ELLIPTIC CURVE PRIMALITY TEST CLASS EQUATION

by

Yasemin YAVA§

August 2006

ELLIPTIC CURVE PRIMALITY TEST
CLASS EQUATION

YaseminYAVAŞ

August 2006

ELLIPTIC CURVE PRIMALITY TEST CLASS EQUATION

by

YaseminYAVAŞ

A thesis submitted to
the Graduate Institute of Sciences and Engineering

of

FatihUniversity

in partial fulfillment of the requirements for the degree of Master of Science

in Mathematics

August 2006 Istanbul, Turkey

APPROVAL PAGE

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ali Şahin
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Barış Kendirli
Supervisor

Examining Committee Members

Prof. Dr. Barış Kendirli

Assist. Prof. Dr. Tevfik Bilgin

Assist. Prof. Dr. Nizamettin Bayyurt

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate Institute of Sciences and Engineering.

Assist. Prof. Dr. Nurullah ARSLAN
Director

Date August 2006

ELLIPTIC CURVE PRIMALITY TEST
CLASS EQUATION

Yasemin YAVAŞ

M. S. Thesis – Mathematics

August 2006

Supervisor: Prof. Dr. Barış KENDIRLİ

ABSTRACT

First, **I** have included and explained some number theoretical facts in the beginning. Then Finite Field has been covered with examples in details. I explained Elliptic Curve Cryptosystems. I gave the maple algorithms which are useful for computing.

Keywords: Finite Field, Elliptic Curve Cryptosystems and maple algorithms.

ELLIPTIC CURVE'DE PRIMALITY TESTIN SINIF EŞİTLEMELERİ

Yasemin YAVAŞ

Yüksek Lisans Tezi - Matematik
Agustos 2006

Tez Yoneticisi: Prof. Dr. Barış KENDIRLİ

Öz

Baslangicta sayilar teorisini ana hatlarıyla açıkladım. Sonra, Finite Field detaylı olarak örneklerle gosterilmiştir. Devamında Elliptic Curve Cryptosistemlerini açıkladım. Hesaplamaları yaparken kolaylık sağlamasi için maple algoritmaları yazılmıştır.

Anahtar Kelimeler: Finite Field , Elliptic Curve Cryptosistemleri ve maple algoritmaları.

DEDICATION

To my parents , Miige ,
Müberra, Barış KENDIRLI

ACKNOWLEDGEMENT

I am glad to take this opportunity to thank firstly my supervisor Prof. Dr. Barış KENDIRLİ for his genuine help and very special encouragement throughout the research.

I wish to give my thank to Prof. Dr. Allaberen ASHYRALYEV, Nizamettin Bayyurt, Tevfik Bilgin, Bulent KOKLUCE and Ibrahim KARATAY for their valuable suggestions and comments.

Lastly, I am thankfull to my parents for their encouragement, understanding, motivation and support for my education.

TABLE OF CONTENTS

ABSTRACT iii
OZ iv
DEDICATION v
ACKNOWLEDGEMENT vi
TABLE OF CONTENT vii
LIST OF TABLES ix
LIST OF FIGURES x
LIST OF SYMBOLS AND ABBREVIATIONS xi
CHAPTER 1 INTRODUCTION 1
CHAPTER 2 FINITE FIELD 3
2.1 Finite Field Arithmetic 3
2.2 Existence and Uniqueness 3
2.3 Prime Fields 4
2.4 Binary Fields 5
2.5 Extension Fields 8
2.6 Subfields of Finite Field ...., ... 10
CHAPTER 3 ELLIPTIC CURVES 11
3.1 Elliptic Curve 11
3.2 Elliptic Curves Over Prime Field 13
3.3 Addition Law 14
3.4 Elliptic Curve Over Binary Finite Fielld 19
3.5 Addition Law ....,...... 20
3.6 Elliptic Curve Domain Parameters Over Prime Finite Field 21
3.7 Elliptic Curve Domain Parameters Over Binary Finite Field 22
3.8 Elliptic Curve Cryptosysterns 23
3.9 Elliptic Curve Discrete Logarithm Problem 23
3.10 Diffie-Hellman Key Exchange 23
3.11 El Gamal 26
3.12 Massey Omura Encryption 28
CHAPTER 4 PRIMALITY TEST 30

4.1 Primality Test......................................., ... 30
4.2 Factorization By Continued Fraction.. 40
4.3 The p-1 Factoring Algorithm (Pollard)... 42
4.4 Rho-Method(Pollard).. 44
4.5 Factor Base Method 47
CONCLUSION...54
REFERENCES...55

LIST OF TABLES

TABLE

2.4.1 Table……………………………………………………………………………………8

LIST OF FIGURES

FIGURE

3.10.1 Figure 1 Diffie-Hellman Key Exchange 25

3.11.1 Figure 2 El-Gamal 27

3.12.1 Figure 3 Massey-Omura Encryption 29

CHAPTER 1

INTRODUCTION

Cryptography is the science of securely transmitting message from a sender to a receiver. The objective is to encrypt the message in a way such that an eavesdropper would not be able to read it. A cryptosystem is a system of algorithms for encrypting and decrypting messages for this purpose.

Cryptography comes from the Greek words “Kryptos” which means hidden and “Graphen” which means to write. Classical cryptosystems, substitution and transposition ciphers, were used until modern cryptography were developed. The earliest known use of cryptography is Egyptian Hieroglyphics. Later, Julius Caesar used a monoalphabetic substitution cipher. Frequency analysis techniques for breaking monoalphabetic substitution ciphers invented around 1000 CE. In 1465, Alberti found polyalphabetic ciphers. Cryptography is performed by hand writing until the early 1900s. It became a mathematical science in the middle of the 19th century. The cryptographic science was known by Russians, Europians and Arabics. They used cryptography in diplomatic and military communications. In the beginning of 20th century US, Germans and Japans made use of simple cryptosystems in military and diplomacy. By the invention of telegraph and radio, cryptology was developed. In the World War I, the Red Army of Russia organized its first cryptographic service. New ciphers were created by the Red Army in 1921-1922. Some ciphering machines were developed and started to be used in 1930s. Germans used Enigma machine. Japans used Krieg, Fuller and Burg, Purple Code machines in World War II. In 1939-1940, Enigma was broken by American and British cryptographers. Moreover, the Purple Code was broken by Americans and Russians cryptographers. In 20th century, contemporary cryptology has displayed a considerable acceleration by the invention of computers.

Diffie and Martin Hellman developed Diffie-Hellman key exchange in 1976. It is public key algorithm and depends on discrete logarithm in a finite field. Later, RSA was discovered by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. El Gamal is introduced by El Gamal cryptosystem. It depends on discrete logarithm. In the middle of 1980s, Koblitz and Miller invented Elliptic Curve Cryptography(ECC) which is based on discrete logarithm on abelian groups

To begin with, I exposed Finite Field. I use maple algorithms to solve examples. Furthermore, third chapter provides Elliptic Curve Cryptosystems. In chapter 3 I draw tables of Diffie-Hellman Key Exchange, El-Gamal and Massey-Omura Cryptosystems. Then, in chapter 4, I have included and explained Primality Test.

In the future, I wish to work on algebraic curves, elliptic and hyper elliptic curves.

CHAPTER 2

FINITE FIELD ARITHMETIC

2.1 FINITE FIELD ARITHMETIC

Number systems, the rational numbers, the complex numbers and the integers modulo a prime number are the examples of fields. A field has addition, substraction, multiplication and division operations.

A field under addition and under multiplication satisfies the following arithmetic properties.

i) (F, +) is an abelian group where the additive identity is 0.
ii) (F\{0}, .) is an abelian group where the multiplicative identity is 1.
iii) The distributive law: for all $c,\alpha,\beta \varepsilon F$, $c(\alpha+\beta)=c\alpha+c\beta$

In a field, subtraction of field elements is described with respect to addition such that $\alpha-\beta=\alpha+(-\beta)$ where $-\beta$ is the unique element of F, that is, $\beta+(-\beta)=0$, for all $\alpha,\beta \varepsilon F$. Division of field elements is described with respect to multiplication such that $\alpha/\beta=\alpha\beta^{-1}$ with $\beta\neq0$ where β^{-1} is the inverse of β. Therefore a field consists two operations, addition which is denoted by + and multiplication which is denoted by •.

2.2 EXISTENCE AND UNIQUENESS

The number of elements in a field is said to be the order of finite field.Assume that F_q be a finite field where q is the order of the finite field , F_q. q is a prime power such that $p^m$where p is a prime number , m is a positive integer. The prime number p is called the characteristic of F. F is called a prime field if m=1. F is called an extension field if $m\geq2$.

2.3 PRIME FIELDS

Assume that p is a prime number. In F_p, addition and multiplication operations are performed modulo p. The elements of F_p is {0, 1, 2,......., p-1} a mod p gives intiger remainder r where r is in the range [0, p-1]. This operation is said to be reduction modulo p.

The addition and multiplication operations are defined as follows:

i) Addition operation : Let α, β ε F_p. $\alpha+\beta=r$ where r ε F_p, r is the remainder when the integer $\alpha+\beta$ is divided by p. This operation is called addition modulo p and written $\alpha+\beta\equiv r$ (mod p).

ii) Multiplication operation : Let α, β ε F_p . $\alpha\beta=s$ where s ε F_p, s is the remainder when the integer $\alpha\beta$ is divided by p. This operation is called multiplication modulo p and written $\alpha\beta\equiv s$ (mod p). The additive identity is the integer 0 and the multiplicative identity is integer 1.

To define subtraction of field elements, we need to describe the additive inverse.

iii) Additive inverse : Let α ε F_p . $(-\alpha)$ is the additive inverse of α in F_p such that $\alpha+(-\alpha)\equiv 0$ (mod p).

To define division of field elements , we need to describe the multiplicative inverse.

iv) Multiplicative inverse : Let α ε F_p where $\alpha \neq 0$. α^{-1} is the multiplicative inverse of α in F_p such that $\alpha\alpha^{-1}\equiv 1$ (mod p).

As it is stated above, subtraction and division are described in terms of additive and multiplicative inverses that is $\alpha- \beta$ (mod p) is $\alpha+ (-\beta)$ (mod p) and α/ β (mod p) is $\alpha(\beta^{-1})$ (mod p).

To illustrate; the elements of F_{23} are {0, 1, 2,....., 22}. The following arithmetic operations are the examples of F_{23}.

i) Addition = 19+20=16 since 39 mod 23 = 16.
ii) Subtraction = 19-20=22 since –1 mod 23 = 26.

iii) Multiplication = 19.20=12 since 380 mod 23 = 12.

iv) Inversion : 19^{-1} = 17 since 19.17 mod 23 = 1.

2.4. BINARY FIELDS (THE FINITE FIELD F_2^m)

There are two ways to construct F_2^m. One of them is polynomial basis representation. The elements of F_2^m are the polynomials whose coefficients are in the field F_2 = {0,1} with degree at most m-1.

$$F_2^m = \{\alpha_{m-1} X^{m-1} + \alpha_{m-2} X^{m-2} + \dots\dots\dots\dots + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \ : \alpha_i \ \varepsilon \ \{0, 1\} \}$$

We choose an irreducible binary polynomial f(x) with degree m, which cannot be factored into binary polynomials whose degrees less than m.

Addition operation in binary fields is the usual addition of polynomials, with coefficient arithmetic performed modulo 2.

i) Addition operation : Let

$$\alpha=\alpha_{m-1} X^{m-1} + \alpha_{m-2} X^{m-2} + \dots\dots\dots\dots + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \ ,$$

$$\beta=\beta_{m-1} X^{m-1} +\beta_{m-2} X^{m-2} + \dots\dots\dots\dots + \beta_2 X^2 + \beta_1 X + \beta_0 \ \ \varepsilon \ F_2^m \ .$$

$$\alpha+\beta=r \text{ where } r \ \varepsilon \ F_2^m \ . \ r= r_{m-1}X^{m-1}+ \dots\dots\dots\dots + r_0 \text{ with } r_i \equiv \alpha_i + \beta_i \ (\text{mod } 2 \ ).$$

Multiplication operation in binary fields is done modulo the reduction polynomial f(x)**,**

ii) Multiplication operation**:** Let

$$\alpha=\alpha_{m-1} X^{m-1} + \alpha_{m-2} X^{m-2} + \dots\dots\dots\dots + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \ ,$$
$$\beta=\beta_{m-1} X^{m-1} +\beta_{m-2} X^{m-2} + \dots\dots\dots\dots + \beta_2 X^2 + \beta_1 X + \beta_0 \ \ \varepsilon \ F_2^m \ .$$

$\alpha\beta$= s where s ε F_2^m . $s=s_{m-1} X^{m-1} + s_{m-2} X^{m-2} + ...+ s_2 X^2 + s_1 X + s_0$ is the remainder as the polynomial s=$\alpha\beta$ is divided by f(x) with all coefficient arithmetic performed modulo 2.

To define subtraction of F_2^m we need to describe the additive inverse.

iii) Additive inverse : Let α ε F_2^m . (- α) is the additive inverse of α in F_2^m such that . $\alpha+(-\alpha)=0$ in F_2^m

To define subtraction of F_2^m we need to describe the additive inverse.

iv) Multiplicative inverse : Let α ε F_2^m where $\alpha \neq 0$. α^{-1} is the multiplicative inverse of α in F_2^m such that $\alpha\alpha^{-1} = 1$ in F_2^m .

As it is stated above, subtraction and division are described with respect to additive and multiplicative inverses that is α - β in F_2^m is equal to α +(- β) in F_2^m and α / β in F_2^m is equal to α (β^{-1}) in F_2^m .

For example; the elements of F_2^4 are the 16 binary polynomials of degree at most 3 such that {0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1}.

We choose the reduction polynomial $f(x) = x^4+x^2+1$ in F_2^4. The following arithmetic operations are the examples of F_2^4.

i) Addition : $(x^3+x^2+1)+ (x^2+x+1) = x^3+x$

ii) Subtraction : $(x^3+x^2+1)- (x^2+x+1) = x^3+x$

Because $-1 = 1$ in F_2 .

iii) Multiplication : $(x^3+x^2+1) (x^2+x+1) = x^2+1$ since

$(x^3+x^2+1) (x^2+x+1) = x^5+x^4+x^3+ x^4+x^3+x^2+ x^2+x+1= x^5+x+1$

$(x^5+x+1) \bmod (x^4+x+1)= x^2+1$

iv) Inversion : $(x^3+x^2+1)^{-1}=x^2$ since $(x^3+x^2+1)(x^2) \bmod (x^4+x+1) = 1$

We find the inversion of (x^3+x^2+1) by performing Euclidean and extended Euclidean Algorithm.

$x^4+x+1 = (x^3+x^2+1)(x) + (x^3+1)$

$x^3+x^2+1 = (x^3+1)\,1 + x^2$

$x^3+1 = x^2+x+1$

$1 = (x^3+1) - x^2\,x$

$= (x^3+1) – x((x^3+x^2+1) - (x^3+1))$

$= (x^3+1) – x(x^3+x^2+1) - x(x^3+1)$

$= (x+1)(x^3+1) – x(x^3+x^2+1)$

$= (x+1)((x^4+x+1) – x(x^3+x^2+1)) – x(x^3+x^2+1)$

$= (x+1)(x^4+x+1) –(x^2+x)(x^3+x^2+1) – x(x^3+x^2+1)$

$= (x+1)(x^4+x+1) – x^2(x^3+x^2+1)$

In maple we can perform finite field arithmetic easily.

Let’s do the example above in maple;

- G: GF (2,4,alpha^4 + alpha+1):
- a:= alpha^3 + alpha^2+1;

a: $\alpha^3+\alpha^2+1$

- a:= G [ConvertIn] (a) ;

a:=($\alpha^3+\alpha^2+1$) mod 2

- b: = alpha^2 + alpha+1;

b: $\alpha^2+\alpha+1$

- b:= G [ConvertIn] (b) ;

b:=($\alpha^2+\alpha+1$) mod 2

\# addition operation #

- addition : = G [`+`] (a,b) ;

addition := ($\alpha^3+\alpha$) mod 2

\# subtraction operation #

- subtraction := G [`-`] (a,b) ;

subtraction:= ($\alpha^3+\alpha$) mod 2

multiplication operation

- multiplication := G [`*`] (a,b) ;

multiplication:= (α^2+1) mod 2

inversion

- inversion := G[inverse](a) ;

inversion := α^2 mod 2

2.4.1 Table 1-reduction polynomial(s)

Field	**Reduction Polynomial(s)**
F_2^{113}	$f(x)= x^{113}+x^{9+}1$
F_2^{131}	$f(x)= x^{131}+x^8+x^3+x^2+1$
F_2^{163}	$f(x)= x^{163}+x^7+x^6+x^3$
F_2^{193}	$f(x)= x^{193}+x^{15}+1$
F_2^{233}	$f(x)= x^{233}+x^{74}+1$
F_2^{239}	$f(x)= x^{239}+x^{36}+1$ **or** $f(x)= x^{239}+x^{158}+1$
F_2^{283}	$f(x)= x^{283}+x^{12}+x^7+x^5+1$
F_2^{409}	$f(x)= x^{409}+x^{87}+1$
F_2^{571}	$f(x)= x^{571}+x^{10}+x^5+x^2+1$

2.5 EXTENSION FIELDS

Let p be a prime and m≥2. The set of all polynomial in the variable x with coefficients from F_p is denoted by F_p [X] and the reduction polynomial is f(x). The elements in F_p^m are the polynomials of degree at most m-1 in F_p [X].

$$F_p^{\,m} = \{\alpha_{m-1} X^{m-1} + \alpha_{m-2} X^{m-2} + \ldots\ldots\ldots\ldots\ldots\ldots + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \;:\; \alpha_i \ \varepsilon\ F_p \}$$

The usual addition of polynomials with coefficient arithmetic performed in F_p is the addition operation.Multiplication operation is performed modulo f(x) which is the reduction polynomial.

For example; Let p=251 and m=5 . The reduction polynomial $f(x)=x^5+x^4+12x^3+9x^2+7$ in $F_{251}[X]$. This reduction polynomial can be used for the construction of $F_{251}{}^5$.

Assume that

$$\alpha=123x^4+76x^2+7x+4 \text{ and } \beta= 196x^4+12x^3+225x^2+76 \text{ in } F_{251}{}^5 .$$

i) Addition : $\alpha+\beta=(123x^4+76x^2+7x+4)+(196x^4+12x^3+225x^2+76)$

$=68x^4+12x^3+50x^2+7x+80$

ii) Subtraction : $\alpha- \beta=(123x^4+76x^2+7x+4)-(196x^4+12x^3+225x^2+76)$

$=178x^4+239x^3+102x^2+7x+17$

iii) Multiplication : $\alpha.\beta=(123x^4+76x^2+7x+4).(196x^4+12x^3+225x^2+76)$

$=117x^4+151x^3+117x^2+182x+217$

iv) Inversion : $\alpha^{-1} =109x^4+111x^3+250x^2+98x+85$

Let's do the example above in maple;

- G: GF (251,5,alpha^5 + alpha^4+12*alpha^3+9*alpha^2+7);

- a:= G [ConvertIn] (123*alpha^4+76*alpha^2+7*alpha+4) ;

  $a:= (123\alpha^4+76\alpha^2+7\alpha+4) \bmod 251$

- b:= G [ConvertIn] (196*alpha^4+12*alpha^3+225*alpha^2+76) ;

  b:=($196\alpha^4+12\alpha^3+225\alpha^2+76$) mod 251

addition operation

- addition : = G [`+`] (a,b) ;

  addition := ($68\ \alpha^4+12\alpha^3+50\alpha^2+7\alpha+80$) mod 25

subtraction operation

- subtraction := G [`-`] (a,b) ;

  subtraction:=($178\alpha^4+239\alpha^3+102\alpha^2+7\alpha+179$)mod251

multiplication operation

- multiplication := G [`*`] (a,b) ;

  multiplication:=($117\alpha^4+151\alpha^3+117\alpha^2+182\alpha+217$)mod25

inversion

- inversion := G[inverse](a) ;

  inversion := ($109\alpha^4+111\alpha^3+250\alpha^2+98\alpha+85$) mod 251

2.6 SUBFIELDS OF FINITE FIELD

F is called a subfield of K if F≤K. In this instance, K is called an extansion field of F. Exactly a finite field $F_p{}^m$ has one subfield of order p^t for each divisor t of m. This means that $\alpha^{pt} = \alpha$ for $\alpha\varepsilon\ F_p{}^m$.

CHAPTER 3

ELLIPTIC CURVES

3.1. DEFINITION OF ELIPTIC CURVE

The generalized Weierstrass Equation for an elliptic curve is

$$y^2+a_1xy+a_3y= x^3+a_2x^2+a_4x+a_6$$

where a_1, a_2, a_3, a_4, a_5, a_6 are constants. We can describe an elliptic curve over F_q in terms of the solutions to an equation in F_q . F_q is a prime finite field or a binary finite field. The form of the equation depends on finite field F_q. If the field is prime finite field, we use the equation $y^2 \equiv x^3+ax+b$ (mod p) . If the field is binary finite field, we use the equation $y^2+xy= x^3+ax^2+b$ in $F_2{}^m$.

Theorem3.1.1 : (Hasse)

Let the elliptic curve E be defined over the finite field F_q. Then the order of $E(F_q)$ is denoted by # $E(F_q)$ which satisfies

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

Theorem 3.1.2:

Let $q=p^m$ where p is prime and m is a positive integer. Let N = q+1-t. The Elliptic Curve E is defined over F_q such that # E (F_q) = N ıf and only ıf $|t| \leq 2\sqrt{q}$ and t satisfies one of the following :

i) gcd (t,p) =1
ii) m is even and $t=\pm 2\sqrt{q}$
iii) m is even , $p \equiv 1$ (mod 3), and $t= \pm\sqrt{q}$

iv) m is odd , p=2 or 3, and $t = \pm p^{(m+1)/2}$
v) m is even, $p \equiv 1 \pmod 4$, and t=0
vi) m is odd and t = 0

Let the order of the base point G be n which is a large prime. The number of points on the curve is equal to nh denoted # E (F_q) =nh . h is the cofactor which is a small integer . Moreover , h is not divisible by n . For efficiency reasons , it is useful to get the cofactor to be as small as possible. In prime finite field , h=1,2 or 4 . In binary finite field h=2 or 4.
Calculating the number of points on an Elliptic Curve over F_p . First , we select an x ε F_p and state if there is corresponding y on the curve that is for a given x we test if $f(x)=x^3+ax+b$ (mod p) is a quadratic residue.

3.1.3 Definition: (The Legendre Symbol):

Let α be an integer and p be an odd prime . The Legendre Symbol (α/p) is defined as follows :

$$(\alpha/p) = \begin{cases} 0 \text{ , if p divides } \alpha \text{ ;} \\ 1 \text{ , if } \alpha \text{ is quadratic residue modulo p ;} \\ -1 \text{ , if } \alpha \text{ is not quadratic residue modulo p ;} \end{cases}$$

We use legendre symbol to find out an integer is a quadratic residue modulo p or not. Then the following cases are based on f(x) is a quadratic residue or not modulo p;

i) if f(x) is quadratic residue , there are two points (x , ±y).
ii) if f(x) divides p , there is a single point (x , 0).
iii) İf f(x) is not quadratic residue , there is no point .

3.1.4 Example : Let E be an Elliptic Curve $y^2 = x^3 + x + 6$ over F_{11}. The point (2,7) has order 13. So $N_{11} = \#E(F_{11})$ is a multiple of 13. Hasse's theorem implies that

$$11+1-2\sqrt{11} \leq N_{11} \leq 11+1+2\sqrt{11}$$

The only multiple of 13 in this range is 13. Hence, $N_{11} = 13$.

3.1.5 Example : The elliptic curve E $y^2 = x^3 - 10x + 21$ is defined over $F_{557.}$ The point (2,3) has order 189. Hasse's theorem implies that

$$557+1-2\sqrt{557} \leq N_{557} \leq 557+1+2\sqrt{557}$$

which means that

$$511 \leq N_{55}$$

Hence, N_{557} is a multiple of 189.The only multiple of 189 in the range

$511 \leq N_{557} \leq 605$ is 3 . 189 = 567. So $N_{557} = \#E(F_{557}) = 567$.

3.2 ELLIPTIC CURVES OVER PRIME FIELD

Assume that F_p is a prime finite field where p is an odd prime number . Let α, β in F_p such that $4\alpha^3 + 27\beta^2$ T 0 (mod p) . A non –singular elliptic curve is the set of solutions or points (x,y) for x,y ε F_p to the equation

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

together with an extra point ϑ is said to be the point at infinity . The equation $y^2 \equiv x^3 + ax + b \pmod{p}$ is said to be the defining equation of $E(F_p)$. The equation $x^3 + ax + b = 0$ has one real root or three real roots. Assume that the point $G = (x_{G,} y_G)$ is given , x_G is called the x-coordinate of G , y_G is called the y-coordinate of G . The identity element is the point at infinity , ϑ

$\#E(F_p)$ is the number of points on $E(F_p)$. The Hasse Theorem says that :

$$p+1-2\sqrt{q} \le \#E(F_p) \le p+1+2\sqrt{q}$$

3.3 ADDITION LAW

1. Adding the point at infinity to itself .
   $\vartheta+\vartheta=\vartheta$
2. Adding the point at infinity to any other point.
   $(x,y)+\vartheta=\vartheta+(x,y)=(x,y)$ for all $(x,y)\ \varepsilon E(F_p)$.
3. Adding two points with the same x-coordinates when the points are either different or have y-coordinate 0.
   $(x,y)+(x,-y)=\vartheta$ for all $(x,y)\ \varepsilon\ E(F_p)$.
   The negative of (x,y) is (x,-y)
4. Adding two points with different x-coordinates
   Let (x_1, y_1) in $E(F_p)$ and $(x_2,y_2)\ \varepsilon\ E(F_p)$.
   These are two points such that $x_1 \neq x_2$.
   $(x_3, y_3) = (x_1, y_1) + (x_2,y_2)$ where

$$\lambda\equiv(y_2-y_1)/(x_2-x_1) \pmod p$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

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

We can compute λ, x_3, y_3 in maple such that;

- Lambda := (Py[2] - Py[1]) / (Px[2] - Px[1]) mod p;
- Px[3] := (lambda^2 – Px[1] – Px[2]) mod p;
- Py[3] := (lambda* (Px[1] – Px[3]) – Py[1]) mod p;

5. Adding a point itself (double a point)
   Let (x_1, y_1) in $E(F_p)$ where $y_1 \neq$

$\lambda \equiv (3x^2{}_1 + a)/ 2y_1 \pmod p$

$x_3 = \lambda^2 - 2x_1 \pmod p$

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

We can compute λ, x_3, y_3 in maple such that;

- Lambda := (3* (Px[1]^2) +a) – (2*Py[1]) mod p;
- Px[3] := ((lambda^2) – (2*Px[1])) mod p;
- Py[3] := (lambda* (Px[1] – Px[3]) – Py[1]) mod p;

The set of points on $E(F_p)$ constructs a group under this addition law. Moreover , the group is abelian .Cryptographic systems depended on Elliptic Curve Cryptography base on scalar multiplication of elliptic curve points.Let k be an integer and Gbe a point $E(F_p)$. The process of adding G to itself k times is called scalar multiplication , denoted by kG . We calculate scalar multiplication of Elliptic Curve points by applying the addition law.

3.3.1 Example :

Let E be the curve $y^2 = x^3 + x + 6$ over F_{11}. To count points on E, we make a list of the possible values of x and we compute the square roots y of $x^3 + x + 6 \pmod{11}$.

x	x^3 +x+6	y	points
0	**6**	**-**	**-**
1	**8**	**-**	**-**
2	**5**	**±4**	**(2,4) (2,7)**
3	**3**	**±5**	**(2,5) (2,6)**
4	**8**	**-**	**-**
5	**4**	**±2**	**(5,2) (5,9)**
6	**8**	**-**	**-**
7	**4**	**±2**	**(7,2) (7,9)**
8	**9**	**±3**	**(8,3) (8,8)**
9	**7**	**-**	**-**
10	**4**	**±2**	**(10,2) (10,9)**
∞	-	∞	∞

Therefore E (F_{11}) has order 13. If any group of prime order is cyclic then E is isomorphic to Z_{13}. Let α = (2,7) is a generator point. We can calculate powers of α which is given below example.

3.3.2 Example : Let compute powers of α = (2,7) ,

calculate 2α = (2,7) + (2,7) by

$$\lambda \equiv (3.2^2 + 1) / (2.7) \pmod{11}$$
$$\equiv 8 \pmod{11}$$
$$x_3 = (8^2 - 2.2) \pmod{11}$$
$$= 5 \pmod{11}$$
$$y_3 = (8 .(2 - 5) - 7) \pmod{11}$$
$$=2 \pmod{11}$$

Hence, $2\alpha = (5,2)$

calculate $3\alpha = (5,2) + (2,7)$ by

$\lambda \equiv (7-2)/(2-5) \pmod{11}$

$\equiv 2 \pmod{11}$

$x_3 = (2^2 - 5 - 2) \pmod{11}$

$= 8 \pmod{11}$

$y_3 = (2.(5-8) - 2) \pmod{11}$

$= 3 \pmod{11}$

Now, let's continue to compute powers of α in maple.

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – x_1 – x_2 mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 3$

$x_5 := 10$

$y_5 := 2$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – x_1 – x_2 mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 9$

$x_6 := 3$

$y_6 := 6$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 10$

$x_7 := 7$

$y_7 := 9$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 7$

$x_8 := 7$

$y_8 := 2$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 10$

$x_9 := 3$

$y_9 := 5$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 9$

$x_{10} := 10$

$y_{10} := 9$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 3$

$x_{11} := 8$

$y_{11} := 8$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 2$

$x_{12} := 5$

$y_{12} := 9$

- lambda := ($y_2 - y_1$) / ($x_2 - x_1$)   mod 11 ;
  x_3 := lambda^2 – $x_1 - x_2$ mod 11 ;
  y_3 := lambda* ($x_1 - x_3$) – y_1 mod 11 ;

$\lambda := 8$

$x_{13} := 2$

$y_{13} := 4$

3.4 ELLIPTIC CURVE OVER BINARY FINITE FIELDS

Assume that a , b ε $F_2{}^m$ where $b \neq 0$ in $F_2{}^m$ .A non-super singular elliptic curve E over the finite field $F_2{}^m$ defined by the parameters a ,b in $F_2{}^m$ consists of the set of solutions or points p=(x ,y) for x , y in $F_2{}^m$ to the equation :

$$y^2+xy=x^3+ax^2+b \text{ in } F_2{}^m$$

together with an extra point ϑ is said to be the point at infinity. # $E(F_2{}^m)$ is the number of points on $E(F_2{}^m)$. The Hasse theorem says that

$$2^m+1-2\sqrt{2^m} \leq E(F_2{}^m) \leq 2^m+1+2\sqrt{2^m}$$

3.5 ADDITION LAW

a. Adding the point at infinity to itself
   $\vartheta + \vartheta = \vartheta$
b. Adding the point at infinity to any other point
   $(x, y) +\vartheta = \vartheta + (x,y) = (x, y)$ for all $(x, y) \varepsilon E(F_2{}^m)$
c. Adding two points with the same x-coordinates when the points are either different or have y-coordinates 0 .
   $(x, y) + (x, x+y) = \vartheta$ for all $(x, y) \varepsilon E(F_2{}^m)$
   The negative of (x, y) is equal to (x, x+y).
d. Adding two points with different x-coordinates . Let (x_1, y_1) in $E(F_2{}^m)$,
   $x_1 \neq x_2$.
   $(x_3, y_3) =(x_1, y_1) + (x_2, y_2)$ where

$$\lambda= (y_1 +y_2)/(x_1+x_2) \text{ in } F_2{}^m$$

$$x_3 = \lambda^2+\lambda+x_1+x_2+a \text{ in } F_2{}^m$$

$$y_3 = \lambda (x_1 +x_3) +x_3 +y_1 \text{ in } F_2{}^m$$

We can compute λ, x_3, y_3 in maple

```
λ := G[`/ `] ( G[` + `] (Py [1] , Py [2] ), (G[`+ `] (Px [1] , Px [2] ) ) ;
Px[3] := G[` + `] ( G[` + `]  (G[` + `] (G[` + `] (G[`^`] ( λ, 2 ), λ ), Px[1] ), Px[2] ), a );
Py[3] := G[` + `] ( G[` + `]  (G[` * `] (G[` + `] ( Px[1] , Px[3] ), λ ), Px[3] ), Py[1] );
```

e. Adding a point itself (double a point)

$\lambda = x_1 + (y_1/x_1)$ in F_2^m

$x_3 = \lambda^2+\lambda+a$ in F_2^m

$y_3 = x_1^2+(\lambda+1)x_3$ in F_2^m

We can compute λ, x_3, y_3 in maple

```
λ := G[` + `] ( G[` / `] ( Py [1] , Px [1] ),  Px [1] ) ;
Px[3] := G[` + `] ( G[` + `]   (G[`^`] ( λ, 2 ), λ ),  a );
Py[3] := G[` + `]   (G[` * `] (G[` + `] ( λ , 1 ), Px[3] ) , G[`^`] ( Px[1] , 2 )  );
```

The set of points on E (F_2^m) constructs an abelian group under this addition law. Cryptographic systems depended on Elliptic Curve Chryptography base on scalar multiplication of elliptic curve points. Let k be an integer and G be a point in E (F_2^m) the process of adding G to itself k times is called scalar multiplication, denoted by kG. We calculate scalar multiplication of elliptic curve points by applying the addition law.

3.6 ELLIPTIC CURVE DOMAIN PARAMETERS OVER PRIME FINITE FIELD

Elliptic Curve domain parameters over finite fields consist of a prime integer p defining the finite field F_p, two elements a,b in F_p defining on elliptic curve E(F_p) specified by the equation $y^2 \equiv x^3 +ax+b$ (mod p), a base point G= (x_G, y_G) on E(F_p), a prime n which is the order of G, and an integer h which is the cofactor that #E(F_p)=hn:

$$T = (p , a , b , G , n , h)$$

The approximate security level in bits desired from the elliptic curve domain parameters must be an integer t ε { 56, 64, 80, 96, 112, 128, 192, 256 }

Validating the elliptic curve domain parameters over F_p is as follows :

i) Confirm that p is an odd prime such that [$\log_2$ p] =2t if t≠256 or such that [$\log_2$ p]=521 if t=256 .

ii) Confirm that a, b, x_G and y_G are integers in the interval [0 , p-1].

iii) Confirm that $4a^3+27b^2 \not\equiv 0 \pmod p$.

iv) Confirm that $y^2_G \equiv x^3_G + ax_G + b \pmod p$.

v) n is prime .

vi) Confirm that h≤4, and that h = $[(\sqrt{p} +1)^2 / n]$.

vii) Confirm that nG =ϑ .

viii) Confirm that $p^B \equiv 1 \pmod n$ for any $1\leq B < 20$,and that nh = p.

3.7 ELLIPTIC CURVE DOMAIN PARAMETERS OVER BINARY FINITE FIELDS

Elliptic Curve domain over binary finite fields consist of a positive integer m defining the finite field $F_2{}^m$ an irreducible binary polynomial f(x) of degree m defining the representation of $F_2{}^m$, two elements a, b in $F_2{}^m$ defining the elliptic curve $E(F_2{}^m)$ specified by the equation $y^2+xy = x^3+ax^2+b$ in $F_2{}^m$, a base point G = (x_G , y_G) on E ($F_2{}^m$), a prime n which is the order of G, and an integer h which is the cofactor that # $E(F_2{}^m)$= hn :

$$T = (m, f(x), a, b, G, n, h)$$

Validating the elliptic curve domain parameters over $F_2{}^m$ is as follows :

i) Assume that t^l implies the smallest integer greater than t in the set { 56, 64, 80, 96, 112, 128, 192, 256 }. Confirm that m is an integer in the set {113, 131, 163, 193, 233, 239, 283, 409, 571 } such that $2t < m < 2t^l$.

ii) Confirm that f(x) is a binary irreducible polynomial of degree m which is listed in Table 1.

iii) Confirm that a, b, x_G, y_G are binary polynomials of degree m-1 or less .

iv) Confirm that $b \neq 0$ in $F_2{}^m$.

v) Confirm that $y^2_G+x_G y_G=x^3_G+ax^2_G+b$ in $F_2{}^m$.

vi) Confirm that n is prime .

vii) Confirm that h ≤ 4 , and that h = $[(\sqrt{2^m} +1)^2 / n$.

viii) Confirm that $nG = \vartheta$.

ix) Confirm that $2^{mB} \equiv 1$ (mod n) for any $1 \leq B < 2$ 0, and that $nh \neq 2^{m}$.

3.8 ELLIPTIC CURVE CRYPTOSYSTEMS

The modren symetric cryptosystems are faster than the asymetric cryptosystems. Symetric cryptosystems are not secure as encryption and decryption keys are the same. On the otherhand, asymetric cryptosystems are secure since encryption and decryption keys are different each other. Public key cryptosystems depends on factorization large integer into primes and discrete logarithm. Elliptic Curve Cryptosystems is based on discrete logarithm on a finite abelian group.

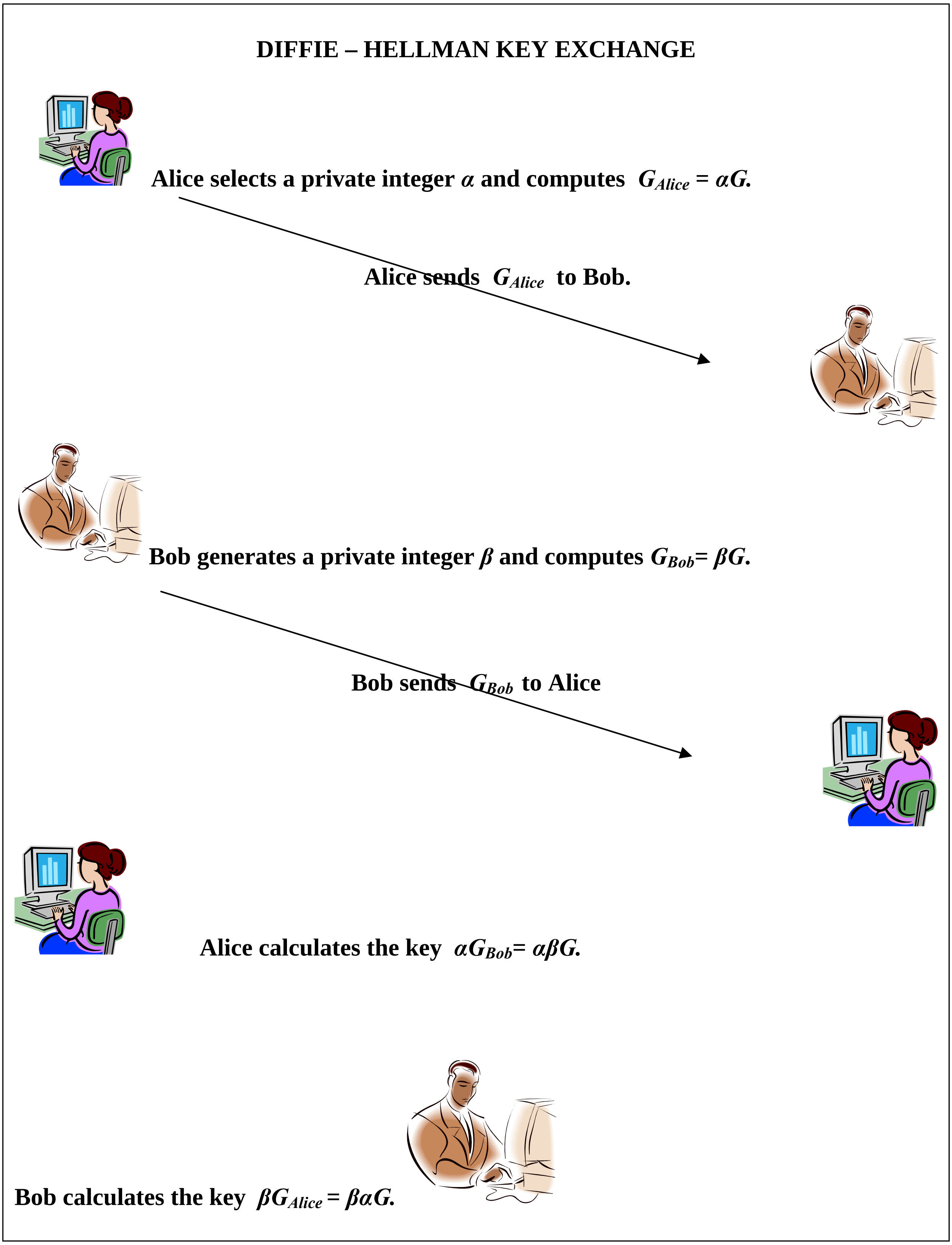
3.9 ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Assume that a base point G and the point kG be given. These points are on the curve. Finding the value of k is called the discrete logarithm problem. It is believed that finding k is really hard problem. Using algebraic groups is desired by many cryptosystems. A group is a set of elements with custom described arithmetic operations on those elements. For elliptic curve groups, these specific operations are described geometrically. There are some limitations on these groups of operations such that the number of points on such a curve creates underlying field for an elliptic curve group.

3.10 DIFFIE-HELLMAN KEY EXCHANGE

Alice and Bob choose an elliptic curve E over a finite field F_q and a base point $G \varepsilon E(F_q)$. We must be careful while choosing curve and base point that order of point must be large prime and the discrete logarithm problem must be hard in $E(F_q)$.

Next, Alice selects a private integer α and computes $G_{Alice} = \alpha G$. Then Alice sends G_{Alice} to Bob. After that, Bob generates a private integer β and compute $G_{Bob} = \beta G$
Then Bob sends G_{Bob} to Alice. Hence, Alice calculates the key such that $\alpha G_{Bob} = \alpha\beta G$. Bob calculates the key such that $\beta G_{Alice} = \beta\alpha G$.
The elliptic curve E, the finite field F_q ,the points G ,G_{Alice} ,G_{Bob} are public . Alice and Bob keep α and β private . Solving discrete logarithm problem in $E(F_q)$ to find α and β is feasible.



3.10 Figure 1-Diffie-Hellman Key Exchange

3.11EL-GAMAL

Bob generates an elliptic curve E over a finite field F_q and a base point $G \varepsilon E(F_q)$ whose order must be a large prime. While choosing an elliptic curve E over finite field $F_{q,}$ the discrete logarithm problem must be very hard. Bob selects a private integer s and calculates B =sG. Bob makes the elliptic curve E, the finite field F_q, the point G, and B public. But, Bob keeps s secret. Then, Alice sends her message to Bob by performing the following :

- Alice represents her message as a point $M \varepsilon E(F_q)$.
- Alice generates a secret integer k at random and calculates M_1=kG.
- Alice calculates M_2=M+kB.
- Alice sends M_1 and M_2 to Bob.

The whole process implemented by Alice is encryption procedure.
Bob decrypts the chipertext by solving

$$M=M_2 – sM_1$$

as

$$M_2 – sM_1 = (M+kB) – skG$$

$$= M+k(sG) –s(kG) = M$$

EL GAMAL

Bob chooses point G in E(Fq). Bob selects a private integer s and calculates $B = sG$. Bob makes E(Fq), G, B public.

Alice represents her message as a point M in Fq

Alice generates a secret integer k at random

Alice calculates $M_1 = kG$

Alice calculates $M_2 = M + kB$

Alice sends M_1 and M_2 to Bob.

Bob decrypts the ciphertext by solving $M = M_2 - sM_1$.

as

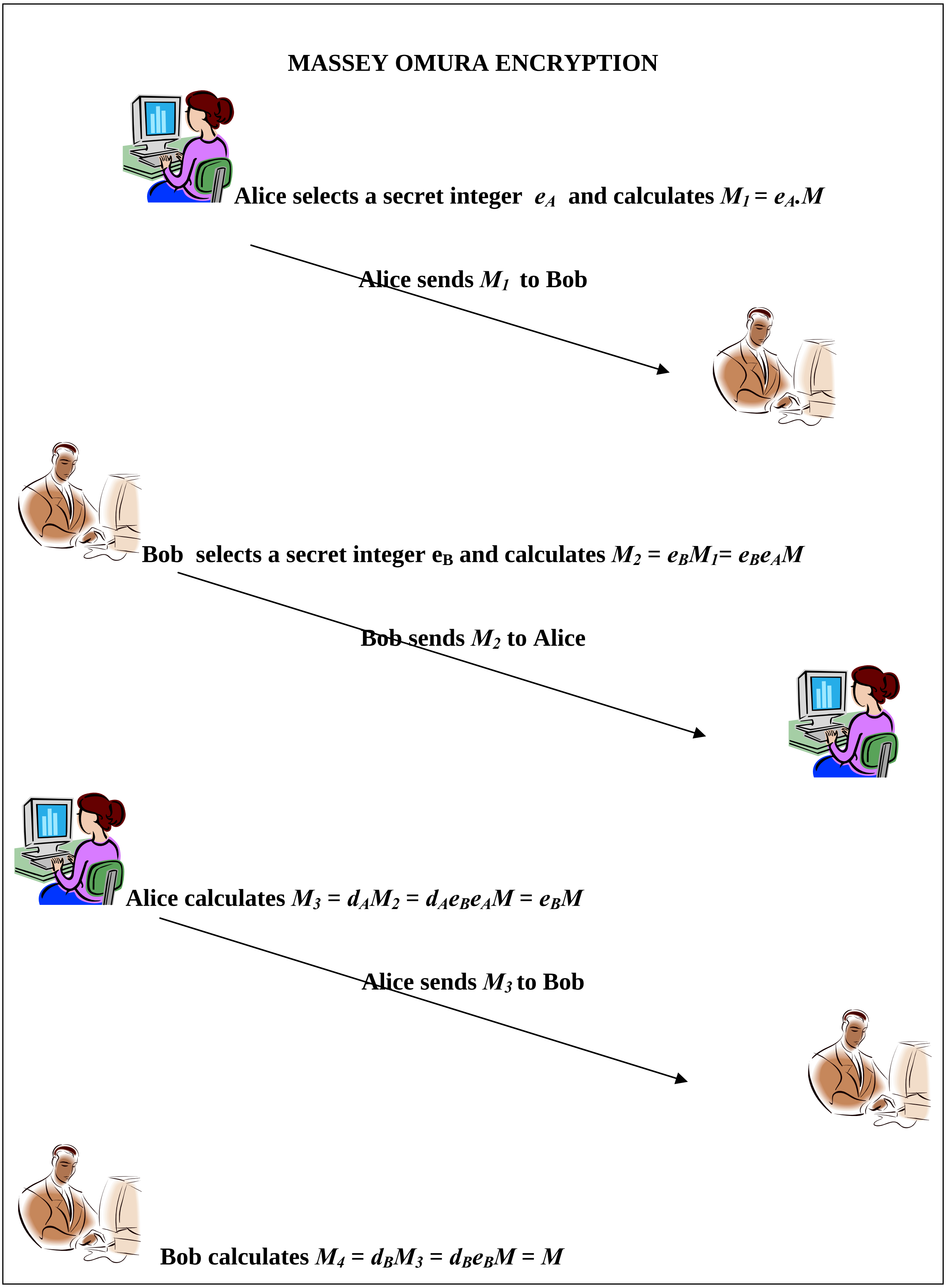
$$M_2 - sM_1 = (M + kB) - skG = M + k(sG) - s(kG) = M$$

3.12**Figure 2-**El Gamal

3.13 MASSEY-OMURA ENCRYPTION

- Alice and Bob an elliptic curve E over a finite field F_q.
  We must be careful while choosing $E(F_q)$ since the discrete logarithm problem must be very hard in $E(F_q)$. Assume that $N = \# E(F_q)$.
- Alice expresses her message as a point $M \varepsilon E(F_q)$
- Alice selects a secret integer e_A with gcd $(e_A, N) = 1$ and calculates $M_1 = e_A M$ and sends M_1 to Bob .
- Bob selects a secret integer e_B with gcd $(e_B, N) = 1$ and calculates $M_2 = e_B M_1$ and sends M_2 to Alice .
- Alice calculates $d_A \varepsilon Z_N$ such that $d_A e_A \equiv 1 \pmod N$ .Then she calculates $M_3 = d_A M_2$ and sends M_3 to Bob .
- Bob calculates $d_B \varepsilon Z_N$ such that $d_B e_B \equiv 1 \pmod N$. Then he calculates $M_4 = d_B M_3$. So, $M_4 = M$ is the original message.

d_A is the inverse of $e_A \pmod N$ and d_B is the inverse of $e_B \pmod N$.



3.12 Figure 3 – Massey Omura Encryption

CHAPTER 4

PRIMALITY TEST

4.1. PRIMALITY TEST

In this section ,we will study more efficient methods as Miller-Rabin test, The rho method,Factor base algorithm, Continued Fraction method and Quadratic Sieve method.

4.1.1 Definition : **Let *m* be a large integer. A primality test determines whether *m* is prime or not.**

Example 4.1. If there exist an integer a such that

$$a^n \not\equiv a (\text{mod } n),$$

then n is not prime integer. It is known that if n is a prime integer then

$$a^n \equiv a (\text{mod } n)$$

for any integer a. Therefore it is a primality test.

4.1.2. Definition : A number n passes the pseduoprime test to base a if

$$a^n \equiv a \ (\text{mod } n).$$

Of course, it doesn't imply that n is prime.

4.1.3. Definition : Let a be a positive integer. If n is a composite(not prime) positive integer and

$$a^n \equiv a \ (\text{mod } n),$$

then n is called a pseudoprime to the base a.

Lemma : If gcd $(a, n) = 1$, then

$$a^n \equiv a \ (\bmod n) \Leftrightarrow a^{n-1} \equiv 1 \ (\bmod n)$$

Proof : gcd(a, n) = 1 implies that a^* mod n exists. Thus we multiply both sides of

$$a^n \equiv a (\bmod n)$$

by a^*.

We multiply both sides of

$$a^{n-1} \equiv 1 (\bmod n)$$

by a.

Example 4.2. For instance

$$2^{340} \equiv 1 \ (\bmod 341)$$

with 341 = 11.31. Hence, 341 is a pseduoprime with base 2.

Example 4.3.

$$2^{560} \equiv 1 (\bmod 561), \ 561 = 3.11.17$$

$\Rightarrow$ 561 is a pseduoprime with base 2.

Example 4.4.

$$3^{90} \equiv 1 (\bmod 91) 91 = 7.13$$

$\Rightarrow$ 91 is a pseduoprime with base 3.

4.1.4. Definition : A composite integer n is said to be a Carmichael integer if

$$a^{n-1} \equiv 1 (\bmod n)$$

for all positive integer a such that

$$\gcd(a, n) = 1,$$

.i.e., it is pseduoprime to any base a, where gcd(a, n) = 1.

Example 4.5.

$$a^{560} \equiv 1 (\bmod 561)$$

for any integer a such that gcd(a, 561) = 1

$$a^2 \equiv 1(\text{mod}3) =) (a^2)^{280} = a^{560} \equiv 1(\text{mod}3) \quad \text{for all integer } a$$
$$a^{10} \equiv 1(\text{mod}11) \Rightarrow (a^{10})^{56} = a^{560} \equiv 1(\text{mod}11) \quad \text{for all integer } a$$
$$a^{16} \equiv 1(\text{mod}17) \Rightarrow (a^{16})^{35} = a^{560} \equiv 1(\text{mod}17) \quad \text{for all integer } a$$

$$\Rightarrow a^{560} \equiv 1(\text{mod}.11.13.17 = 561)$$

A simple characterization of Carmichael integer is given by the following lemma:

Lemma : A positive integer n is a Carmichael integer $\Leftrightarrow$ It is a product of distinct odd primes

$$n = p_1\, p_2 \cdots p_m$$

such that $p_i - 1 \mid n - 1$ for $1 \leq i \leq m$.

Proof: $n > 2$ since it is composite.

$$b^{n\text{-}1} \equiv 1(\text{mod } n)$$

for all positive integers b.There exist an integer a such that

$$\text{ord}_n a = \lambda(n).$$

Since $a^{n\text{-}1} \equiv 1(\text{mod } n)$,it follows that

$$\lambda(n) \mid n - 1.$$

$$n > 2 \Rightarrow \lambda(n) \text{ is even } \Rightarrow n \text{ is odd.}$$

Now, suppose that $\exists$ an odd prime p such that

$$p^k \mid n$$

for $k \geq 2$.Then

$$\lambda(p^k) = \phi(p^k) = p^{k\text{-}1}(p - 1) \mid \lambda(n)$$

$$\Rightarrow p^{k\text{-}1}(p - 1) \mid (n - 1) =) p \mid n - 1$$

contradiction.Thus,

$$n = p_1\, p_2 \cdots p_m,$$

where $p_1, p_2, \cdots, p_m$ are distinct odd primes. Since

$$\lambda(n) = \text{lcm }\{\phi\,(p_1) = p_1 - 1, \phi(p_2) = p_2 - 1,\ldots\ldots, \phi(p_m) = p_m - 1\},$$

obviously ,$p_i - 1 \mid \lambda(n)$ thus,

$$p_i - 1 \mid n - 1$$

for $1 \le i \le m$.

Let n be a product of distinct prime integers, i.e.,

$$n = p_1\, p_2 \cdots p_m$$

Let a be a positive integer which is relatively prime to n. Then

$$\gcd(a, p_i) = 1 \text{ for } 1 \le i \le m \Rightarrow$$

$$a^{p_i - 1} \equiv 1(\bmod p_i) \text{ for } 1 \le i \le m.$$

Since $p_i - 1 \mid n - 1$ for $1 \le i \le m$,

$$\exists \text{ integers } r_i \text{ for } 1 \le i \le m$$

such that

$$n - 1 = r_i(p_i - 1) \text{ for } 1 \le i \le m. \Rightarrow$$

$$a^{n-1} = (a^{p_i - 1})^{r_i} \equiv 1(\bmod p_i) \text{ for } 1 \le i \le m \Rightarrow$$

$$a^{n-1} \equiv 1(\bmod n).$$

But this means that n is a Carmichael integer.

Example 4.6. 561 is Carmichael integer since

$$561=3.11.17$$

and

$$2 \mid 560, 10 \mid 560, 16 \mid 560.$$

This one is shorter than the proof of the previous example.

Example 4.7. 1729 = 7.13.19 is Carmichael integer since

$$6 \mid 1728, 12 \mid 1728, 18 \mid 172$$

Example 4.8. $41041 = 7.11.13.41$ is Carmichael integer since

$$6 \mid 41040, 10 \mid 41040, 12 \mid 41040, 40 \mid 41040$$

a)$825265 = 5.7.17.19.73$

b)$321197185 = 5.19.23.29.37.137$

c)$5394826801 = 7.13.17.23.31.67.73$

d)$232250619601 = 7.11.13.17.31.37.73$

e)$9746347772161 = 7.11.13.17.19.31.37.41.641$

f)$1436697831295441 = 11.13.19.31.37.41.43.71.127$

g)$60977817398996785 = 5.7.17.19.23.37.53.73.79.89.233$

h)$7156857700403137441 = 11.13.17.19.29.37.41.43.61.97.109.127$.

Corollary :A Carmichael integer is a product of at least three distinct primes.

Proof: Suppose $n = p.q$, where p and q are distinct primes. Assume that $p < q$. By previous lemma

$$n - 1 \equiv 0(\text{mod}(q - 1))$$

But

$$n - 1 = pq - 1 = p(q - 1 + 1) - 1 = p(q - 1) + p - 1$$

which implies that $q - 1 \mid p - 1$. But it contradicts $p < q$.

4.1.5. Definition: Let n be an odd composite integer and a be an integer such that $\gcd(a, n) = 1$. If

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\bmod n),$$

where $\left(\frac{a}{p}\right)$ is the is the Jacobi symbol,then n is called an Euler pseduoprimeto the base a

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\bmod n),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Example 4.9. $n = 1105$ is an Euler pseduoprime to the base $a = 2$ since

$$2552 \equiv 1(\text{mod} 1105)$$

and

$$\left(\frac{2}{1105}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{13}\right)\left(\frac{2}{17}\right) = (-1)^{\frac{5^2-1}{8}}(-1)^{\frac{13^2-1}{8}}(-1)^{\frac{17^2-1}{8}}$$
$$= (1)^{3+21+36} = 1$$

Proposition : If n is an Euler pseduoprime to the base a, then it is also a pse- duoprime to the base a.

Proof :

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(\text{mod } n) \Rightarrow (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 (\text{mod } n)$$

which obviously implies that

$$a^{n-1} \equiv 1(\text{mod} n).$$

4.1.6. Definition: Let n be an integer with

$$n - 1 = 2^{\mathbf{r}},$$

where $\mathbf{r}$ is a nonnegative integer and s is an odd integer.If

$$a^s \equiv 1(\text{modn}) \text{ or } a^{s2^{\mathbf{j}}} \equiv -1(\text{mod} n)$$

for some $0 \leq \mathbf{j} \leq \mathbf{r} - 1$ for an integer a, then we say that n passes strong pseduoprime test to base a.

4.1.7 Definition: A composite integer n which passes the strong pseduoprime test for the base a is called a strong pseduoprime to the base a

Example 4.10. $n = 1105 \Rightarrow$

$$n\text{-}1 = 1104 = 2^4 69$$
$$2^{69} \equiv 967 \text{ (mod } 1105 \text{)}$$
$$2^{2.69} \equiv 259 \text{ (mod } 1105 \text{)}$$
$$2^{2^2.69} \equiv 781 \text{ (mod } 1105 \text{)}$$
$$2^{2^3.69} \equiv 1 \text{ (mod } 1105\text{)}$$

Therefore 1105 is not a strong pseduoprime to the base 2. Because we didn’**t** get

$$(-1)$$

one step before getting 1.

Example 4.11. $n = 15790321 \Rightarrow$

$$n - 1 = 15790320 = 2^4\, 986895$$
$$2^{986895} \equiv 128 (\text{mod} 15790321)$$

but

$$2^{2s} = 2^{2.986895} \equiv 16384 (\text{mod} 15790321)$$
$$2^{4s} = 2^{4.986895} \equiv -1 (\text{mod} 15790321)$$

which means that $n = 15790321$ passes strong pseduoprime test to base 2.

4.1.1. Theorem If p is a prime and p - a, then p passes strong pseduoprime test to base a.

Proof: $\text{p} - 1 = 2^{\mathbf{r}} s$. Let

$$b_{\text{k}} = a^{\frac{p-1}{2^k}} = a^{s 2^{r-k}} \quad \text{for } 0 \leq \text{k} \leq \text{r}$$
$$= a^{\text{p-1}} \equiv 1 \text{ (mod p)}$$
$$b_1^2 = b_0 \equiv 1 \text{ (mod p).}$$

So,

$$b_1 \equiv 1 \pmod{p} \text{ or } b_1 \equiv -1 \pmod{p}$$

If $b_1 \equiv 1 \pmod{p}$ then

$$b_2^2 \equiv b_1 \equiv 1 \pmod{p}.$$

Thus, $b_2 \equiv 1 \pmod{p}$ or $b_2 \equiv -1 \pmod{p}$. So if ..

$$b_o \equiv b_1 \equiv b_2 \equiv b_3 \equiv \ldots\ldots\ldots \equiv b_k \equiv 1 \pmod{p}$$

with $k < r$, then since $b_{k+1}^2 \equiv b_k \equiv -1 \pmod{p}$.

$$b_{k+1} \equiv 1 \pmod{p} \text{ or } b_{k+1} \equiv -1 \pmod{p}$$

Consequently, either

$$b_r \equiv 1 \pmod{p}$$

or $\exists$ k such that $0 \leq k \leq r$ and

$$b_k \equiv -1 \pmod{p}.$$

It means that p passes strong pseduoprime test to base a. The strong pseduoprime test to base a is stronger than Euler pseduoprime test to base a, as it can be seen in following proposition.

Proposition: If n is a strong pseduoprime to base a, then it is an Euler pseduo- prime to the base a.

Proof : Let

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots\ldots\ldots\ldots\ldots p_m^{k_m},$$

$n-1 = 2^{\mathbf{r}}s$, where s is odd integer and

$$a^S \equiv 1 (\text{mod} n) \text{ or } a^{S2^{\mathbf{j}}} \equiv -1$$

for some $0 \leq \mathbf{j} \leq \mathbf{r} - 1$.

case1:$a^S \equiv 1(\text{mod} n)$: Let a prime p divides n. Then

$$\text{ord}_p a \setminus s$$

since $a^S \equiv 1 (\mathrm{mod} p)$ which implies that

$$\mathrm{ord}_p\, a$$

is odd. But $\mathrm{ord}_p\, a$ also divides $p - 1$.Thus, **it** divides $p - 1$.Thus, it divides $\frac{p-1}{2}$ too. Therefore,

$$a^{\frac{p-1}{2}} \equiv 1 \ (\bmod\ n) \Rightarrow \left(\frac{a}{p}\right) = 1$$

by Euler's criterion. The Jacobi symbol is

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots\ldots p_m^{k_k}}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{k_i} = 1$$

$a^{\frac{n-1}{2}} = \left(a^8\right)^{2^{r-1}} \equiv 1$ (mod n). Thus ,

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) = 1$$

case2: $a^{s2^j} \equiv -1 (\mathrm{mod} n)$ forsome $0 \leq \mathbf{j} \leq \mathbf{r} - 1$: Again let a prime p divides n. Then

$$a^{s2^j} \equiv -1 (\mathrm{mod p}) \Rightarrow (a^{s2^j})^2 \equiv 1 (\mathrm{mod p}) \Rightarrow$$

$$a^{s2^{j+1}} \equiv 1 (\mathrm{mod p}) \Rightarrow \mathrm{ord}_p a \mid s2^{\mathbf{j}+\mathbf{1}} \text{ and } \mathrm{ord}_p a \ \backslash \ s2^j \Rightarrow \mathrm{ord}_p\, a = w2^{\mathbf{j}+\mathbf{1}},$$

,where w is an odd integer.Since

$$\mathrm{ord_p} a \mid \mathrm{p} - 1, 2^{\mathbf{j}+1} \mid \mathrm{p} - 1,$$

we have $\mathrm{p} = \mathrm{u}2^{\mathbf{j}+1} + 1$ for some integer u.

$$a^{\frac{ord_p a}{2}} \equiv -1 \ (\bmod\ p\ ) \Rightarrow \left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} = a^{\frac{ord_p a}{2}\left(\frac{p-1}{ord_p a}\right)} \equiv$$

$$(-1)^{\left(\frac{p-1}{ord_p a}\right)} = (-1)^{\frac{p-1}{w2^{j+1}}} = (-1)^{\frac{u}{w}} = (-1)^u$$

which implies that

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{m}\left(\frac{a}{p_i}\right)^{k_i} = \prod_{i=1}^{m}((-1)^{u_i})^{k_i} =$$

$$\prod_{i=1}^{m}(-1)^{u_i k_i} = (-1)^{k_1u_1+k_2u_2+.........+k_mu_m}$$

Now

$$n = p_1^{k_1}\, p_2^{k_2} \cdots p_m^{k_m} = (u_1 2^{j+1} + 1)^{k_1}\, (u_2 2^{j+1} + 1)^{k_2} \cdots (u_m 2^{j+1} + 1)^{k_m} \equiv$$

$$(1 + 2^{j+1} k_1 u_1)(1 + 2^{j+1} k_2 u_2) \cdots (1 + 2^{j+1} k_m u_m) (\text{mod } 2^{2j+2})$$

$$\equiv 1 + 2^{j+1}(k_1 u_1 + k_2 u_2 + \cdots + k_m u_m)(\text{mod } 2^{2j+2}) \Rightarrow$$

$$s2^{r-1} = \frac{n-1}{2} \equiv 2^j\, (k_1 u_1 + k_2 u_2 + \cdots + k_m u_m))(\text{mod } 2^{2j+2}) \Rightarrow$$

$$s2^{r-1-j} \equiv k_1 u_1 + k_2 u_2 + \cdots + k_m u_m (\text{mod } 2^{j+1})$$

and

$$a^{\frac{n-1}{2}} = \left(a^{s2^j}\right)^{2^{r-1-j}} \equiv ((-1)^s)^{2^{r-1-j}} = ((-1)^s)^{2^{r-1-j}} = (-1)^{k_1 u_1 + k_2 u_2 + \cdots + k_m u_m}$$

since $(a^{\frac{n-1}{2}})^2 \equiv 1$ (mod n) and $a^{s2^j} \equiv \left(\frac{a}{n}\right)$ (mod n). Thus

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(\text{mod} n)$$

which means that n is an Euler pseduoprime to the base a.

Remark : The converse is not true. We have seen that 1105 is an Euler pseduoprime to the base 2, but it is not strong pseduoprime to the base 2

Theorem 4.1.2. The Solovay-StrassenProbabilistic Primality Test:Let n be a positive integer. Select, at random, k integers less than n, and perform Euler pseduoprıme test on n for each of these bases. If any of these test fails, then n is composite. If n is composite, the probability that n passes all k tests is less than

$$\left(\frac{1}{2}\right)^k$$

Theorem 4.1.3. Rabin-Miller Probabilistic Primality Test:Let n be an integer. Select, at random, k different positive integers less than n, and perform strong pseduoprime test on n for each of these bases. If any of these test fails, then n is composite. If n is composite, the probability that n passes all k tests is less than

$$\left(\frac{1}{4}\right)^k$$

Of course, Rabin-Miller test is better than the Solovay-Strassen test

4.2. FACTORIZATION BY CONTINUED FRACTION

Let's see the generalization of Fermat factorization .in the following lemma.

Lemma : It is possible to factor n if $\exists$ positive integers x and y such that

$$x^2 \equiv y^2 \ (\text{mod } n)$$
$$0 < y < x < n, \text{and } x + y \neq n$$

Proof: The inequalities imply that n doesn't divide $(x - y)$ and doesn't divide $(x + y)$. Consequently

$$\gcd(n, x - y) \neq n, \gcd(n, x + y) \neq n$$
$$n \mid (x - y)(x + y) \Rightarrow \gcd(n, x - y) \neq 1$$

for otherwise, $n \mid x + y$ which is contradiction. By the same way
Hence

$$\gcd(n, x + y) \neq 1.$$

are proper divisors of n.

Example 4.10. $51^2 - 39^2 = 1080 \equiv 0 (\text{mod} 216).$

$$\gcd(216, 51 - 39) = 12, \gcd(216, 51 + 39) = 18$$

So 12 and 18 are factors of 1080.

Now, we can express the theorem on the factorization by means of continued fractions.

$$P_k^2 \equiv (-1)^{k+1} V_{k+1} (\mathrm{mod}\, n)$$

where pk and Vk+1 are defined. Suppose that k + 1 is even, and Vk+1
is a square, i.e.,

$$V_{k+1} = r^2$$

for some integer r. Then

$$P_k^2 \equiv r^2 (\mathrm{mod}\, n)$$

which we can use it for obtaining the factors of n. Therefore,it is enough to look at the terms with even indices in

$$\{V_k\}$$

which are squares.

Example 4.11. Let's factor 649 by continued fraction algorithm. Let

$$\alpha_0 = \sqrt{649} = \frac{0+\sqrt{649}}{1}.$$

Then

$$U_0 = 0,\ V_0 = 1,\ a_0 = \lfloor\sqrt{649}\rfloor = 25.\ \Rightarrow\ p_0 = 25,\ q_0 = 1.$$

So

$$p_0 = 25,\ q_0 = 1$$

$$U_1 = a_0 V_0 - U_0 = a_0 = 25,\ V_1 = \frac{649 - U_1^2}{V_0} = 649 - 25^2 = 24$$

$$\alpha_1 = \frac{U_1 + \sqrt{649}}{V_1} = \frac{25+\sqrt{649}}{24} = 2.103\ldots.$$

It implies that

$$a_1 = 2 \Rightarrow p_1 = 25.2 + 1 = 51,\ q_1 = 2$$

$$U_2 = a_1 V_1 - U_1 = 2.24 - 25 = 23,\ V_2 = \frac{649 - 23^2}{24} = 5$$

But 5 is not a square.

$$\alpha_2 = \frac{23+\sqrt{649}}{5} = 9.695 \ldots \Rightarrow a_2 = 9 \Rightarrow$$

$$p_2 = 9.51 + 25 = 484 = 535,\ q_2 = 9.2 + 1 = 19$$

$$U_3 = 9.5 - 23 = 22\ ,\ V_3 = \frac{649-22^2}{5} = 33$$

$$\alpha_3 = \frac{22+\sqrt{649}}{33} = 1.438 \ldots \Rightarrow a_3 = 1$$

$$\Rightarrow\ p_3 = 1.484 + 51\ ,\ q_3 = 1.19 + 2 = 21$$

$$U_4 = 1.33 - 22 = 11\ ,\ V_4 = \frac{649-11^2}{33} = 16 = 4^2$$

since

$$p_o = a_o, q_o = 1, p1 = a_O a_1 + 1, q_1 = a_1,$$

$$p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}$$

for $k \geq 2$. Consequently,

$$535^2 \equiv 4^2 (\text{mod } 649)$$

But

$$535 - 4 = 529 = 3^2.59 \text{ and } 535 + 4 = 539 = 7^2 11$$

$$\gcd(649, 3^2.59) = 59, \text{gacd}(649, 7^2 11) = 11$$

$$\Rightarrow\ 59.11 \mid 649.$$

In fact

$$649 = 59.11.$$

4.3. THE p-1 FACTORING ALGORITHM(POLLARD)

Let n be an odd composite integer and p be one of its unknown prime factor. Choose M such that it covers all small prime factors of $p - 1$ (Here, we assume that $p - 1$ has only small prime factors). Then,

$$2^{M!} \equiv 1 (\text{mod} p)$$

if $p-1 \mid M!$.

$$u = \gcd(2^{M!} - 1, n)$$

gives a nontrivial factorization of n if $u = 1$ and $u = n$.Here, the diffuculty is to find a good large M to find the solution. The method is succesful if n has a prime factor p such that $p-1$ has small prime factors.

Example 4.12. Let $n = 12657$ .Take $M = 3$.

$$2^{3!} - 1 = 2^6 - 1 = 63.$$
$$\gcd(63, 12657) = 3$$

Hence, 3 is a factor of 12657.In fact, $12657 = 3.4219$.

Example 4.13. Let $n = 34567$.

$$2^{1!} \equiv 2(\text{mod} 34567) \Rightarrow \gcd(2-1, 34567) = 1$$
$$2^{2!} \equiv 4(\text{mod} 34567) \Rightarrow \gcd(4-1, 34567) = 1$$
$$2^{3!} \equiv 64(\text{mod} 34567) \Rightarrow \gcd(64-1, 34567) = 1$$
$$2^{4!} \equiv 12221(\text{mod} 34567) \Rightarrow \gcd(12221-1, 34567) = 13$$

Hence $34567 = 13.2659$

Example 4.14. Let $n = 36287$

$$2^{1!} \equiv 2(\text{mod} 36287) \Rightarrow \gcd(2-1, 36287) = 1$$
$$2^{2!} \equiv 4(\text{mod} 36287) \Rightarrow \gcd(4-1, 36287) = 1$$
$$2^{3!} \equiv 64(\text{mod} 36287) \Rightarrow \gcd(64-1, 36287) = 1$$
$$2^{4!} \equiv 12622(\text{mod} 36287) \Rightarrow \gcd(12622-1, 36287) = 1$$
$$2^{5!} \equiv 34644(\text{mod} 36287) \Rightarrow \gcd(34644-1, 36287) = 1$$
$$2^{6!} \equiv 27347(\text{mod} 36287) \Rightarrow \gcd(27347-1, 36287) = 1$$
$$2^{7!} \equiv 25133(\text{mod} 36287) \Rightarrow \gcd(25133-1, 36287) = 1$$

$$2^{8!} \equiv 34505 (\mathrm{mod} 36287) \Rightarrow \gcd(34505 - 1, 36287) = 1$$

$$2^{9!} \equiv 5844 (\mathrm{mod} 36287) \Rightarrow \gcd(5844 - 1, 36287) = 1$$

$$2^{10!} \equiv 14473 (\mathrm{mod} 36287) \Rightarrow \gcd(14473 - 1, 36287) = 1$$

$$2^{11!} \equiv 18162 (\mathrm{mod} 36287) \Rightarrow \gcd(18162 - 1, 36287) = 1$$

$$2^{12!} \equiv 6589 (\mathrm{mod} 36287) \Rightarrow \gcd(6589 - 1, 36287) = 1$$

$$2^{13!} \equiv 18734 (\mathrm{mod} 36287) \Rightarrow \gcd(18734 - 1, 36287) = 131.$$

Thus, 131 is a factor of 36287. In fact,36287 = 131.277.

Remark : To find the least positive remainder of $2^{M!}$ modulo n, we can do the following computations

$$s_2 \equiv 2^2 \bmod n \text{ , } s_3 \equiv s_2^3 \bmod n \text{ , } s_4 \equiv s_3^4 \bmod n \text{ , } \ldots\ldots\ldots 2^{M!} = s_M \equiv s_{M-1}^M \bmod n$$

since modular exponention can be done efficiently.

Remark: Later, we will see the elliptic factorization method which is the advanced form of p − 1 factoring algorithm.

4.4. Rho-Method(POLLARD):

Again, let n be an odd composite integer and p be one of its unknown prime fac- tor. Choose a polynomial with integer coefficients $f(x)$ of degree at least 2. For instance

,

$$f(x) = x^2 + 1.$$

Select a particular value $x = x_o$ at random. Calculate

$$x_1 = f(x_o), x_2 = f(x_1) = f(f(x_o)),$$

$$x_i = f(x_{i-1}),$$

Stop at M th step, where

$$x_M \not\equiv x_K (\bmod n) \text{ and } x_M \equiv x_K (\bmod p) \text{ for some } 1 \le k \le M$$

Example 4.15 : $n = 1041$. Let $x_0 = 2$ and $f(x) = x^2 + 1$.

$$x_1 = 5 \Rightarrow 5 \not\equiv 2 (\text{mod}1041) \text{ and } 5 - 2 = 3 \mid 1041 \Rightarrow$$

$$1041 = 3.347$$

Example 4.16:. $n = 36287$. Let's select $x = x_0 = 2$ and $f(x) = x^2 + 1$

$$x_1 = 5 \Rightarrow 5 \not\equiv 2 (\text{mod } 36287) \text{ and } 5 - 2 = 3 \text{ doesn't divide } 36287$$

$$x_2 = 26 \Rightarrow 26 \not\equiv 2 (\text{mod } 36287), \gcd(24, 36287) = 1$$

$$26 \not\equiv 5 (\text{mod } 36287), \gcd(21, 36287) =$$

$$x_3 = 677 \Rightarrow 677 \not\equiv 2 (\text{mod } 36287), \gcd(675, 36287) =$$

$$677 \not\equiv 5 (\text{mod } 36287), \gcd(672, 36287) = 1$$

$$677 \not\equiv 26 (\text{mod } 36287), \gcd(651, 36287) = 1$$

$$x_4 = 458330 \equiv 22886 (\text{mod } 36287) \Rightarrow$$

$$22886 = 2 (\text{mod } 36287), \gcd(22884, 36287) = 1$$

$$22886 = 5 (\text{mod } 36287), \gcd(22881, 36287) = 1$$

$$22886 = 26 (\text{mod } 36287), \gcd(22860, 36287) = 1$$

$$22886 = 677 (\text{mod } 36287), \gcd(22209, 36287) = 1$$

$$x_5 = 210066388901 \equiv 2439 (\text{mod } 36287) \Rightarrow$$

$$2439 = 2 (\text{mod } 36287), \gcd(2437, 36287) = 1$$

$$2439 = 5 (\text{mod } 36287), \gcd(2434, 36287) = 1$$

$$2439 = 677 (\text{mod } 36287), \gcd(1762, 36287) = 1$$

$$2439 = 22886 (\text{mod } 36287), \gcd(20447, 36287) = 1$$

$$x_6 = 33941 \Rightarrow 33941 = 2 (\text{mod } 36287), \gcd(33939, 36287) = 1$$

$$33941 = 5 (\text{mod } 36287), \gcd(33936, 36287) = 1$$

$$33941 = 26 (\text{mod } 36287), \gcd(33915, 36287) = 1$$

$$33941 = 677 (\text{mod } 36287), \gcd(33264, 36287) = 1$$

$$33941 = 22886 (\text{mod } 36287), \gcd(11055, 36287) = 1$$

$$33941 = 2439 (\text{mod } 36287), \gcd(31502, 36287) = 1$$

$$x_7 = 24380 \Rightarrow 24380 = 2 (\text{mod } 36287), \gcd(24378, 36287) = 1$$

$$24380 = 5 (\text{mod } 36287), \gcd(24375, 36287) = 1$$

$$24380 = 26 (\text{mod } 36287), \gcd(24354, 36287) = 1$$

$24380 \equiv 677 \pmod{36287}, \gcd(23703, 36287) = 1$

$24380 \equiv 2288 \pmod{36287}, \gcd(1494, 36287) = 1$

$24380 \equiv 2439 \pmod{36287}, \gcd(21941, 36287) = 1$

$24380 \equiv 33941 \pmod{36287}, \gcd(9561, 36287) = 1$

$x_8 = 3341 \Rightarrow 3341 \equiv 2 \pmod{36287}, \gcd(3339, 36287) = 1$

$3341 \equiv 5 \pmod{36287}, \gcd(3336, 36287) = 1$

$3341 \equiv 26 \pmod{36287}, \gcd(3315, 36287) = 1$

$3341 \equiv 677 \pmod{36287}, \gcd(2664, 36287) = 1$

$3341 \equiv 22886 \pmod{36287}, \gcd(20222, 36287) = 1$

$3341 \equiv 2439 \pmod{36287}, \gcd(902, 36287) = 1$

$3341 \equiv 33941 \pmod{36287}, \gcd(30600, 36287) = 1$

$3341 \equiv 24380 \pmod{36287}, \gcd(21039, 36287) = 1$

$x_9 = 22173 \Rightarrow 22173 \equiv 2 \pmod{36287}, \gcd(22171, 36287) = 1$

$22173 \equiv 5 \pmod{36287}, \gcd(22168, 36287) = 1$

$22173 \equiv 677 \pmod{36287}, \gcd(21496, 36287) = 1$

$22173 \equiv 22886 \pmod{36287}, \gcd(713, 36287) = 1$

$22173 \equiv 2439 \pmod{36287}, \gcd(19734, 36287) = 1$

$22173 \equiv 33941 \pmod{36287}, \gcd(11764, 36287) = 1$

$22173 \equiv 24380 \pmod{36287}, \gcd(2207, 36287) = 1$

$22173 \equiv 3341 \pmod{36287}, \gcd(18832, 36287) = 1$

$x_{10} = 25654 \Rightarrow 25654 \equiv 2 \pmod{36287}, \gcd(25652, 36287) = 1$

$25654 \equiv 5 \pmod{36287}, \gcd(25649, 36287) = 1$

$25654 \equiv 26 \pmod{36287}, \gcd(25628, 36287) = 1$

$25654 \equiv 677 \pmod{36287}, \gcd(24977, 36287) = 1$

$25654 \equiv 22886 \pmod{36287}, \gcd(2768, 36287) = 1$

$25654 \equiv 2439 \pmod{36287}, \gcd(23215, 36287) = 1$

$25654 \equiv 33941 \pmod{36287}, \gcd(8287, 36287) = 1$

$25654 \equiv 24380 \pmod{36287}, \gcd(1274, 36287) = 1$

$25654 \equiv 3341 \pmod{36287}, \gcd(22313, 36287) = 1$

$25654 \equiv 22173 \pmod{36287}, \gcd(3481, 36287) = 1$

$x_{11} = 26685 \Rightarrow 26685 \equiv 2 \pmod{36287}, \gcd(26683, 36287) = 1$

$26685 \equiv 5 \pmod{36287}, \gcd(26680, 36287) = 1$

$$26685 = 26 (\text{mod } 36287), \gcd(26659, 36287) = 1$$
$$26685 = 677 (\text{mod } 36287), \gcd(26008, 36287) = 1$$
$$26685 = 22886 (\text{mod } 36287), \gcd(3799, 36287) = 131$$

Thus ,131 is a factor of 36287.In fact,36287 = 131.277.

4.5. FACTOR BASE METHOD:

Let n be an integer.We calculate

$$x^2 - n$$

for several values of x,i.e.,for $a_o, a_1, \ldots, a_m$.Suppose that we find

$$a_{i_1}, a_{i_2}, \ldots, a_{i_k}$$

among them, such that

$$(a_{i_1}^2 - n)(a_{i_2}^2 - n), \ldots\ldots, (a_{i_k}^2 - n) \equiv b^2 (\text{mod } n).$$

for some integer b. Then, we can obtain the factors of n since

$$a_{i_1}^2 a_{i_2}^2 \ldots\ldots a_{i_k}^2 \equiv b^2 (\text{mod } n).$$

We select the values of x such that $x^2 - n$ is a small integer. Thus, it has small prime factors. Therefore, we may select x in the interval

$$\sqrt{n} - M < x < \sqrt{n} + M$$

for some integer M. Then, we try to factorize $x^2 - n$ for which x is in the interval.We select a set of primes

$$\wp = \{ -1 , p_1, p_2, \ldots\ldots\ldots, p_k \}$$

,called a factor base satisfying p < B.B is an integer depending on the size of n. -1 is also included in $\wp$.

Construct the following table

$\wp$	$\sqrt{n} - M < x < \sqrt{n} + M$	$x^2 - n$
p_1	x_1	$x_1^2 - n = p_1^{a_{11}} p_2^{a_{21}} \ldots\ldots p_k^{a_{k1}}$

p_2	x_2	$x_2^2 - n = p_1^{a_{12}} p_2^{a_{22}} \ldots\ldots p_k^{a_{k2}}$
.	.	
.	.	
.	.	
p_k		
	x_u	$x_u^2 - n = p_1^{a_{1u}} p_2^{a_{2u}} \ldots\ldots p_k^{a_{ku}}$

Select those x whose prime factors are contained in $\wp$. Now, we have to find integer

$$h_1, h_2, \ldots\ldots h_u$$

which are 0 or 1 such that

$$(p_1^{a_{11}} p_2^{a_{21}} \ldots\ldots p_k^{a_{k1}})^{h_1} (p_1^{a_{12}} p_2^{a_{22}} \ldots\ldots p_k^{a_{k2}})^{h_2} \ldots\ldots (p_1^{a_{1u}} p_2^{a_{2u}} \ldots\ldots p_k^{a_{ku}})^{h_u}$$

is a perfect square.Obviously, it holds if and only if

$$a_{11} h_1 + a_{12} h_2 + \cdots + a_{1u} h_u \equiv 0 \pmod 2$$
$$a_{21} h_1 + a_{22} h_2 + \cdots + a_{2u} h_u \equiv 0 \pmod 2$$

.

$$a_{k1} h_1 + a_{k2} h_2 + \cdots + a_{ku} h_u \equiv 0 \pmod 2$$

if and only if

$$\begin{pmatrix} a_{11} & a_{12} \ldots\ldots a_{1u} \\ a_{21} & a_{22} \ldots\ldots a_{2u} \\ \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots \\ a_{k1} & a_{k2} \ldots\ldots a_{ku} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ . \\ . \\ . \\ h_u \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}$$

So, the vector $(h_1, h_2, \ldots, h_u)$ can be found from row-reduced echelon matrix by apply- ing the elementary row operations to the matrix

$$\begin{pmatrix} a_{11} \bmod 2 & a_{12}.\mathrm{mod} & a_{1u} \bmod 2 \\ a_{21} \bmod 2 & a_{22} \bmod 2 & a_{2u} \bmod 2 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{k1} \bmod 2 & a_{k2}.\mathrm{mod}\,2 & a_{ku} \bmod 2 \end{pmatrix}$$

Example 4.18. $n = 4633$.Let $\wp = \{2, 3, 5\}$

$\sqrt{4633} = 68.07$………………..Let $38 \le x \le 98$. By Maple define

$$H(x) = x^2 - 4633$$

$$H = \begin{pmatrix} 38 \\ 39 \\ 40 \\ 41 \\ 42 \\ 43 \\ 44 \\ 45 \\ 46 \\ 47 \\ 48 \\ 49 \\ 50 \\ 51 \\ 52 \\ 53 \\ 54 \\ 55 \\ 56 \\ 57 \\ 58 \\ 59 \\ 60 \\ 61 \\ 62 \\ 63 \\ 64 \\ 65 \end{pmatrix} = \begin{pmatrix} -3189 \\ -3112 \\ -3033 \\ -2952 \\ -2869 \\ -2784 \\ -2697 \\ -2608 \\ -2517 \\ -2424 \\ -2329 \\ -2232 \\ -2133 \\ -2032 \\ -1929 \\ -1824 \\ -1717 \\ -1608 \\ -1497 \\ -1384 \\ -1269 \\ -1152 \\ -1033 \\ -912 \\ -789 \\ -664 \\ -537 \\ -408 \end{pmatrix} = \begin{pmatrix} -3 \times 1063 \\ -2^3 389 \\ -3^2 337 \\ -2^3 3^2 41 \\ -19 \times 151 \\ -2^5 3 \times 29 \\ -3 \times 29 \times 31 \\ -2^4 163 \\ -3 \times 839 \\ -2^3 3 \times 101 \\ -17 \times 137 \\ -2^3 3^2 31 \\ -3^3 79 \\ -2^4 127 \\ -3 \times 643 \\ -2^5 3 \times 19 \\ -17 \times 101 \\ -2^3 3 \times 67 \\ -3 \times 499 \\ -2^3 173 \\ -3^3 47 \\ -2^7 3^2 \\ -1033 \\ -2^4 3 \times 19 \\ -3 \times 263 \\ -2^3 83 \\ -3 \times 179 \\ -2^3 3 \times 17 \end{pmatrix} =$$

$$H = \begin{pmatrix} 66 \\ 67 \\ 68 \\ 69 \\ 70 \\ 71 \\ 72 \\ 73 \\ 74 \\ 75 \\ 76 \\ 77 \\ 78 \\ 79 \\ 80 \\ 81 \\ 82 \\ 83 \\ 84 \\ 85 \\ 86 \\ 87 \\ 88 \\ 89 \\ 90 \\ 91 \\ 92 \\ 93 \\ 94 \\ 95 \\ 96 \\ 97 \end{pmatrix} = \begin{pmatrix} -277 \\ -144 \\ -9 \\ 128 \\ 267 \\ 408 \\ 551 \\ 696 \\ 843 \\ 992 \\ 1143 \\ 1296 \\ 1451 \\ 1608 \\ 1767 \\ 1928 \\ 2091 \\ 2256 \\ 2423 \\ 2592 \\ 2763 \\ 2936 \\ 3111 \\ 3288 \\ 3467 \\ 3648 \\ 3831 \\ 4016 \\ 4203 \\ 4392 \\ 4583 \\ 4776 \end{pmatrix} = \begin{pmatrix} -277 \\ -2^4 3^2 \\ -3^2 \\ 2^7 \\ 3 \times 89 \\ 2^3 3 \times 17 \\ 19 \times 29 \\ 2^3 3 \times 29 \\ 3 \times 281 \\ 2^5 31 \\ 3^2 127 \\ 2^4 3^4 \\ 1451 \\ 2^3 3 \times 67 \\ 3 \times 69 \times 31 \\ 2^3 241 \\ 3 \times 17 \times 41 \\ 2^4 3 \times 47 \\ 2423 \\ 2^5 3^4 \\ 3^2 307 \\ 2^3 367 \\ 3 \times 17 \times 61 \\ 2^3 3 \times 137 \\ 3467 \\ 2^6 3 \times 19 \\ 3 \times 1277 \\ 2^4 251 \\ 3^2 467 \\ 2^3 3^2 61 \\ 4583 \\ 2^3 3 \times 199 \end{pmatrix} =$$

We select those which are factorizable only by means of $\{2, 3, 5\}$:

$$x_1^2 = 59 \equiv -1152 = -2\ .3\ .5\ \ (\text{mod}4633)$$

$$x_2^2 = 67 \equiv -144 = -2\ 3\ 5\ \ (\text{mod}4633)$$

$$x_3^2 = 68 \equiv -9 = -2\ 3\ 5\ \ (\text{mod}4633)$$

$$x_4^2 = 69 \equiv 128 = 2\ 3\ 5\ \ (\text{mod}4633)$$

$$x_5^2 = 85 \equiv 2592 = 2\ 3\ 5\ \ (\text{mod}4633)$$

$$x_6^2 = = \ 96 \equiv -50 = -2\ 3\ 5\ \ (\text{mod}4633)$$

Therefore, the matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 7 & 4 & 0 & 7 & 5 & 1 \\ 2 & 2 & 2 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} (\text{mod } 2) =$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

It is row equivalent to

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The corresponding solutions are

$$\begin{pmatrix} h_1 = (h_4 + h_5 + h_6) \\ h_2 = (h_3 + h_4 + h_5) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

for free h_3, h_4, h_5, h_6.In particular ,

$$\begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

is a solution, i.e.,

$$68^2 69^2 96^2 = (-2^0 3^2 5^0)\ (2^7 3^0 5^0)\ (-2^1 3^0 5^2) = (-1)^2 2^8 3^2 5^2$$

$$\gcd(\ 68.69.96 - 2^4 35, 4633) = 113$$

Thus

$$4633 = 41.113$$

CHAPTER 5

CONCLUSION

In Chapter 1, I explained the history and development of cryptography.

In Chapter 2, I exposed finite field, I have included and explained prime finite field and boundary finite field in details. Extensive exercises are included for arithmetic of finite field.

In Chapter 3, Elliptic Curves defined on finite field has been covered with examples. I exposed the Diffie-Hellman Key Exchange, El – Gamal, Massey – Omura Encryption.

In Chapter 4, I exposed Primality Test.

Some maple commands have been written for finite field arithmetic.

REFERENCES

- Adams : W.W.Adams,L.J.Goldstein,*Introduction to Number Theory*, Prentice- Hall,Inc.

- A.G.Konheim,*Cryptography,A Primer*,John Wiley and Sons,1981

- A.K.Lensta ,*İnteger factoring.Designs,Codes and cryptography*,2000

- A.Salomaa,*Public-Key Cryptography*,Springer-Verlag,1990

- Adams, William W. and Goldstein, Larry Joel, *Introduction to Number Theory*, Prentice-Hall, New Jersey, 1976.

- Agrawal : M.Agrawal,N..Kayal and N.Saxena, *Prımes is in P,* Annals of Mathematics,2004

- Apostd, Tom M., Introduction to Analytic Number Theory, Springer-Verlag, United States of America, 1976.

- B.Schneıer,*Applied Cryptography,Protogols,Algorithms and Source Code in C* ,Second Edition.John Wiley and Sons,1995

- Cox : David A.Cox,*Primes of the Form*,New York,1989

- D.Welsh ,*Codes and Cryptography.*Oxford Science Publications,1988.

- DBoneh.,*The decision Diffie-Hellman problem.Lecture Notes in Computer Science,*1423

- DigitalSignature *Standard.Federal Informatıon Processing Standard Publication*,1994

- Fraleigh, John B., *Abstract Algebra*, Addison-Wesley, 1999.

- G.Brassard and P.Bratley,*Fundamentals of Algorithmics.Prentice* Hall,1995

- Gardner, Martin, *Codes, Ciphers and Secret Writing*, Dover Publications, Inc. New York, 1984.

- H.C.Williams,*A modification of the RSA public-key encryptıon procedure,IEEE Transactıons on Information Theory*,1980

- I.Blake,G.Seroussı And N.Smart,*Elliptic Curves in Cyptography*.Cambridge Unıversity Press,1999

- J.C.A.Van Der Lubbe,Basic *Methods of Cryptography.Cambridge* ,1988

- J.K.Gıbson,*Discrete Logarithm hash function that is collision free and one way*,IEE Proceedings-E,1991

- J.M.Delaurentıs,*A further Weakness in the common modulus protocol for the RSA cryptosystem*,1984

- Janus : Gerald J.Janusz ,Algebraic Number Fields,American Mathematical Society 1996

- K.Kurosawa,T.Ito and M.Takeuchı.*Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number*.Cryptologia,1988

- Kendirli ,Barış *Introductıon to Number Theory with Cryptographıc Applıcatıons,*Fatih Unıversıty ,2006

- K.Lam,"Decomposition of prime ideals in the extensions",2004-Dynamical Systems and Applications,GBS Publishers&Distributors(India)

- Koblitz, Neal, *A Course in Number Theory and Cryptograph*, 2nd ed., Springer-Verlog, New York, 1994.

- Koblitz, Neal, *Algebraic Aspects of Cryptography*, Springer-Verlag New York, 1999
.
- M.Bellare,J.Kılıan and P.Rogaway,*The securıty of the cıipher block chaining message authentication code.Journal of Computer andSystem sciences*,2000

- Manjul : M.Bhargava*,"Higher composition laws I,Annals of Mathematics*,159(2004) 217-250

- N.Koblitz,A. Menezes and S.Vanstone.*The state of elliptic curve cryptography.Designs,Codes and Cryptography,2000*

- Niedereiter, Harald and Lidl, Rudolf, *Introduction to finite fields and their applications*, Revised ed., Cambridge University Press, Great Britain, 1994

- P.Garett,*Making,Breaking Codes:An Intoductıon To Cryptography,*Prentice Hall,2001

- R.Lıdl and H.Nıderreiter,*Finite fields,Second Edition*.Cambrıdge University Press,1997

- Rosen : K.H.Rosen,Elementary Number Theory,Addison Wesley.Amsterdam,1999.

- Rosen, Kenneth H., *Elementary Number Theory and its applications*, 4th ed., Addision Wesley Longman, United State of America, 2000.

- Schneir, Bruce, *Applied Cryptography*, 2nd ed., John Willey & Sons, Inc., Canada, 1996.

- Secure Hash Standard.*Federal Information Processing Standard Publication*,2000

- Spillman, Richard J., *Classical and Contemporary Cryptology*, Pearson Prentice Hall, New Jersey, 2005.

- Stallings, William, *Cryptography and Network Security*, 3rd ed., Printice Hall, New Jersey, 2003.

- Stinson, Douglas R., *Cryptography Theory and Practice*, 3nd ed., Chapman & Hall / CRC, United States of America, 2002.

- T.Beth,*Cryptography Proceedings,Lecture Notes in Computer Science*,1985

- T.ElGamal,*A public key cryptosystem and a signature scheme based on discrete logarıthms*,1985

- U.Maurer and S.Wolf,*The Diffie-Hellman Protocol.Designs,Codes and Crytography,*2000

- W.Alexı,B.Chor,O.Goldreıch and C.P.Schnorr.*RSA and Rabin functıons:certain parts are as hard as the whole.Sıam Journal on computing,*1988

- Washington : L.C.Washington,Elliptic Curves,Chapman&Hall/CRC.Boca Raton 2003

- Washington, Lawrance C., *Elliptic Curves Number Theory and Cryptography*, Chapman & Hall / CRC, USA,2003.

- W.Stallings,*Principles andPractice,second Edition* Prentice Hall,1999

- W.Davies.*Advanced in cryptography-Eurocrypt'91*,Springer-Verlag,1991