FACTORIZATION METHODS FOR CRYPTOGRAPHY

by

Bikem PAMUKÇU

August 2006

FACTORIZATION METHODS FOR CRYPTOGRAPHY

by

Bikem PAMUKÇU

A thesis submitted to

the Graduate Institute of Sciences and Engineering

of

Fatih University

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

FACTORIZATION METHOD FOR CRYPTOGRAPHY

Bikem PAMUKÇU

M. S. Thesis - Mathematics
August 2006

Supervisor: Prof. Dr. Barış KENDİRLİ

ABSTRACT

First, I have included and explained some number theoretical facts in the beginning. Then RSA has been covered with examples in details. I explained factorization methods. I gave the maple algorithms which are useful for computing.

Keywords: RSA, factorization methods, public key cryptography and maple algorithms.

KRİPTOGRAFİ İÇİN FAKTORİZASYON METODLARI

Bikem PAMUKÇU

Yüksek Lisans Tezi – Matematik
Ağustos 2006

Tez Yöneticisi: Prof. Dr. Barış KENDİRLİ

ÖZ

Başlangıçta, sayılar teorisini ana hatlarıyla açıkladım. Sonra, RSA detaylı olarak örneklerle gösterilmiştir. Devamında, faktorizasyon metodlarını açıkladım. Hesaplamaları yaparken kolaylık sağlaması için maple algoritmaları yazılmıştır.

Anahtar Kelimeler: RSA, faktorizasyon ve maple algoritmaları.

DEDICATION

To my parents, Görkem,Mehmet
and Barış Kendirli

ACKNOWLEDGEMENT

I am glad to take this opportunity to thank firstly my supervisor Prof. Dr. Barış KENDİRLİ 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, Bülent KÖKLÜCE and İbrahim 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

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF SYMBOLS AND ABBREVIATIONS

SYMBOL / ABBREVIATION

$n \mid m$	:	Divides
$n \nmid m$	:	Does not divide
$a \equiv b \pmod{n}$	:	Congruent
$a \neq b \pmod{n}$	:	Incongruent
$\phi(n)$	:	Euler's phi-function
gcd (a,b)	:	Greatest common divisor
Σ	:	Sum
C	:	Ciphertext
P	:	Plaintext

CHAPTER 1

INTRODUCTION

The Greek words “Kryptos”, hidden, and “Graphen”, written, form the word “Cryptography”. Symmetric key cryptosystems have been used by Egyptian since early ages. There are two kinds of classical cryptosystems; transposition and substitution ciphers. In transposition ciphers elements in plaintext are rearrenged. In substitution ciphers elements in plaintext are mapped into another. Encryption and decrypiton keys are the same in symmetric key cryptosystems. They are faster, but not secure. Public key cryptography has been used since early 1970s. Asymmetric key cryptography depends on discrete logarithm and factorization large integers. Encryption and decryption keys are different each other. This makes this system secure and important for 21th century. Diffie-Hellman, ElGamal, Massey-Omura, Elliptic curve and Hyperelliptic curve cryptosystems are based on discrete logarithm. RSA depends on factorization. Elliptic curve cryptography challenges to RSA. Moreover, public key cryptosystems are slower than symmetric key cryptosystems. Hence, nowadays especially data is encrypted in modern symmetric keys by using DES, AES etc. Keys of classical cryptosystems are encrypted by performing public key cryptosystems.

I explained number theory in chapter 2. I give the definition of divisor, Euclidean algorithm, Chinese Remainder Theorem etc. In chapter 3 I described factoring algorithm wıth examples. In chapter 4 I exposed RSA cryptosystem in detail. In chapter 5 primality testing is defined.

In the future, I will continue to work on Elliptic Curve and Hyperelliptic Curve Cryptosystems.

CHAPTER 2

NUMBER THEORY

2.1. DIVISIBILITY

2.1.1. Divisors and divisibility

A factor of an integer m is an integer k which divides m, denoted by $k \mid m$. Otherwise it is denoted by $k \nmid m$. Divisors can be negative or positive. 1 and -1 are factors of every integer. Moreover, every integer is a divisior of zero and itself.

2.1.2. Properties of divisibility

Let a,b,c,d be any integers.

1) $a \mid b$ and $a \mid c$ imply $a \mid (b+c)$
2) $a \mid b$ and $b \mid c$ imply $a \mid c$
3) $a \mid b$ and $b \mid a$ imply $a=b$ or $a= -b$
4) $a \mid b$ implies $a \mid bd$
5) $a \mid b$ implies $a \mid -b$, $-a \mid b$, $-a \mid -b$
6) $a \mid b$ implies $da \mid db$ for all $d \in$z
7) $a \mid b$ and $d \mid a$ imply $d \mid b$
8) $a \mid bc$ and gcd (a,b) = 1 imply $a \mid c$

The command in mapple is divisors (n).

For example;

```
> divisors (20); {1,2,4,5,10,20}
```

Assume that $m>1$ if the only proper divisor of m is 1, then it is called to a prime number.

For example; 2,3,5,7,11,................................ are prime numbers.

The command in maple is prime (n) which demonstrates whether n is prime or not.

For example;

```
> is prime (19);
                true
> is prime (20);
                false
```

The maple command next prime (n) returns the smallest prime which is larger than n. Furthermore, the maple command pseduoprime (n) returns the largest prime which is less than n.

For example;

```
> next prime (22);
                23
> next prime (29);
                31
> next prime (37);
                41
```

A positive integer m is said to be composite number if and only if m has a positive divisor other than 1 or itself.

2.2. THE GREATEST COMMON DIVISOR

A positive integer d is called common divisor of a and b if $d \mid a$ and $d \mid b$. If the largest divisor of a and b is d, then d is said to be the greatest common divisor.

The maple command igcd (x_1, x_2, x_3,.............) calculates the greatest common divisor of integers.

For example;

```
> igcd (10,6,8);
                2
```

If the greatest common divisor of a and b equals to 1, then a and b are called relatively prime integers. We calculate GCD by Euclidean algorithm.

Example 2.1: This example uses the Euclidean algorithm to find the greatest common factor between 36 and 123.

3 is the last nonzero remainder.

$$3 = 5\ (123) - 17\ (36)$$

$$123 = 3\ (36) + 15$$

$$36 = 2\ (15) + 6$$

$$6 = 2\ (3) + 0$$

2.3. PROCEDURE OF EUCLIDEAN ALGORITHM

Assume that a and b are positive integers $b \neq 0$ and $a>b$. Let $a=r_0$, $b=r_1$, q_1 be quotient and r_2 be remainder

$$r_0 = r_1 \,.\, q_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 \,.\, q_2 + r_3 \qquad 0 \le r_3 < r_2$$

$$r_2 = r_3 \,.\, q_3 + r_4 \qquad 0 \le r_4 < r_3$$

$$r_3 = r_4 \,.\, q_4 + r_5 \qquad 0 \le r_5 < r_4$$

.

.

.

$$r_{k-2} = r_{k-1} \,.\, q_{k-1} + r_k \qquad 0 \le r_k < r_{k-1}$$

$$r_{k-1} = r_k \,.\, q_k$$

The greatest common divisor of a and b equals to r_k.

The maple command igcdex (*a, b, 's', 't'*) gives the greatest common divisor of a and b. The commands s; and t; give values of s and t.

For example;

```
> igcdex (15,7, 's','t');
                              1
> s; t;
                              1
                             -2
```

Example2.2. Find the gcd of 81 and 57 by Euclidean algorithm.

$$81 = 1\,(57) + 24$$

$$57 = 2\,(24) + 9$$

$$24 = 2\,(9) + 6$$

$$9 = 1\,(6) + 3$$

$$6 = 2\,(3) + 0$$

Then

3 = 9 – 1 (6)

└──→ 24-2 (9) s_0;

3 = 9-1 (24-2(9)) = 3 (9) – 1 (24)

└──→ 57-2 (24) s_0;

3 = 3 (57-2(24)) – 1 (24) = 3 (57) – 7(24)

└──→ 81-1 (57) giving us;

3 = 3 (57) – 7 (81-1 (57)) = 10 (57) – 7 (81)

p = -7 and s = 10

2.4. EULER'S THEOREM

2.4.1. Theorem (Euler's Theorem): Let n be a positive integer. The Euler phi-function ϕ (n) is defined to be the number of integers in the range $0 < \phi(n) < n$ where $\phi(n)$ is coprime to n. $\phi(n)$ gives the size of multiplicative group of integers modulo n.

Euler product formula is written as;

$$\phi(n) = n \underset{p|n}{\pi} \left(1-\frac{1}{p}\right) \qquad \text{with distinct primes } p.$$

Let $n = p^{k1} . p_2^{k2} . p_3^{k3}$ .... p_i^{ki} with distinct primes pr

$$\phi(n) = (p_1^{-1})\ p_1^{k_1-1}\ (p_2^{-1})\ p_2^{k2-1} \ \ldots\ldots\ldots\ldots\ldots\ (pi\text{-}1)\ p_i^{ki-1}$$

Theorem:

$$\sum_{\phi|n} \phi(d) = n \qquad \text{where } d \mid n \text{ and } n \in Z^+$$

2.5. CONGRUENCES

a is called congruent to be modulo m if m divides a-b, $\forall\ a, b \in Z$ and $m \in Z^+$

It is denoted by $a \equiv b$ (mod m). On the other hand, a is incongruent to b modulo m, denoted by $a \equiv b$ (mod m)

The command in maple is a mod m

For example;

```
> 2625 mod 13;
                    12
```

2.5.1. Properties of Congruences:

1) $a \equiv a$ (mod m)

2) If $a \equiv b$ (mod m), then $b \equiv a$ (mod m)

3) If $a \equiv b$ (mod m) and $b \equiv c$ (mod m) imply $a \equiv c$ (mod m)

4) $a^\ell \equiv b^\ell$ (mod m), where $\ell > 0$, for $a \equiv b$ (mod m)

5) If $ac \equiv bc$ (mod m) and gcd $(c,m) = d$, then $a \equiv b$ (mod m/d)

6) $a \equiv b (\text{mod } m)$ c^{-1} is a arithmetic inverse of c modulo m

if and only if gcd(c,m)=1 and $a.c^{-1} \equiv b.c^{-1} (\text{mod } m)$

2.6. CHINESE REMAINDER THEOREM

Suppose that $N=n_1,\ n_2,\ n_3,$ .... n_k where $n_1,\ n_2,\ n_3$............. n_k are pairwise relatively prime positive integers that is if $i \neq j$, then gcd $(ni,\ nj) = 1$

Let $a_1,\ a_2,\ a_3$ .... a_k be integers. There exists an integer x such that

$$x \equiv a_1 \ (\text{mod } n_1)$$
$$x \equiv a_2 \ (\text{mod } n_2)$$
$$x \equiv a_3 \ (\text{mod } n_3)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r \ (\text{mod } n_r)$$

has a unique solution modulo N.

Proof: Define $N_i = \dfrac{N}{n_i}$ for $1 \leq i \leq k$ as follows:

$N_1 = N/n_1$. There exists M_1 such that $N_1\ M_1 \equiv 1 \ (\text{mod } n_1)$

$N_2 = N/n_2$. There exists M_2 such that $N_2\ M_2 \equiv 1 \ (\text{mod } n_1)$

$N_3 = N/n_3$. There exists M_3 such that $N_3\ M_3 \equiv 1 \ (\text{mod } n_1)$

.

.

.

$N_K = N/n_K$. There exists M_K such that $N_K\ M_K \equiv 1 \ (\text{mod } n_K)$

Next, compute

$$x = \sum_{i=1}^{k} a_i\ N_i\ M_i \qquad \text{mod } N$$

Therefore,

$$x \equiv a_1 N_1 M_1 \equiv a_1 \bmod n_1$$

$$x \equiv a_2 N_2 M_2 \equiv a_2 \bmod n_2$$

$$x \equiv a_3 N_3 M_3 \equiv a_3 \bmod n_3$$

.

.

.

$$x \equiv a_k N_k M_k \equiv a_k \bmod n_k$$

The maple command of chinese remainder theorem is chrem (U, m).
The list of modulo m are pairwise coprime positive integers. The list of U and M is the some size n such that.

U – list [$U_1, U_2, U_3 .... U_n$] and M – list [$m_1, m_2, m_3, ... m_n$]

For example;

```
> chrem ( [1,2], [5,7]);
                       16
```

Example 2.3. Suppose r=2, m_1 = 5 and m_2 = 3, so M = 17. Then the function x has the function following values:

x (0) = (0,0)	x (1) = (1,1)	x (2) = (2,2)
x (3) = (3,0)	x (4) = (4,1)	x (5) = (0,2)
x (6) = (1,0)	x (7) = (2,1)	x (8) = (3,2)
x (9) = (4,0)	x (10) = (0,1)	x (11) = (1,2)
x (12) = (2,0)	x (13) = (3,1)	x (14) = (4,2)
x (15) = (0,0)	x (16) = (1,1)	

Example 2.4. Find the smallest multiple of 10 which has remainder 2 when divided by 3, and remainder 3 when divided by 7.

We are looking for a number which satisfies the congruences, x=2 (mod3), x=3 (mod 7), x=0 (mod 2) and x=0 (mod 5). Since 2,3,5,7 are all relatively prime pairs, the Chinese Remainder Theorem that there is a unique solution modulo:

$$2.3.5.7 = 210$$

Now we will calculate M_i's and Y_i's as follows:

$$M_2 = 210 / 2 = 105;\ Y_2 = (105)^{-1} \pmod 2 = 1$$
$$M_3 = 210 / 3 = 70;\ Y_3 = (70)^{-1} \pmod 3 = 1$$
$$M_5 = 210 / 5 = 42;\ Y_5 = (42)^{-1} \pmod 5 = 3$$
$$M_7 = 210 / 7 = 30;\ Y_7 = (30)^{-1} \pmod 7 = 4$$
$$X = 0\ .\ (M_2\ Y_2) + 2\ (M_3\ Y_3) + 0\ (M_5\ Y_5) + 3\ (M_7\ Y_7)$$
$$0 + 2\ (70)\ .(1) + 0 + 3\ (30)\ .(4)$$
$$0 + 140 + 0 + 360$$
$$140 + 360 = 500$$
$$500 \equiv 80 \pmod{210}$$

2.6.1. Theorem: Assume that g is a multiplicative group element of order n. The order of g divides n.

2.6.2. Theorem:İf gcd $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$

2.7. FERMAT'S LITTLE THEOREM

Suppose p is prime and $p \nmid a$. Then,

$$a^{p-1} \equiv 1 \pmod p$$

2.7.1 Theorem: Z_p^* is a cyclic group if p is prime.

β whose order is p-1 modulo p is said to be a primitive element modulo p.

$$Z_p^* = \{\text{“}\beta\text{”} : 0 \leq i \leq p-2\}$$

p is prime and β is a primitive element modulo p.

gcd $(p-1, i) = 1$ $\phi\ (p-1)$ gives the number of primitive elements modulo p.

α is itself a primitive element if and only if $\alpha = \beta_i$ in the range $0 \leq i \leq p-2$

Example 2.5. : Suppose p=14. The results proven establish that there are exactly four primitive elements modulo 14. First, by computing succesive powers of 2, we can verify that 2 is a primitive element modulo 14.

2^0 mod 14 = 1

2^1 mod 14 = 2

2^2 mod 14 = 4

2^3 mod 14 = 8

2^4 mod 14 = 2

2^5 mod 14 = 4

2^6 mod 14 = 8

2^7 mod 14 = 2

2^8 mod 14 = 4

2^9 mod 14 = 8

2^{10} mod 14 = 2

2^{11} mod 14 = 4

2^{12} mod 14 = 8

2^{13} mod 14 = 2

The element 2^i is primitive if and only if gcd (i, 13) = 1, i.e. if and only if

i = 1,5,7,11.

2.7.2 Theorem: Assume that p is prime and $\beta \in Zp^*$. If $\beta^{(p-1)|q} \neq 1 \pmod p$, then β is a primitive element modulo p. (q is prime such that $q\,/(p-1)$)

CHAPTER 3

FACTORING ALGORITHMS

3.1. THE POLLARD *p*-1 ALGORITHM

This algorithm is proposed by John M. Pollard in 1974. Fermat's little theorem is the main idea for this method.

That is for any prime number p; that you select and another number a

$$a^{(p-1)} \equiv 1 \pmod{p}$$

This equal to; $2^x \equiv c \pmod{n}$

$$2^x \equiv c + kn \ (k \text{ integer})$$

3.1.1. Methods of (*p*-1) algorithm

1) We pick a number m

2) pick a number $1 < a < m$. For example $a = 2$

3) pick a number 2. for example $s = 2$

4) if gcd $(a,m) \neq 1$ then the factor is found.

5) When $s = a\ell \pmod{m}$

6) When d=GCD $(s-1, m)$

7) We apply the division algorithm to find if d is an element of m. There are two options. If the answer is yes, then the factor is found. If the answer is no, then we swich a and or 1 and go back to step 4.

Example 3.1.2 :

Suppose n = 15770708441. If we select B = 180 we find that α= 11620221425 and d is computed to be 135979. In fact, the complete factorization of n into primes is;

15770708441 = 135979 . 115979

In this example, the factorization succeeds because 135978 has only "small" prime factors:

135978 = 2.3.131.173

$B \geq 173$ then $135979 \mid \beta!$

3.2. THE POLLARD RHO ALGORITHM

John M. Pollard proposed another factorization algorithm that improves over trial division in 1975.

An iteration of the form

$x_j = f(x_{j-1}) \pmod{n}$

we are looking for two distinct values x_i, $x_j \in x$, then gcd $(x_j - x_i, n) > 1$ for all $i<j$

if $x_i \equiv x_j \pmod{p}$

$f(x_i) \equiv f(x_j) \pmod{p}$ and $x_{j+1} = f(x_i)$

$x_{j+1} = f(x_j)$

Therefore similarly $x_{j+1} \bmod p = f(x_j) \bmod p$

$i < j$ $x_i \equiv x_j \pmod{p}$

3.2.1. Methods of Rho Algorithm

1) Select a number m, you wish to factor.

2) Choose any two numbers (mod m) x_i and x_j

3) If the differences x_i-x_j is equal to 0 in modulo *m*, then gcd (x-y,*m*) then we have a factor.

4) If the differences isn't 0 then we go back to step two.

3.2.2 Example :

Let n = 1387 x_1 =2 and f(x) =x^2-1. We obtain x_1=2 x_2=3 x_3=8, x_4=63, x_5=1194, x_6=1186

gcd (x_2 - x_1, 1387) = gcd (1,1387) = 1

gcd (x_4 – x_2, 1387) = gcd (60,1387) = 1

gcd (x_6 – x_3, 1387) = gcd (1178,1387) = 19

19 is the factor of 1387. Sequence is 3 and a non-trivial factor is obtained after 3 comparisons and GCD calculations.

3.2.3 Definition= Let n be an odd composıte ınteger and let p be a prıme ınteger s.t $p \mid n$.

Take a polynomıal f(x) of degree 2(at least) with integer coefficients. Then let x_0 be a random integer.

Calculate x_1=f(x_0)
Calculate x_2=f(x_1)
Calculate x_3=f(x_2)

Stop at k th place x_k=f(x_{k-1}) where $x_k \not\equiv x_i \pmod n$ for $0 \le i < k-1$

3.2.4 Example :

n=1041

x_0=2 f(x)=x^2+1

x_1=f(x_0)=f(2)=2^2+1=5

x_1-x_0=5-2=3

of course $x_1 \equiv x_0 \pmod 3$

Since $5 \equiv 2 \pmod 3$

g.c.d(x_1-x_0,1041)

g.c.d(3,1041)=3

$\Rightarrow 1041 = 3.347$

$x_1 = x_1{}^1 + k_1.n \qquad \Leftarrow x^1 \equiv f(x_0) \pmod{n}$

$x_2 = x_2{}^1 + k_2.n \qquad \Leftarrow x_2{}^1 \equiv f(x_1) \pmod{n}$

.
.
.
.
.
.
.

$x_p = x_{p1} + k.n \qquad \Leftarrow x_p \not\equiv x_i \pmod{n} \Leftrightarrow x_p \not\equiv x_i \pmod{n}$

$\Leftarrow x_p{}^1 \equiv x_i \pmod{m} \Leftrightarrow x_p \equiv x_i \pmod{m}$

3.2.5 Example :

N=36287 $x_0=2$ $f(x)=x^2+1$

$X_1=2^2+1=5$ $\Rightarrow 5 \not\equiv 2 \pmod{36287}$ and gcd (5-2,36287)=1

$X_2=5^2+1=26$ $\Rightarrow 26 \not\equiv 2 \pmod{36287}$ and gcd (26-2,36287)=1

$\Rightarrow 26 \not\equiv 5 \pmod{36287}$ and gcd (26-5,36287)=1

$X_3=26^2+1=677$ $\Rightarrow 677 \not\equiv 2 \pmod{36287}$ and gcd (677-2,36287)=1

$\Rightarrow 677 \not\equiv 5 \pmod{36287}$ and gcd (677-5,36287)=1

$\Rightarrow 677 \not\equiv 26 \pmod{36287}$ and gcd (677-26,36287)=1

.
.
.
.
.
.

$X_7=24380$ $\Rightarrow 24380 \not\equiv 2 \pmod{36287}$ and gcd(24380-2,36287)=1

$\Rightarrow 24380 \not\equiv 5 \pmod{36287}$

$\Rightarrow 24380 \not\equiv 26 \pmod{36287}$

$\Rightarrow 24380 \not\equiv 677 \pmod{36287}$

$\Rightarrow 24380 \not\equiv 22886 \pmod{36287}$

$\Rightarrow 24380 \not\equiv 2439 \pmod{36287}$

$\Rightarrow 24380 \not\equiv 33941 \pmod{36287}$

3.3. DIXON'S RANDOM SQUARES ALGORITHM

Congruence of square is the base of this method. It works very well on parallel processors for each processor can be managed on it's own random r_k.

If x doesn't equal y in modulo n, then square of x doesn't equal square of y. Therefore n doesn't divide x's difference from y and it's sum.

$x \neq \mp y \pmod{n}$ such that $x^2 \equiv y^2 \pmod{n}$. Then

$$n \mid (x-y) \,.\, (x+y)$$

We choose any number r, square it (mod m), factor it to find out if the number is square. If it is square then the root be different from r as a result we have two numbers which are congruent mod (m).

3.3.1 Example :

The three vectors a_1, a_2, a_3 are follows:

$a_1 = (1, 0, 0, 1, 0, 1)$

$a_2 = (0, 1, 1, 0, 0, 0)$

$a_3 = (1, 1, 1, 1, 0, 1)$

$a_1+a_2+a_3 = (0, 0, 0, 0, 0, 0) \pmod 2$

3.4. ELLIPTIC CURVE FACTORIZATION

In the 80's Victor Miller and Neal Koblitz produced (ECC). Elliptic curve cryptography is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. In the elliptic curve (x,y) are the answers to the form

$y^2 = x^3 + AX + B$ together with the point at infinity (0)

For applications to cryptography we consider finite fields of *q* elements. For the equation $y^2 = x^3 + AX + B$ we write E, and for the set of points (x,y) with the point 0, with coordination in the field *F-q*

The set of points on an elliptic curve forms a group under a certain addition rule. The point 0 is the identity element of the group.

Given a point P = (x,y) and a positive integer *n* we define;

$n.P = P + P + P + \dots\dots\dots + P$ (*n* times)

The order of a point P = (x,y) is the smallest positive integer n such that $n.P = 0$

Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as, Lenstra elliptic curve factorization, but this use of elliptic curves is not usually referred to as "elliptic curve cryptography".

3.5 FACTOR BASE METHOD

Let n be an integer. We calculate

$$x^2 - n$$

for several values of x, i.e.,for $a_0, a_1, \dots, a_m$. Suppose that we find

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

among them, such that

$$(a_{i_1}^2 - n)(a_{i_2}^2 - n), \dots\dots, (a_{i_k}^2 - n) \equiv b^2 \pmod{n}.$$

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

$$a_{i_1}^2 a_{i_2}^2 \dots\dots a_{i_k}^2 \equiv b^2 \pmod{n}.$$

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

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

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_u	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

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

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 applying the elementary row operations to the matrix

$$\begin{pmatrix} a_{11} \bmod 2 & a_{12} \bmod 2 & a_{1u} \bmod 2 \\ a_{21} \bmod 2 & a_{22} \bmod 2 & a_{2u} \bmod 2 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{k1} \bmod 2 & a_{k2} \bmod 2 & a_{ku} \bmod 2 \end{pmatrix}$$

Example 3.6 $n = 4633$.Let $\wp = \{2, 3, 5\}$

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

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

$$\begin{pmatrix} 38 \\ 39 \\ \\ \\ \end{pmatrix} \quad \begin{pmatrix} -3189 \\ -3112 \\ \\ \\ \end{pmatrix} \quad \begin{pmatrix} -3 \times 1063 \\ -2^3 389 \\ \\ \\ \end{pmatrix}$$

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

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

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

$$x_1^2 = 59 \equiv -1152 = -2.3.5 \pmod{4633}$$

$$x_2^2 = 67 \equiv -144 = -2\ 3\ 5 \pmod{4633}$$

$$x_3^2 = 68 \equiv -9 = -2\ 3\ 5 \pmod{4633}$$

$$x_4^2 = 69 \equiv 128 = 2\ 3\ 5 \pmod{4633}$$

$$x_5^2 = 85 \equiv 2592 = 2\ 3\ 5 \pmod{4633}$$

$$x_6^2 = 96 \equiv -50 = -2\ 3\ 5 \pmod{4633}$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 7 & 4 & 0 & 7 & 5 & 1 \\ 2 & 2 & 2 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \pmod{2} =$$

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

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 $h3, h4, h5, h6$. 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 4

PUBLIC KEY CRYPTOGRAPHIC SYSTEM DEPENDS ON FACTORIZATION

4.1. RSA

Nowadays, RSA is the most popular public key cryptosystem depended on large integers RSA was found in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. Let plaintext message units be blocks of k letters and ciphertext message units be block of ℓ letters ($k<\ell$). First Alice and Bob agree upon a N- letter alphabet. Bob generates to distinct large prime integers p and q. Then Bob calculates $n=p.q$. n is in the interval (N^k, N^ℓ).

p, $p \in Z/N$z. We obtain k and ℓ by computing

$$k \leq [\log N^n] < \ell$$

The command in maple to compute k and ℓ is as follows;

```
> k: = round (evalf (log [N] (n) ))
> ℓ : k + 1;
```

Next, Bob calculates (p-1). (q-1) which equals to ϕ (n)

The command in maple to compute ϕ (n) is phi (n);

Then Bob chooses a secret integer e, which is coprime to $\phi(n)$. e is between 1 and $\phi(n)$. Also e is said to be public. The pair (n,e) is enciphering key. Bob makes (n,e) public and p,q secret. Alice converts her message into numerical equivalence P. The encryption transformation is;

$C \equiv P^e \pmod{n}$ where $0 \leq P \leq N^k -1$

The maple command to compute ciphertext is;

```
> c: p ☋^ ℓ (mod n);
```

Then Alice send ciphertext to Bob. Bob computes the decryption exponent d by using the equation below.

$$d \equiv e^{-1} \pmod{\phi(n)}$$

The maple commond to calculate d is

```
> d: (1/e) mod ϕ (n)
```

Bob decipheries the ciphertext c by solving the equation

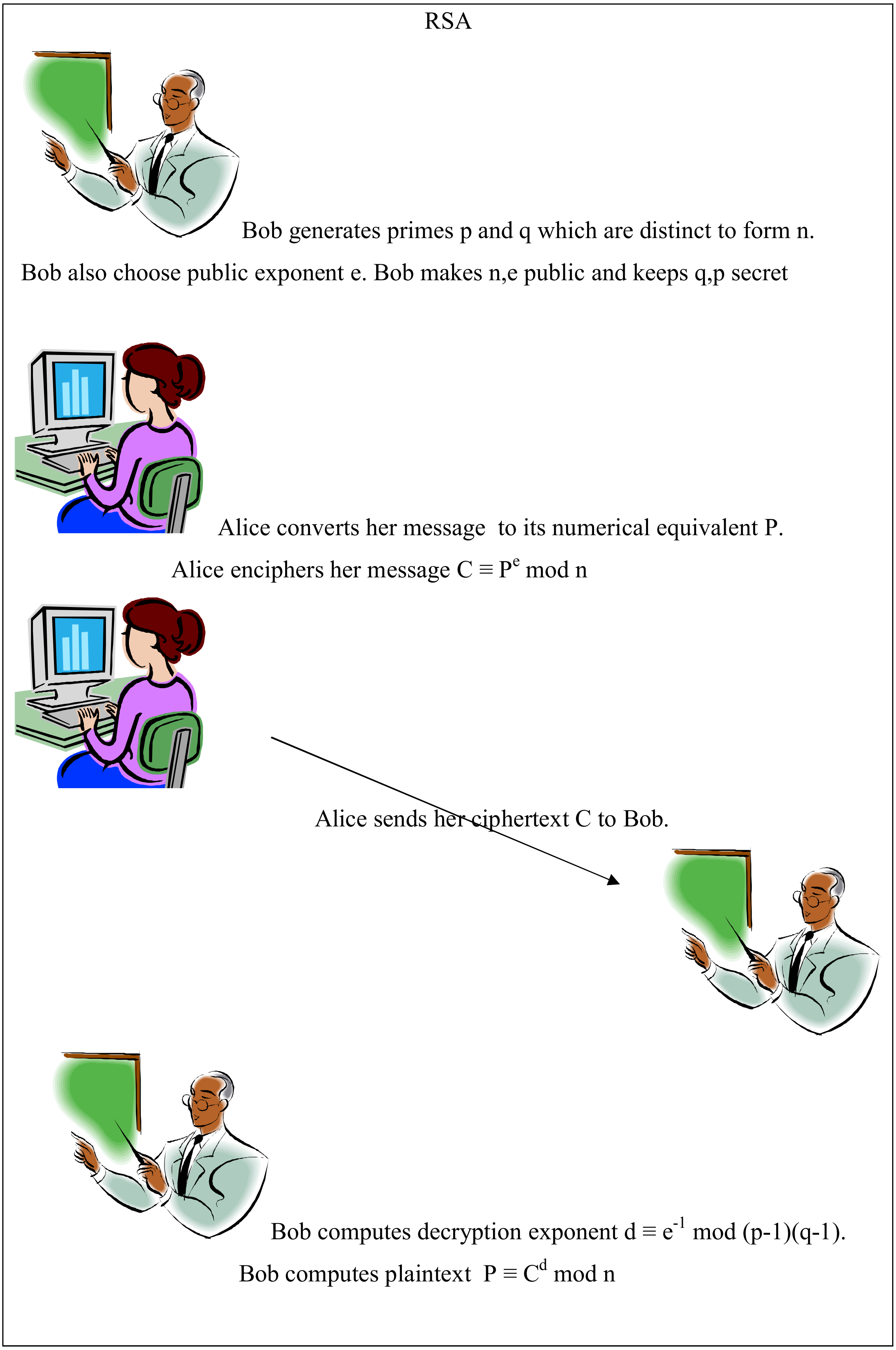
$$P \equiv C^{d} \equiv (P^{e})^{d} \equiv P^{ed} \pmod{n}$$

This works as ed-1 is a multiple of $\phi(n)$, $ed - 1 = k.\phi(n)$

$$C^{d} \equiv P^{ed} \equiv P^{1+k\phi(n)} \equiv \mathrm{P'}.P^{k\phi(n)} \equiv P(1)^{k} \equiv P \pmod{n}$$

Encryption and decryption transformations are

$$Z/Nz \text{ to } \mathrm{Z}/Nz$$



4.2 Figure of RSA

3.4.1 Example :

Plaintext and ciphertext letters are writen in Turkish letter alphabet written in 29 – letter. Plaintext message block is 2. And ciphertext message block ℓ is 3. My plaintext is “danger”

$e = 1009$

$p = 23$

$q = 101$

$n = p.q = 23.101 = 2323$

$\phi\,(n) = (p\text{-}1).\,(q\text{-}1) = 22.100 = 2200$

$d = 689$

“danger”

Table 4.3 Turkish Letter Alphabet

a	b	c	ç	d	e	f	g	ğ	h	ı	I	J	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

“da” = 0+4.29 = 116

$C_1 = 116^{1009} \pmod{2323} = 1772$

“ng” = 7 + 16 . 29 = 471

$C_2 = 471^{1009} \pmod{2323} = 1372$

“er” = 20 + 5 .29 = 165

$C_3 = 165^{1009} \pmod{2323} = 1297$

Then we will find it ciphertext;

$C_1 = 1772 = 2 \,.\, 29^2 + 3 \,.\, 29 + 3$ = “cçç”

$C_2 = 1372 = 1 \,.\, 29^2 + 18 \,.\, 29 + 9$ = “böh”

$C_3 = 1297 = 1 \,.\, 29^2 + 15 \,.\, 29 + 21$ = “bms”

The ciphertext is “CÇÇBÖHBMS”

3.4.2 Example : Plaintext message units are digraphs and ciphertext message units are trigraphs. In both plaintext and ciphertext, 26-letter alphabet is used. My ciphertext is;

"ADSCIOASTBFDBZZ"

Enciphering key (n,e) is (2257,133)

First convert ciphertext blocks to their numerical equivalence.

C_1 = "ADS" = $18 + 3 . 26 + 0 . 26^2 = 96$
C_2 = "CIO" = $14 + 8 . 26 + 2 . 26^2 = 1574$
C_3 = "AST" = $19 + 18 . 26 + 0 . 26^2 = 487$
C_4 = "BFD" = $3 + 5 . 26 + 1 . 26^2 = 809$
C_5 = "BZZ" = $25 + 25 . 26 + 1 . 26^2 = 1351$

First we compute $d \equiv e^{-1} \pmod{\phi(n)}$

$n = p . q$

$p = 61$ and $q = 37$

$n = p.q = 61.37 = 2257$

$\phi(n) = (p-1) . (q-1)$

$\phi(n) = (61-1) . (37-1)$

$60.36 = 2160$

$d = 877 \pmod{2160}$

$P_1 = 96^{877} \pmod{2257} = 17 = 17 + 0 . 26$ = "ar"
$P_2 = 1574^{877} \pmod{2257} = 446 = 4 + 17 . 26$ = re"
$P_3 = 487^{877} \pmod{2257} = 487 = 19 + 18 . 26$ = "st"
$P_4 = 809^{877} \pmod{2257} = 320 = 8 + 12 . 26$ = ".mi"
$P_5 = 1351^{877} \pmod{2257} = 264 = 4 + 10 . 26$ "ke"

The plaintexts is "arrestmike"

CHAPTER 5

PRIMALITY TESTING

5.1 PRIMALITY TESTING

In settings up the RSA Cryptosystem,it is necessary to generate large''random prımes .

5.1.1 Definition: Suppose p is an odd prime and a is an integer. a is defined to be a quadratic residue modulo p if $a \not\equiv 0 \pmod{p}$ and the congruence $y^2 \equiv a \pmod{p}$ has a solution y € Z_P. a is defined to be a quadratic non-residue modulo p if $a \not\equiv 0 \pmod{p}$ and a is not a quadratıc residue modulo p.

Example 5.1: In Z_{11}, we have that $1^2=1$, $2^2=4$, $3^2=9$, $4^2=5$, $5^2=3$, $6^2=3$, $7^2=5$, $8^2=9$, $9^2=4$, and $(10)^2=1$.
Therefore the quadratic residues modulo 11 are 1,3,4,5 and 9, and the quadratic non-residues modulo 11 are 2,6,7,8 and 10.

5.1.1 Theorem: Suppose that p is an odd prime and a is quadratic residue modulo p. Then there exists y € Z_P^* such that $y^2 \equiv a \pmod{p}$. Clearly, $(-y)^2 \equiv a \pmod{p}$, and $y \not\equiv y \pmod{p}$ because p is odd. Now consider the quadratic congruence $x^2-a \equiv 0 \pmod{p}$. This congruence can be factored as

$$(x-y).(x+y) \equiv 0 \pmod{p},$$

which is the same thing as saying that $p \mid (x-y).(x+y)$. Now, because p is prime, it follows that $p \mid (x-y)$ or $p \mid (x+y)$. In other words, $x \equiv \pm y \pmod{p}$, and we conculude that there are exactly two solutions (modulo p) to the congruence $x^2-a \equiv 0 \pmod{p}$. Moreover, these two solutions are negatives of each other modulo p.

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

5.1.3 Definition : A number n passes the pseudoprime test to base a if

$$a^n \equiv a \pmod{n}.$$

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

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

$$a^n \equiv a \pmod{n},$$

then n is called a pseudoprime to the base

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

$$a^n \equiv a \pmod{n} \Leftrightarrow a^{n-1} \equiv 1 \pmod{n}$$

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

$$a^n \equiv a \pmod{n}$$

by $a^\star$.

We multiply both sides of

$$a^{n-1} \equiv 1 \pmod{n}$$

by a.

Example 5.2. For instance

$$2^{340} \equiv 1 \pmod{341}$$

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

Example 5.3:

$$3^{90} \equiv 1 \pmod{91} = 7.13$$

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

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

$$a^{n-1} \equiv 1 \pmod{n}$$

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 5.4:

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

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

$$a^2 \equiv 1(\text{mod } 3) \Rightarrow (a^2)^{280} = a^{560} \equiv 1(\text{mod } 3) \text{ for all integer } a$$
$$a^{10} \equiv 1(\text{mod } 11) \Rightarrow (a^{10})^{56} = a^{560} \equiv 1(\text{mod } 11) \text{ for all integer } a$$
$$a^{16} \equiv 1(\text{mod } 17) \Rightarrow (a^{16})^{35} = a^{560} \equiv 1(\text{mod } 17) \text{ for all integer } a$$
$$\Rightarrow a^{560} \equiv 1(\text{mod}.11.13.17 = 561)$$

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.

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

for all positive integers b. $\exists$ an integer a such that

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

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

$$\lambda(n) \mid n - 1.$$
$$n > 2 \Rightarrow \lambda(n) \text{ is even } \Rightarrow n \text{ is odd.}$$

Now, suppose that there exist an odd prime p such that

$$p^k \mid n$$

for $k \geq 2$. Then

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

contradiction. Thus,

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

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

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

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 $1 \le i \le m$,

There exist integers r_i 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 5.5 :1729 = 7.13.19 is Carmichael integer since

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

Example 5.6: 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 $p < q$.

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

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

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

We know that if p is an odd prime and a is an integer not divisible by p, then

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

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

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

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

5.1.7 Definition: Let n be an integer with

$$n - 1 = 2^r,$$

where r is a nonnegative integer and s is an odd integer. If

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

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

5.1.8 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 5.7: $n = 15790321 \Rightarrow$

$$n - 1 = 15790320 = 2^4 986895$$

$$2^{986895} \equiv 128(\text{mod } 15790321)$$

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.

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

Proof: $p - 1 = 2^r s$. Let

$$b_k = a^{\frac{p-1}{2^k}} = a^{s2^{r-k}} \quad \text{for } 0 \le k \le r$$

$$= a^{p-1} \equiv 1 \pmod{p}$$

$$b_1^2 = b_0 \equiv 1 \pmod{p}.$$

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 ..

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

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 $0 \le k \le r$ 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 pseduoprime to the base a

Proof : Let

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

$n - 1 = 2^r s$, where s is odd integer and

$$a^S \equiv 1 (\text{mod } n) \text{ or } a^{S^{2j}} \equiv -1$$

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

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

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

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

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: $a^{S2^j} \equiv -1(\text{mod n})$ for some $0 \leq \mathbf{j} \leq \mathbf{r} - 1$: Again let a prime p divides n. Then

$$a^{S2^j} \equiv -1(\text{mod p}) \Rightarrow (a^{S2^j})^2 \equiv 1(\text{mod p}) \Rightarrow$$

$$a^{S2^{j+1}} \equiv 1(\text{mod p}) \Rightarrow \text{ord}_p a \mid s2^{j+1} \text{ and } \text{ord}_p a \setminus s2^j \Rightarrow \text{ord}_p\, a = w2^{j+1},$$

,where w is an odd integer.Since

$$\text{ord}_p\, a \mid p - 1, 2^{j+1} \mid p - 1,$$

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

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

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

which implies that

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

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

Now

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

$$\equiv (1 + 2^{j+1}k_1u_1)(1 + 2^{j+1}k_2u_2)\cdots(1 + 2^{j+1}k_mu_m) \pmod{2^{2j+2}}$$

$$\equiv 1 + 2^{j+1}(k_1u_1 + k_2u_2 + \cdots + k_mu_m) \pmod{2^{2j+2}} \Rightarrow$$

$$s.2^{r-1} = \frac{n-1}{2} \equiv 2^j (k_1u_1 + k_2u_2 + \cdots + k_mu_m)) \pmod{2^{2j+2}} \Rightarrow$$

$$s2^{r-1-j} \equiv k_1u_1 + k_2u_2 + \cdots + k_mu_m \pmod{2^{j+1}}$$

and

$$a^{\frac{n-1}{2}} = \left(a^{s2^j}\right)^{2^{r-1-j}} \equiv ((-1)^s)^{2^{r-1-j}} = ((-1)^s)^{2^{r-1-j}} = (-1)^{k_1u_1+k_2u_2+\cdots+k_mu_m}$$

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

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

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

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

Theorem 5.1.10: The Solovay-Strassen Probabilistic 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 5.1.11: 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

5.2. FACTORIZATION BY CONTINUED FRACTION

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

Lemma : It is possible to factor n if there exist positive integers x and y such that

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

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 5.1: $51^2 - 39^2 = 1080 \equiv 0 (\text{mod } 216)$.

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

So 12 and 18 are factors of 1080.

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

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

where p_k and V_{k+1} are defined. Suppose that $k + 1$ is even, and V_{k+1}
is a square, i.e.,

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

for some integer r. Then

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

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

$$\{Vk\}$$

which are squares.

Example 5.2: 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.

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

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

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

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

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

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

since

$$p_0 = a_0, q_0 = 1, p_1 = a_0 a1 + 1, q_1 = a_1,$$

$$p_k = a_k p_k - 1 + p_k - 2, q_k = a_k q_k - 1 + q_k - 2$$

for $k \geq 2$. Consequently,

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

But

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

$$\gcd(649, 3^2.59) = 59, \gcd(649, 7^2 11) = 11$$
$$\Rightarrow 59.11 \mid 649.$$

In fact

$$649 = 59.11.$$

5.3 AGRAWAL-KAYAL-SAXENA PRIMALITY TESTING

Now I want to explain this primality test. It is also a nice applications of what we have learned until now. First we need some lemmas:

Lemma : Let a be an integer and p be a positive integer. Suppose that a is relatively prime to p. Then p is prime if and only if

$$(x + a)^p \equiv (x^p + a)(\text{mod } p)$$

Proof: For $0 < i < p$, the coefficient of x^i in

$$(x + a)^p - (x^p + a)(\text{mod p})$$

is $\binom{p}{i} a^p - i$ and $p \mid \binom{p}{i}$ Therefore

$$(x + a)^p - (x^p + a) \equiv 0(\text{mod } p).$$

Conversely, let q be a prime which divides p and let $q^k \,||\, p$, then q^k does not divide

$$\binom{p}{q}$$

Obviously, a^{p-q} is relatively prime to q^k since a is relatively prime to p. Thus,

$$p \text{ doesn't divide } \binom{p}{q} a^{p-q}$$

Lemma :1. Let p and r be prime integers, $p \neq r$. Let $h(x)$ be any factor of the polynomial

$$x^r - 1 \in Fp\,[x].$$

If $m \equiv k(\text{mod } r)$, then

$$x^m \equiv x^k \ (\text{mod } h(x))$$

2.The order of [x] in

$$\mathrm{F}p\,[\mathrm{x}]/ < h(\mathrm{x}) >$$

is r and

$$\frac{x^r - 1}{x - 1}$$

is product of irreducible polynomials of degree $\mathrm{ord}_r\ p$.

Proof: 1.Let $m = n.r + k$. Then

$$\mathrm{x}^{nr+k} - \mathrm{x}^k = \mathrm{x}^k(\mathrm{x}^{nr} - 1) = \mathrm{x}^k\ (\mathrm{x} - 1)(\mathrm{x}^{r(n-1)} + \cdots + 1).$$

Thus,

$$h(\mathrm{x}) \mid \mathrm{x}^{nr+k} - \mathrm{x}^k$$

2.Let $d = \mathrm{ord}_r p$ and $h(\mathrm{x})$ be an irreducible factor of

$$\frac{x^r - 1}{x - 1},$$

with deg(h) = k. Then,

$$\mathrm{F}p\,[\mathrm{x}]/ < h(\mathrm{x}) >$$

is a field of pk elements. Let $g(\mathrm{x})$ be a generator of

$$\mathrm{F}p\,[\mathrm{x}]/ < h(\mathrm{x}) > \setminus \{0\}$$

Then,

$$g(\mathrm{x})^p \equiv g(\mathrm{x}^p)(\mathrm{mod}\ p)$$

$$\Rightarrow g(\mathrm{x})^{p^d} \equiv g(\mathrm{x}^{p^d})(\mathrm{mod}\ p).$$

Since $p^d \equiv 1(\mathrm{mod}\ r)$, by the first part of the lemma we have

$$\mathrm{x}^{p^d} \equiv \mathrm{x}(\mathrm{mod}\ h(\mathrm{x})).$$

Thus,

$$g(\mathrm{x}^{p^d}) \equiv g(\mathrm{x})(\mathrm{mod}\ h(\mathrm{x}))$$

which implies that

$$g(\mathrm{x})^{p^d} \equiv g(\mathrm{x})(\mathrm{mod}\ h(\mathrm{x})).$$

So,

$$g(\mathrm{x})p^d - 1 \equiv 1(\mathrm{mod}\ h(\mathrm{x})),$$

thus,

$$p^k - 1 \mid p^d - 1.$$

If, $k \mid d$,

On the other hand,

$$x^r = 1 \text{ in } Fp\,[x]/ < h(x) >$$

since $h(x) \mid x^r - 1$.Thus, order of x in

$$Fp\,[x]/ < h(x) >$$

is r since r is prime and $x - 1 \notin < h(x) >$. So, $r \mid p^k - 1$, i.e,

$$p^k \equiv 1 (\text{mod } r).$$

It implies that d | k. Consequently

$$k = d.$$

5.3.1 Definition: Let f be a polynomial in Fp [x], where p is a prime integer. Let r be a fixed prime integer different from p. A positive integer m is called introspective for f (x) if

$$(x)^m = f(x^m) \text{ in } Fp\,[x]/(x^r - 1)$$

Now we want to prove some properties of introspective integers for f .

Lemma: If m, m' are introspective integers for $f \in Fp\,[x]$, then so is $m\,m'$

Proof: Since m, m' are introspective integers,

$$f(x)^m = f(x^m) \text{ in } Fp\,[x]/(x^r - 1)$$

and

$$f(x)^{m'} = f(x^{m'}) \text{ in } F\,[x]/(x^r - 1).$$

Substitute x^m in place of x in the second congruence

$$f(x^m)m' = f((x^m)m') \text{ in } F\,[x]/(x^{mr} - 1)$$

$$\Rightarrow f(x^m)m' = f(x^{mm'}) \text{ in } F\,[x]/(x^{mr} - 1)$$

$$\Rightarrow f(x^m)m' = f(x^{mm'}) \text{ in } F\,[x]/(x^r - 1)$$

since $(x^r - 1) \mid (x^{mr} - 1)$.

By applying the first congruence we get

$$f(x^{mm'}) = f(x^m)^{m'} = (f(x)^m)^{m'} = f(x)^{mm'} \text{ in } F\,[x]/(x^r - 1).$$

learned until now. First we need some lemmas:

Lemma: If m is introspective for f(x) and g(x) then it is also introspective for f(x)g(x).

Proof: Obviously,

$$(f(x)\, g(x))^{m} = f(x)^{m}\, g(x)^{m} = f(x^{m})\, g(x^{m}) \text{ in } F_{p}\,[x]/(x^{r} - 1).$$

Corollary : Let n, l, and r be positive integers. Let p be a prime divisor of n. Suppose that

$$(x + a)^{n} \equiv x^{n} + a(\text{mod}(x^{r} - 1), n)$$

for every a, $0 \leq a \leq$ l. Then any number in the set

$$I=\{\left(\frac{n}{r}\right)^{i} p^{j} : i, j \geq 0\}$$

is introspective for any polynomial of the form

$$\prod_{a=0}^{l} (x+a)^{ea}, ea \geq 0$$

Proof: $(x + a)^{n} \equiv x^{n} + a(\text{mod}(x^{r} - 1), n)$

$\Rightarrow$ $(x + a)^{n} \equiv x^{n} + a$ in $F_p\,[x]/(x^{r} - 1)$

since p | n.

$(x + a)^{p} \equiv x^{p} + a$ in $F_p[x]/(x^{r} - 1)$.

Now by equation, we have

$$\left((x+a)^{n/p}\right)^{p} \equiv \left(x^{n/p} + a\right)^{p} \text{ in } F_{p}[x]/(x^{r} - 1)$$

Since

$$\text{LH S} = (x + a)^{n}, \text{ RH S} \equiv (x^{n/p})^{p} + a \text{ in } F_p\,[x]/(x^{r} - 1).$$

Let $\text{ord}_{r}\, p = u > 1$. We have

$$((xp + a)^{n/p}) \equiv (x^{p})^{n/p} + a) \text{ İn } F_p\,[x]/(x_{r} - 1),$$

which implies that

$$((x^{p^{u}} + a)^{n/p}) \equiv ((x^{p^{u}})^{n/p} + a) \text{ in } F\,[x]/(x_{r} - 1)$$

since r | $p^{u} - 1$. Therefore,

$$(x + a)^{n/p} \equiv (x)^{n/p} + a \text{ in } F_p\,[x]/(x_{r} - 1).$$

By previous lemmas it follows that any integer in I is introspective for any polynomial of the form

$$\prod_{a=0}^{l}(x+a)^{ea}, ea \geq 0$$

Now we need to define two groups:

5.3.2 Definition: Assume that gcd(n, r) = 1 and p a prime divisor of n. Then

$$G=\{\left(\frac{n}{p}\right)^{i} p^{j} \bmod r : i, j \geq 0\}$$

is a subgroup of Z_p^*

Obviously, G is generated by n mod r and p mod r, so |G| = t ≥ $\text{ord}_r(n)$.

5.3.3 Definition: Let p, r, n be as in the previous definition. Assume that r is prime. Let l be a fixed positive integer. Assume that $\text{ord}_r(p) > 1$. Let h(x) be irreducible polynomial of degree $\text{ord}_r(p)$ in Fp [x] which is a divisor of

$$\frac{x^r - 1}{x - 1}$$

Let

$$G=\{\prod_{o \leq a \leq l} ((x+a)^{ta} + < h(x) >): ta \geq 0, \forall 1 \leq a \leq \ell \}$$

i.e., the subgroup of

$$Fp[x]/ < h(x) > \setminus \{0\}$$

generated by the cosets of

x, x + 1, x + 2, . . . ,x+l

Lemma: Let l< p. Then G is a cyclic group such that

$$|G| \geq \binom{t+\ell}{\ell+1} = \binom{t+\ell}{t-1}$$

Proof:G is a cyclic group since it is a subgroup of cyclic group

$$Fp[x]/ < h(x) > \setminus \{0\}$$

.

Now x is a primitive r − th root of unity by Lemma. Let f and g be two distinct polynomials of degree less than t and f = g in G. Let m ∈ I, so

$$(f(x))^m = (f(x^m)) \text{ in } Fp[x]/(x^r - 1),$$

and

$$(g(x))^m = (g(x^m)) \text{ in } Fp\,[x]/(x^r - 1).$$

The equalities are also true in $Fp\,[x]/ < h(x) >$ since $h(x) \mid x^r - 1$. Obviously,

$$(f(x))^m = (g(x))^m$$

in $Fp\,[x]/ < h(x) >$ too. Consequently, we get

$$f(x^m) = g(x^m) \text{ in } Fp\,[x]/ < h(x) > .$$

So x^m is a root of the polynomial

$$s(y) = f(y) - g(y) \forall m \in G.$$

Since $\gcd(m, r) = 1$, x^m is also a primitive $r-$th root of unity $\forall\ m \in G$. Therefore,

$$\exists\ |G| = t$$

distinct roots of $s(y)$ in $Fp\,[x]/ < h(x) >$. But it contradicts the fact that $\deg(s) < t$.

Thus,

$$f \neq g \text{ in } Fp\,[x]/ < h(x) >$$

Since $\ell < p$, $i \neq j$ in Fp for $1 \leq i \neq j \leq \ell$. So the elements

$$x, x+1, x+2, \ldots, x+\ell$$

are all distinct in $Fp\,[x]/ < h(x) >$. The number of elements in

$$\{ \prod_{o \leq a \leq l} ((x+a)^{ta} : ta \geq 0, \forall\, 1 \leq a \leq \ell, \sum_{0 \leq a \leq \ell} ta \leq t-1 \}$$

is

$$\binom{t-1+\ell+1}{\ell+1} = \binom{t+\ell}{\ell+1} = \binom{t+\ell}{t-1}$$

Now let's find an upper bound for $|G|$:

Lemma: Assume that $\sqrt{t} < \ell$. If n is not a power of p then

$$|G| \leq n^{\sqrt{t}}$$

Proof: Look at the following subset of I :

$$J = \{ \left(\frac{n}{p}\right)^i p^j : 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor \}$$

It has obviously

$$(1 + \lfloor \sqrt{t} \rfloor)^2$$

distinct numbers since n is not a power of p. Since

$$|G| = t < (1 + \lfloor\sqrt{t}\rfloor)^2,$$

$\exists$ $m_1 > m_2$ in J such that

$$m_1 \equiv m_2 (\text{mod } r).$$

Thus,

$$x^{m_1} = x^{m_2} \text{ in } Fp\,[x]/ < x^r - 1 > .$$

Let

$$f(x) = \prod_{o \le a \le l} ((x + a)^{ta} : ta \ge 0$$

Then,

$$(f(x))m^1 = f(x^{m'}) \text{ in } Fp\,[x]/ < x^r - 1 >$$
$$= f(x^{m^2}) \text{ in } Fp\,[x]/ < x^r - 1 >$$
$$= (f(x))^{m^2} \text{ in } Fp\,[x]/ < x^r - 1 > .$$

It implies that

$$(f(x))m^2 = (f(x))m^2 \text{ in } Fp\,[x]/ < h(x) >,$$

where h(x) is an irreducible polynomial of degree $\text{ord}_r(p)$ in Fp [x] which is a divisor of x^r^–

$$\frac{x^r - 1}{x - 1}$$

Thus, f(x) $\in$ G is a root of the polynomial

$$q^y = y^{m^1} - y^{m^2}$$

in the field Fp [x]/ < h(x) >. Since f is arbitrary in G, it follows that q'(y) has at least |G| distinct roots in Fp [x]/ < h(x) >. But the degree of q'(y) is

$$m_1 \le \left(\frac{n}{p}.p\right)^{[\sqrt{t}]} \le n^{[\sqrt{t}]} \le n^{\sqrt{t}}$$

Therefore,

$$|G| \le n^{\sqrt{t}}$$

Lemma: Assume that $\log^2 n <$ t and $\ell = \sqrt{\phi(r)}\ \log n$. Then

$$|G| > n^{\sqrt{t}}$$

$$|G| \geq \binom{t+\ell}{t-1} = \binom{\ell+1+t-1}{t-1}.$$

$$\geq \binom{\ell+1\left[\sqrt{t}\log n\right]}{\left[\sqrt{t}\log n\right]}$$

since $\log^2 n$<t$\Rightarrow \sqrt{t}$ >log n which implies that

$$\text{t-1} \geq \left\lfloor \sqrt{t}\log n \right\rfloor.$$

Than it becomes

$$\geq \binom{2\left[\sqrt{t}\log n\right]+1}{\left[\sqrt{t}\log n\right]}$$

since g is a subgroup of Z_r^* we have $\phi(r) \geq t$. İt is greater than

$$>2^{1+\left[\sqrt{t}\log n\right]} \geq 2^{\sqrt{t}}\log n = 2^{\log n^{\sqrt{t}}} = n^{\sqrt{t}}.$$

Lemma: lcm(1, 2, . . . , m) $\geq 2^m$
for $m \geq 7$

Now for the main theorem, we need some lemmas for the existence of a proper integer r for a given integer n.

Lemma: There exist an

$$r \leq \max\ \{\ 3, [\log^n n]\}$$

such that $\text{ord}_r\ (n) > \log^2\ n$.

Proof: It is obvious if n = 2 and r = 3 since $\text{ord}_3(2) = 2 > \log_2 2 = 1$. Now assume that n> 2. Let r be the smallest integer greater than 1 which doesn't divide the product

$$n^{[\log B]}\prod_{i=1}^{[\log^2 n]}(n^i - 1),$$

where B = $[\log_5\ n]$. Let d = gcd(r, n). Let p be a prime such that $p \mid d$ and $p^k \mid\mid r$ for some positive integer k.

$$r \leq \mathrm{B} \Rightarrow p \ \leq \mathrm{B} \Longrightarrow k \leq \left(\frac{\log B}{\log p}\right) \leq \log B$$

which implies that

$$p^{k} \mid n^{[\log B]}$$

If this is true for all prime divisors of r, then

$$r \mid n^{[\log B]}$$

which is contradiction. Thus, $d < r$. But d also doesn't divide

$$n^{[\log B]} \prod_{i=1}^{[\log^2 n]} (n^i - 1)$$

Since r was the smallest integer greater than 1 which doesn't divide

$$n^{[\log B]} \prod_{i=1}^{[\log^2 n]} (n^i - 1),$$

it follows that $d = 1$.So we can talk about $\mathrm{ord}_r\, n$ since $\gcd(r, n) = 1$. Now

$$\mathrm{ord}_r\ n > \log^2\ n$$

since r doesn't divide any of $n^i - 1$ for $1 \leq i \leq \log^2\ n$.In order to see $r \leq \mathrm{B}$,

$$n^{[\log B]} \prod_{i=1}^{[\log^2 n]} (n^i - 1) < n^{[\log B]} \prod_{i=1}^{[\log^2 n]} n^i =$$

$$n^{[\log B]} n^{\log^2 n(\log^2 n+1)/2} \leq n^{\log^4 n} \leq 2^{\log^5 n} \leq 2^{B}$$

Lemma: Implies that the least common multiple of first B integers is at least 2^{B}.

Consequently

$$r \leq \mathrm{B}.$$

Remark:The existence of a suitable small integer r is a consequence of results from analytic number theory which states that

$$\left| \{p : p \text{ is prime}\ , p \leq \mathrm{x} \text{ and } P\,(p-1) > \mathrm{x}^{2/3}\} \right| \geq c\frac{x}{\log x} \quad ,$$

where $P\,(n)$ denote the greatest prime divisor of n.

Now we can give the main theorem

5.3.1 AGRAWAL, KAYAL, SAXENA

5.3.1 Theorem:(Agrawal, Kayal, Saxena):The following algorithm returns prime if and only if n is prime.

Algorithm: Input: integer $n > 1$.

- If ($n = a^b$ for a positive integer a and $b > 1$), output composite.
- Find the smallest r such that $\text{ord}_r(n) > \log^2 n$
- İf $1<\gcd(a,n)<n$ for some $a \leq r$ output composite
- For a=1 to [$\sqrt{\phi(r)}\log n$] do if $((x+a)^n \neq x^n + a$ in $Z_{n[x]}/<x^r - 1>$), output composite
- Output prime

Proof ⇒:Case1: The algorithm returns prime in step 4: If n was not prime then There exist would be a prime integer a such that $a \mid n$. Then

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

which implies that the algorithm would return composite in step 3. But it is contradiction.

⇒:Case 2: The algorithm returns prime in step 6: r was found in step 2 such

$$\text{ord}^r(n) > \log^2 n \leq 1$$

Therefore, there exists a prime divisor p of n such that

$$\text{ord}_r(p) > 1$$

If $p < n$, we should have composite by step 3. If $p = n$, then we should have prime by step 4. Therefore,

$$p > r.$$

Now

$$\gcd(r, n) = 1 \text{ thus, } \gcd(r, p) = 1$$

since for otherwise, we should have composite in step 3. Therefore,

$$n, r \in Z_r^*$$

We have the group G and

$$|G| = t \geq \text{ord}_r(n) > \log^2 n$$

Let

$$\ell = \left\lfloor \sqrt{\phi(n)} \log_n \right\rfloor$$

Consider the group G defined. We have

$$\varphi(r) \geq \text{ord}_r(n) > \log^2 n \geq 1$$

Thus ,

$$\log n < \sqrt{\phi(r)} \Rightarrow \ell = [\sqrt{\phi(r)}\ \log n] < \varphi(r) < r < p$$

$$\text{So } |G| \geq \binom{t+\ell}{t-1}$$

Now,

$$|G| > n^{\sqrt{t}}$$

On the other hand, since G is a subgroup of Z_r^*

$$t = |G| \leq \varphi(r).$$

It implies that

$$\sqrt{t} \leq \sqrt{\phi(r)}$$

so $t \leq \ell$. We conclude that n should be a power of p. But we should have composite in step 1.

$\Leftarrow$:Step 1 and Step 3 can not return composite. Assume that step 4 doesn't return prime. Then step 5 doesn't return composite. The proof of the following theorem can be found.

5.3.2 Theorem: The runtime of the ALGORITHM is polynomial in the number of digits

CHAPTER 6

CONCLUSION

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

In Chapter 2, I exposed number theory, I have included and explained divisors and divisibility and the greatest common divisor in details. Extensive exercises are included for number theory.

In Chapter 3, factoring algorithm defined on number theory has been covered with examples. I exposed the pollard p-1 algorithm, the pollard rho algorithm, dixon's random squares algorithm, elliptic curve factorization, factor base method.

InChapter 4, I exposed public key cryptographic system which depends on factorization and RSA.

In Chapter 5, I explained primality testing and, I have included and explained manindra agrawal's theorem.

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 ciipher 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