol göstericidir. Ancak aritmetik hesaplamalar için geometrik yaklaşım pratik çözüm olmadığından, cebirsel formüller oluşturularak bu hesaplamalar verimli bir şekilde yapılmaktadır.

- İki Farklı P ve Q Noktasının Eklenmesi:

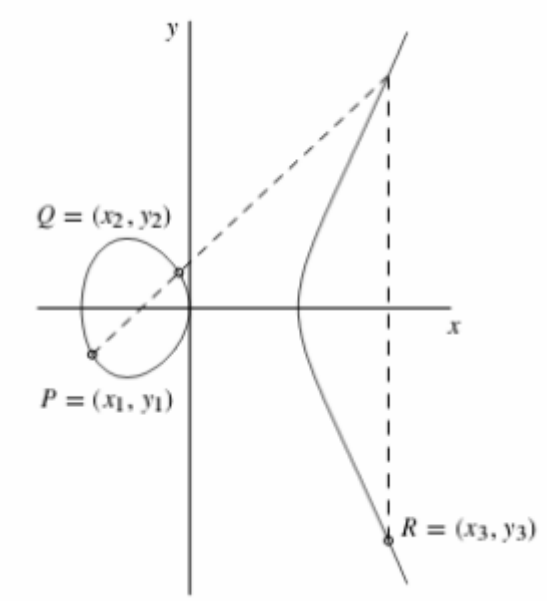
Şayet $P(x_p, y_p)$, $Q(x_q, y_q)$, $R(x_r, y_r)$ ve $P \neq -Q$ olsun;

$P + Q = R$ için, λ P noktası ile Q noktasını birleştiren çizginin eğimidir.

$$\lambda = \frac{y_p - y_q}{x_p - x_q}$$

$$x_r = \left[\lambda^2 - x_p - x_q\right] \pmod p$$

$$y_r = \left[-y_p + \lambda\left(x_p - x_r\right)\right] \pmod p$$



Şekil 3.13. $y^2 = x^3 - x$ Eliptik Eğrisi Üzerinde P + Q = R Toplama İşlemi

Şekil 3.13'de $y^2 = x^3 - x$ eliptik eğrisi üzerinde iki farklı P ve Q noktasının eklenmesi işlemi incelenebilir.

Örnek

F_{23} üzerinde tanımlı eliptik eğri, E: $y^2 = x^3 - 17x + 16$ ve $P = (0, -4)$ ve $Q = (1, 0)$ ise;

$P + Q = R = (x_3, y_3)$ şöyle bulunabilir:

$$\lambda=\frac{-4-0}{0-1}=4$$

$$x_r=\left[4^2-0-1\right]=15\equiv 15 \pmod{23}$$

$$y_r=\left[-(-4)+4\left(0-15\right)\right]=-56\equiv 13 \pmod{23}$$

$P + Q = R = (15, 13)$

- P Noktasının Aynılanması (Çiftlenmesi):

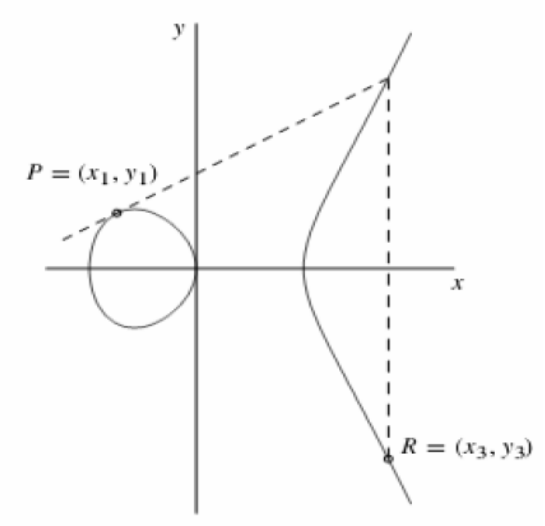
$y_p \neq 0$ ise $P + P = 2.\ P = R$ için;

λ, P noktasından eliptik eğriye çizilen teğetin eğimi, a ise eliptik eğri oluşturulurken seçilen sabittir.

$$\lambda=\frac{3x_p^2+a}{2y_p}$$

$$x_r=\left[\lambda^2-2x_p\right] \pmod{p}$$

$$y_r=\left[-y_p+\lambda\left(x_p-x_r\right)\right] \pmod{p}$$



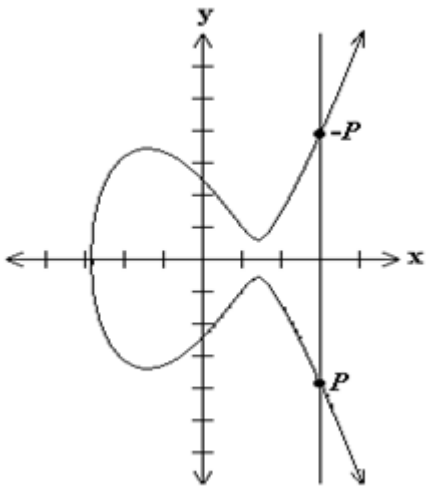
Şekil 3.14. $y^2 = x^3 - x$ Eliptik Eğrisi Üzerinde P + P = 2P = R P Noktasının Çiftlenmesi

Şekil 3.14'de $y^2 = x^3 - x$ eliptik eğrisi üzerinde *P* noktasının çiftlenmesi işlemi incelenebilir.

- Aynı Noktanın (P) Tersi (-P) İle Toplanması:

P ve *–P* noktalarını birleştiren çizgi, eğriyi üçüncü bir noktada kesmez. Buna göre *P* ve *–P* noktaları birinci adımda verilen iki farklı noktanın toplanması işleminde verilen toplama işlemi gibi toplanamaz. Bu sayede eliptik eğri, sonsuzluk noktası *O*'yu içerir. Şekil 3.15'de $y^2 = x^3 - 6x + 6$ eliptik eğrisi üzerindeki aynı noktanın tersi ile toplanması işlemi incelenebilir.

$P + (-P) = O,\ P + O = (-P)$



Şekil 3.15. $y^2 = x^3 - 6x + 6$ Eliptik Eğrisi Üzerinde Aynı Noktanın Tersi İle Toplanması

3.5.6. Eliptik Eğrilerde Şifreleme Sistemleri, Problem Çözüm Yöntemleri ve Yaklaşımları

Sonlu alanlar için ALP'nin varsayılan zorluğuna dayanan birçok şifreleme sisteminin, eliptik eğrilere uygulaması bulunmaktadır. Bu sistemlerde açık metnin her bir karakteri alanın bir elemanı ile eşlenmektedir. Eliptik eğrilerde ise, karakter dizilerinin eliptik eğri üzerindeki noktalarla eşlenmesi gerekmektedir.

- EEDH: A (Gönderici) ve B (Alıcı) çiftinin, iletişim için bir gizli anahtar üzerinde anlaşmak istediklerini varsayalım. İlk olarak her ikisi açık olarak bir Fq sonlu alanı

ve bu alan üzerinde eliptik eğri E belirlerler. Yine açık olarak E üzerinde rasgele bir nokta P belirlenir. A, gizli olarak bir tamsayı *a* seçer ve *a*P'yi hesaplar. Benzer şekilde, B, gizli olarak bir tamsayı *b* seçer ve *b*P'yi hesaplar. A ve B, sırasıyla *a* ve *b* tamsayılarını gizli tutarken, *a*P ve *b*P açıklanır. A gizli *a* değerine, B gizli *b* değerine sahiptir. Hem A, hem de B *ab*P'yi hesaplayabilmektedirler ve bu anlaşılmış ortak gizli anahtardır. Sadece P, *a*P ve *b*P verilmişken, *ab*P'nin hesaplanmasının EEALP'yi (Eliptik Eğri Ayrık Logaritma Problemi) çözmeyi gerektirdiğine inanılmaktadır [43].

- EEALP: Tüm kriptografik sistemlerin temelinde, patrikte hesaplama yolu ile çözümü oldukça zor olan matematiksel problemler yatar. ALP, eliptik eğri şifreleme sistemlerinin de dahil olduğu birçok kriptografik sistemin temelini oluşturur. Eliptik eğri şifreleme sistemleri EEALP'ye dayanmaktadır. Matematiksel işlemlerin tamsayı alanlarından eğri üzerindeki noktalara taşınmasıyla ortaya çıkan EALP, klasik ALP'den çok daha zor gözükmektedir.

Z_p^* çarpımsal grubu göz önüne alınarak ALP açıklanacak olursa:

p asal sayısı, *r* ve *q* da verilen elemanlar olmak üzere,

$r = q.\ k \pmod{p}$ eşitliğini sağlayan bir *k* değeri bulma işlemidir.

Eğer eliptik eğri grubu çarpımsal notasyon kullanılarak tanımlanacak olursa, bu durumda *P* ve *Q* noktaları için ortaya çıkan EEALP;

P.*k* = *Q* eşitliğini sağlayan bir *k* değeri bulma işlemidir ve *Q noktasının P tabanında ayrık logaritması* olarak adlandırılır.

Örnek

F_{23}'te tanımlanmış olan $y^2 = x^3 + 9x + 17$ eliptik eğrisi üzerinde bulunan *Q* = (4, 5) noktasının *P* = (16, 5) tabanına göre ayrık logaritması olan *k* hesaplanacak olursa; çözümün elde edilmesi için yapılacak işlem basitçe *P* noktasının katları şu şekildedir;

P = (16, 5), 2.*P* = (20, 20), 3.*P* = (14, 14), 4.*P* = (19, 20), 5.*P* = (13, 10), 6.*P* = (7, 3), 7.*P* = (8, 7), 8.*P* = (12, 17), 9.*P* = (4, 5)

9.P = (4, 5) = *Q* olduğundan, *Q*'nun *P* tabanına göre hesaplanan ayrık logaritması $k = 9$ yani $\log_P(Q)=9$'dur.

EEALP, skaler çarpma sonucu elde edilen noktalarının takibinin zorluğuna dayanmaktadır [16].

Tanım (Skaler Çarpma)

Bir eliptik eğri grubu tanımlanırken toplamsal notasyon kullanılır. Çarpımsal notasyon, toplamsal notasyon kullanılarak tanımlanacak olursa; *k.P*'nin hesaplanması, *P* noktasının *k* defa kendisi ile toplanmasıdır.

EEALP çözümünde genel ve özel çözüm yöntemleri bulunmaktadır. Özel yöntemler; eğri üzerindeki noktaların eşdeğerlik kümelerine bölünebildiği durumlardan faydalanan eşdeğerlik kümeleri yöntemi [43], süper tekil olarak adlandırılan, *q* asal üssel sayısı kadar noktaya sahip olan ve istisna eğriler olarak adlandırılan eğrilerin özelliklerinden faydalanan istisna eğriler yöntemi [44], *q* asal sayısının üssel değerlerinin uzun süre 1 değeri vermediği, süper tekil olarak adlandırılan eğrilerin özelliklerinden faydalanan MOV yöntemi [27] sayılabilir. Bu tür eğriler oldukça seyrek (örneğin, seçilen bir eğrinin istisna eğrilerden olması ihtimali $1/4\sqrt{q}$ dur) ve seçilen eğrilerin bu sınıflara girip girmediğinin tespit edilmesi olanaklı olduğundan, eliptik eğri ayrık logaritma probleminin çözümü için çok fazla yardımcı olamamaktadır. Genel yöntemler aşağıda açıklanmıştır.

- Kaba Çözüm Yaklaşımı: EEALP çözümü için en temel yöntem üretici Q'nun katlarının hesaplanması ve bunların bir tabloda tutulmasıdır. Her bir işlemin eliptik eğri toplama olduğu akılda tutulmak üzere, bu yöntem tablonun oluşturulması için O(*n*) süre ve tablonun tutulması için O(*n*) alan gerektirir. Bu en kötü durum sıralamasının üzerine aşağıdaki yöntemlerle oldukça ilerleme sağlanmıştır.
- Pohlig-Hellman Yöntemi: Bu yöntem [45], taban noktasının düzeyi olan *n*'nin çarpanlara ayrılmasından faydalanmaktadır. Yöntem, *l* değerinin bulunmasını *l* mod(*n*'nin asal çarpanlarının her birisi) düzeyine indirmektir. Her bir çarpan için hesaplama yapıldıktan sonra *l* değeri hesaplanır. Bu yöntem düzeyi çok büyük asal çarpanlara sahip bir eliptik eğri için işlevselliğini yitirmektedir.

- Shank Yöntemi (Bebek Adımı, Dev Adımı): Daniel Shanks tarafından ortaya konmuş olan yöntem [46] karmaşıklığı $O(n^{\frac{1}{2}} \log n)$ ve gereken alanı $O(\sqrt{n})$ düzeylerine indirmektedir. Bu yöntem *p* asal sayısının tam değerini değil, yaklaşık değerlerini kullanmaktadır. Bu algoritmanın eliptik eğri uyulmaması şu şekildedir: Q'nun *n* düzeyinde bir üretici olduğunu varsayalım, A noktası verildiğinde kQ = A olacak şekilde k değerini bulmak istiyoruz. $m = \sqrt{n}$ olsun. $(m-1) \geq j \geq 0$ için L1 listesinde (j, jmQ) çiftleri tutulur. Bu liste çiftlerin ikinci elemanlarına göre sıralanır. $(m-1) \geq i \geq 0$ $(m-1)$ için (i, -iQ + A) çiftlerinden oluşan ikinci bir liste, L2 yaratılır ve bu liste de ikinci elemanlarına göre sıralanır. Listeler (j, P) ∈ L1 ve (i, P) ∈ L2 bulununcaya kadar taranır. Bu durumda:

  $p = 3 \bmod 4$ ise ($p = 4u + 3$ gibi bir değere sahipse);

  - $y = a^{u+1} \bmod p$
  - eğer $y^2 = a$ ise, sonuç bulunmuştur, aksi takdirde y değeri yoktur.

  $p = 5 \bmod 8$ ise ($p = 8u + 5$ gibi bir değere sahipse);

  - $y = a \cdot (2a)^u \cdot [(2a)^{2u+1} - 1] \bmod p$
  - eğer $y^2 = a$ ise, sonuç bulunmuştur, aksi taktirde y değeri yoktur.

  $p = 1 \bmod 4$ ise ($p = 4u + 1$ gibi bir değere sahipse);

  - $Q = g$; $0 \leq P \leq p$ olmak üzere rasgele bir değer alınır.
  - Lucas Sıra Elamanları bulunur:

    $$U_0 = 0, U_1 = 1, \ldots U_k = PU_{k-1} - QU_{k-1} \; (2 \leq k)$$

    $$V_0 = 0, V_1 = P, \ldots V_k = PV_{k-1} - QV_{k-1} \; (2 \leq k)$$

  - $U = U_{2u+1}$, $V = V_{2u+1} \bmod p$ elemanları hesaplanır.
  - $V^2 = 4Q$ ise $y = V/2 \bmod p$ olur.
  - $U \neq 1$ ise y değeri yoktur.
  - Başka bir P değeri ile işlemler baştan tekrarlanır.

  $$P = jmQ$$

  $$P = -iQ + A$$

  $$jmQ = -iQ + A$$

  $$(jm + i)\, Q = A$$

  olur ve $k = (jm + i)$ olarak bulunmuştur.

- Pollard'ın ρ (ro) Yöntemi: EEALP çözümü için bilinen en iyi yöntem, Pollard'ın ρ yöntemidir [47]. Karmaşıklığı O(√n), gerektirdiği bellek alanı ise 6 değerin tutulmasına kadar indirgenmiştir.

  A, katsayısı bilinmeyen nokta; Q, *n* seviyesinde eğrinin üreteci olsun. A=*x*Q olduğuna inanıyor ve *x*'i arıyorsak;

  a_0, $q_0 \in Z_n$ seçilir. $x_0 = q_0 + a_0A$ atanır. $\{x_i\}$, $\{a_i\}$ ve $\{q_i\}$ aşağıdaki şekilde oluşturulur:

$$x_i = \begin{cases} Q+x_{i-1} & x_{i-1} \in S_0 \text{ ise} \\ 2x_{i-1} & x_{i-1} \in S_1 \text{ ise} \\ A+x_{i-1} & x_{i-1} \in S_2 \text{ ise} \end{cases}$$

$$a_i = \begin{cases} a_{i-1} & x_{i-1} \in S_0 \text{ ise} \\ 2a_{i-1} & x_{i-1} \in S_1 \text{ ise} \\ 1+a_{i-1} & x_{i-1} \in S_2 \text{ ise} \end{cases}$$

$$q_i = \begin{cases} 1+q_{i-1} & x_{i-1} \in S_0 \text{ ise} \\ 2q_{i-1} & x_{i-1} \in S_1 \text{ ise} \\ q_{i-1} & x_{i-1} \in S_2 \text{ ise} \end{cases}$$

  $x_i = x_j$ olduğunda:

  $a_iA + q_iQ = a_jA + q_jQ$

  $(a_i - a_j)A = (q_j - q_i)Q$

  $A = [(q_j - q_i)/(a_i - a_j)]Q$

  $(a_i - a_j)$ tersi alınabilir bir değer ise sonuç bulunmuştur. Bellek yönünden $x_i = x_j$ bulmak için en etken işleyiş $x_i = x_{2i}$ bulmaya çalışmaktır. Bu şekilde ilk $x_i = x_j$ bulunamayabilir, ancak sadece 6 değerin, x_i, x_{2i}, a_i, a_{2i}, q_i ve q_{2i}, tutulması yeterli olmaktadır. Son çalışmalar bu yöntemin √2 kat hızlandırılabileceğini göstermiştir. Bu durumda geliştirilmiş Pollard'ın ρ yöntemi için karmaşıklık $O(\sqrt{(\pi n)/2})$ olmaktadır.

Odlyzko'nun [48] 1995 yılında yaptığı çalışmadaki hesaplamalarına göre dünyadaki tüm bilgisayarların binde biri birlikte çalıştırıldığında 2014 yılında 1010 ila 1011 MIPS yıl toplam işlem gücüne erişeceği sonucuna varılmıştır. Tablo 3.3'de [48] Pollard ρ yöntemi kullanılarak EEALP çözümü için öngörülen MIPS tahminleri verilmiştir.

Tablo 3.3. Pollard ρ Yöntemi Kullanılarak EEALP Çözümü İçin Gereken İşlem Gücü

q(ikil)	MIPS yıl
160	$8{,}5 \times 10^{11}$
186	$7{,}0 \times 10^{15}$
234	$1{,}2 \times 10^{23}$
354	$1{,}3 \times 10^{41}$
426	$9{,}2 \times 10^{51}$

- Eliptik Eğri Anahtar Değişim Algoritması: ADA, SKIPJACK [52] algoritmasının açıklanmasıyla duyulan ABD'nin Anahtar Değişim Algoritmasıdır. Algoritmanın eliptik eğrilerle uygulanması şu şekildedir: Fp üzerinde E eliptik eğrisi ve q asal düzeyinde E eğrisi üzerinde bir P noktası açıktır. A, gizli $x_A \in Z_q$ seçer, x_AP değerini hesaplar ve açıklar. B gizli $x_B \in Z_q$ seçer, x_BP değerini hesaplar ve açıklar. B ile haberleşmek için A, rasgele bir değer $r_A \in Z_q$ seçer ve r_AP değerini hesaplayarak B'ye gönderir. B, rasgele bir değer $r_B \in Z_q$ seçer ve r_BP değerini hesaplayarak B'ye gönderir. A artık r_A, x_A ve r_BP değerlerini, benzer şekilde B r_B, x_B ve r_AP değerlerini bilmektedir. A, $w_A = r_A(x_BP) + x_A(r_BP)$ değerini; B, $w_B = r_B(x_AP) + x_B(r_AP)$ değerini hesaplar. $w_A = w_B$ olduğundan, A ve B gizli anahtar üzerinde anlaşmıştır [49].
- ECDSA: Eliptik eğri sayısal imza algoritması 1998 yılında Amerikan Ulusal Standartlar Enstitüsü (ANSI) X9.62 Standardı [50] ile veri ve mesaj güvenliğinin sağlanması ve amacıyla imza yaratılması ve onaylanması için standartlaştırılmıştır. Algoritmanın işleyişi için A ve B eliptik eğri alan parametreleri, eğri üzerinde açık anahtar olarak kullanılacak bir Q noktası ve bir hash fonksiyonu üzerinde anlaşırlar; A bir gizli anahtar d belirler Anlaşma sağlandıktan sonra A geçici kullanım için bir tamsayı k ve eğri üzerinde $R(x_R, y_R)$ noktası belirler. $r = \leftarrow x_R$ ve gönderilecek ileti hash fonksiyonundan geçirilerek elde edilen değer k ve $r.d$ değerleriyle işleme alınarak s elde edilir. Elde edilen $S = (r, s)$ imzası ve M iletisi B'ye gönderilir. B aldığı iletideki M değerini hash fonksiyonundan geçirdikten sonra s ile çarparak u_1 ve $r \,.\, s$ çarpımını yaparak u_2 değerlerini elde eder. Buradan $R = (x_R, y_R) = u_1G + u_2Q$ elde edilir. Eğer elde edilen $x_R = \leftarrow r$ ise imza doğrulanmıştır yoksa geçersizdir. İşlemler aşağıda özetlenmiştir.

Parametreler: T (m, f(x), a, b, G, n, h) veya T (p, a, b, G, n, h) eliptik eğri parametreleri

Q noktası ve imzalayacak taraf için d değeri

İmza, S(r, s) : Geçici k değeri ve yine geçici R = (x_R, y_R) noktası elde edilir.

$r = \leftarrow x_R$

e = hash (M)

$s = k\text{-}1.(e+r.d) \bmod n$

İmza Onayı: e = hash (M)

$u_1 = e \,.\, s\text{-}1$

$u_2 = r \,.\, s\text{-}1$

$R = (x_R, y_R) = u_1G + u_2Q$

$v = \leftarrow x_R$

$r = v$ ise, imza doğrulanmıştır [51].

Güvenli bir haberleşme ortamı oluşturabilmek için seçilen açık anahtar kriptosisteminde, bir takım kriterlerin göz önünde bulundurulması gerekir. Bu kriterlerin başında fonksiyonellik, güvenlik ve performans gelir. Bölüm içinde bahsedilen RSA, ALP ve ECC kriptosistemleri bugün şifreleme, imza ve anahtar düzenleri için en yaygın kullanılan kriptosistemlerdir. Araştırmacılar açık anahtarlı kriptosistemlerin sağladığı güvenliği ve fonksiyonelliği arttırmak için yeni teknikler geliştirmeye devam etmektedirler. Açık anahtar algoritmalarının performansı matematiksel problemlerin zorluğuna dayandığı için sistem tasarımcıları bu durumu göz önünde bulundururlar.

Açık anahtarlı kriptosistemleri güvenlik açısından incelediğimizde, bu sistemi kırmak için, sistemin dayandığı matematiksel problemin çözülmesi gerekir. Tamsayıları çarpanlarına ayırma problemini çözen en hızlı algoritma olan RSA ve ALP algoritmaları sub-exponansiyel çalışma süresine sahiptir. EEALP çözmek için bilinen algoritmalar ise exponansiyel beklenen çalışma süresine sahiptir. Bu yüzden aynı anahtar uzunluğu kullanarak EEALP çözmek, tamsayıları çarpanlarına ayırma problemini ve ALP çözmekten daha uzun zaman alır. Bu avantaj, ECC algoritmasının aynı güvenlik seviyesini daha küçük anahtar uzunluğuyla ve daha yüksek işlem verimliliğiyle elde edilmesine izin verir. Bir algoritmanın dayandığı matematiksel problem kriptosistemin verimliliğini belirlemede kullanılan yollardan biridir. Tablo 3.4'de ECC ve RSA asimetrik anahtar

şifreleme düzenlerinin eşdeğer güvenlik seviyelerinde kullandıkları anahtar uzunlukları verilmiştir.

Tablo 3.4. Eşit Güvenlik Seviyeleri İçin ECC ve RSA Algoritmalarının Anahtar Uzunlukları

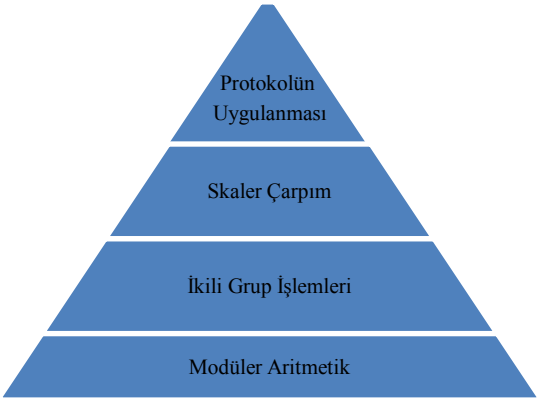
	Security Level (Bits)				
	80 (SKIPJACK)	112 (Triple-DES)	128 (AES-Small)	192 (AES-Medium)	256 (AES-Large)
ECC	160	224	256	384	512
RSA	1024	2048	3072	8192	15360

Anahtar uzunluklarına göre, ECC algoritmasının gerektirdiği bant genişliği tamsayıları çarpanlarına ayırma ve ALP'yi kullanan sistemlerden daha fazla verimlilik sağlar. Bu daha yüksek hız, daha düşük güç tüketimi ve azaltılmış kod boyutu anlamına gelir.

3.6. Eliptik Eğri Kriptosistemleri

Eliptik eğrilerin kullanılmasıyla oluşturulan kriptosistemde en önemli durum, seçilen eğrinin kriptografik özelliklerinin iyi olmasıdır. Pratikte istenen eğri üzerindeki asal olan noktaların cyclic grup ya da alt grup oluşturması ve kriptografik zayıflığa sebep olan bazı matematiksel özelliklerin ekarte edilmesidir. Tüm bu belirtilen özellikler, kolay olmayan ve hesaplama gerektiren işlemler sonucunda elde edilir.

Eliptik eğrileri ECC kriptosistemine uygularken, bu kriptosistemi dört katmanlı bir yapı olarak düşünmek yararlı olacaktır. Şekil 3.16'da görüldüğü gibi en alt katmanda modüler aritmetik yer alır. Bu katman içinde ekleme, çıkarma, çarpma ve ters alma işlemleri gerçekleştirilir. Üçüncü katman ise ikili grup işlemleridir, bu katmanda nokta ekleme ve nokta aynılama işlemleri yapılır. Bir üst katmanda ise bir önceki ikili grup işlemleri katmanının işlem sonuçlarını kullanarak skaler çarpım yapılır. En üst katmanda mevcut protokol uygulanır, örneğin EEDH.



Şekil 3.16. ECC Kriptosisteminin Yapısı

EEK iki farklı sonlu cebirsel yapı içerir, biri GF(P) sonlu alanında tanımlanan eğriler diğeri ise eğri üzerindeki noktaların oluşturduğu cyclic gruplardır.

Şifreleme işleminde seçilen eğrinin bilinen tüm ataklara karşıda dirençli olması sağlanmalıdır.

- Pollard- ρ atağına karşı koymak için $E(F_q)$'nun yeterince büyük bir n asal sayı çarpanı olmalıdır.($n > 2^{160}$)
- Weil ve Tate ikili atakları için n'nin (q^k-1) sayısını $1 \leq k \leq C$ için bölmemesi gerekir.

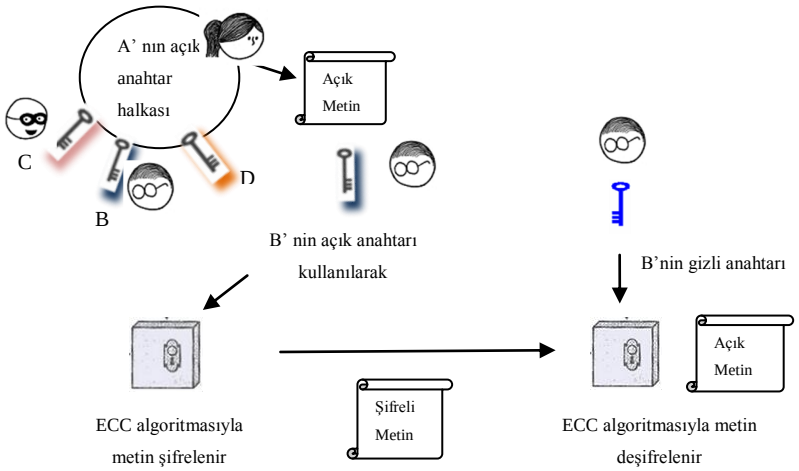
Eliptik eğri kullanan açık anahtarlı şifreleme sistemlerinde sadece açık anahtarların bilinmesiyle şifre çözme işleminin yapılması pratikte mümkün değildir. Bu tarz güvenliğin sağlanması için bu sistemlerde ALP kullanılmaktadır.

Eliptik eğriler kullanılarak yapılacak olan şifreleme işlemlerinde EEALP temel olarak alınmaktadır. Temel alınan P noktasının skaler çarpma yöntemi ile elde edilen katları kullanılarak şifreleme yapılacak materyalin güvenliği sağlanmış olur. Bu noktada ECC metodunda kullanılan parametreler ve adımlar incelenmelidir:

Literatürde, eliptik eğriler yardımıyla şifreleme ve deşifreleme yapan birçok yöntem bulunmaktadır. İncelenen yönteme göre; sistem içerisindeki ilk görev, plaintext mesaj olan m'yi, bir x-y koordini ile belirlenmiş P_m noktası şeklinde göndermek üzere şifrelemektir. Bu P_m noktası bir chipertext gibi şifrelenecek daha sonrasında da deşifre edilecektir. Bir mesajı x ya da sadece y koordinat noktası olarak basitçe şifreleyemeyiz çünkü tüm olası noktalar $E_F(a, b)$ içinde bulunmayabilir. Şifreleme işlemi için de birçok yöntem mevcuttur.

Şekil 3.17'de ECC algoritmasının kullandığı şifreleme yöntemi kabaca gösterilmiştir. Başlıca adımlar aşağıdaki gibidir:

- Her ağdaki her son sistem (A, B, C, D) mesaj alındığında şifreleme ve deşifreleme işlemleri için kullanacağı anahtar parçasını yaratır.
- Her sistem şifreleme anahtarını herkese erişebilecek bir dosya içerisine kaydeder ve bu dosya içinden açık olan anahtarı paylaşır, gizli anahtarı saklı tutulur.
- Eğer A, B'ye bir mesaj yollamak isterse, mesajı B'nin açık anahtarını kullanarak şifreler.
- B mesajı aldığında kendi özel anahtarını kullanarak deşifre işlemini gerçekleştirir. Diğer hiçbir kullanıcı mesajı deşifreleyemez. Çünkü mesaj sadece B'nin özel anahtarıyla deşifrelenebilir.



Şekil 3.17. ECC Kriptosisteminde Şifreleme

Ağdaki her kullanıcı Şekil 3.17'de de görüldüğü gibi birbirinin açık anahtarına erişim hakkına sahiptir. Her katılımcı özel anahtarını lokal olarak yaratır. Bu yüzden özel anahtarların paylaşılmasına gerek yoktur. Herhangi bir sebepten dolayı özel anahtarın değiştirimesi gerekebilir, bu durumda değiştirilmiş olan yeni açık anahtar ilgili yerlere yeniden gönderilir.

Anahtar çifti oluşturma işleminde, l gibi bir tamsayı [1, n −1] aralığında seçilir ve l defa nokta toplama islemi yapılarak $Q = l.P$ gibi eliptik eğri üzerinde, O'dan farklı yeni bir $Q = (x, y) \in E$ (F_q) noktasına ulaşılır. Seçilen l tamsayı degeri gizli anahtar (private key), Q nokta değeriyse, açık anahtar bilgisini tanımlar. Seçilecek l tamsayı değeri [1, n −1] aralığında olacağından büyük bir sayıdır. l defa nokta toplama işlemi yapmanın zaman ve işlemci maliyeti çok yüksektir. İşlem maliyetini düsürmek için kullanılan cisim ve aritmetik işlem tipine bağlı olarak çeşitli algoritmalar önerilmektedir. [39]

ECC kriptosisteminde şifreleme ve deşifreleme işlemleri matematiksel olarak ifade edilmeden önce anahtar değişimine değinmek gerekir. Eliptik eğriler kullanılarak anahtar değişimi işleminde öncelikle, $p \approx 2^{180}$ olacak şekilde bir p asal sayısı ve Eş. 3.4 denklemindeki eliptik eğri parametreleri olan a ve b seçilsin. Bu, eliptik noktalar grubu olan $E_F(a, b)$'yi oluşturur. Sonrasında $E_F(a, b)$ içerisinden, başlangıç noktası $G = (x_1, y_1)$ seçilsin. G'nin seçilmesindeki en önemli kriter; $nG=0$ eşitliğini sağlayan en küçük n değerinin çok büyük bir asal sayı olması gerekliliğidir. $E_F(a, b)$ ve G, kriptosistemin tüm katılımcılarca bilinecek parametreleridir.

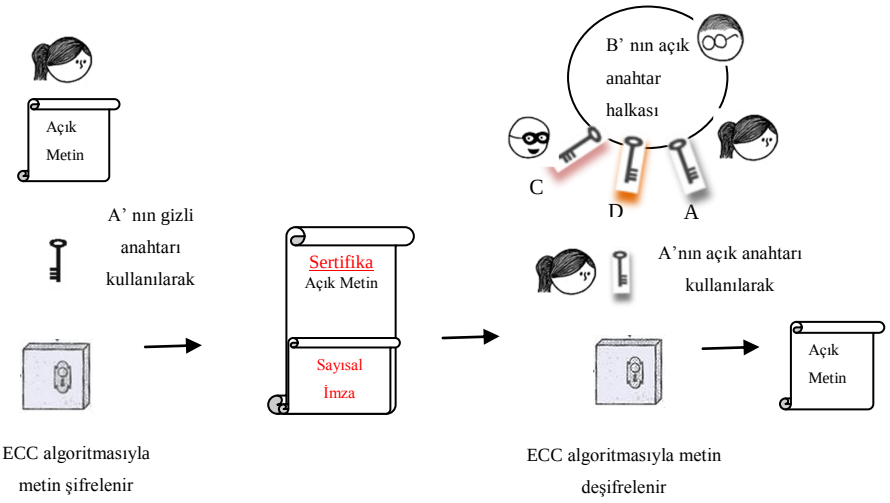
Anahtar değişimi sistemi, yukarıda da belirtildiği gibi parametre olarak bir G noktası ve bir $E_F(a, b)$ eliptik grubuna ihtiyaç duyar. A ve B kullanıcıları arasındaki anahtar değişimi aşağıdaki gibidir:

- A, n'den küçük bir n_A tamsayısı seçer. n_A A'nın özel anahtarıdır. Daha sonra A, $P_A = n_A \cdot G$ hesabıyla $E_F(a, b)$'nin bir noktası olan açık anahtarını oluşturur.
- B'de aynı metotla kendi açık anahtarı olan P_B'yi oluşturur.
- A gizli anahtarı $K = n_A \cdot P_B$ ile B'de gizli anahtarı $K = n_B \cdot P_A$ ile elde eder.

Üçüncü aşamadaki iki hesaplamanın da sonucu aynıdır. Çünkü

$$n_A \cdot P_B = n_A \cdot (n_B \cdot G) = n_B \cdot (n_A \cdot G) = n_B \cdot P_A\text{'dır.} \quad (3.5)$$

Alıcı ve göndericinin, birbirlerinin gizli anahtarlarını bilmeden aynı sonuca ulaşabilecekleri Eş. 3.5'te verilmiştir. Bu eşitlik bölüm 3.5.6'da verilen sayısal imza yapısıdır. Bir kriptosistemde iletilen mesajlara ait bütünlük, inkar edilemezlik ve kimlik doğrulama ilkeleri sayısal imza işlemiyle gerçeklenir. Şekil 3.18'de ECC algoritması kullanılarak oluşturulan sayısal imza ve kimlik doğrulama yapısı gösterilmiştir.



Şekil 3.18. ECC Kriptosisteminde Kimlik Doğrulama

ECC algoritmasıyla herhangi bir mesaj için sayısal imza oluşturulmak istenirse, göndericinin (A) gizli anahtarı kullanılarak mesajın bir kopyası şifrelenir. Şifrelenmiş bu veri, sayısal imza olarak adlandırılır. Oluşturulan sayısal imza, mesaj ve göndericiye ait sertifikayla birlikte sistemden alıcıya iletilir. Sayısal imza, alıcı tarafında ancak ve ancak, göndericiye ait sertifikayla içerisinde alıcıya iletilen açık anahtar (A kullanıcısına ait) kullanılarak deşifre edilebilir böylelikle kimlik doğrulama işlemi gerçekleştirilmiş olur.

EEK'da, diğer kriptosistemlerde olduğu gibi, güvenliğin en zayıf halkasını, anahtarın gizliliği oluşturmaktadır bu nedenle taraflar bu bilgiyi çok dikkatli bir şekilde saklamalıdırlar.

3.6.1. Eliptik Eğri ElGamal Kriptosistemi

Eliptik eğri ElGamal kriptosistemi açık anahtarlı bir kriptosistem olup, şifreleme ve deşifreleme işlemlerinde eliptik eğrileri kullanırlar. Sistemde alıcı ve gönderici tarafların yaptığı temel şifreleme, deşifreleme ve sayısal imza işlemi aşağıdaki gibidir:

ElGamal Temel Şifreleme Deşifreleme:

- Gönderici A,

  E: $y^2 = x^3 + ax + b \bmod p$ eğrisi üzerinde şifrelemek istediği mesajını x noktası olarak belirler.

$1 \leq k \leq p\text{-}2$ rasgele bir k tamsayısı seçer.

Public olan *a* ve β noktalarını kullanarak,

$y_1 = k \cdot a$, $y_2 = x + k \cdot \beta$ değerlerini hesaplar, y_1 ve y_2 çiftlerini Alıcı B'ye gönderir.

- Alıcı B, A yukarıdaki adımları gerçekleştirmeden,

  p çok büyük bir asal sayı olmak üzere GF(p) üzerinde bir E eliptik eğrisini,

  E: $y^2 = x^3 + ax + b \bmod p$ eğrisi üzerinden *a* başlangıç noktasını,

  Gizli bir tamsayı olan a'yı seçer. $1 \leq a \leq p\text{-}2$

  $\beta = a \cdot a = \sum_1^a a$ noktasını hesaplar.

  a ve β noktaları public hale getirir. Fakat a değerini gizli tutar.

ElGamal kriptosisteminde şifreleme ve deşifreleme işlemini bir örnekle açıklayacak olursak:

Örnek

p = 8831,

a = (4, 11),

Eliptik eğri denklemi E: $y^2 = x^3 + 3x + 45 \bmod 8831$,

Şifrelenecek mesaj: x = (5, 1743) olsun,

B kullanıcısı gizli bir a=3 tamsayısı ile β değerini hesaplar ve public hale getirir.

$\beta = a \cdot a = 3 \cdot (4, 11) = (413, 1808)$

a ve β noktaları A kullanıcısı tarafından alınır, rasgele k=8 tamsayısı seçer şifrelenmiş mesajı y_1 ve y_2 çiftleri olarak B kullanıcısına gönderir.

$y_1 = k \cdot a = (5415, 6631)$ ve $y_2 = x + k \cdot \beta = (5, 1743) + 8 \cdot (413, 1808) = (6626, 3576)$

Deşifreleme işleminde B kullanıcısı;

$a \cdot y_1 = 3 \cdot (5415, 6631) = (673, 146)$

$x = y_2 - a \cdot y_1 = (6626, 3576) - (673, 146) = (6626, 3576) - (673, -146) = (5, 1743)$ mesajı elde edilir.

ElGamal Sayısal İmza İşlemi:

ElGamal kriptosisteminde sayısal imza diğer kriptosistemlerde olduğu gibi mesajın doğru kişiden gelip gelmediğini kontrol etmek için kullanılır. Sadece şifreli metin yerine imzalanmış şifreli metin gönderilerek, metnin istenen kişiden gelip gelmediğini kontrol etmeye yarar. A kullanıcısının açık anahtarı ($p, \alpha, \alpha^a = y$), gizli anahtarı ise a olsun,

İmzalama işleminde kullanıcı A x mesajını,

- Rasgele bir t tamsayısı seçer $1 \leq t \leq p-2$ ve $\gcd(t, p-1) = 1$ olmalıdır. Yani seçilen t ile $p-1$ sayısı aralarında asal olmalıdır.
- $r = \alpha^t$ ve $s = t^{-1} \cdot (x - r \cdot a) \bmod (p-1)$
- (x, r, s) A'nın imzalı mesajıdır.

İmza doğrulama işleminde B kullanıcısı, A'dan gelen (x, r, s) şeklinde ifade edilen mesajı,

- Öncelikle $1 \leq t \leq p-1$ olduğunu kontrol eder. Eğer değilse imzayı reddeder.
- $v = \alpha^x$ ve $w = y^r \cdot r^s$ değerleri hesaplanır. y A'nın açık anahtarıdır.
- Eğer $v = w$ eşitliği sağlanıyorsa imza kabul edilir, aksi takdirde reddedilir.

Örnek

Gönderici A,

$p = 2939$, $\alpha = 2$, gizli anahtarı $a = 1783$ seçsin.

$\alpha^a \bmod p = 2^{1783} \bmod 2939 = 2002$ olduğundan açık anahtarı (2939, 2, 2002) olur.

İmza oluşturma işlemi için mesaj $x = 1667$, $t = 1511$ seçsin.

$r = \alpha^t \bmod p = 2^{1511} \bmod 2939 = 794$,

$t^{-1} \bmod (p-1) = 1511^{-1} \bmod (2938) = 35$,

$s = t^{-1} \cdot (x - r \cdot a) \bmod (p-1) = 35 \cdot (1667 - 794 \cdot 1783) \bmod (2938) = 2323$,

İmzalı mesajı (1667, 794, 2323) olarak B kullanıcısına gönderir.

B aldığı mesajı doğrulamak için önce,

$v = \alpha^x \bmod p = 2^{1667} \bmod 2939 = 1227,$

$w = y^r \cdot r^s \bmod p = 2002^{794} \cdot 794^{2323} \bmod 2939 = 1227$

Sonuç olarak $v = w$ olduğu için imza doğrulanmış olur.

3.6.2. Menezes Vanstone Eliptik Eğri Kriptosistemi

Menezes Vanstone EEK [54] ElGamal kriptosistemi gibi temelde eliptik eğrileri kullanır. Bu iki kriptosistem arasındaki temel farklılık; Menezes Vanstone kriptosisteminde, gönderici A şifrelenecek metni E eliptik eğrisi üzerine gömmek yerine maskeler. Bu da ElGamal kriptosisteminde şifrelenecek mesajın mutlaka eğri üzerindeki bir nokta olarak ifade edilmesi zorunluluğunu gösterir.

E ayrık logaritma probleminin imkansız olduğu bir H cyclic alt grubunu içermek üzere, Z_p'de ($p > 3$ olan bir asal sayı ya da ($n > 1$ için) $GF(p^n)$'de tanımlanmış bir eğri olsun [54].

$P = Z_p^* \times Z_p^*$, $C = E \times Z_p^* \times Z_p^*$ olsun. Bu durumda $\alpha \in E$ için,

Anahtar seti $K = \{(E, \alpha, a, \beta) : \beta = a \cdot \alpha\}$ olarak tanımlanır.

α ve β publictir, a ise gizli tutulur.

k rasgele seçilmiş ve $k \in Z_{|H|}$ ve $x = (x1, x2) \in Z_p^* \times Z_p^*$ kurallarını sağlayan bir tamsayıdır. Menezes Vanstone kriptosisteminde temel şifreleme ve deşifreleme adımları aşağıda verilmiştir.

Menezes Vanstone Temel Şifreleme ve Deşifreleme:

- Gönderici A,
  E: $y^2 = x^3 + ax + b \bmod p$ eğrisi üzerinde α başlangıç noktasını belirler.
  Şifrelemek istediği $x = (x_1, x_2)$ mesajını seçer. Bu mesajı belirten x_1 ve x_2 noktaları E eliptik eğrisi üzerinde yer almaz.
  Rasgele bir k sayısı seçer.
  $y_0 = k \cdot \alpha,$
  $(c_1, c_2) = k \cdot \beta,$
  $y_1 = c_1 \cdot x_1 \bmod p,$
  $y_2 = c_2 \cdot x_2 \bmod p,$

Eşitliklerini hesaplayıp (y_0, y_1, y_2) olarak mesajı B kullanıcısına gönderir.

- Alıcı B,

  a gizli anahtarını seçip,

  $(c_1, c_2) = a \cdot y_0$,

  $x = (y_1 \cdot c_1^{-1} \bmod p, y_2 \cdot c_2^{-1} \bmod p)$ işlemlerini yaparak açık metni elde etmiş olur.

Örnek

$p = 23$,

$\alpha = (4, 7)$,

Eliptik eğri denklemi E: $y^2 = x^3 + x + 4 \bmod 23$,

Şifrelenecek mesaj: $x = (9, 1)$ olsun,

B kullanıcısı gizli bir a=3 tamsayısı ile β değerini hesaplar ve public hale getirir.

$\beta = a \cdot \alpha = 3 \cdot (4,7) = (13, 11)$

α ve β noktaları A kullanıcısı tarafından alınır, rasgele k = 5 tamsayısı seçer şifrelenmiş mesajı y_0, y_1 ve y_2 noktaları olarak B kullanıcısına gönderir.

$y_0 = k \cdot \alpha = 5 \cdot (4,7) = (8, 8)$,

$(c_1, c_2) = k \cdot \beta = 5 \cdot (13, 11) = (22, 18)$,

$y_1 = c_1 \cdot x_1 \bmod p = 22 \cdot 9 \bmod 23 = 14$

$y_2 = c_2 \cdot x_2 \bmod p = 18 \cdot 1 \bmod 23 = 18$

Eşitliklerini hesaplayıp (y_0, y_1, y_2) = ((8, 8), 14, 18) olarak mesajı B kullanıcısına gönderir.

Deşifreleme işleminde B kullanıcısı,

$(c_1, c_2) = a \cdot y_0 = 3 \cdot (8, 8) = (22, 18)$,

$x = (y_1 \cdot c_1^{-1} \bmod p, y_2 \cdot c_2^{-1} \bmod p)$,

$= (14 \cdot 22^{-1} \bmod 23, 18 \cdot 18^{-1} \bmod 23)$,

= (9,1) açık metni elde etmiş olur.

3.6.3. Koyama – Maurer – Okamoto - Vanstone (KMOV) Kriptosistemi

KMOV [55,56] kriptosisteminde B kullanıcı öncelikle p ve q olmak üzere iki büyük asal sayı seçer. $n = p \cdot q$ eşitliği hesaplanarak n sayısı bulunur. $0 < b < p$ ve $b < q$ olmak üzere, $N = lcm\ (p+1, q+1)$ hesaplanır. B kullanıcısının açık anahtarı e N sayısıyla aralarında asal yani $gcd\ (e, N) = 1$ olmalıdır. B'nin gizlianahtarı d, $d = e^{-1} \bmod N$ eşitliğinin sonucudur. KMOV kriptosisteminin temel şifreleme ve deşifreleme adımları aşağıdaki gibidir:

KMOV Temel Şifreleme ve Deşifreleme:

- A kullanıcısı,
  M mesajını $E_n(0, b)$ eliptik eğrisi üzerindeki P_M noktasına dönüştürür. $\Theta = e \cdot P_M$ değerini hesaplayıp Θ noktasını B kullanıcısına gönderir.
- Alıcı B,
  $d \cdot \Theta = P_M$ eşitliğiniden P_M noktasını hesaplayarak mesaja ulaşır.

3.6.4. Ertaul Kriptosistemi

Ertaul kriptosisteminde [56], E eliptik eğrisi üzerinden P başlangıç noktası seçilir. x özel anahtar, $y = x \cdot P$ olup y açık anahtardır. Bu kriptosistemde $H((x_i, y_i)) = Hash\ (x_i \otimes y_i)$ eşitliği gibi bir hash fonksiyonu kullanılır. Ertaul kriptosisteminin temel şifreleme ve deşifreleme adımları aşağıdaki gibidir.

Ertaul Temel Şifreleme ve Deşifreleme:

- Gönderici A,
  Şifrelenecek mesaj M'yi seçer,
  E eliptik eğrisi üzerinden başlangıç noktası seçer,
  r rasgele seçilmiş bir tamsayısı,
  $U = r \cdot P$ ve $V = H\ (r \cdot y) \otimes M$ değerlerlini hesaplayıp B kullanıcısına $C = (U, V)$ şifreli metnini gönderir.
- Alıcı B,
  x özel anahtarını seçip,
  $x \cdot U = x \cdot r \cdot P = r \cdot x \cdot P$ değerini hesaplar,
  Son olarak açık metni elde etmek için,

$V \otimes H(r \cdot x \cdot P) = H(r \cdot y) \otimes M \otimes H(r \cdot x \cdot P) = M$ işlemini yapar.

3.6.5. Massey Omura Kriptosistemi

Masse Omura kriptosistemi'nde [38,56] alıcı ve gönderici arasında dört kez iletim yapılmalıdır. Bu nedenle bu kriptosistem hız açısından etkili bir çözüm değildir. N $E_p(a, b)$ üzerindedir. A kullanıcısının özel anahtarı n_A, B kullanıcısının özel anahtarı n_B olmak üzere, $\gcd(n_A, N) = 1$ ve $\gcd(n_B, N) = 1$ olmalıdır. $N \cdot R = \alpha$ ve her R noktası Lagrange Teoremine (Eş. 3.6) göre eğri üzerinde bulunmalıdır.

$$n_B^{-1} \cdot P_{M3} = n_B^{-1} \cdot n_B \cdot n_A^{-1} \cdot n_A \cdot P_M = n_B^{-1} \cdot n_B \cdot (P_M + qN\, P_M) = n_B^{-1} \cdot n_B \cdot P_M \qquad (3.6)$$

Massey Omura kriptosisteminde temel şifreleme ve deşifreleme işlemleri aşağıda verilmiştir.

Massey Omura Temel Şifreleme ve Deşifreleme:

- Gönderici A,
  Açık metin M yi E eliptik eğrisi üzerindeki noktalara dönüştürüp P_M noktasını oluşturur. Alıcı B'ye $P_{M1} = n_A \cdot P_M$ denkleminden elde ettiği P_{M1} noktasını gönderir.
- Alıcı B,
  A kullancısına, $P_{M2} = n_A \cdot P_{M1}$ denkleminden elde ettiği P_{M2} noktasını gönderir.
- Gönderici A,
  B kullanıcısına $P_{M3} = (n_A^{-1} \bmod N) \cdot P_{M2}$ eşitliğinden elde ettiği $\cdot P_{M3}$ noktasını gönderir.
- Alıcı B,
  $(n_B^{-1} \bmod N) \cdot P_{M3} = P_M$ işlemiyle P_M açık metnine ulaşır.

BÖLÜM 4

UYGULAMA

Bu bölümde, üçüncü bölümde verilen teorik bilgilerin uygulaması yer almaktadır.

Tez kapsamında, modellemesi yapılan kriptosistemin temelinde Menezes Vanstone kriptosistemi kullanılmıştır. Geliştirilen sistemde, gönderici tarafı isteğine bağlı olarak hem nokta hem mesaj şifreleyebilir. Kullanıcı eğer mesaj şifrelemek isterse, göndermek istediği mesajın öncelikle boyutu hesaplanıp, mesaj bu boyut sayısı kadar bloklara ayrılır, her blokta sadece bir karakter yer alır. Ayrılan her karakterin hexadecimal (16 tabanlı sayı sistemi) karşılıkları hesaplanır. Şekil 4.1'de karakterlerin hexadecimal karşılıkları verilmiştir.

Hex	Char	Hex	Char	Hex	Char	Hex	Char
00	NUL	20	SP	40	@	60	`
01	SOH	21	!	41	A	61	a
02	STX	22	"	42	B	62	b
03	ETX	23	#	43	C	63	c
04	EOT	24	$	44	D	64	d
05	ENQ	25	%	45	E	65	e
06	ACK	26	&	46	F	66	f
07	BEL	27	'	47	G	67	g
08	BS	28	(	48	H	68	h
09	HT	29	)	49	I	69	i
0A	LF	2A	*	4A	J	6A	j
0B	VT	2B	+	4B	K	6B	k
0C	FF	2C	,	4C	L	6C	l
0D	CR	2D	-	4D	M	6D	m
0E	SO	2E	.	4E	N	6E	n
0F	SI	2F	/	4F	O	6F	o
10	DLE	30	0	50	P	70	p
11	DC1	31	1	51	Q	71	q
12	DC2	32	2	52	R	72	r
13	DC3	33	3	53	S	73	s
14	DC4	34	4	54	T	74	t
15	NAK	35	5	55	U	75	u
16	SYN	36	6	56	V	76	v
17	ETB	37	7	57	W	77	w
18	CAN	38	8	58	X	78	x
19	EM	39	9	59	Y	79	y
1A	SUB	3A	:	5A	Z	7A	z
1B	ESC	3B	;	5B	[	7B	{
1C	FS	3C	<	5C	\	7C	|
1D	GS	3D	=	5D	]	7D	}
1E	RS	3E	>	5E	^	7E	~
1F	US	3F	?	5F	_	7F	DEL

Şekil 4.1. Karakterlerin Hexadecimal Tabandaki Karşılıkları

Karakterlerin hexadecimal karşılıklarının alınmasının sebebi, şekilden de görüleceği gibi her karakterin hexadecimal karşılığının 2 basamaklı olmasıdır bu da şifreleme işlemi yapılırken, karakterin bir nokta olarak ifade edilmesinde kolaylık sağlar. Hexadecimal karşılığın onlar basamağı (x_1) birler basamağı (x_2) değeri olarak gönderilir. Eğer birler basamağındaki değer harfle (A, B, C, D, E, F) ifade ediliyorsa bu harf onluk sayı sistemine dönüştürülür (A→10, B→11, C→12, D→13, E→14, F→15). Blok sayısı kadar nokta her defasında şifreleme algoritmasına gönderilir ve karşı tarafa bloklar halinde iletilir. Böylelikle, güvensiz iletişim ortamında veriyi elde etmeye çalışan kişi mesajı karakter olarak göremez, ayrıca (x_2) olarak ifade edilen noktanın decimal karşılığına ulaşacağı için noktayı anlamlandıramaz. Aşağıda geliştirilen kriptosistemin temel anahtar yapısı, şifreleme ve deşifreleme adımları verilmiştir.

Anahtar yapısı Menezes Vanstone kriptosistemindeki gibidir.

α eliptik eğri üzerinde belirlenmiş bir noktadır ($\alpha \in E$).

$P = Z_p^* \times Z_p^*$, $C = E \times Z_p^* \times Z_p^*$ olsun.

Anahtar seti $K = \{(E, \alpha, a, \beta) : \beta = a \cdot \alpha\}$ olarak tanımlanır.

α ve β publictir, a ise gizli tutulur.

k rasgele seçilmiş ve $k \in Z_{|H|}$ ve $x = (x1, x2) \in Z_p^* \times Z_p^*$ kurallarını sağlayan bir tamsayıdır.

Temel Şifreleme ve Deşifreleme:

- Gönderici A,
  E: $y^2 = x^3 + ax + b \bmod p$ eğrisi üzerinde α başlangıç noktasını belirler.
  Şifrelemek istediği x mesajını seçer.
  x mesajını n adet bloğa böler. Her blokta tek karakter olacak şekilde mesajı ayırır.
  Bloktaki her karakteri hexadecimal tabana dönüştürür ve (mn) şeklinde ifade eder.
  mn sayısının birler basamağı içinde harf varsa (A→10, B→11, C→12, D→13, E→14, F→15) dönüşümü yapar.
  $m \rightarrow x_1$, $n \rightarrow x_2$ olmak üzere;
  Her karakter (x_{1i}, x_{2i}) olacak şekilde nokta olarak ifade edilir ve $i = \{1,2,., n\}$'dir.

Rasgele bir k sayısı seçer.

$y_0 = k \cdot \alpha$,

$(c_1, c_2) = k \cdot \beta$,

$y_{1i} = c_1 \cdot x_{1i} \bmod p$,

$y_{2i} = c_2 \cdot x_{2i} \bmod p$,

Eşitliklerini hesaplayıp (y_0, y_{1i}, y_{2i}) olarak mesajın her karakterini n kez B kullanıcısına gönderir.

- Alıcı B,

  a gizli anahtarını seçip,

  $(c_1, c_2) = a \cdot y_0$,

  $x_i = (y_{1i} \cdot c_1^{-1} \bmod p, y_{2i} \cdot c_2^{-1} \bmod p)$ işlemlerini yaparak açık metni nokta şeklinde elde etmiş olur.

  Bu noktalar üzerinde $(x_{1i} \cdot 16 + x_{2i})$ işlemi yapıp elde ettiği değeri karaktere çevirerek mesajı elde etmiş olur.

Şifreleme ve deşifreleme işlemlerini bir örnekle açıklayacak olursak:

Örnek

$p = 101$,

$\alpha = (9, 23)$,

Eliptik eğri denklemi E: $y^2 = x^3 + 7x + 40 \bmod 101$,

Şifrelenecek mesaj: x = " SIFRE: " kelimesi olsun,

B kullanıcısı gizli anahtar olan a = 3 değerini seçip, β değerini hesaplar ve public hale getirir.

$\beta = a \cdot \alpha = 3 \cdot (9, 23) = (55, 94)$;

α ve β noktaları A kullanıcısı tarafından alınır,

Rasgele k = 6 tamsayısı seçer,

"SIFRE:" mesajı boyutu kadar, n = 6 adet bloğa ayrılır. Her bloktaki karakter;

Hexadecimal tabana dönüştürülür:

S→53, I→49, F→46, R→52, E→45, : →3A,

Bu karakterler (x_{1i}, x_{2i}) şeklindeki noktalara dönüştürülür:

S→(5, 3), I→(4, 9), F→(4, 6), R→(5, 2), E→(4, 5), : →(3, 10),

Her bir blok için:

$y_0 = k \cdot \alpha = 6 \cdot (9, 23) = (14, 16)$ ve $(c_1, c_2) = k \cdot \beta = 6 \cdot (55, 94) = (52, 97)$ değeri sabit olup,

S karakteri için;

$y_{11} = c_1 \cdot x_{11} \bmod p = 52 \cdot 5 \bmod 101 = 58$,

$y_{21} = c_2 \cdot x_{21} \bmod p = 91 \cdot 3 \bmod 101 = 89$,

$(y_0, y_{11}, y_{21}) = ((14, 16), 58, 89)$ şifresini B kullanıcısına gönderir.

I karakteri için;

$y_{12} = c_1 \cdot x_{12} \bmod p = 52 \cdot 4 \bmod 101 = 6$,

$y_{22} = c_2 \cdot x_{22} \bmod p = 91 \cdot 9 \bmod 101 = 65$,

$(y_0, y_{12}, y_{22}) = ((14, 16), 6, 65)$ şifresini B kullanıcısına gönderir.

F karakteri için;

$y_{13} = c_1 \cdot x_{13} \bmod p = 52 \cdot 4 \bmod 101 = 6$,

$y_{23} = c_2 \cdot x_{23} \bmod p = 91 \cdot 6 \bmod 101 = 77$,

$(y_0, y_{12}, y_{22}) = ((14, 16), 6, 77)$ şifresini B kullanıcısına gönderir.

R karakteri için;

$y_{14} = c_1 \cdot x_{14} \bmod p = 52 \cdot 5 \bmod 101 = 58$,

$y_{24} = c_2 \cdot x_{24} \bmod p = 91 \cdot 2 \bmod 101 = 93$,

(y_0, y_{14}, y_{24}) = ((14, 16), 58, 93) şifresini B kullanıcısına gönderir.

E karakteri için;

$y_{15} = c_1 \cdot x_{15} \bmod p = 52 \cdot 4 \bmod 101 = 6$,

$y_{25} = c_2 \cdot x_{25} \bmod p = 91 \cdot 5 \bmod 101 = 81$,

(y_0, y_{15}, y_{25}) = ((14, 16), 6, 81) şifresini B kullanıcısına gönderir.

: karakteri için;

$y_{16} = c_1 \cdot x_{16} \bmod p = 52 \cdot 3 \bmod 101 = 55$,

$y_{26} = c_2 \cdot x_{26} \bmod p = 91 \cdot 10 \bmod 101 = 61$,

(y_0, y_{16}, y_{26}) = ((14, 16), 55, 61) şifresini B kullanıcısına gönderir.

Deşifreleme işleminde B kullanıcısı,

$(c_1, c_2) = a \cdot y_0 = 3 \cdot (14, 16) = (52, 97)$ c_1, c_2 noktaları her blok için sabit olup;

Her blok için, $x_{1i} = (y_{1i} \cdot c_{1i}^{-1} \bmod p, y_{2i} \cdot c_{2i}^{-1} \bmod p)$ işlemi yapılarak blokta şifrelenen mesajın hexadecimal değerleri elde edilir ve bu değerlerin karakter karşılıkları bulunup mesaja ulaşılmış olur.

S karakteri için; $x_{11} = (58 \cdot 52^{-1} \bmod 101, 89 \cdot 97^{-1} \bmod 101) = (5, 3) = S$;

I karakteri için; $x_{12} = (6 \cdot 52^{-1} \bmod 101, 65 \cdot 97^{-1} \bmod 101) = (4, 9) = I$;

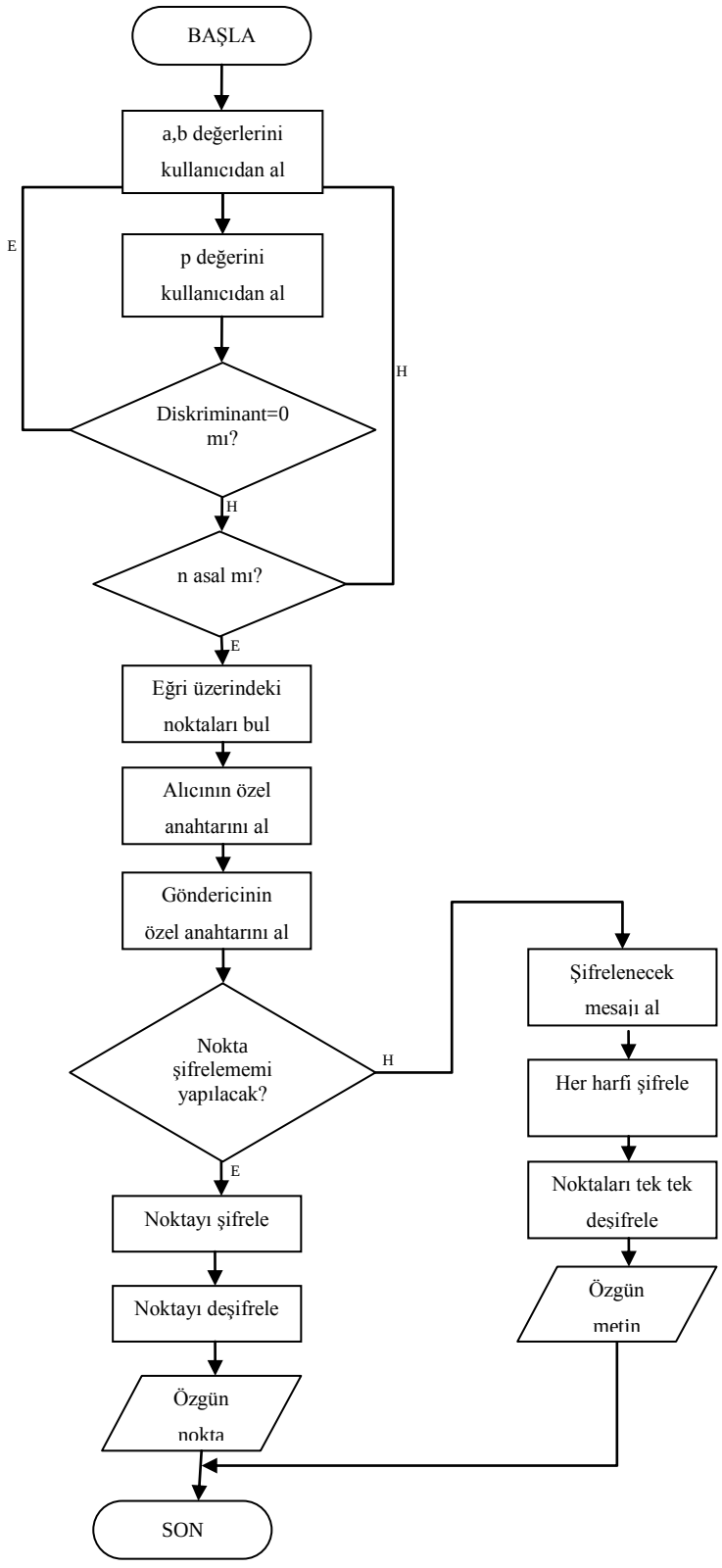
F karakteri için; $x_{13} = (6 \cdot 52^{-1} \bmod 101, 77 \cdot 97^{-1} \bmod 101) = (4, 6) = F$;

R karakteri için; $x_{14} = (58 \cdot 52^{-1} \bmod 101, 93 \cdot 97^{-1} \bmod 101) = (5, 2) = R$;

E karakteri için; $x_{15} = (6 \cdot 52^{-1} \bmod 101, 81 \cdot 97^{-1} \bmod 101) = (4, 5) = E$;

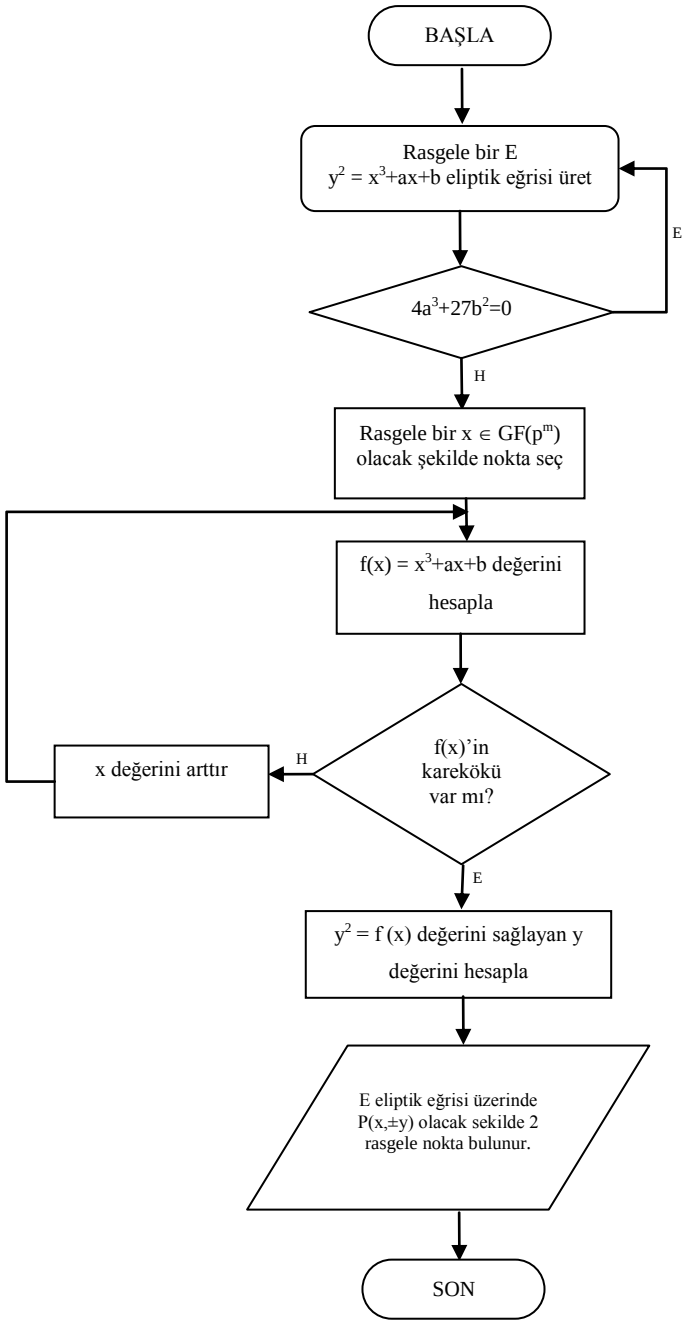
: karakteri için; $x_{16} = (55 \cdot 52^{-1} \bmod 101, 61 \cdot 97^{-1} \bmod 101) = (3, 10) = :$

Şekil 4.2'de modellenen kriptosistemin akış diyagramı verilmiştir. Bu akış diyagramına göre, öncelikle eliptik eğri kontrolü yapılır, eğer belirtilen şartlar sağlanmazsa farklı değerler girmesi için kullanıcı yönlendirilir.



Şekil 4.2. Modellenen Kriptosistemin Akış Diyagramı

Uygun eğri seçildikten sonra, eğri üzerindeki noktalar Şekil 4.3'de [30] verilen akış diyagramındaki adımlar uygulanarak bulunur.

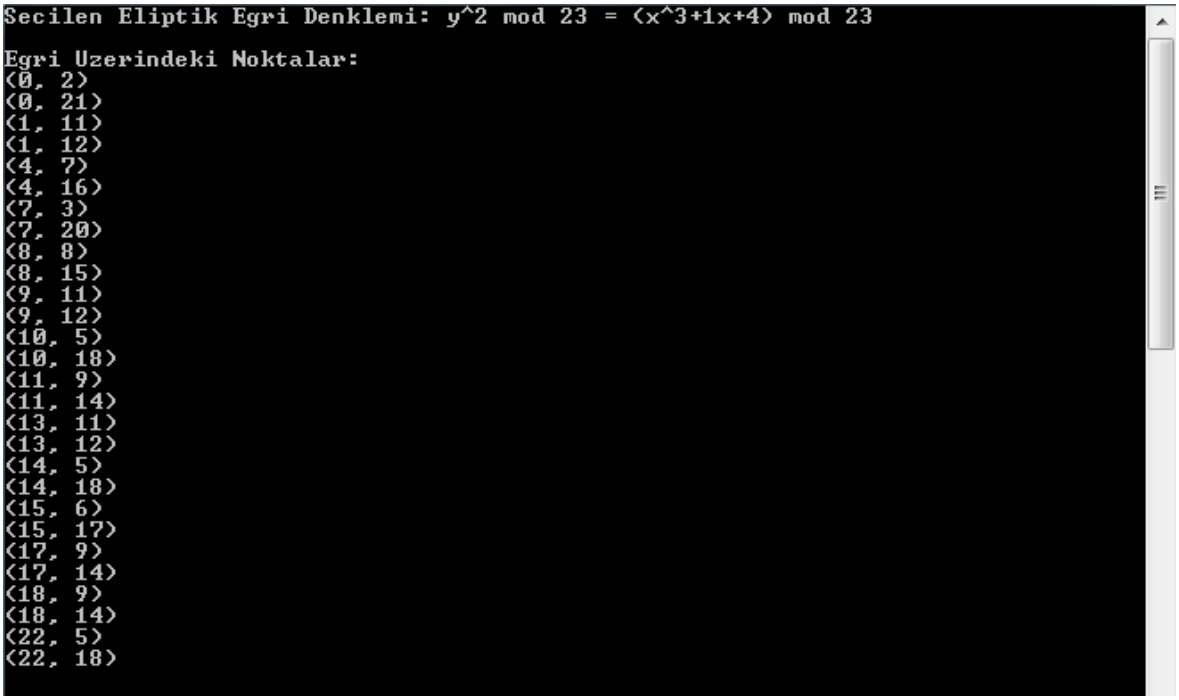


Şekil 4.3. Eliptik Eğri Üzerindeki Noktaların Bulunması

Kriptosistemi kullanacak olan gönderici ve alıcının özel anahtarları alındıktan sonra, sadece nokta şifreleme mi, yoksa mesaj şifreleme mi yapılacağı bilgisi göndericiden (A) alınır. Eğer nokta şifreleme yapılacaksa; kullanıcıdan koordinat sistemi üzerindeki x ve y

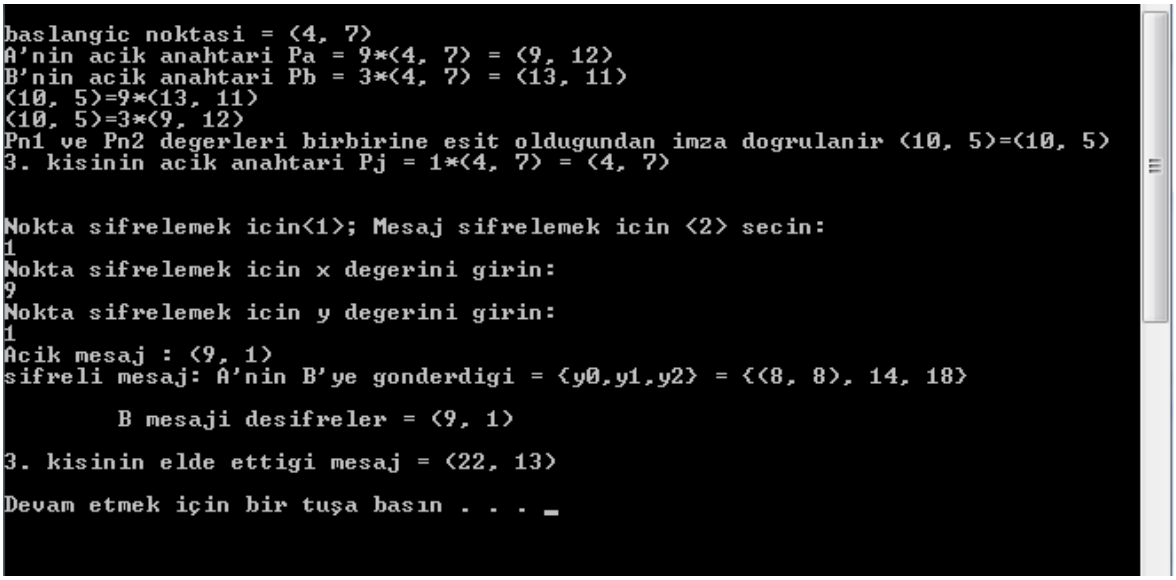
eksenlerinin değerleri alınır. Bu değerler bölüm içinde verilen şifreleme adımları uygulanarak alıcıya (B) iletilir, B kullanıcısıda deşifreleme adımlarındaki işlemleri uygulayarak gönderilen noktayı deşifreler. Mesaj şifreleme seçeneği seçildiğinde, A kullanıcısı, şifreleyeceği mesajı ekrana girdikten sonra, mesaj, boyutu kadar bloklara ayrılır ve her bloktaki karakter nokta haline dönüştürülür verilen şifreleme adımları uygulanarak B'ye iletilir. B kullanıcısıda her bloktaki noktaları deşifreleyerek mesaja ulaşır.

Nokta şifreleme ve deşifreleme işlemi için, bölüm 3.6.2 içinde sayısal örneği verilen şifreleme ve deşifreleme işlemleri doğrulanmıştır. Şekil 4.4'de E: $y^2 = x^3 + x + 4 \bmod 23$ eliptik eğrisi üzerinde bulunan noktalar sunulmuştur.



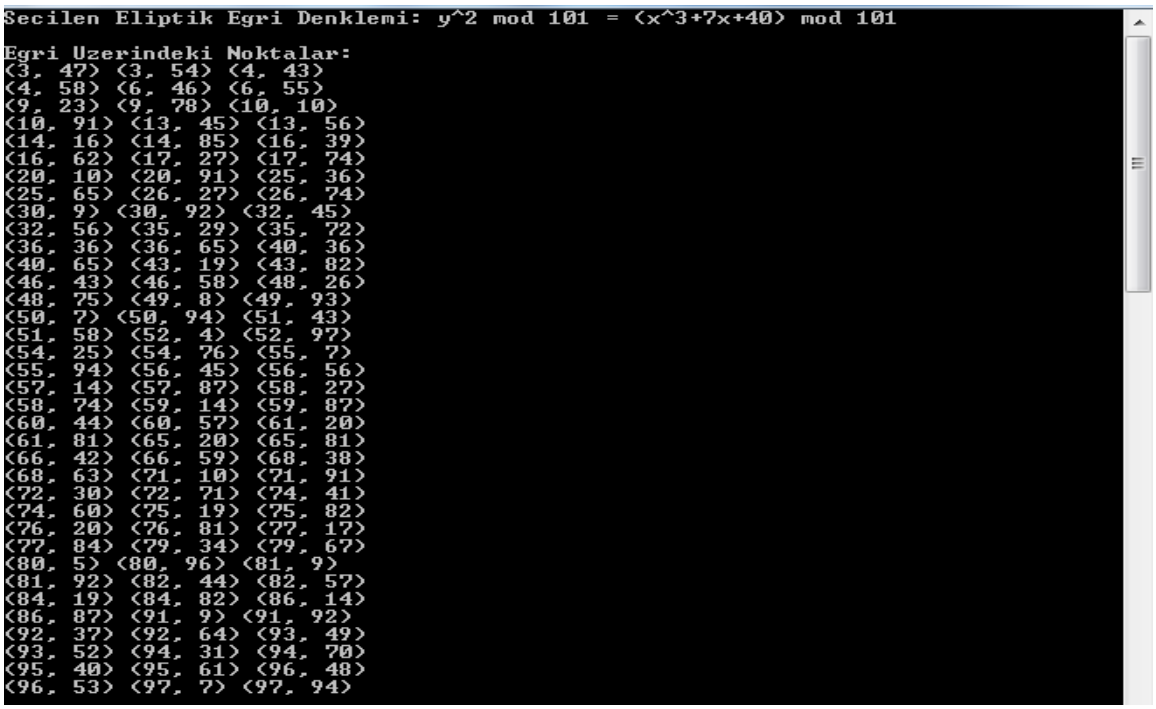
Şekil 4.4. E: $y^2 = x^3 + x + 4 \bmod 23$ Eliptik Eğrisi Üzerindeki Noktalar

Şekil 4.5'de ise bu eliptik eğri kullanılarak nokta şifreleme ve deşifreleme işlemi gösterilmiştir.



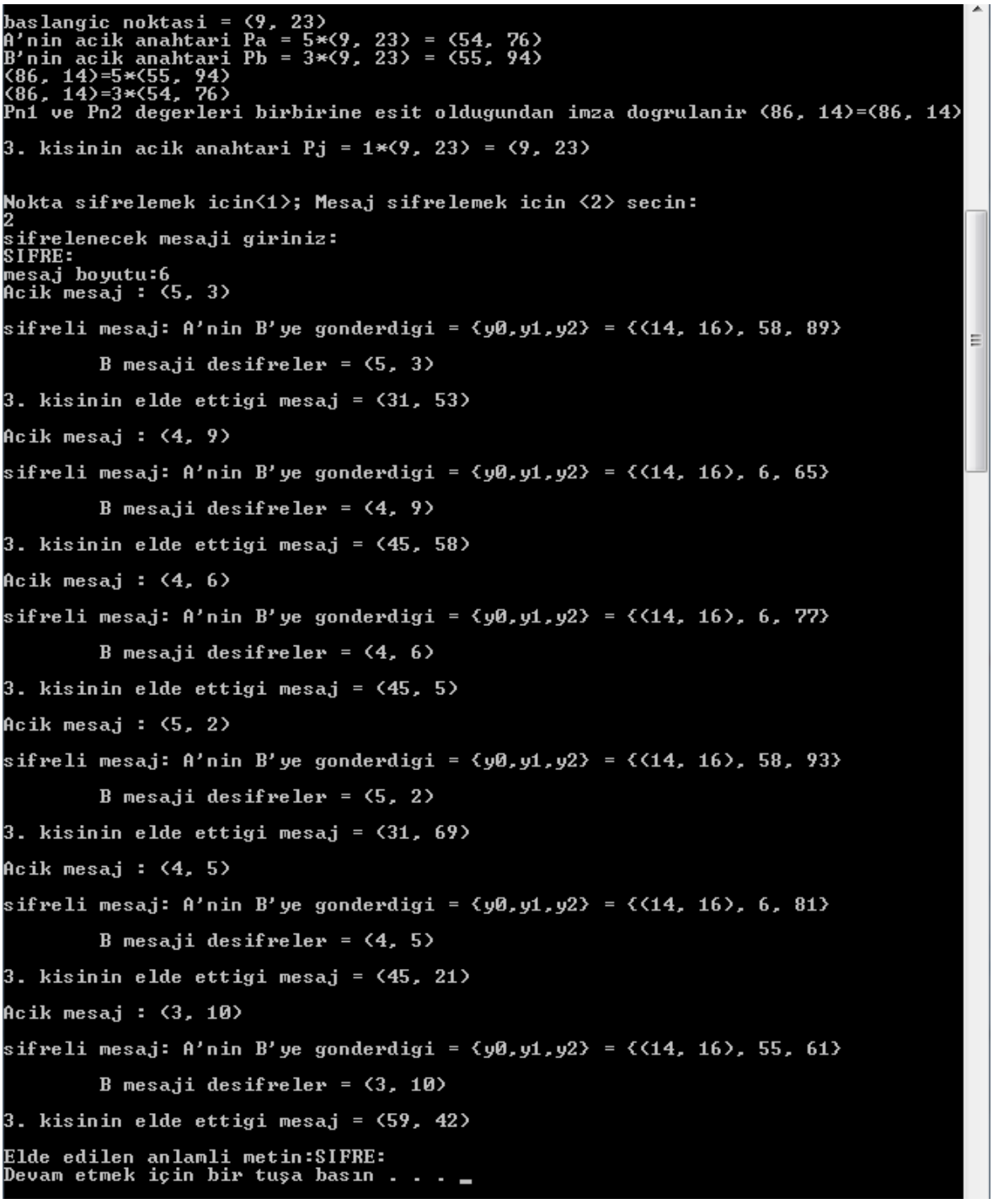
Şekil 4.5. E: $y^2 = x^3 + x + 4 \mod 23$ Eliptik Eğrisi Üzerindeki (9, 1) Noktasının Şifrelenmesi ve Deşifrelenmesi

Mesaj şifreleme ve deşifreleme işlemi için, bölüm içinde verilen örnekteki şifreleme ve deşifreleme işlemleri doğrulanmıştır. Şekil 4.6'da E: $y^2 = x^3 + 7x + 40 \mod 101$ eliptik eğrisi üzerindeki noktalar verilmiştir.



Şekil 4.6. E: $y^2 = x^3 + 7x + 40 \mod 101$ Eliptik Eğrisi Üzerindeki Noktalar

Şekil 4.7'de mesaj şifreleme ve deşifreleme işlemlerinin adımları verilmiştir.



Şekil 4.7. E: $y^2 = x^3 + 7x + 40 \bmod 101$ Eliptik Eğrisi Üzerinde "SIFRE:" Mesajının Şifrelenmesi ve Deşifrelenmesi

BÖLÜM 5

SONUÇ

Bilim ve teknolojinin paralel hızla ilerlemesi ve gelişmesi sonucunda, günümüzde bilgilerin istenmeyen kişi veya kişilerden korunması önemli bir konu halini almıştır. Bu durum bilgilerin korunması ve güvenli iletişim gibi kavramlar üzerinde yapılan çalışmaların daha da artmasına sebep olmuştur. Çalışmalar göstermiştir ki; güvenli bir iletişim ortamı oluşturmak için güçlü kriptosistemlere ihtiyaç vardır. Bu nedenle, simetrik ve asimetrik kriptosistemlerin önemi hızla artmaktadır.

Asimetrik kriptosistemler, simetrik kriptosistemlerden farklı olarak şifreleme ve deşifreleme işlemleri için iki ayrı anahtar kullanırlar. Bu da asimetrik sistemleri daha güvenilir kılar. Asimetrik kriptosistemlerin, en güvenilir ve son zamanlardaki en popüler sistemi Eliptik Eğri Kriptosistemidir. Eliptik eğri kriptosistemi eliptik eğrileri temel alıp, bu eğriler üzerindeki noktalarla işlem yapar. Bu kriptosistem, diğer bir asimetrik kriptosistem olan RSA ile karşılaştırıldığında eşit güvenlik seviyesinde, daha küçük anahtar uzunluğu gerektirir. Daha küçük anahtar uzunluğu kullanımı, bilgisayar kaynaklarının sınırlı olduğu durumlarda üst düzey performans sağlar. Bu nedenle günümüzde önemi artmakta olan sayısal imza gibi akıllı kart kullanılan uygulamalarda eliptik eğri sistemi tercih edilmektedir.

Temelde eliptik eğri kullanan birçok kriptosistem geliştirilmiş ve uygulamaya geçirilmiştir. Bu kriptosistemlerden uygulanabilirlik açısından uygun ve hızlı olan Menezes Vasntone kriptosistemi tez kapsamında incelenmiş olup, temelde bu kriptosistemi kullanan ancak şifreleme adımında iyileştirilmeler yapılmış kriptosistemin uygulaması gerçeklenmiştir. Menezes Vanstone kriptosisteminde mesajın karakterleri rasgele noktalarla ifade edilir ancak bu durum veriye ulaşmak isteyen üçüncü kişi tarafından üretilen rasgele değerlerle eşleşebilir, ya da bu rasgele üretilen noktaların hangi karaktere karşılık geldiğine dair bilgiyi içeren dosya alıcıya gönderilmesi gerektiği için; bu dosya üçüncü kişi tarafından haberleşme ortamında ele geçirilebilir. Bu noktada güvenlik seviyesinin arttırılması için, karakterlerin hexadecimal karşılıklarının değerlerinin

noktalarla ifade edildiği ve mesajın bloklar halinde alıcıya iletildiği bir sistem önerilmiştir. Bu durumda üçüncü kişi veriye ulaşsa bile, veri bloklar halinde gönderildiğinden tüm bloğa ulaşamama durumunda sadece birkaç noktaya ulaşır. Ayrıca bu noktaların nasıl anlamlandıracağını bilmediği için açık mesaja ulaşamaz. Tüm bloktaki verilere ulaştığını varsayarsak, karakterin hexadecimal karşılığında, birler basamağında harfle ifade edilen değerlerde sayısal değere çevrileceğinden, bu karakterlerin dönüşümü yapılamaz.

KAYNAKLAR

1. C. Paar, J. Pelzl, ***Understanding Cryptography***, (Springer-Verlag, Berlin, Heidelberg, 2010).
2. N. Koblitz, ***A course in Number theory and Cryptography***, (Springer Verlag, 1994).
3. R. L. Rivest, A. Shamir ve L. Adleman, ***A Method for Obtaining Digital Signatures and Public-Key Cryptosystems***, Communications of the ACM, 21(2):120-126, February (1978).
4. S. Atay, ***Eliptik Eğri Tabanlı Kriptografik Protokol ve Akıllı Kart Üzerinde Bir Uygulama***, Ağ ve Bilgi Güvenliği Sempozyumu, (2005).
5. N. Koblitz, ***Elliptic Curve Cryptosystems***, Mathematics of Computation, vol. 48(177), pp. 203-209, (1987).
6. B. Schneider, ***Applied Cryptography***, (John Wiley & Sons Inc., New York, USA, 2nd edition, 1996).
7. T. Yerlikaya, E. Buluş, N. Buluş, ***Kripto Algoritmalarının Gelişimi Ve Önemi***, Akademik Bilişim Konferansları 2006-Ab2006, Denizli-Türkiye, (2006).
8. C. Çimen, S. Akleylek, E. Akyıldız, ***Şifrelerin Matematiği***, (Kriptografi, ODTÜ Gelistirme Vakfı Yayıncılık, Ankara, 2007).
9. Y. Tsunoo, E. Tsujihara, K. Minematsu, H. Miyauchi, ***Cryptanalysis of Block Ciphers Implemented on Computers with Cache***, ISITA, (2002).
10. NBS FIPS PUB 46, ***Data Encryption Standard***, (National Bureau of Standarts, U.S. Departman of Commerce, January 1977).
11. M. Tektaş, F. Baba, M. Çalışkan, ***Şifreleme Algoritmalarının Sınıflandırılması Ve Bir Kredi Kartı Uygulaması***, 3RD Internatıonal Advanced Technologies Symposıum, Ankara, (2003).
12. D.R. Stinson, ***Cryptography Theory and Practice***, (Chapman & Hall/CRC, CRC Press Company, 2nd Edition, 2002).
13. W. Diffie, M. E. Hellman, ***New Directions in Cryptography***, IEEE Transactions on Information Theory, IT-22:644-654, (1976).

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

15. C. Ellison, B. Schneier, ***Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure***, Computer Security Journal, vol. 16, no. 1, pp. 1-7, (2000).

16. D. Hankerson, A. J. Menezes, S. A. Vanstone, ***Guide to Elliptic Curve Cryptography***, (Springer – Verlag, New York, 25 – 152, 1 st Edition, 2004).

17. E. Berlekamp, ***Algebraic Coding Theory***, (Aegean Park Press, 1984).

18. M. Agrawal, N. Kayal, N. Saxena, ***Primes in P***, Annals of Mathematics, vol. 160, no. 2, pp. 781-793, (2004).

19. S. Singh, ***Fermat'nın Son Teoremi***, (Pan Yayıncılık, İstanbul, 1999).

20. D. B. Gilles, ***Three New Mersenne Primes and a Statistical Theory***, Mathematics of Computation, vol. 18, no. 85, pp. 93-97, (1964).

21. I. M. Vinogradov, ***Elements of Number Theory***, (Dover Publications, USA, 2003).

22. D. M. Arnold, ***Abelian Groups and Representations of Finite Partially Ordered Sets***, (Springer-Verlag, New York, 2000).

23. O. Yayenie, ***A Note on Fibonacci Sequences***, Applied Mathematics and Computation, vol. 217, no. 12, pp. 5603-5611, (2011).

24. R. Peralta, V. Shoup, ***Primality Testing With Fewer Random Bits***, Computational Complexity, vol. 3, no. 4, pp. 355-367, (1993).

25. B. Y. Lemeshko, S. B. Lemeshko, ***Statistical Distribution Convergence and Homogeneity Test Power for Smirnov and Lehmann—Rosenblatt Tests***, Measurement Techniques, vol. 48, no. 12, pp. 1159-1166, (2005).

26. L. C. Washington, Z. Xianke, ***Modification of Cohen-Lenstra Heuristics for Ideal Class Groups and Numbers of Certain Real Quadratic Fields***, Chinese Science Bulletin, vol. 42, no. 23, pp. 1959-1962, (1997).

27. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, ***Handbook of Applied Cryptography***, (CRC Press, USA, 1996).

28. P. L. Montgomery, ***Modular Multiplication Without Trial Division***, Mathematics of Computation,vol. 44, no. 170, pp. 519-521, (1985).

29. T. El Gamal, ***A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology: Proceedings of CRYPTO 84***, Springer Verlag, pp. 10-18, (1988).

30. T. Yerlikaya, ***Yeni Şifreleme Algoritmalarının Analizi***, Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, (2006).

31. P1398, ***Standard Specifications For Public−Key Cryptography***, IEEE, October (1998).

32. NESSIE Consortium, ***NESSIE Security Report***, Technical report NESSIE (2003).

33. A. Baki, ***The Use of Elliptic Curves in Cryptography***, The Graduate School of Natural and Applied Sciences of Middle East Technical University in Partial Fulfillment For The Degree of Master of Science in Mathematics, (1994).

34. G. Dalkılıç, G.Öztaşır, ***Eliptik Eğri Şifrelemesine Karşı Ataklar***, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu-ABG2005, İstanbul-TÜRKİYE, Haziran, (2005).

35. F. Arnault, ***Rabin Miller Primality Test: Composite Numbers Which Pass It***, Mathematics of Computation, vol. 64, no. 209, pp. 355-361, (1995).

36. D. Husemöller, ***Elliptic Curves***, Graduate Text in Mathematics, Springer Verlag, pp. 14, (1987).

37. D. Tall, ***Chords, Tangents and the Leibniz Notation***, Mathematics Education Research Centre, Warwick University, (1985).

38. L. C. Washington, ***Elliptic Curves, Number Theory and Cryptography***, (Chapman and Hall/CRC, 2003).

39. S. Atay, ***Eliptik Eğri Kriptosisteminin Yazılım Uygulamalarında Hız Problemi***, Doktora Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, (2006).

40. M. O. Rabin, ***Digitalized Signatures and Public Key Functions as Intractable as Factorization***, Teknik Rapor, MIT Laboratory for Computer Science, (1979).

41. C. P. Schnorr, ***Efficient Signature Genetarion by Smart Cards***, Journal of Cryptology, vol. 4, pp. 161-174, (1991).

42. K. Nyberg, R. A. Rueppel, ***Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem***, Designs Codes and Cryptography, vol. 7, pp. 61-81, (1996).

43. R. Gallant, R. Lambert, S. Vanstone, ***Improving the Parallelized Pollard Lambda Search on Binary Anomalous Curves***, Mathematics of Computation, vol. 69, pp. 1699-1705, (2000).

44. I. Semaev, ***Evaluation of Discrete Logarithms in a Group of P-torsion Points of an Elliptic Curve in Characteristic p***, Mathematics of Computation, vol 67, pp. 353-356, (1998).

45. S. Pohlig, M. Hellman, ***An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance***, IEEE Transactions on Information Theory, vol. 24, pp. 106-110, (1978).

46. D. Shanks, ***Class Number, a Theory of Factorization and Genera, Proceedings of Symposium on Pure Mathematics***, American Mathematical Society Providence, vol. 34, pp. 415-440, (1971).

47. J. Pollard, ***Monte Carlo Methods for Index Computation mod p, Mathematics of Computation***, vol. 32, pp. (1978).

48. A. Odlyzko, ***The Future Integer Factorization, Crypto-Bytes – The Technical Newsletter of RSA Laboratories***, 1(2), pp. 5-12, (1995).

49. NIST, FIPS 186-2, ***Digital Signature Standard (+change notice)***, National Institute of Standards and Technology, (2000).

50. ANSI, X9.62 ***Public Key Cryptography For the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm***, (1998).

51. Ö. Ö. Bozkurt, ***Eliptik Eğri Şifreleme Kullanarak Güvenli Soket Katmanı Protokolü'nün Gerçeklenmesi ve Performansının Değerlendirilmesi***, Doktora Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, (2005).

52. E. Eryumaz, I. Ertürk, S. Atmaca, ***Implementation of Skipjack Cryptology Algorithm for WSNs Using FPGA***, Application of Information and Communication Technologies, Bakü, (2009).

53. K. Altan, K. Kaşkaoğlu, N. Kındap, Ç. Özakın, Z. Saygı, E. Yıldırım, M. Yıldırım, S. Yıldız, ***Kriptolojiye Girişi Ders Notları***, Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü ODTÜ, Türkiye, (2004).

54. A. Menezes, S. Vanstone, ***Elliptic Curve Cryptosystems and Their Implementation***, Journal of Cryptography 6 (4), pp. 209-224, (1993).

55. K. Koyama, U. Maurer, T. Okamoto, S. A. Vanstone, ***New Public Key Schemes Based on Elliptic Curves over the Ring*** $\boldsymbol{Z_n}$, Proceedings of Crypto' 91, LNCS 576, Springer Verlag, pp. 252-266, (1992).

56. L. Ertaul, W. Lu, ***ECC Based on Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in Manet(I)***, International Federation for Information Processing, LNCS 3462, pp. 102-113, (2005).

ÖZGEÇMİŞ

Meltem KURT 1987 yılında Çorlu'da doğdu. 2010 yılında Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Aynı yıl Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı. 2012 yılında Kocaeli Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisi olarak göreve başladı. Halen Kocaeli Üniversitesi'nde araştırma görevliliğini sürdürmektedir.

TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER

Ulusal Kongre ve Sempozyum Bildirileri

1. M. Kurt, T. Yerlikaya, ***Eliptik Eğrilerin Şifreleme Bilimi Yönünden İncelenmesi ve Eliptik Eğri Şifreleme Algoritmasının Uygulaması***, 25. Ulusal Matematik Sempozyumu, Niğde, (2012).