NUMBER THEORETICAL APPLICATIONS TO CRYPTOGRAPHY

by

Müberra GÜREL

June 2005

NUMBER THEORETICAL APPLICATIONS TO CRYPTOGRAPHY

by

Müberra GÜREL

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

June 2005
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 _____

Prof. Dr. Yılmaz Akyıldız _____

Assist. Prof. Dr. Tevfik Bilgin _____

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
June 2005

NUMBER THEORETICAL APPLICATIONS TO CRYPTOGRAPHY

Müberra GÜREL

M. S. Thesis - Mathematics
June 2005

Supervisor: Prof. Dr. Barış KENDİRLİ

ABSTRACT

First , I have included and explained some number theoretical facts in the beginning.Then classical cryptography has been covered with examples in details.After that I exposed the Public Cryptography with examples.At last maple algorithms have been written for cryptography.

Keywords: Classical , public key cryptography and maple algorithms

SAYILAR TEORİSİNİN KRİPTOGRAFİYE UYGULAMASI

Müberra GÜREL

Yüksek Lisans Tezi – Matematik
Haziran 2005

Tez Yöneticisi: Prof. Dr. Barış KENDİRLİ

ÖZ

Başlangıçta, sayılar teorisini ana hatlarıyla açıkladım. Sonra, klasik şifreleme detaylı olarak örneklerle gösterilmiştir. Devamında, asimetrik kriptografiyi örneklerle ifade ettim. Son olarak şifreleme için maple algoritmaları yazılmıştır.

Anahtar Kelimeler: Klasik, asimetrik kriptografi ve maple algoritmaları.

DEDICATION

To my parents, Buğra Kaan,
Barış and Yasemin Kendirli

ACKNOWLEDGEMENT

I am glad to take this oppotunity 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. Yılmaz AKYILDIZ, Prof. Dr. Allaberen ASHYRALYEV , 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 SYSMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION

$O(g)$	Big-O notation
$n \mid m$	Divides
$n \nmid m$	Does not divide
$p^k \| m$	Exactly divides
$\varphi(n)$	Euler's phi-function
$a \equiv b \pmod{n}$	Congruent
$a \not\equiv b \pmod{n}$	Incongruent
$\left(\frac{p}{q}\right)$	Legendre symbol
$\left(\frac{a}{n}\right)$	Jacobi symbol

CHAPTER 1

INTRODUCTION

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. Crytography 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 beginnig 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. 56 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. Morover, 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. DES, Data Encryption Standart, was created by IBM in the middle of 1970s. Whitfield

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. RSA is based on factoring extremely large numbers. In 1985, T. El Gamal introduced 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 number theory and algebra ,that is needed for ancient and modern cryptography, with examples. Furthermore, second and third chapter provide a general bacground. Then, in chapter 4, I have included and explained classical cryptosytems. Extensive exercises are included for shift, affine and vigénere ciphers in detail. Asymmetric cryptosystems, RSA, Diffie-Hellman key Exchange, El Gamal, Massey Omura cryptosystem for message transmission and Digital Signature are covered with examples in chapter 5. Finally, I wrote maple algorithms for public key cryptosystems.

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

CHAPTER 2

NUMBER THEORY

2.1 COMPLEXITY OF COMPUTATION

Efficiency of algorithms can be measured in different ways. For example, one can consider readibility of an algorithm, or its time and space consumption. However, the running time of an algorithm is the most important issue in cryptology. As we know, enciphering and deciphering algorithms are based on four basic arithmetic operations namely addition, subtraction, multiplication, and division. So, it is reasonable to measure the running time of algorithms in terms of arithmetic operations. Since numbers in computers are represented in binary system, that is, in bits, time complexity of each arithmetic operation is defined as a function of binary digits(bits) of numbers to be, for example multiplied or added. To do this we must introduce the concept of bit operation. Addition of two bits is called a bit operation.

While we are adding two binary numbers, first we look top and bottom binary digits and there is a carry or not above the top binary digit. If both top and bottom binary digits are zero without carry, then put down zero and move on. If both bottom and top binary digits are zero with a carry, then put down 1, move on. If one of binary digits is 1, the other one is 0 without a carry then put down 1, move on. If one of binary digits is 1, the other one is 0 with a carry, then put down 0 and put the carry next column and move on. If both binary digits are 1 with a carry, then put down 1 and put the carry next column and move on. If both binary digits are 1 without a carry, then put down 0 and put the carry next column and move on.

According to the above definition of bit operation, addition of two integers a and b requires at most $\max([\log_2 a]+1, [\log_2 b]+1)$ bit operations, while multiplication of the integers requires $([\log_2 a]+1)([\log_2 b]+1)$ bit operations.

In general, complexity of computation is defined in terms of big-O notation. If $f(n)$ and $g(n)$ are two positive functions and if $\lim_{n\to\infty}\left(\frac{f(n)}{g(n)}\right) = c$ where c is constant and different from zero, then we write $f = O(g)$ or f is $O(g)$. For example, let $f(n) = n^2 + n + 1$. Then $f = O(n^2)$ since $\lim_{n\to\infty}\left(\frac{n^2+n+1}{n^2}\right) = 1$.

2.2 DIVISIBILITY and EUCLIDEAN ALGORITHM

2.2.1 Divisors and Divisibility:

An integer n divides integer m if and only if $m = kn$ where $n \neq 0$ and k is an integer n is said to be a *divisior* of m. n divides m or m is divisible by n is denoted by $n \mid m$. If n does not divide m, then it is denoted by $n \nmid m$.

By maple

- divisors(9);

{1,3,9}

Properties of Divisibility:

n, m, t, and s are any integers

1) $n \mid m$ implies $n \mid -m$, $-n \mid m$, and $-n \mid -m$.
2) $n \mid m$ implies $n \mid mt$.
3) $n \mid m$ and $m \mid s$ imply $n \mid s$.
4) $m \mid n$ and $n \mid m$ imply $m = \pm n$
5) $n \mid m$ and $n \mid s$ imply $n \mid m \pm s$
6) $n \mid m$ and $n \mid s$ imply $n \mid mx + sy$ for all $x, y \in Z$
7) $n \mid m$ implies $tn \mid tm$ for all $t \in Z$
8) $n \mid m$ and $t \mid n$ imply $t \mid m$
9) For all $n > 0$ and $m > 0$, $n \mid m$ implies $n \leq m$.

A positive integer p greater than 1 is *prime* if the only divisors of p are ± 1 and $\pm p$. To illustrate, 2, 3, 5, 7, 11, 13, 17, ……are prime numbers.

By maple
➢ isprime(p);

A positive integer greater than 1 is *composite* number if and only if it is not prime. Let p be a prime number and k, m be positive integers. p^k exactly divides m, denoted by $p^k \| m$, such that

i) $p^k \mid m$

ii) $p^{k+1} \nmid m$

Let *k, l, m, n* be nonnegative integers and p be prime.

i) $p^k \| m$, and $p^l \| n$, imply $p^{k+l} \| mn$

ii) $p^k \| m$ implies $p^{k\alpha} \| m^{\alpha}$

iii) Let $k \neq l$, $p^k \| m$ and $p^l \| n$ imply $p^{min(k,l)} \| m + n$

2.2.2 Unique Factorization :

Let n be a positive integer grater than 1. n can be factorized into prime powers such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_l^{\alpha_l}$ where $p_1, p_2, \ldots\ldots, p_l$ are distinct primes.

By maple
➢ ifactor(n);

The number of positive divisors of n can be computed by $(\alpha_1 + 1)(\alpha_2 + 1)\ldots\ldots(\alpha_l + 1)$. To illustrate, factorization of 360 is equal to $2^3 3^2 5$. Number of positive divisors of 360 is $(3+1)(2+1)(1+1) = 24$.

2.2.3 The Greatest Common Divisor:

Let a and b be integers. There exists a positive integer d such that $d \mid a$ and $d \mid b$. d is said to be common divisor. If d is the largest divisor common to a and b then d is called *the greatest common divisor* of a and b. We write d = gcd(a, b). For example, gcd(15,60) = 15, gcd(21,35) = 7 and gcd(27,72,36) = 9.

By maple ➢ igcd(a, b);

a and b are called *coprime or relatively prime* integers if gcd(a,b) = 1.

Let two integers a and b are given. Let d be the smallest positive integer, such that $a \mid d$ and $b \mid d$, then d is called the least common multiple of a and b. We denoted by lcm(a, b). To illustrate, lcm(20,30) = 60 and lcm(33,18) = 198.

By maple ➢ ilcm(a, b);

Theorem2.2.1(*Koblitz, Neal***.):** Let a and b be positive integers.

$$\text{lcm}(a, b) = (ab) / \text{gcd}(a, b)$$

Theorem2.2.2(*Koblitz, Neal***.):** Time(gcd(a,b)) = $O((\log_2 a)^3)$.

2.2.4 The Euclidean Algorithm:

Division Algorithm:

If a is an integer and b is a positive integer, there exists unique pair of integers q and r such that

$$a = bq + r \qquad \text{with} \quad 0 \le r < b$$

If $b \mid a$ then $r = 0$. We use Euclidean algorithm in order to find the greatest common divisor of two integers by applying division algorithm.

Procedure of Euclidean Algorithm:

We want to find gcd(a, b). Let a, b be positive integers that b does not divide a and $a > b$. Let $a = r_0$ by $b = r_1$. Quotient is q_1 and the remainder is r_2. Then we find

$$r_0 = r_1 q_1 + r_2 \qquad \text{where } 0 \le r_2 < r_1$$

If we repeat the division algorithm, we obtain

$$r_1 = r_2 q_2 + r_3 \qquad \text{where } 0 \le r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4 \qquad \text{where } 0 \le r_4 < r_3$$

.....

$$r_{k-3} = r_{k-2} q_{k-2} + r_{k-1} \qquad \text{where } 0 \le r_{k-1} < r_{k-2}$$

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

$$r_{k-1} = r_k q_k$$

Then, the last nonzero remainder r_k is gcd(a, b).

Example1: Find the greatest common divisor of 2125 and 63.

Solution:

$$2125 = 63.33 + 46$$
$$63 = 46.1 + 17$$
$$46 = 17.2 + 12$$
$$17 = 12.1 + 5$$
$$12 = 5.2 + 2$$
$$5 = 2.2 + 1$$
$$2 = 1.2$$

Hence, gcd(2125,63) = 1.

Theorem2.2.3(*Koblitz, Neal***.):** Time(finding gcd(a, b) using Euclidean algorithm) = $O((\log_2 a)^3)$.

Theorem2.2.4(*Rosen, Kenneth H.***)**: If gcd(a, b) = d then there exists integers u and v such that $d = au + bv$.

Theorem2.2.5(*Koblitz, Neal***.) :** Time(finding d as linear combination $au + bv$) = $O((\log_2 a)^3)$.

By maple

- igcdex(a, b, 'u', 'v');

  1

- u; v;

Example 2:

Express 1 as a linear combination of 2125 and 63.

Solution:

$$1 = 5 - 2.2 = 5 - 2(12 - 5.2)$$
$$= 5.5 - 2.12 = 5(17 - 12.1) - 2.12$$
$$= 5.17 - 7.12 = 5.17 - 7(46 - 17.2)$$
$$= 19.17 - 7.46 = 19(63 - 46.1) - 7.46$$
$$= 19.63 - 26.46 = 19.63 - 26(2125 - 63.33)$$
$$= 877.63 - 26.2125$$

2.2.5 Euler's Teorem

Definition2.2.1(*Rosen, Kenneth H.***):** Let n be an element of Z^+. The Euler phi-function $\varphi(n)$ denotes the number of positive integers in the interval $(0,n)$ which are coprime to n. In order

to find the value of $\varphi(n)$, we factorize n into prime powers such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_l^{\alpha_l}$.

Theorem2.2.6(*Koblitz, Neal***.):** $n \in Z^+$

$$\varphi(n) = n\prod_{i=1}^{l}(1-\frac{1}{p_i})$$

$\varphi(n) = \varphi(\ p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_l^{\alpha_l}\ ) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots\ldots p_l^{\alpha_l-1}(p_l-1)$.

Special case:

i) $\varphi(1) = 1$

ii) $\varphi(p) = p\text{-}1$ if p is prime

iii) $\varphi(p^\alpha) = p^\alpha(1-\frac{1}{p}) = p^{\alpha-1}(p-1)$ if p is prime and $\alpha \geq 1$.

iv) $\varphi(n)$ is multiplicative arithmetic function. If gcd(a,b) = 1 then φ(ab) = φ(a)φ(b).

v) If gcd = d then φ(ab) = φ(a)φ(b)(d / φ(d)).

By maple
➢ phi(n);

Theoem2.2.7(*Rosen, Kenneth H.***):** $\sum_{d/n}\varphi(d) = n$ where n is positive integer .

For example, $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$.

Theorem2.2.8(*Koblitz, Neal***.):** Time($\varphi(n)$) = $O((\log_2 n)^3)$.

In particular, if $n = ab$ then Time(computing $\varphi(n)$ knowing a and b) = $O(\log_2 n)$.

Moreover, Time(computing a and b knowing n and $\varphi(n)$) = $O((\log_2 n)^3)$.

Example3: Let's find the value of $\varphi(n)$ where $1 \leq n \leq 10$.

$\varphi(1) = 1$ $\varphi(2) = 2 - 1 = 1$

$\varphi(3) = 3 - 1 = 2$ $\varphi(4) = \varphi(2^2) = 2^{2-1}(2 - 1) = 2$

$\varphi(5) = 5 - 1 = 4$ $\varphi(6) = \varphi(2.3) = (2 - 1)(3 - 1) = 2$

$\varphi(7) = (7 - 1) = 6$ $\varphi(8) = \varphi(2^3) = 2^{3-1}(2 - 1) = 4$

$\varphi(9) = \varphi(3^2) = 3^{2-1}(3-1) = 6$ $\varphi(10) = \varphi(2.5) = (2 - 1)(5 - 1) = 4$

n	$\varphi(n)$	N	$\varphi(n)$	n	$\varphi(n)$
11	10	41	40	71	70
12	4	42	12	72	24
13	12	43	42	73	72
14	6	44	20	74	36
15	8	45	24	75	40
16	8	46	22	76	36
17	16	47	46	77	60
18	6	48	16	78	24
19	18	49	42	79	78
20	8	50	20	80	32
21	12	51	32	81	54
22	10	52	24	82	40
23	22	53	52	83	82
24	8	54	18	84	24
25	20	55	40	85	64
26	12	56	24	86	42
27	18	57	36	87	56
28	12	58	28	88	40
29	28	59	58	89	88
30	8	60	16	90	24
31	30	61	60	91	72
32	16	62	30	92	44
33	20	63	36	93	60
34	16	64	32	94	46
35	24	65	48	95	72
36	12	66	20	96	32
37	36	67	66	97	96
38	18	68	32	98	42
39	24	69	44	99	60
40	16	70	24	100	40

Some values of Euler's Phi-Function table $11 \leq n \leq 100$

2.3 CONGRUENCES

Definition2.3.1: For all $a, b \in Z$ and $n \in Z^+$, if $n \mid a - b$ then we say that a is congruent to b modulo n, and we write

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

Otherwise, we say that a and b are incongruent modulo n, and we write

$$a \not\equiv b \pmod{n}$$

By maple
➢ a mod n;

Properties of Congruences:

1) $a \equiv a \bmod n$ (Reflexive property)
2) $a \equiv b \bmod n$ implies $b \equiv a \pmod{n}$ (Symmetric property)
3) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$ (Transitive Property)
4) If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $a + b \equiv a' + b' \bmod n$, $a-b \equiv a'-b' \bmod n$ and $ab \equiv a'b' \bmod n$
5) For $a \equiv b \bmod n$, $a^k \equiv b^k \bmod n$ where $k > 0$.
6) $ac \equiv bc \bmod n$, and $(c,n) = d$ imply $a \equiv b \bmod n/d$ (Cancellation Law)
7) $a \equiv b \bmod n$, $a \equiv b \bmod m$, and $\gcd(m,n) = 1$ imply $a \equiv b \bmod mn$.
8) Let $a \equiv b \pmod{n}$. If $\gcd(c,n) = 1$ then $ac^{-1} \equiv bc^{-1} \bmod n$. c^{-1} is arithmetic inverse of c modulo n .

Theorem2.3.1(*Rosen, Kenneth H.***):** The arithmetic inverse a^* exists modulo n i.e $a.a^* \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$.

Time(finding a^* modulo n) = $O((\log_2 n)^3)$.

Let a be an integer. The set of integers is congruent to a modulo m is called congruence classes modulo m. It is denoted by $\hat{a}$. To rephrase;

$$\hat{a} = \{x \in Z \mid x \equiv a \bmod m\}.$$

Properties of congruence classes:

1) $\hat{a} = \hat{c}$ if and only if $a \equiv c \bmod m$
2) $\hat{a} \neq \hat{c}$ if and only if $\hat{a} \cap \hat{c} = \varnothing$
3) For modulo m, number of congruence classes is m.

Another definition of congruence classes is that the equivalence classes modulo m, denoted by Z/mZ, are called residue or congruence classes modulo m.

For instance Z/5Z

$\{\ldots, -15, -10, -5, 0, 5, 10, 15,\ldots.\} \cup \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \cup$

$\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \cup \{\ldots, -12, -7, -2, 3, 8, 13, 18, .. \} \cup$

$\{\ldots., -11, -6, -1, 4, 9, 14, 19, \ldots.\} = Z$

In general, Z/mZ becomes a ring under addition and multiplication of residue classes. If m is prime integer then Z/mZ becomes a field.

2.3.1 Linear Congruence

The basic form of linear congruence is in one variable $ax \equiv b \bmod m$ where $a \in Z$, $b \in Z$, and $m \in Z^+$.

1) $ax \equiv b \bmod m$ has solutions if $\gcd(a,m) = d$ and $d \mid b$

   i) if $d = 1$, $ax \equiv b \bmod m$ has only one incongruent solution.

   ii) if $d > 1$ then solve $(\frac{a}{d})x \equiv (\frac{b}{d}) \bmod (\frac{m}{d})$.

Let x_0 be the solution of $(\frac{a}{d})x \equiv (\frac{b}{d}) \bmod (\frac{m}{d})$. There are d incongruent solutions of $ax \equiv b \bmod m$ such that

$x = x_0 + k\,(m/d)\ \ 0 \le k \le d\text{-}1$

2) $ax \equiv b \bmod m$ has exactly one solution if m is prime and $a \not\equiv 0 \pmod m$

Theorem2.3.2(*Koblitz, Neal*.): Time(finding solution of $ax \equiv b \bmod m$) = $O((\log_2 m)^3)$.

Example1: Let's find all of the solutions of linear congruences.

A) $8x \equiv 1 \bmod 11$

First, we find gcd(8, 11) by using Euclidean algorithm such that

$$11 = 8.1 + 3$$
$$8 = 3.2 + 2$$
$$3 = 2.1 + 1$$

Hence, gcd(8, 11) = 1. Next, we compute inverse of 8 by applying extended euclidean algorithm such that

$$1 = 3 - 2.1 = 3 - (8 - 3.2).1 = 3.3 - 8.1$$
$$= (11 - 8.1)3 - 8.1 = 11.3 - 8.4$$

Therefore, $8^{-1} = -4 \equiv 7 \bmod 11$.

Then , we multiply both sides of this congruence by the inverse of 8, which is 7.

$$7.8\,x \equiv 7.1 \bmod 11$$

$$x \equiv 7 \bmod 11.$$

As you see, there is only one solution since gcd(8, 11) = 1

B) $18x \equiv 81 \bmod 99$

First, we find gcd(18, 99) by using Euclidean algorithm such that

$$99 = 18.5 + 9$$

$$18 = 9.2$$

Hence, gcd(18, 99) = 9 . It implies that there exists exactly nine incongruent solutions as $9 \mid 81$.

$$(\frac{18}{9})x \equiv (\frac{81}{9}) \bmod (\frac{99}{9})$$

We consider $2x \equiv 9 \bmod 11$ to find a particular solution. By Euclidean algorithm

$$11 = 2.5 + 1,$$

Therefore, $1 = 11 - 2.5$. Hence, inverse of 2 is $-5 \equiv 6 \bmod 11$.

Then , we multiply both sides of this congruence by the inverse of 2, which is 6.

$$6.2\,x \equiv 6.9 \bmod 11$$

$$x \equiv 9 \bmod 11.$$

Therefore, solutions of $18x \equiv 81 \bmod 99$ is $9 + (99/9)\,k$ where $0 \le k \le 8$ such that

$$x_1 = 9 + 11.0 = 9, \quad x_2 = 9 + 11.1 = 20, \; x_3 = 9 + 11.2 = 31,$$

$$x_4 = 9 + 11.3 = 42, \; x_5 = 9 + 11.4 = 53, \; x_6 = 9 + 11.5 = 64,$$

$$x_7 = 9 + 11.6 = 75, \; x_8 = 9 + 11.7 = 86, \; x_9 = 9 + 11.8 = 97.$$

Theorem2.3.3: (Fermat's Little Theorem(*Koblitz, Neal***.))** If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem2.3.4: (Euler's Theorem(*Rosen, Kenneth H.***))** gcd $(a,n) = 1$ implies $a^{\varphi(n)} \equiv 1 \bmod n$. where $\varphi(n)$ is the notation of Euler's phi-function.

To illustrate, let $a = 3$ $n = 4$. Since gcd(3,4) = 1. $3^{\varphi(4)} = 3^2 = 9 \equiv 1 \bmod 4$.

Theorem2.3.5: (Wilson's Theorem(*Rosen, Kenneth H.***))** $(p-1)! \equiv -1 \bmod p$ if p is prime

Corollary: $p \nmid a$ and $n \equiv m \bmod (p-1)$ imply $a^n \equiv a^m \bmod p$ where $n > m$

2.3.2 Chinese Remainder Theorem

Let $M = m_1, m_2, m_3, \ldots, m_k$ where $m_1, m_2, m_3, \ldots, m_k$ are pairwise coprime positive integers. If $i \neq j$ gcd $(m_i, m_j) = 1$. Let $u_1, u_2, \ldots\ldots, u_k$ be arbitrary integers . ∃ an integer a such that

$$a \equiv u_1 \pmod{m_1}$$

$$a \equiv u_2 \pmod{m_2}$$

……..

$$a \equiv u_k \pmod{m_k}$$

has only one solution modulo M

Proof: Let's define $M_1, M_2, M_3, M_4, \ldots\ldots\ldots, M_k$

$M_1 = M / m_1$ then ∃ N_1 such that $M_1N_1 \equiv 1 \bmod m_1$

$M_2 = M / m_2$ then ∃ N_2 such that $M_2N_2 \equiv 1 \bmod m_2$

……

$M_k = M / m_k$ then ∃ N_k such that $M_kN_k \equiv 1 \bmod m_k$

Then, compute $a = u_1M_1N_1 + u_2M_2N_2 + \ldots\ldots\ldots + u_kM_kN_k$. Hence

$$a \equiv u_1M_1N_1 \equiv u_1 \pmod{m_1}$$

$$a \equiv u_2M_2N_2 \equiv u_2 \pmod{m_2}$$

……..

$$a \equiv u_kM_kN_k \equiv u_k \pmod{m_k}$$

By maple
➢ chrem(u, m);

Example2:

Let's solve the system $x \equiv 6 \bmod 11$

$x \equiv 2 \bmod 6$

$x \equiv 1 \bmod 7$

we have $M = 11.6.7 = 462$, then we compute $M_1 = 462/11 = 42$, $M_2 = 462/6 = 77$, $M_3 = 462/7 = 66$.To find N_1, we solve $42N_1 \equiv 1 \bmod 11$ which is equal to $9N_1 \equiv 1 \bmod 11$.

This gives $N_1 \equiv 5 \bmod 11$. To determine N_2, we solve $77N_2 \equiv 1 \bmod 6$, or equivalently, $5N_2 \equiv 1 \bmod 6$. We find $N_2 \equiv 5 \bmod 6$. Finally we solve $66N_3 \equiv 1 \bmod 7$ so as to find N_3. This yields $N_3 \equiv 5 \bmod 7$. Therefore,

$$a \equiv 6.42.5 + 2.77.5 + 1.66.5 \equiv 2360 \equiv 50 \bmod 462$$

2.4 MODULAR EXPONENTION BY THE REPEATED SQUARE METHOD

Let b, n and m are positive integers and $b < m$. We write n in binary digits such that

$n = (n_k n_{k-1} \ldots\ldots n_1 n_0)_2 = n_0 + 2n_1 + \ldots\ldots + 2^{k-1} n_{k-1} + 2^k n_k$. Next we compute the least nonnegative residues of $b^{n_0}, (b^2)^{n_1}, \ldots\ldots\ldots, (b^{2^{k-1}})^{n_{k-1}}, (b^{2^k})^{n_k}$ modulo m.

Finally, we multiply $b^{n_0} (b^2)^{n_1} \ldots\ldots\ldots (b^{2^{k-1}})^{n_{k-1}} (b^{2^k})^{n_k}$ to find b^n.

Proposition2.4.1: Time $(b^n \bmod m) = O((\log_2 m)^2 \log_2 n)$.

By maple

- b ^ n mod m;

or

- b &^ n mod m;

Example1:

Let's use the repeated squaring method to find 7^{75} modulo 101

For $n_0 = 1$, $a = 7^1 \equiv 7 \bmod 101$

For $n_1 = 1$, $7^2 \equiv 49 \bmod 101$ then $a = 7.49 = 343 \equiv 40 \bmod 101$

For $n_2 = 0$, $a = 40$

For $n_3 = 1$, $7^8 \equiv 24 \bmod 101$ then $a = 40.24 = 960 \equiv 51 \bmod 101$

For $n_4 = 0$, $a = 51$

For $n_5 = 0$, $a = 51$

For $n_6 = 0$, $7^{64} = 7^{4.16} = 78^{16} \equiv 81 \bmod 101$ then $a = 51.81 \equiv 91 \bmod 101$

2.5 SOME APPLICATION TO FACTORING

Proposition2.5.1: Let $b \in Z$ and $m \in Z^+$.

$b^m - 1 = (b - 1)(b^{m-1} + b^{m-2} + \ldots\ldots + b^2 + b + 1)$

Corollary: Let $b \in Z$ and $n, m \in Z^+$.

$b^{nm}-1 = (b^n - 1)(b^{n(m-1)} + b^{n(m-2)} + \ldots\ldots\ldots + b^{2n} + b^n + 1)$

Proposition2.5.2: Let a be prime to n, and $b, c \in Z^+$.

$a^b \equiv 1 \bmod m$, $a^c \equiv 1 \bmod m$ and $\gcd(b, c) = d$ imply $a^d \equiv 1 \bmod m$.

Proposition2.5.3: Let p be prime and $p \mid b^n - 1$.

i) $p \mid b^d - 1$ where $d \mid n$.

ii) 1) $n \mid p-1$ if $p > 2$ and n is odd

2) $2n \mid p-1$

Example1:

To determine whether $2^{23} - 1 = 8388607$ is prime or not, we look a prime not exceeding $\sqrt{8388607} = 2896{,}30\ldots..$ Thus, we test $p = 47, 139, \ldots\ldots$ We obtain the prime factorization of $8388607 = 47.178481$.

Example2:

To factor $5^{15} - 1$, we first look for factors of 5^d-1 for $d = 1, 3, 5$ such that $5^1 - 1$, $5^3 - 1$, $5^5 - 1$ .This gives 2^2, 11, 31, 71 and we obtain $\frac{5^{15}-1}{2^2.11.31.71} = 315121$. Remaining prime factor must be congruent to 1 modulo 30. We look for primes less than $\sqrt{315121} = 561{,}3564$. Thus, we test $p = 31, 61, 151, 181, \ldots..$ We find that $315121 = 181.1741$. 1741 is also a prime integer. Thus, $5^{15}-1 = 2^2.11.31.71.181.1714$ is the prime factorization.

Example3:

To factor $7^{12} - 1 = 13841287200$, we first try the factors of $7^d - 1$ for $d = 1, 2, 3, 4, 6$ such that $7^1 - 1$,$7^2 - 1$, $7^3 - 1$, $7^4 - 1$, and $7^6 - 1$. We reach 2^5, 3^2, 5^2, 19, 43. $\frac{13841287200}{2^5.3^2.5^2.19.43} = 2353$. Then as 2353 is not prime, we look for $\sqrt{2353} = 48{,}5077$. We check $p = 13, 37, \ldots\ldots$ We find that $2353 = 13.181$. $13 \equiv 1 \bmod 12$.

Hence, $7^{12} - 1 = 2^5.3^2.5^2.13.19.43.181$.

CHAPTER 3

FINITE FIELD AND QUADRATIC RESIDUES

Let's review some basic concepts from algebra.

3.1 GROUPS

A set G under a binary operation, denoted by o, is said to be a *group* if the following rules are satisfied.

1) Closure law: $x \in G$ and $y \in G$ then $xoy \in G$
2) Associative law: $x \in G$, $y \in G$, $z \in G$ such that $(xoy)oz = xo(yoz)$
3) Existence of identity element: e is an identity element of the binary operation o on G such that $xoe = eox$ for all $x \in G$. Under addition operation, identity element is 0. Under multiplication operation, identity element is 1.
4) Existence of inverse element: For any x in G, there is an inverse of x, denoted by x^{-1}, in G such that $xox^{-1} = x^{-1}ox = e$. In addition operation, inverse of x is –x. In multiplication operation, inverse of x is 1/x.

Example1: $Z=\{0, \pm1, \pm2, \pm3, \ldots\ldots\ldots\ldots\}$ is a group under addition operation.

Example2: R, the reals, is a group under addition operation.

Example3: R is not a group under multiplication operation since 0 does not have inverse.

Example4: $C \setminus \{0\}$ is a group under multiplication operation.

Example5: $Z_3 = \{0, 1, 2\}$ is a group under addition operation.

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

3.1.1 Abelian Groups:

A group G is called *abelian* if it satisfies the commutative law such that xoy = yox for all $x \in G$, $y \in G$. To illustrate, Z is an abelian group under addition.

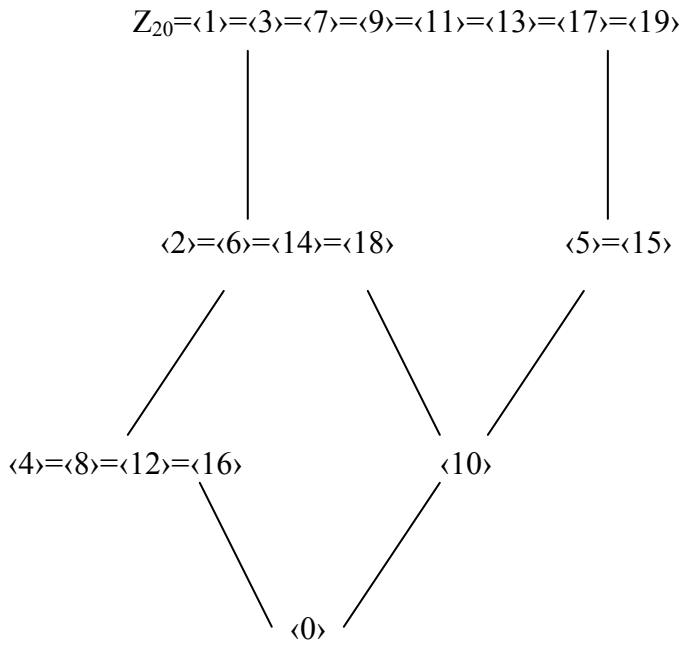
3.1.2 Finite And Infinite Groups:

A group G is called *finite group* if it has a finitely many elements. Otherwise, it is said to be *infinite group*. The number of elements in G is called the order of G, denoted by |G|.

3.1.3 Subgroups:

Let H be a subset of G which is a group by itself under the binary operation of G. Then it is called a subgroup of G, denoted by H<G. For example, R is a subgroup of C.

Example6: Let's find all subgroups of $Z_{20} = \{0, 1, 2, 3, \ldots\ldots\ldots, 17, 18, 19\}$



3.1.4 Cyclic Groups:

Let G be a group. If there is an element *a* in G such that all element in G is a power of *a*, or $\langle a \rangle = \{a^n; n \in Z\} = G$, then G is said to be *cyclic group* and *a* is called a generator of G. For example, generator of Z_2 is 1. There can be several generators in a cyclic group. For example, the generators of Z_5 are 1,2,3, and 4 and the generators of $Z_5 \setminus \{0\}$ are 2 and 3.

Definition3.1.1: If a cyclic group G has distinct elements such that

$$\{a, a^2, a^3, \ldots\ldots a^{n-1}, a^n = e\}$$

then it is called a finite cyclic group. Order of *a* is *n* .

Lemma: Let G be a finite cyclic group of orden n. Let a be a generator of G.

i) order of $a \mid n$

ii) a^n = e (identity)

iii) order of a^k = (order of a) / (gcd (k, order of a))

Z_n X Z_m is a cyclic group if and only if gcd (n,m) = 1.

Each cyclic group is abelian but not vice versa.

Number of generators of $Z_p \setminus \{0\}$ is equal to $\varphi(p\text{-}1)$ where p is prime.

3.2 RINGS

Let R be a set with two operations (addition and multiplication) satisfying the following axioms:

1) R is an abelian group under addition.
2) Under multiplication R satisfies
   i. closure law
   ii. associative law
   iii. both left and right distributive law over addition such that

   x(y + z) = xy + xz (left distributive law)

   (x + y)z = xz + yz (right distributive law)

Then, R is called a *ring*.

Example1: Z is a ring.

Example2: R is a ring.

Example3: C is a ring.

3.2.1 Commutative Ring:

A ring R is a *commutative ring* if the property xy = yx is satisfied for all x$\in R$, y$\in R$. For example, Z, R, C are all commutative rings.

Definition3.2.1: Let a and b be nonzero elements of a ring R. If $ab = 0$ then a and b are called *zero divisors*.

Example4: R = Z_{12}, 3.4 = 0. Hence, 3 and 4 are zero divisors.

3.2.2 Integral Domain:

A commutative ring with unity (multiplicative identity), and without zero divisors is called an *integral domain.*

Corollary: Z_p is an integral domain if p is prime.

To illustrate, Z_7 is an integral domain since 7 is prime.

Theorem3.2.1(*Fraleigh, John B.***):** A finite integral domain D is a Field.

3.3 FIELDS

A field F is a set with addition and multiplication operations if the following axioms are satisfied:

I. F is an abelian group under addition.
   a) Closure law: $a \in F, b \in F$ such that $a + b \in F$
   b) Associative law: $a \in F, b \in F, c \in F$ such that $(a + b) + c = a + (b + c)$
   c) Identity element: a is an element of F such that $a + 0 = 0 + a$ for all $a \in F$
   d) Inverse element: For all a in F there is an element b of F such that $a + b = b + a = 0$
   e) Commutative law: $a, b \in F$ such that $a + b = b + a$

II. Under multiplication the following familiar properties are obeyed over F:
   a) Closure law: $a \in F, b \in F$ such that $ab \in F$
   b) Associative law: $a \in F, b \in F, c \in F$ such that $a(bc) = (ab)c$
   c) Distributive law
      i. $a(b + c) = ab + ac$
      ii. $(a + b)c = ac + bc$
   d) Identity element: There is a multiplicative identity 1 such that $a1 = 1a = a$ for all $a \in F\backslash\{0\}$
   e) Commutative law: $a, b \in F$ such that $ab = ba$
   f) Inverse element: There is an multiplicative inverse, denoted by a^{-1}, for all $a \in F\backslash\{0\}$ such that $aa^{-1} = 1 = a^{-1}a$.

Remark: $F\backslash\{0\}$, group of nonzero elements, is an abelian group under multiplication operation.

Example1: The set of complex numbers is a field.

Example2: Z_2 is a field.

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

Example3: The set of rational numbers is a field.

3.3.1 General Properties of Fields:

I)

A field F is contained in a field K. In this case, K is called an *extension field* of F, denoted by $F \leq K$ and F is said to be a *subfield* of K. An extension field K can be regarded as a vector space over the field F. A vector space V, collection of vectors such that $V=\{\alpha, \beta, \gamma, \ldots\ldots\ldots\}$, have to satisfy the following axioms:

a) closure under addition: for all $\alpha, \beta \in V$ such that $\alpha + \beta \in V$.

b) associative under addition: for all $\alpha, \beta, \gamma \in V$ such that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

c) additive identity: for all $\alpha \in V$ such that $\alpha + 0 = 0 + \alpha = \alpha$. (existence of zero vector)

d) additive inverse: for each α in V there is β in V such that $\alpha + \beta = \beta + \alpha = 0$. (existence of additive inverse)

e) commutative under addition: for all $\alpha, \beta \in V$ such that $\alpha + \beta = \beta + \alpha$.

As stated above, any vector space over F, have to be an abelian group under addition operation. Furthermore;

f) closure under multiplication: for all $c \in F$, $\alpha \in V$ such that $c\alpha \in V$

g) distributive law: for all $c \in F$, $\alpha, \beta \in V$ such that $c(\alpha + \beta) = c\alpha + c\beta$.

h) associative under multiplication: for all $c, c' \in F$ and $\alpha \in V$ such that $(c\, c')\alpha = c(c'\alpha)$.

Every vector space has a basis. The cardinality of a basis of any vector space is called the *dimension* of the vector space. If it is finite dimensional then there exists $\{ \alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_f\}$ a basis i.e $\{ c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + \ldots\ldots + c_f\alpha_f : c_i \in F\} = K$.

K is isomorphic to $F \times F \times F \times \ldots \times F$. Therefore $|K| = |F|^f$. If K is finite field, K is finite dimensional vector space over F_p where p is the characteristic of F.

II)

The ring of polynomials over the field F in the variable x is denoted by $F[x]$. If leading coefficient in x is 1 then the polynomial in $F[x]$ is called *monic*. $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$ is called *irreducible* if it can not be divided by a nonconstant polynomial of lower degree. For example, $x^2 + 1$ is irreducible over R but $x^2 + 1$ is reducible over C.

Another example is $x^2 - 2$ over Q. It is irreducible over Q since $\sqrt{2}$ is not rational number. In general $x^2 - p$ is irreducible over Q if p is prime.

Theorem3.3.1(*Fraleigh, John B.***):** $F[x]$ is Unique factorization domain.

III)

Let K be an extension field of F. Also let β be an element of the field K. Then β is called *algebraic* over F if there exists a polynomial $f(x)$ in $F[x]$ such that $f(\beta) = 0$. Otherwise, β is called *transcendental* over F.

Example4: π is not algebraic over Q since there exists no polynomial $f(x) \in Q[x]$ such that $f(\pi) = 0$.

Example5: i is algebraic over R since i is a root of $x^2 + 1 \in R[x]$.

Example6: $Q \leq Q(\sqrt{2}) = \{a + b\sqrt{2} : a,b \in Q\}$

$\sqrt{2}$ is algebraic over Q as $\sqrt{2}$ is a root of $x^2 - 2 \in Q[x]$.

Theorem3.3.2(*Fraleigh, John B.***):** The set of all algebraic numbers in C is countable. Hence, transcendental numbers are uncountable.

Let $F \leq K$, α be in K and α is algebraic over F. ∃ a polynomial $f(x) = a_0 + a_1x + \ldots\ldots + a_nx_n$ such that $f(\alpha) = 0$ where $f \in F[x]$. It implies that there is a unique monic irreducible polynomial $\text{Irr}(\alpha,F)(x)$ such that $\text{Irr}(\alpha,F)(\alpha) = 0$.

Example7: $Q \leq C$

As $i \in C$, $\text{Irr}(i,Q)(x) = x^2 + 1$

Example8: $Q \leq Q(\sqrt{2})$

As $\sqrt{2} \in Q(\sqrt{2})$, $\text{Irr}(\sqrt{2},Q)(x) = x^2 - 2$

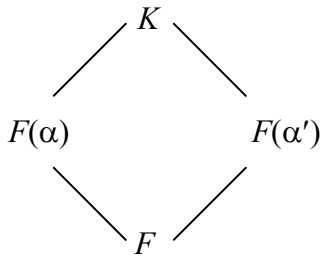
Theorem3.3.3(*Fraleigh, John B.***):** Let α be an algebraic element in K over F of degree $k(k = \deg(\text{Irr}(\alpha,F)(x))$.

Then $F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \ldots\ldots + a_k\alpha^k : a_i \in F\} \subset K$.

If α′ is another root of $\text{Irr}(\alpha,F)(x)$ i.e $\text{Irr}(\alpha,F)(\alpha') = 0$, it implies that α′ is algebraic over F and $\deg(\text{Irr}(\alpha',F)(x)) = \deg(\text{Irr}(\alpha,F)(x))$ and it is called conjugate of α.

$F(\alpha)$ is isomorphic to $F(\alpha')$ since there is an isomorphism between two fields.

Definition3.3.1: An isomorphisim from F to F itself is called an *automorphism*.



IV)

Let F be a field. And let a polynomial $f(x) = a_0 + a_1x + \ldots\ldots + a_nx_n$ be in $F[x]$. α is a root of order r if $f(x)$ is equal to $(x-\alpha)^r g(x)$ where $g(x)$ is a nonzero polynomial in F[x]. If r is 1 then α is called *simple root*. If r is greater than 1 then α is called a *multiple root*. r is called α's *multiplicity*. The derivative of polynomial $f(x)$ can be calculated as usual : $(h(x))' = ((x-\alpha)^r g(x))' = r((x-\alpha)^{r-1} g(x)) + (x-\alpha)^r g'(x)$.

If r is greater than 1, α is a root of derivative of $f(x)$. In that case it implies that α is a root of $\gcd(f(x), f'(x))$.

Corollary: Let α be a root of f. If α is not a root of $f'(x)$, it implies that α is a simple root.

V)

Let F be a field. And let $f(x)$ be contained in $F[x]$. The splitting field of f is a smallest extension field of $K[x]$ such that all roots of $f(x)$ lie in $K[x]$. To illustrate, $Q(\sqrt{13})$ is splitting field of $x^2 - 13$ over Q.

VI)

Let F be a field. The characteristic of F is the smallest positive integer p such that sum of the multiplicative identity 1, p times equals to zero. Then p is called *characteristic* of the field F. If $\exists$ no such positive integer p then we say that the characteristic of the field is zero. In other words, it is said to be *characteristic zero*.

Example9:

i. $\text{char}(Q) = 0$
ii. $\text{char}(R) = 0$
iii. $\text{char}(C) = 0$
iv. $\text{char}(Q(\sqrt{2})) = 0$
v. $\text{char}(Z_2) = 2$
vi. $\text{char}(Z_{13}) = 13$

vii. $\text{char}(Z_p) = p$ if p is prime.

	Group	Abelian group	Ring	Commutative ring	Integral domain	Field
Closure under addition	√	√	√	√	√	√
Associativity of addition	√	√	√	√	√	√
Additive identity	√	√	√	√	√	√
Additive inverse	√	√	√	√	√	√
Commutative of addition		√	√	√	√	√
Closure under multiplication			√	√	√	√
Associativity of multiplication			√	√	√	√
Distributive law			√	√	√	√
Commutativity of multiplication				√	√	√
Multiplicative identity					√	√
No zero divisors					√	√
Multiplicative inverse						√

Table 3.3.1

3.4 FINITE FIELDS

Finite field is a field consisting of a finite number of elements. Let F_q be a finite field. q denotes the number of elements in F_q. Let F_q have characteristic p. Then F_p is the subfield of F_q. F_q can be regarded as a finite dimensional vector space over F_p. Hence $|F_q| = |F_p|^f$ where f is dimension of the vector space F_q over F_p. Therefore, q is equal to p^f where p is prime integer f is positive integer. $F_q \backslash \{0\}$, denoted by F^*, means under multiplication. Order of F_q^* is q-1. Let a be in F_q^*. Then, order of a divides q-1. In other words, a is a zero of the polynomial x^{q-1}-1.

Theorem3.4.1(*Fraleigh, John B.***):** F_q is a splitting field of x^q-x over F_p.

Let $f(x)$ be in $F[x]$. $\exists$ a smallest extension field E such that $F \leq E$ and all the roots of f are in E. Such E is called *splitting field* of f over F. F_q^* which is an abelian group is isomorphic to $Z_{p_1}^{k_1} \times Z_{p_2}^{k_2} \times \ldots\ldots\ldots \times Z_{p_m}^{k_m}$ where $p_1, p_2, \ldots, p_m$ are distinct prime integers.

Theorem3.4.2(*Fraleigh, John B.***):** F_q^* is a cyclic group.

F_q is a cyclic group. Let a be a generator. Then, a^k is also a generator of F_q^* if and only if gcd(k, ord$a$) = 1. Order of a is q-1. Number of generators of F_q^* is equal to $\varphi(q-1)$. For example, F_{11}^* has 4 generators such that $\varphi(11\text{-}1) = \varphi(10) = (2\text{-}1)(5\text{-}1) = 4$. $\{2,6,7,8\}$ is the set of all generators of F_{11}^*.

Theorem3.4.3(*Fraleigh, John B.***):** Let G be a finite abelian group of order n. G is isomorphic to $Z_{p_1}^{k_1} \times Z_{p_2}^{k_2} \times \ldots\ldots\ldots \times Z_{p_m}^{k_m}$ such that $p_1^{k_1} p_2^{k_2} \ldots\ldots p_m^{k_m} = n$ where $p_1, p_2, \ldots,$ p_m are prime integers.

3.4.1 Existence of a Finite field

As it is stated above, q is equal to p^f where p is prime and f is a positive integer.

Theorem3.4.4(*Fraleigh, John B.***):** The *splitting field* of $x^q - x = x^{p^f} - x$ is exactly a field such that $F_p \leq E$, E is the set of all roots of x^q-x. In fact the roots of $x^{p^f} - x$ in E become a field. For all fields F there exists an extension field $\bar{F}$, which is called the algebraic closure of F, such that if $f(x)$ is in $F[x]$ then it can be written as the product of linear polynomials in $\bar{F}$ [x]. F is the subset of $\bar{F}$. Hence F_q can be regarded as the roots of $x^{p^f} - x$ in the algebraic closure $\bar{F}$ of F_p.

Lemma3.4.1: Let E be a field of characteristic p. Then $(\alpha+\beta)^p = \alpha^p + \beta^p$.

Corollary: Let E be a field of characteristic p.Then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$

Theorem3.4.5(*Fraleigh, John B.***):** $x^{p^f} - x$ is the product of all monic irreducible polynomials over F_p of degree d which is a divisor of f.

Let's find all irreducible polynomials of degree 2 over Z_3.

$$x^{3^2} - x = x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) = x(x^2 - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1) =$$
$$= x(x-1)(x+1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1)$$

Hence ∃ only three irreducible polynomials of degree 2 in $z_3[x]$.

3.4.2 Explicit Construction

Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ since $\langle f(x)\rangle$ is maximal ideal, $F[x] / \langle f(x)\rangle$ is a field. F can be regarded as a subfield of $F[x] / \langle f(x)\rangle$ via the definition $a \to a + \langle f(x)\rangle$. Let α be a root of f in F such that $F(\alpha) = \{1, \alpha,\alpha^2,...,\alpha^{n-1}\} = \{a_1 + a_2\alpha + a_3\alpha^2 + ... + a_{n-1}\alpha^{n-1} : a_i \in F\}$ is a basis of the vector space $F(\alpha)$ over F where $n = \deg f$.

Number of distinct monic irreducible polynomials of degree f over F_p is $\dfrac{p^f - p}{f}$

where p is prime and f is a positive integer. If p is not prime, number of distinct monic irreducible polynomials of degree d in $F_p[x]$ is equal to $\dfrac{p^f - \sum_{d/n} dn_d}{f}$ where the summation is over all divisors d of f.

Proposition: Let F_q be a finite field. q is equal to p^f where p is prime and f is a positive integer.

$G: x \to x^p$ .Then G is an automorphism, which is called Frobenius automorpism, of F_q. It is one to one. And G is onto since $\#F_q$ is finite.

Let γ be an automorphism of F_p^f leaving the element of F_p fixed.There exists i such that $\gamma = G^i$.

Lemma3.4.2: If ς is an automorphism of F_p^f then it is identify on F_p.

3.4.3 Construction of Finite Fields

Let's construct F_9. We take monic irreducible polynomials of degree 2 in $F_3[x]$. List of all monic polynomials degree 2 are x^2, $x^2 \pm 1$, $x^2 \pm x$, $x^2 \pm x + 1$, $x^2 \pm x + 2$.

Elements of F_3 are 0,1 and 2. To illustrate, substituting in $x^2 + 2x + 2$ gives the values; 0 + 0 + 2 = 2 , 1 + 2 + 2 ≡ mod 3 , 4 + 4 + 2 ≡ 1 mod 3. Hence $x^2 + 2x + 2$ is irreducible. If we do the same procedure for the monic polynomial of degree 2 stated above, we see that $x^2 + 1$, $x^2 \pm x + 2$ are the only monic irreducible polynomials of degree 2 in $F_3[x]$. $F_9\backslash\{0\}$ is cyclic and its order is 8. Let α be a root of $x^2 + x + 2$. $\alpha_2 + \alpha + 2 = 0 \Rightarrow \alpha_2 = 2\alpha + 1$.

Let's find elements of $F_9\backslash\{0\}$ by finding powers of α:

$\alpha^1 = \alpha$, $\alpha^2 = 2\alpha + 1$, $\alpha^3 = 2\alpha + 2$, $\alpha^4 = 2$, $\alpha^5 = 2\alpha$, $\alpha^6 = \alpha + 2$, $\alpha^7 = \alpha + 1$, $\alpha^8 = 1$

Therefore, $x^2 + x + 2$ is primitive.

Now let's construct F_8. We take monic irreducible polynomials of degree 3 in $F_2[x]$ as $8 = 2^3$. List of all monic polynomials of degree 3 are $x^3 + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^3 + x^2 + x + 1$. Elements of F_2 are 0 and 1. $x^3 + x + 1$, $x^3 + x^2 + 1$ are the only monic irreducible cubic polynomials. Let α be a root of $x^3 + x + 1$. $\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$.

Then let's find the elements of $F_8\backslash\{0\}$ by finding powers of α:

$\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$, $\alpha^7 = 1$.

3.5 PRIMITIVE ROOT

Lemma: Assume that g is a generator of F_q^* where q is equal to p^f.

1) If nk is divisible by q-1 then g^k is n-th rooth of unity.
2) Number of n-th rooth of unity = gcd (n, q-1).
3) If $n \mid q$-1 then F_q has primitive n-th rooth of unity.
4) ξ which is primitive n-th rooth of unity in F_q provides that ξ^k is primitive n-th rooth of unity if and only if k is relatively prime to n.

Definition3.5.1: j is called n-th rooth of unity if $j^n = 1$ in F_q or j is a rooth of x^n-1 in F_q.

Definition3.5.2: ξ is primitive n-th rooth of unity if $\{ \xi, \xi^2, \ldots\ldots, \xi^{n-1}, \xi^n = 1\}$ are all distinct. In any field, α is primitive n-th rooth of unity if and only if number of $\{ \alpha , \alpha^2, \ldots\ldots, \alpha^{n-1}, \alpha^n = 1\}$ is equal to n.

Corollary 3.5.1: If n is relatively prime to q-1 then 1 is the only n-th rooth of unity.

For example; 5-th rooth of unity is 1 in F_9 since gcd (5, 8) = 1.

Corollary3.5.2: There exists -1 in F_q such that -1 is a zero $x^2 + 1$ in F_q if and only if $q \equiv 1 \pmod 4$.

3.6 QUADRATIC RESIDUES

Let p be prime and $p > 2$. Let α be a nonzero element of F_p and relatively prime to p. In other words, α is an element of F_p^*. α is called a quadratic residue modulo p if $x^2 \equiv \alpha \bmod p$ has a solution, i.e, there exists $b \in F_p$ such that $b^2 \equiv \alpha \bmod p$. Otherwise, α is called a quadratic non-residue. For example, let p be 7 . In order to determine quadratic residues of F_7, we calculate squares of 1,2,3,4,5,6 mod 7 . We find that $1^2 \equiv 6^2 \equiv 1 \bmod 7$, $2^2 \equiv 5^2 \equiv 4 \bmod 7$, $3^2 \equiv 4^2 \equiv 2 \bmod 7$. So the quadratic residues of F_7 are 1,2,4 and the quadratic non-residues of F_7 are 3,5, and 6. There exists exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues. In terms of generator we can characterize qauadratic residue in the following way:

Let g be in F_p and be a generator of F_p^*. g^k is a quadratic residue if and only if ∃ g^l in F_p^* such that $(g^l)^2 \equiv g^k \bmod p$ where $2l = k$ if and only if k is even.

Lemma3.6.1: Let g be a generator of F_p^*.

Quadratic residues are $g^2, g^4, g^6, g^8, \ldots\ldots, g^{p-1}$. Quadratic non-residues are $g, g^3, g^5, g^7, g^9, \ldots\ldots, g^{p-2}$.

To illustrate, 3 is a generator of F_7^*.

3, $3^3 = 6$, $3^5 = 5$ are all quadratic non-residues. $3^2 = 2$, $3^4 = 4$, $3^6 = 1$ are all quadratic residues.

3.6.1 Legendre Symbol

We use legendre symbol to find out an integer is a quadratic residue or not. Let p be an odd prime. Let a be an integer

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a; \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

By maple
➢ legendre(a, p);

Euler's Criterion:

Let p be prime and $p > 2$. Let a be an integer coprime to p.

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

proof:

1.case: If p divides a then $\left(\frac{a}{p}\right) = 0$

$a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0 \bmod p$

2.case: Assume that p doesn't divide a. Let g be a generator of F_p^*.

i. Assume $\left(\frac{a}{p}\right) = 1$. a is a quadratic residue modulo p then $a = g^k$ where k is even. By

Fermat's Little Theorem, $\left(g^k\right)^{\frac{p-1}{2}} \equiv g^{\left(\frac{k}{2}\right)(p-1)} \equiv 1 \bmod p$. Hence $\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \bmod p$ if $\left(\frac{a}{p}\right) = 1$.

ii. Assume $\left(\frac{a}{p}\right) = -1$. a is a quadratic non-residue modulo p then $a = g^k$ where k is odd. $\left(g^k\right)^{\frac{p-1}{2}} \equiv -1 \bmod p$ since k is odd.. Hence $\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \bmod$ p if $\left(\frac{a}{p}\right) = -1$.

In other words, $a^{\left(\frac{p-1}{2}\right)} \equiv \pm 1 \bmod p$.

To illustrate, let a be 3 and p be 7. $3^3 \equiv -1 \bmod 7$. According to Euler's criterion $\left(\frac{3}{7}\right) = -1$. So 3 is quadratic non-residue. Let a be 2 and p be 7. $2^3 \equiv 1 \bmod 7$. Thus $\left(\frac{2}{7}\right) = 1$ and 2 is a quadratic residue.

Properties of Legendre symbol:

Let p be odd prime $p \nmid a, p \nmid b$.

1) If $a \equiv a' \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ where b is prime to p.

4) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} =$

1 if $p \equiv \pm 1 \bmod 8$

-1 if $p \equiv \pm 3 \bmod 8$

6) Law of quadratic reciprocity:

If q is an odd prime then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{otherwise} \end{cases}$$

3.6.2 Jacobi Symbol:

Definition3.6.1: Let m be an odd integer greater than 2 and a be an integer.

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}.....\left(\frac{a}{p_k}\right)^{\alpha_k} \quad \text{where } m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}.....{p_k}^{\alpha_k}.$$

By maple
➢ jacobi (a, p);

Properties of Jacobi Symbol:

1) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$

2) $\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$ if and only if $a \equiv b \bmod n$.

3) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}} =$ 1 if $m \equiv 1 \bmod 4$

-1 if $m \equiv -1 \bmod 4$

4) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}} =$ 1 if $m \equiv \pm 1 \bmod 8$

-1 if $m \equiv \pm 3 \bmod 8$

5) Let n and m be odd integers greater than 2 and n be relatively prime to m.

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

CHAPTER 4

CRYPTOGRAPHY

4.1 SOME SIMPLE CRYPTOSYSTEMS

Cryptology is a mathematical science dealing with cryptography and cryptanalysis. The area of enciphering or encryption is said to be *cryptography*. The area of analysis of ciphertext and decryption of ciphertext without knowing key is called *crytanalysis*. *Plaintext* is the original message or data which is readable and unencrypted. Encrypted form of original text or data is called *ciphertext*. Transforming plaintext to disguised message is said to be *encryption* or *enciphering*. Rebuilding the original message from the ciphertext is called *decryption* or *deciphering*. *Cipher* is an algorithm for enciphering or deciphering with a key. A *code* is any set of words, phrases or signs which are transformed into something having special meaning. A cipher can be compared with a code. In cipher, an algorithm and a key are needed for encryption or decryption. Otherwise, in code, we need only a codebook to form a codetext or restoring plaintext. For example, the dot code, the knot code, the playing card code, the red-blue code and the crease code etc. There are three types of ciphers which are classical, rotor machines and contemporary. This chapter, we will describe classical cryptosystems.

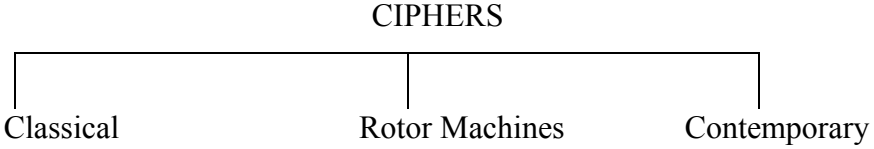


Figure 1 - Ciphers

In classical cryptosystems, we use the same key for encryption and decryption. A plaintext and ciphertext messege units can be single-letter, digraph which is block of

two letters, trigraph which is block of three letters etc. Let P be set of all possible plaintext message units and let C be set of all possible ciphertext message units. Enciphering transformation is a mapping f such that $f:P\rightarrow C$. Deciphering transformation is a mapping f^{-1} such that $f^{-1}:C\rightarrow P$. Both enciphering and deciphering transformation are one-to-one and onto. Such a system is called a *cryptosystem.*

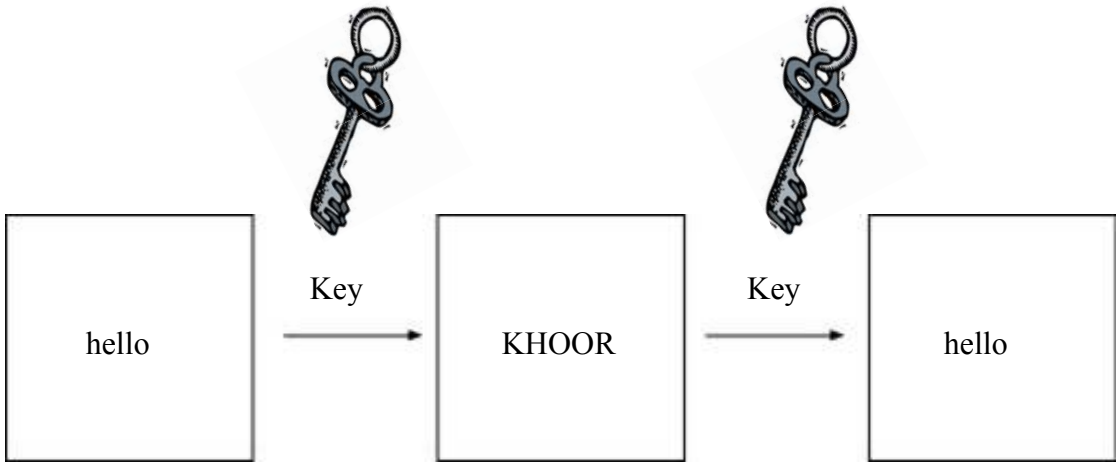


Figure 2 – Classic Cryptography

To encrypt a plaintext, we need to convert plaintext message units P into their numerical equivalents. For eaxample, let P be single-letter. Assume that we use 26-letter alphabet. Letters A-Z correspond to their numerical equivalents 0-25 such that A→0, B→1, C →2, D→3, E→4, F→5, G→6, H→7, I→8, J→9, K→10, L→11, M→12, N→13, O →14, P→15, Q→16, R→17, S→18, T→19, U→20, V→21, W→22, X→3, Y→24, Z →25. For digraphs, suppose that numerical equivalents of x and y, two letters of digraph, be an element of {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} . We label digraphs by $26x + y$. Then each digraph is in the interval [0,675].

4.1.1 Substitution Ciphers

4.1.1.1 Shift Cipher

Shift Cipher depends on modular arithmetic. It is defined over Z_m. For example, since English letter alphabet consists of 26-letter, it is defined over Z_{26}. K is the key, $0 \leq K \leq$ m-1. Letters in the plaintext or ciphertext are converted to their numerical equivalents 0,1,2,.....,m-2,m-1 to encrypt or decrypt. For enciphering, numerical

equivalent of each letter in original message is shifted by K places such that $C \equiv P + K \pmod{m}$, where P is the numerical equivalents of plaintext message unit and C is the numerical equivalent of ciphertext message unit. Decryption algorithm is $P \equiv C - K \pmod{m}$. Caesar Cipher is the special case of shift Cipher. Caesar Cipher is defined over Z_{26} and K is 3.

$$C \equiv P + K \pmod{26}$$
and
$$P \equiv C - K \pmod{26}$$

Caesar Cipher

There are exactly N different shift transformations with an N-letter alphabet.

Eample 1 :

By Caesar cipher, we will encrypt plaintext "caesar cipher was used by julius caesar". To begin with, we transform letters into their numerical equivalents

2,0,4,18,0,17,2,8,15,7,4,17,22,0,18,20,18,4,3,1,24,9,20,11,8,20,18,2,0,4,18,0,17

Next, we use $C \equiv P + 3 \bmod 26$, this yields

5,3,7,21,3,20,5,11,18,10,7,20,25,3,21,23,21,7,6,4,1,12,23,14,11,23,21,5,3,7,21,3,20

Corresponding letters of ciphertext are

FDHVDUFLSKHUZDVXVHGEBMXOLXVFDHVDU.

Example 2:

Suppose that key is 3 and ciphertext is "FDHVDUFLSKHULVXQVHFXUH". First, we translate each letter in ciphertext to their numerical equivalents.

5,3,7,21,3,20,5,11,18,10,7,20,11,21,23,16,21,7,5,23,20,7 .

Applying $P \equiv C\text{-}3 \pmod{26}$, we obtain

2,0,4,18,0,17,2,8,15,7,4,17,8,18,20,13,18,4,2,20,17,4.

Corresponding letters of plaintext is "caesarcipherisunsecure".

Example 3:

In this example, we use frequency analysis to decrypt the message "OZQNZ XHFJXFWZXJIHFJXFWHNUMJWYTHTRRZSNHFYJBNYMMNXXTQINJWX". It is enciphered by shift transformation and plaintext message units are on single-letter in 26-letter alphabet. It is known that the most occurring letter in the plaintext is "S". First we count each letter in the ciphertext and the most occurring letter is “X”

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number of occurrences	0	1	0	0	0	5	0	5	2	6	0	0	3

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number of occurrences	6	1	0	2	2	1	3	1	0	4	7	3	4

As the most occurring letter in the ciphertext is "X", "X" corresponds to "S". If this is so, then $23 \equiv 18+K \pmod{26}$. Hence, $K \equiv 5 \pmod{26}$. Next, subtract 5 from the numerical equivalents of "OZQNZXHFJXFWZXJIHFJXFWHNUMJWYTHTRRZSNHFYJBNYMMNXXTQINJ WX". Be careful that subtraction is in modulo 26.

"OZQNZXHFJXFWZXJIHFJXFWHNUMJWYTHTRRZSNHFYJBNYMMNXXTQINJWX"=14,25,16,13,25,23,7,5,9,23,5,22,25,23,9,8,7,5,9,23,5,22,7,13,20,12,9,22,24,19,7,19,17,17,25,18,13,7,5,24,9,1,13,24,12,12,13,23,23,19,16,8,13,9,22,23→9,20,11,8,20,18,2,0,4,18,0,17,20,18,4,3,2,0,4,18,0,17,2,8,15,7,4,17,19,14,2,14,12,12,20,13,8,2,0,19,4,22,8,19,7,7,8,18,18,14,11,3,8,4,17,18="JULIUSCAESARUSEDCAESARCIPHERTOCOMMUNICATEWITHHISSOLDIERS".

Example 4:

Let plaintext and ciphertext message units be digraph. For encyription and decryption, 27-letter alphabet is used in which A-Z correspond to 0-25 and blank = 26. Alice wants to send her message "be careful" to Bob. To encrypt the message, she breaks it into groups of two letters and converts the letters into their numerical equivalents. And she obtains

“be” = 31 " ‘blank’c” = 704 “ar” = 17 “ef” = 113 “ul” = 551.

The key is 300, known by Bob and Alice. Then she encrypts the message by using shift transformation $C \equiv P + 300 \pmod{729}$, and she obtains 331,275,317,413,122.

Next, she translates back to letters such that

331 = 12.7 + 7 = "MH"

275 = 10.27 + 5 = "KF"

317 = 11.27 + 20 = "LU"

413 = 15.27 + 8 = "PI"

122 = 4.27 + 14 = "ED"

Encyrpted message becomes MHKFLUPIED, and she sends the message to Bob. Bob knows that ciphertext is digraph and the key is 300. For decryption, he first translates digraphs into their numarical equivalents and this yields

"MH" = 331, "KF" = 275, "LU" = 317, "PI" = 413, "ED" = 122.

Applying shift transformation $P \equiv C$-300(mod 729) , he obtains 31,704,17,113,551.

Then, he changes back to letters such that

31 = 1.27+4 = "be"

704 = 26.27+2 = " c"

17 = 0.27 + 17 = "ar"

113 = 4.27 + 5 = "ef"

551 = 20.27 + 11 = "ul".

He obtains the message "be careful".

Example 5:

The message GVCTXSPSKCMWEQEXLIQEXMGEPWGMIRGIHIEPMRKA MXLGVCTXSKVETLCERHGVCTXEREPCWMW was encrypted by shift transformation of single-letter plaintext message units in the 26-letter alphabet. The most occurring letter in the ciphertext is "E". "E" is the encryption of "A".

"E" in the ciphertext corresponds to "A" in the plaintext such that $4 \equiv 0 + K$(mod 26). Then

$K \equiv 4$(mod 26). The deciphering transformation is $P \equiv C$ - 4(mod 26), $0 \leq P \leq 25$. We first change letters in ciphertext into their numerical equivalents.

6,21,2,19,23,18,15,18,10,2,12,22,4,16,4,23,11,8,16,4,23,12,6,4,15,22,6,12,8,17,6,8,7,8, 4,15,12,17,10,0,12,23,11,6,21,2,19,23,18,10,21,4,19,11,2,4,17,7,6,21,2,19,23,4,17,4,15, 2,22,12,22.

Next we perform deciphering transformation to recover plaintext, and we obtain

2,17,24,15,19,14,11,14,6,24,8,18,0,12,0,19,7,4,12,0,19,8,2,0,11,18,2,8,4,13,2,4,3,4,0,11 ,8,13,6,22,8,19,7,2,17,24,15,19,14,6,17,0,15,7,24,0,13,3,2,17,24,15,19,0,13,0,11,24,18, 8,18 = "cryp tologyisamathematicalsciencedealingwithcryptographyandcryptanalysis".

4.1.1.2 Affine Cipher

Affine cipher is monoalphabetic and symmetric. It is the generalization of shift cipher such that $C \equiv aP + b$(mod m),$0 \leq C \leq$ m-1 with gcd (a,m) =1 and $b \in Z_m$, $a \in Z_m^*$. m is the size of alphabet. If $a = 1$ then affine cipher is a shift cipher. To cryptanalyze,

we first convert letters in ciphertext to numerical equivalents. The relationship $P \equiv a^{-1}(C-b) \pmod{m}$, $0 \leq P \leq m-1$, is used to restore numerical equivalents of original message. a^{-1} is the inverse of a modulo m and an element of Z_m^*. In affine transformation, a and b are keys.

Another special case of affine transformation is linear transformation such that, if $b = 0$, $P \equiv aC \pmod{m}$ and $C \equiv a^{-1}P \pmod{m}$. There are $N\varphi(N)$ different affine enciphering transformations with an N-letter alphabet. For digraphs in an N-letter alphabet there are $N^2\varphi(N^2)$ different afine enciphering transformations.

Example6:

Let $a = 7$ and $b = 9$. We use single message units in the 27-letter alphabet. In this alphabet, the letters A-Z have numarical equivalents 0-25 and blank = 26. We work in Z_{27} and want to encipher the message "shift and linear transformations are special case of affine transformation". We first convert letters into their numerical equivalents. This becomes

18,7,8,5,19,26,0,13,3,26,11,8,13,4,0,17,26,19,17,0,13,18,5,14,17,12,0,19,8,14,13,18,26,0,17,4,26,18,15,4,2,8,0,11,26,2,0,18,4,26,14,5,26,0,5,5,8,13,4,26,19,17,0,13,18,5,14,17,12,0,19,8,14,13. Applying affine transformation $C \equiv 7P + 9 \pmod{27}$, we obtain

0,4,11,17,7,2,9,19,3,2,5,11,19,10,9,20,2,7,20,9,19,0,17,26,20,12,9,7,11,26,19,0,2,9,20,10,2,0,6,10,23,11,9,5,2,23,9,0,10,2,26,17,2,9,17,17,11,19,10,2,7,20,9,19,0,17,26,20,12,9,7,11,26,19.

Changing back to letters, we obtain

AELRHCJTDCFLTKJUCHUJTAR UMJHL TACJUKCAGKXLJFCXJAKC RC JRRLTKCHUJTAR UMJHL T.

Example7:

Suppose that $a = 3$ and $b = 2$. We use digraph message units in the 26-letter alphabet in which A-Z have numerical equivalents 0-25. The plaintext is the string "TherewillbeanexplosionatLeventsubway ". To encrypt, we first break it into groups of two letters. "Th er ew il lb ea ne xp lo si on at le ve nt su bw ay". Converting message units into their numerical equivalents x and y correspond to the integer $26x + y$, we have

494,121,126,219,287,104,338,598,300,476,117,19,290,550,357,488,48,24.

Using the affine transformation $C \equiv 3P + 2 \pmod{676}$, we obtain

1484,365,380,659,863,314,1016,1796,902,1430,353,59,872,1652,1073,1466,146,74.

Converting back to letters , we obtain

FC, OB, OQ, ZJ, HF, MC, NC, RC, IS, DA, NP, CH, HO, LO, PH, EK, FQ, CW. And the ciphertext is “FCOBOQZJHFMCNCRCISDANPCHHOLOPHEKFQCW".

Example8:

Let enciphering keys be a = 5 and b = 27. We are working in the 28-letter alphabet in which A-Z have numerical equivalents 0-25, “blank” = 26 and “.” =27. To encrypt, we use trigraph message units. Plaintext is "Mr. President will be poisoned by arsenic". Writing plaintext in groups of three, we obtain "Mr." , " Pr","esi","den","t w","ill", " be", " po","iso","ned", " by"," ar","sen","ic.". Translating message units into thier numerical equivalents x, y and z correspond to the integer $28^2x + 28y + z$, we obtain

9911,20821,3648,2477,15646,6591,20416,20818,6790,10307,20436,20401,14237,6355

. Using affine transformation $C \equiv 5P + 27 (\text{mod } 28^3)$, this becomes

5678,16324,18267,12412,12401,11030,14299,16309,12025,7658,14399,14224,5356,9850.

Changing back to the letters, we have “HGW”,”UXA”,”XIL”,”PXI”,”PWZ”,”OB ", “SGT”,”UWN”,”PJN”,” JVO”, “SKH”,”SEA”,”GXI”,”MPW”.

Hence encrypted message is HGWUXAXILPXIPWZOB SGTUWNPJNJVOSKHSE AGXIMPW.

Example9:

We work on single letter in the 27-letter alphabet with A-Z correspond to 0-25 and “blank” = 26. Suppose that a = 17 and b = 24. To cryptanalyze the message “YBBZCLHE ZJILQHZGHMTCTYWJIYOLXZEHYCVHGAMMLXQZE”, we need to find inverse of a modulo 27 as $P \equiv a^{-1}(C-b) (\text{mod } 27)$. By Euclidean algorithm, we obtain

$$27 = 1.17+10$$

$$17 = 1.10+7$$

$$10 = 1.7+3$$

$$7 = 2.3+1$$

Hence gcd (27,17) = 1

By Extended Euclidean algorithm, we have

$$1 = 7-2.3$$

$$= 7\text{-}2(10\text{-}1.7)$$
$$= 3.7\text{-}2.10$$
$$= 3(17\text{-}1.10)\text{-}2.10$$
$$= 3.17\text{-}5.10$$
$$= 3.17\text{-}5(27\text{-}1.17)$$
$$= 8.17\text{-}5.27$$

Therefore, $17^{-1} \equiv 8(\text{mod } 27)$.

First, we convert letters to their numerical equivalents.

24,1,1,25,2,11,7,4,25,9,8,11,16,7,25,6,7,12,19,2,19,24,22,9,8,24,14,11,23,25,4,7,24,2,21,7,6,0,12,12,11,23,16,25,4 .

Then we obtain by using $P \equiv 8(C\text{-}24) \text{ (mod } 27)$.

0,5,5,8,13,4,26,2,8,15,7,4,17,26,8,18,26,12,14,13,14,0,11,15,7,0,1,4,19,8,2,26,0,13,3,26,18,24,12,12,4,19,17,8,2.

Next we translate back to letters and we have "affine cipher is monoalphabetic and symmetric".

Example10:

We are working in Z_{26}. The letter A-Z have numerical equivalents 0-25 and affine cipher operates on single letter. Intercepted ciphertext is “SOLAIUIBPOBQYLZYJT ZIS”. We know that the last word in plaintext is "him". In other words, “ZIS” corresponds to "him". This implies, “S” corresponds to "m", “I” corresponds to "i" and “Z” corresponds to "h". By using the affine transformation $C \equiv aP + b(\text{mod } 26)$, we will find keys, a and b.

$$12a + b \equiv 18(\text{mod } 26)$$
$$7a + b \equiv 25(\text{mod } 26)$$

The solution of this system is $a \equiv 9(\text{mod } 26)$ and $b \equiv 14(\text{mod } 26)$. By using Euclidean and extended Euclidean algorithm we obtain

$$26 = 2.9+8$$
$$9 = 1.8+1$$
$$1 = 9\text{-}1.8$$
$$= 9\text{-}1(26\text{-}2.9)$$
$$= 3.9\text{-}1.26$$

We see that, inverse of 9 is 3 modulo 26. Letters in the ciphertext correspond to 18,14,11,0,8, 20,8,1,15,14,1,16,24,11,25,24,9,19,25,8,18.We have $C \equiv 9P+14 \pmod{26}$ and $P \equiv 3(C-14) \pmod{26}$. Correspondence of letters for ciphertext is given in table.

Ciphertext

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
10	13	16	19	22	25	2	5	8	11	14	17	20
K	N	Q	T	W	Z	C	F	I	L	O	R	U

Plaintext

Ciphertext

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
23	0	3	6	9	12	15	18	21	24	1	4	7
X	A	D	G	J	M	P	S	V	Y	B	E	H

Plaintext

By using the correspondence, decryption of ciphertext is "markisindangerhelphim". Therefore original message is "Mark is in danger. Help him".

Example11:

We work on trigraph in the 30-letter alphabet in which A-Z correspond to 0-25, “blank” = 26, “‘” = 27, “!” = 28, “.” = 29.

The ciphertext is

“ADDLUDGYB!AFVSHEERWDGXX'BLGRFYE DIZUCFYTUYKFQSEG'FN KVG JQJNQIZJ.KM!ECCTU.FYQIQDAFUESMGYIPYKFQQNBM' DGMG!Y BEDQPYKFQDWY'PUC G.UYGX'ZUPQARJ'VFCA!SIGUCUEHSVYKZYXZQ' OH'Q BNFYADFRYCUEH'QGCGYJOSPTW”.

We know that the most frequently occurring trigraphs in the ciphertext are "KFQ" and "UEH", in that order. "KFQ" and "UEH" are encryption of "THE" and "ION", respectively. What is needed to be done firstly to decrypt the message is that we change "KFQ" , "UEH" ,"THE" and "ION" into their numerical equivalents $900x + 30y + z$ to obtain keys a and b .

"KFQ" = 900.10 + 30.5 + 16 = 9166 $\rightarrow$ "THE" = 900.19 + 30.7 + 4 = 17314

"UEH"= 900.20 + 30.4 + 7 = 18127 $\rightarrow$"ION" = 900.8 + 30.14 + 13 = 7633

Next, we solve the pair of congruences

$$a17314 + b \equiv 9166 (\text{mod } 27000)$$

$$a7633 + b \equiv 18127 (\text{mod } 27000)$$

By subtracting two congruences, we obtain $9681a \equiv -8961 (\text{mod } 27000)$.

Since gcd (9681,27000)=3 and $3 \mid 8961$, we solve

$$(9681/3)a \equiv (-8961/3) \text{ mod}(27000/3)$$

$$3227a \equiv -2987 (\text{mod } 9000)$$

and there are three soultions of a modulo 27000.

Inverse of 3227 is found by using Euclidean and extended Euclidean algorithm such that

$$9000 = 2.3227 + 2546$$

$$3227 = 1.2546 + 681$$

$$2546 = 3.681 + 503$$

$$681 = 1.503 + 178$$

$$503 = 2.178 + 147$$

$$178 = 1.147 + 31$$

$$147 = 4.31 + 23$$

$$31 = 1.23 + 8$$

$$23 = 2.8 + 7$$

$$8 = 1.7 + 1$$

Then

$$1 = 8-1.7$$

$$= 8-(23-2.8)$$

$$= 3.8-23$$

$$= 3(31-23)-23$$

$$= 3.31-4.23$$

$$= 3.31-4(147-4.31)$$

$$= 19.31-4.147$$

$$= 19(178-1.147)-4.147$$

$$= 19.178-23.147$$

$$= 19.178-23(503-2.178)$$

$$= 65.178-23.503$$

= 65(681-1.503)-23.503

= 65.681-88.503

= 65.681-88(2546-3.681)

= 329.681-88.2546

= 329(3227-1.2546)-88.2546

= 329.3227-417.2546

= 329.3227-417(9000-2.3227)

= 1163.3227-417.9000

Thus , $a = 1163(-2987) \equiv 119 (\text{mod } 9000)$

There are 3 solutions such that

$$a \equiv 119 + \text{k } 9000,\ 0 \leq \text{k} \leq 2$$

Hence $a_1 = 119$, $a_2 = 9119$, $a_3 = 18119$

For $a_1 = 119$, $b_1 = 800$

For $a_2 = 9119$, $b_2 = 18800$

For $a_3 = 18119$, $b_3 = 9800$

We try all three posibilities.

Case 1: $a_1 = 119$

First, we convert trigraphs into their numerical equivalents x,y,and z correspond to $900x + 30y + z$. Next , we need to know inverse of 119 modulo 27000 and $(119)^{-1} \equiv 12479 (\text{mod } 27000)$. Then, applying affine transformation $P \equiv 12479(C\text{-}800) (\text{mod } 27000)$ to numerical equivalents of ciphertext message units, we obtain

"AAD" = 3 → 17237 = "TER"

"LUD" = 10503 → 15737= "ROR"

"GYB" = 6121 → 7759 = "IST"

"!AF" = 25205 → 16995 = "S P"

"VSH" = 19447 → 9913 = "LAN"

"EER" = 3737 → 11823 = "NED"

"WDG" = 19896 → 23984 = " TO"

"XX ' " = 21417 → 23543 = " EX"

"BLG" = 1236 → 13844 = "PLO"

"RFY" = 15474 → 2846 = "DE "

"E D" = 4383 → 257 = "AIR"

"IZU" = 7970 → 23430 = " BA"

"CFY" = 1974 → 16346 = "SE "

"TUY" = 17724 → 596 = "AT "

"KFQ" = 9166 → 17314 = "THE"

"SEG" = 16326 → 23954 = " SO"

" 'FN" = 24463 → 18577 = "UTH"

"KVG" = 9636 → 23444 = " BO"

" JQ" = 23686 → 15394 = "RDE"

"JNQ" = 8506 → 16174 = "R.E"

"IZJ" = 7959 → 21161 = "XPL"

".KM" = 26412 → 13148 = "OSI"

"!EC" = 25322 → 19038 = "VES"

"CTU" = 2390 → 23610 = " HA"

".FY" = 26274 → 19046 = "VE "

"QIQ" = 14656 → 1024 = "BEE"

"DAF" = 2705 → 12495 = "N P"

"UES" = 18138 → 9902 = "LAC"

"MGY" = 11004 → 3716 = "ED "

"IPY" =7674 → 1646 = "BY "

"KFQ" = 9166 → 17314 = "THE"

"QNB" = 14791 → 11689 = "M.T"

"M ' " =11636 → 6444 = "HEY"

"DGM" = 2892 → 24068 = " WI"

"G!Y" = 6264 → 10256 = "LL "

"BED" = 1023 → 1817 = "CAR"

"WPY" = 20274 → 16046 = "RY "

"KFQ" = 9166 → 17314 = "THE"

"DWY" = 3384 → 7736 = "IR "

".PU" = 26570 → 13830 = "PLA"

"C G" =2586 → 12494 = "N O"

".UY" = 26724 → 18596 = "UT "

"GX' " = 6117 → 11843 = "NEX"

"ZUP" = 23115 → 17885 = "T F"

"QAR" = 14417 → 15543 = "RID"

"J'V" = 8931 → 749 = "AY."

"FCA" = 4560 → 22040 = "YOU"

"!SI" = 25748 → 16092 = "R M"

"GUC" = 6002 → 7758 = "ISS"

"UEH" = 18127 → 7633 = "ION"

"SVY" = 16854 → 24866 = " 'S "

"KZY" = 9774 → 17546 = "TO "

"XZQ" = 21466 → 14014 = "PRE"

" 'OH" = 24727 → 19033 = "VEN"

" 'QB" = 24781 → 17899 = "T T"

"NFY" = 11874 → 6446 = "HE "

"ADF" = 95 → 4305 = "EXP"

"RYC" = 16022 → 10338 = "LOS"

"UEH" = 18127 → 7633 = "ION"

" 'QG" = 24786 → 26294 = ".GO"

"CGY" = 2004 → 12716 = "OD "

"JOS" = 8538 → 10502 = "LUC"

"PTW" = 14092 → 9868 = "K!!"

Case 2: $a_2 = 9119$

First, we convert trigraphs into their numerical equivalents x, y,and z correspond to $900x + 30y + z$. Next , we need to know inverse of 9119 modulo 27000 and $(9119)^{-1} \equiv 3479 \pmod{27000}$. Then, applying affine transformation $P \equiv 3479(C\text{-}18800) \pmod{27000}$ to numerical equivalents of ciphertext message units, we obtain

"AAD" = 3 → 26237 = ".ER"

"LUD" = 10503 →→ 24737 = " 'OR"

"GYB" = 6121 → 7759 = "IST"

"!AF" = 25205 → 7995 = "I P"

"VSH" = 19447 → 9913 = "LAN"

"EER" = 3737 → 2823 = "DED"

"WDG" = 19896 → 5984 = "GTO"

"XX ' " = 21417 → 5543 = "GEX"

"BLG" = 1236 → 22844 = "ZLO"

"RFY" = 15474 → 11846 = "NE "

"E D" = 4383 → 9257 = "KIR"

"IZU" = 7970 → 14430 = "QBA"

"CFY" = 1974 → 25346 = "!E "

"TUY" = 17724 → 9596 = "KT "

"KFQ" = 9166 → 17314 = "THE"

"SEG" = 16326 → 5954 = "GSO"

" 'FN" = 24463 → 18577 = "UTH"

"KVG" = 9636 → 5444 = "GBO"

" JQ" = 23686 → 15394 = "RDE"

"JNQ" = 8506 → 16174 = "R.E"

"IZJ" = 7959 → 3161 = "DPL"

".KM" = 26412 → 22148 = "YSI"

"!EC" = 25322 → 10038 = "LES"

"CTU" = 2390 → 14610 = "QHA"

".FY" = 26274 → 1046 = "BE "

"QIQ" = 14656 → 1024 = "BEE"

"DAF" = 2705 → 3495 = "D P"

"UES" = 18138 → 18902 = "VAC"

"MGY" = 11004 → 12716 = "OD "

"IPY" = 7674 → 10646 = "LY "

"KFQ" = 9166 → 17314 = "THE"

"QNB" = 14791 → 11689 = "M.T"

"M ' " = 11636 → 24444 = " 'EY"

"DGM" = 2892 → 6068 = "GWI"

"G!Y" = 6264 → 19256 = "VL "

"BED" = 1023 → 10817 = "MAR"

"WPY" = 20274 → 25046 = " 'Y "

"KFQ" = 9166 → 17314 = "THE"

"DWY" = 3384 → 16736 = "SR "

".PU" = 26570 → 4830 = "FLA"

"C G"= 2586 → 21494 = "X O"

".UY" = 26724 → 596 = "AT "

"GX' " = 6117 → 20843 = "XEX"

"ZUP" = 23115 → 26885 = ". F"

"QAR" = 14417 → 6543 = "HID"

"J'V" = 8931 → 9749 = "KY."

"FCA" = 4560 → 4040 = "EOU"

"!SI" = 25748 → 7092 = "H M"

"GUC" = 6002 → 25758 ="!SS"

"UEH" = 18127 → 7633 = "ION"

"SVY" = 16854 → 6866 = "HS "

"KZY" = 9774 → 26546 = ".O "

"XZQ" = 21466 → 14014 = "PRE"

" 'OH" = 24727 → 19033 = "VEN"

" 'QB" = 24781 → 17899 = "T T"

"NFY" = 11874 → 15446 = "RE "

"ADF" = 95 → 22305 = "YXP"

"RYC" = 16022 → 1338 = "BOS"

"UEH" = 18127 → 7633 = "ION"

" 'QG" = 24786 → 8294 = "JGO"

"CGY" = 2004 → 21716 = "YD "

"JOS" = 8538 → 19502 = "VUC"

"PTW" =14092 → 9868 = "K!!"

Case 3: $a_3 = 18119$

First, we convert trigraphs into their numerical equivalents x, y,and z correspond to $900x + 30y + z$. Next , we need to know inverse of 18119 modulo 27000 and $(18119)^{-1} \equiv 21479 \pmod{27000}$. Then, applying affine transformation $P \equiv 21479(C-95800) \pmod{27000}$ to numerical equivalents of ciphertext message units, we obtain

"AAD" = 3 → 8237 = "JER"

"LUD" = 10503 → 6737 = "HOR"

"GYB" = 6121 → 7759 = "IST"

"!AF" = 25205 → 25995 = "! P"

"VSH" = 19447 → 9913 = "LAN"

"EER" = 3737 → 20823 = "XED"

"WDG" = 19896 → 14984 = "QTO"

"XX ' " = 21417 → 14543 = "QED"

"BLG" = 1236 → 4844 = "FLO"

"RFY" = 15474 → 20846 = "XE "

"E D" = 4383 → 18257 = "UIR"

"IZU" = 7970 → 5430 = "GBA"

"CFY" = 1974 → 7346 = "IE "

"TUY" = 17724 → 18596 = "UT "

"KFQ" = 9166 → 17314 = "THE"

"SEG" = 16326 → 14954 = "QSO"

" 'FN" = 24463 → 18577 = "UTH"

"KVG" = 9636 → 14444 = "QBO"

" JQ" = 23686 → 15394 = "RDE"

"JNQ" = 8506 → 16174 = "R.E"

"IZJ" = 7959 → 21161 = "NPL"

".KM" = 26412 → 4148 = "ESI"

"!EC" = 25322 → 1038 = "BES"

"CTU" = 2390 → 5610 = "GHA"

".FY" = 26274 → 10046 = "LE "

"QIQ" = 14656 → 1024 = "BEE"

"DAF" = 2705 → 21495 = "X P"

"UES" = 18138 → 902 = "BAC"

"MGY" = 11004 → 21716 = "YD "

"IPY" = 7674 → 19646 = "VY "

"KFQ" = 9166 → 17314 = "THE"

"QNB" = 14791 → 11689 = "M.T"

"M ' " = 11636 → 15444 = "REY"

"DGM" = 2892 → 10068 = "QWI"

"G!Y" = 6264 → 1256 = "BL "

"BED" = 1023 → 19817 = "WAR"

"WPY" = 20274 → 7046 = "HY "

"KFQ" = 9166 → 17314 = "THE"

"DWY" = 3384 → 25736 = "!R "

".PU" = 26570 → 22830 = "ZLA"

"C G" = 2586 → 3494 = "D O"

".UY" = 26724 → 9596 = "KT "

"GX' " = 6117 → 2843 = "CEX"

"ZUP" = 23115→ 8885 = "J F"

"QAR" = 14417 → 24543 = "'ID"

"J'V" = 8931 → 18749 = "UY."

"FCA" = 4560 → 13040 = "OOU"

"!SI" = 25748 → 25092 = " ' M"

"GUC" = 6002 → 16758 = "SSS"

"UEH" = 18127 → 7633 = "ION"

"SVY" = 16854 → 15866 = "RS "

"KZY" = 9774 → 8546 = "JO "

"XZQ" = 21466 → 14014 = "PRE"

" 'OH" = 24727 → 19033 = "VEN"

" 'QB" = 24781 → 17899 = "T T"

"NFY" = 11874 → 24446 = " 'E "

"ADF" = 95 → 13305 = "OXP"

"RYC" = 16022 → 19338 = "VOS"

"UEH" = 18127 → 7633 = "ION"

" 'QG" = 24786 → 17294 = "TGO"

"CGY" = 2004 → 3716 = "ED "

"JOS" = 8538 → 1502 = "BUC"

"PTW" = 14092 → 9868 = "K!!"

We see that only the first one $P \equiv 12479(C\text{-}800)(\text{mod } 27000)$ gives a meaningful plaintext. The message is "terrorists planned to explode air base at the south border.explosives have been placed by them. they will carry their plan out next friday.your mission's to prevent the explosion. good luck!!

4.1.1.3 Vigenére Cipher

Vigenére cipher was invented by Blaise Vigenére. Vigenére cipher is a polyalphabetic substitution cipher. Several Caesar ciphers in sequence are used in vigenére cipher. Vigenére cipher is defined over Z_{26} . A vigenére table is used with a keyword for encryption.

In table 4.1.1, row is for key character and column is for plaintext character. Intersection of row and column gives us ciphertext character. To illustrate, assume that keyword is code and plaintext is " a polyalphabetic substitution cipher consist of two or more cipher alphabets".

First, we write keyword below plaintext repeating it until it equals the length of plaintext.

PLAINTEXT: apolyalphabeticsubstitutioncipherconsistsoftwoormorecipheralphabets

KEY: codecodecodecodecodecodecodecodecodecodecodecodecodecodecodecodecod

The first character of plaintext "a", corresponds to"c", intersection of down column "a" and over row "c". Second plaintext character "p" corresponds to "d", intersection of down column "p", and over row "o" .If we repeat the same procedure we obtain the ciphertext

"CDRPAOOTJOEIVWFWWPVXKHXXKCQGKDKITQRRUWVXUCIXYCRVOCU IEWSLGFDPRVDFGHV".

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B		B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C		C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D		D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E		E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F		F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G		G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H		H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I		I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L		L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M		M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N		N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O		O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P		P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q		Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R		R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S		S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T		T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U		U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V		V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W		W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X		X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y		Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z		Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 4.1.1

Algebriacially, in Z_{26}, let $P_1,P_2,P_3,.....,P_j$ be numerical equivalents of plaintext, $C_1, C_2, C_3, ..., C_j$ be numerical equivalents of ciphertext and $K_1, K_2, K_3, ..., K_j$ be numerical equivalents of keyword. Let i is the length of keyword. Vigenére encryption transformation is $C_n \equiv P_n + K_n \pmod{26}$ where $0 < n \leq j$ and decryption transformation is $P_n \equiv C_n - K_n \pmod{26}$ where $0 < n \leq j$

a	b	c	d	e	f	g	h	i	j	k	l	m
.082	.015	.028	.043	.127	.022	.020	.061	.070.	.002	.008	.040	.024

n	o	p	q	r	s	t	u	v	w	x	y	z
.067	.075	.019	.001	.060	.063	.091	.028	.010	.023	.001	.020	.001

Table 4.1.2 : Frequencies of Letters in English

The frequencies of letters in English are different from each other "e" has the highest frequency. To turn out key, we use frequency analysis. In order to find key length using the index of coincidence, we pursue the following procedure.

1) Write the ciphertext

2) Below ciphertext write ciphertext again by shifting ; displacements.

For a displacement one

C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P	V	X
	C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P	V
						*									*				

K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W	V	X
X	K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W	V
			*												*				

U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F	D	P
X	U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F	D

R	V	D	F	G	H	V	
P	R	V	D	F	G	H	V

For a dispalcement two

C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P	V	X
		C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P
															*				

K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W	V	X
V	X	K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W
										*									

U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F	D	P
V	X	U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F

R	V	D	F	G	H	V		
D	P	R	V	D	F	G	H	V

For a displacement 3

C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P	V	X
			C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W
									*							*			

K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W	V	X
P	V	X	K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U
		*																	

U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F	D	P
W	V	X	U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G

R	V	D	F	G	H	V			
F	D	P	R	V	D	F	G	H	V

For a displacement 4

C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W	W	P	V	X
				C	D	R	P	A	O	O	T	J	O	E	I	V	W	F	W
									*										

K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R	U	W	V	X
W	P	V	X	K	H	X	X	K	C	Q	G	K	D	K	I	T	Q	R	R
			*	*				*											

U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L	G	F	D	P
U	W	V	X	U	C	I	X	Y	C	R	V	O	C	U	I	E	W	S	L
*			*		*				*										

R	V	D	F	G	H	V				
G	F	D	P	R	V	D	F	G	H	V
		*								

3) Point characters in the same location in above and below lines.

4) Count characters in the same location. We obtain that

Displacement:	1	2	3	4	5
Coincidences:	4	2	3	9	1

We see that displacement 4 has the most coincidences. Hence, length of key is 4.

Finding the key:

In ciphertext, we look for occurrences of every fourth letter starting with the first in order to find the first letter of the key. We have

A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	1	0	1	0	2	0	0	1	3	0	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	0	0	1	0	1	2	1	1	0	1	0

The most occurring letters are K, G, U. The best choice is G = e, and therefore the first key is 2 = c.

We now look for occurrences of every fourth letter starting with second.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	4	2	0	1	0	2	0	0	0	0	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	2	1	1	0	0	0	0	1	3	0	0	0

The most occurring letters are C, D, H, O, Q. The best choice is S = e, and therefore the first key is 14 = o.

We now look for occurrences of every fourth letter starting with third.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	0	2	1	1	0	0	1	0	1	0	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	0	1	3	1	0	1	3	0	1	0	0

The most occurring letters are R, V, D, I. The best choice is H = e, and therefore the first key is 3 = d.

We now look for occurrences of every fourth letter starting with fourth.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	0	0	0	1	1	0	3	0	0	1	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	2	0	1	0	1	0	1	1	4	0	0

The most occurring letters are X, I, P . The best choice is I = e, and therefore the first key is 4 = e.

Example12:

We wish to encipher a plaintext: "meet me at nine", keyword is "danger" for Vigenére cipher. First, translate letters in plaintext and keyword into their numerical equivalents such that

$P_1 = 12$, $P_2 = 4$, $P_3 = 4$, $P_4 = 19$, $P_5 = 12$, $P_6 = 4$, $P_7 = 0$, $P_8 = 19$, $P_9 = 13$, $P_{10} = 8$, $P_{11} = 13$, $P_{12} = 4$,

and

$K_1 = 3$, $K_2 = 0$, $K_3 = 13$, $K_4 = 6$, $K_5 = 4$, $K_6 = 17$

Using encryption transformation $C_n \equiv P_n + K_n \pmod{26}$, we have

$C_1 \equiv 12+3 \equiv 15 \pmod{26}$

$C_2 \equiv 4+0 \equiv 4 \pmod{26}$

$C_3 \equiv 4+13 \equiv 17 \pmod{26}$

$C_4 \equiv 19+6 \equiv 25 \pmod{26}$

$C_5 \equiv 12+4 \equiv 16 \pmod{26}$

$C_6 \equiv 4+17 \equiv 21 \pmod{26}$

$C_7 \equiv 0+3 \equiv 3 \pmod{26}$

$C_8 \equiv 19+0 \equiv 19 \pmod{26}$

$C_9 \equiv 13+13 \equiv 0 \pmod{26}$

$C_{10} \equiv 8+6 \equiv 14 \pmod{26}$

$C_{11} \equiv 13+4 \equiv 17 \pmod{26}$

$C_{12} \equiv 4+17 \equiv 21 \pmod{26}$

Converting back to letters, we obtain "PERZQVDTAORV".

Example13:

The message "XUVKLMFAPGTWALQ" is encrypted with key "success". To decipher, we first convert letters in ciphertext and keyword into their numerical equivalents.

$C_1 = 23$, $C_2 = 20$, $C_3 = 21$, $C_4 = 10$, $C_5 = 11$, $C_6 = 12$, $C_7 = 5$, $C_8 = 0$, $C_9 = 15$, $C_{10} = 6$, $C_{11} = 19$, $C_{12} = 22$, $C_{13} = 0$, $C_{14} = 11$, $C_{15} = 16$

and

$K_1 = 18$, $K_2 = 20$, $K_3 = 2$, $K_4 = 2$, $K_5 = 4$, $K_6 = 18$, $K_7 = 18$

Applying vigenére decryption transformation $P_n \equiv C_n - K_n \pmod{26}$, we obtain

$$P_1 \equiv 23-15 \equiv 5 \pmod{26}$$
$$P_2 \equiv 20-20 \equiv 0 \pmod{26}$$
$$P_3 \equiv 21-2 \equiv 19 \pmod{26}$$
$$P_4 \equiv 10-2 \equiv 8 \pmod{26}$$
$$P_5 \equiv 11-4 \equiv 7 \pmod{26}$$
$$P_6 \equiv 12-18 \equiv 20 \pmod{26}$$
$$P_7 \equiv 5-18 \equiv 13 \pmod{26}$$
$$P_8 \equiv 0-18 \equiv 8 \pmod{26}$$
$$P_9 \equiv 15-20 \equiv 21 \pmod{26}$$
$$P_{10} \equiv 6-2 \equiv 4 \pmod{26}$$
$$P_{11} \equiv 19-2 \equiv 17 \pmod{26}$$
$$P_{12} \equiv 22-4 \equiv 18 \pmod{26}$$
$$P_{13} \equiv 0-18 \equiv 8 \pmod{26}$$
$$P_{14} \equiv 11-18 \equiv 19 \pmod{26}$$
$$P_{15} \equiv 16-18 \equiv 24 \pmod{26}$$

Next, we translate back to letters to obtain. "fatihuniversity ".

Example14:

Alice wishes to send the message "Clacton is a small quiet and beautiful village in southeast of London. Clacton isn't crowded. We visited Horwich, Ipswich, Cambridge, Colchester, London and Canterbury in England. In London, we went to Madamme Tussad's where there were mummies of famous people. We had a tour of the Thames River. We went to Bigben and Cambridge University." to Bob. Alice uses 26-letter alphabet in which A-Z correspond to 0-25 . Alice chooses a keyword, "trip". First, she

converts letters into their numerical equivalents to encrypt. As key length is 4, write them in groups of four.

2,11,0,2	19,14,13,8	18,0,18,12	0,11,11,16	20,8,4,19
0,13,3,1	4,0,20,19	8,5,20,11	21,8,11,11	0,6,4,8
13,18,14,20	19,7,4,0	18,19,14,5	11,14,13,3	14,13,2,11
0,2,19,14	13,8,18,13	19,2,17,14	22,3,4,3	22,4,21,8
18,8,19,4	3,7,14,17	22,8,2,7	8,15,18,22	8,2,7,2
0,12,1,17	8,3,6,4	2,0,11,2	7,4,18,19	4,17,11,14
13,3,14,13	0,13,3,2	0,13,19,4	17,1,20,17	24,8,13,4
13,6,11,0	13,3,8,13	11,14,13,3	14,13,22,4	22,4,13,19
19,14,12,0	3,0,12,12	4,19,20,18	18,0,3,18	22,7,4,17
4,19,7,4	17,4,22,4	17,4,12,20	12,12,8,4	18,14,5,5
0,12,14,20	18,15,4,14	15,11,4,22	4,7,0,3	0,19,14,20
17,14,5,19	7,4,19,7	0,12,4,18,	17,8,21,4	17,22,4,22
4,13,19,19	14,1,8,6	1, 4,13,0	13,3,2,0	12,1,17,8
3,6,4,20	13,8,21,4	17,18,8,19	24.	

and

Keyword:19,17,8,15

Applying vigenére enciphering transposition $C_n \equiv P_n + K_n \pmod{26}$, we obtain

21,2,8,17,12,5,21,23,11,17,0,1,19,2,19,5,13,25,12,8,19,4,11,16,23,17,2,8,1,22,2,0,14,25
,19,0,19,23,12,23,6,9,22,9,12,24,12,15,11,10,22,20,4,5,21,18,7,4,10,0,19,19,1,3,6,25,0,
2,12,19,25,3,15,20,12,18,15,21,3,23,11,25,1,19,22,24,22,6,15,25,10,22,1,6,0,11,1,19,15
,17,19,3,9,6,1,20,14,19,21,5,19,17,0,21,0,8,23,8,19,3,6,20,22,2,19,4,11,17,19,4,1,19,10,
18,2,6,17,25,21,19,6,23,19,15,6,20,16,2,4,5,21,18,7,4,4,19,15,21,21,8,12,5,20,15,22,17,
20,1,23,10,2,7,11,17,11,7,15,24,12,6,23,10,15,19,10,21,4,19,10,21,20,9,5,3,16,19,11,5,
13,20,19,3,22,9,11,6,12,3,8,2,12,11,23,24,8,18,19,10,22,9,10,5,13,8,0,21,1,22,19,3,12,7
,10,25,3,19,10,13,12,11,23,4,1,5,7,18,16,21,20,21,21,15,6,20,10,15,5,18,25,23,22,23,12
,9,6,25,3,19,10,9,16,8,17.

Next, Alice translates back to letters and she sends the encrypted messages "VCIRMFVXLRABTCTFNZMITELQXRCIBWCAOZTATXMXGJWJMYMPLKWU
EFVSHEKATTBDGZACMTZDPUMSPVDXLZBTWYWGPZKWBGALBTPRTDJG
BUOTVFTRAVAIXITDGUWCTELRTEBTKSCGRZVTGXTPGUQCEFVSHEETPV

VIMFUPWRUBXKCHLRLHPYMGXKPTKVETKVUJFDQTLFNUTDWJLGMDIC
MLXYISTKWJKFNIAVBWTDMHKZDTKNMLXEBIHSQVUVVPGUKPFSZXWX
MJGZDTKJQIR" to Bob.

Bob needs keyword to decipher the ciphertext. To turn out keyword, Bob first finds key length. Below the ciphertext, he writes the ciphertext again by shifting 1. He repeats this process for shifting 2, 3, 4, 5, 6 and 7(it is enough to find out key length). He marks characters in the same location in both lines and obtains the following data:

Shift:	1	2	3	4	5	6	7
Coincidence:	4	7	7	13	10	12	10

The most coincidences is shift of 4. Hence, length of keyword is 4.

Secondly, Bob finds frequency of letters at the 1st, 5th, 9th, 13th,..... letters and he obtains

A	B	C	D	E	F	G	H	I	J	K	L	M
2	4	0	0	2	2	7	3	1	0	7	6	4

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	5	0	2	0	10	1	2	3	6	0	0

The most occurence letter is T, though G, K, X and L are close behind. The best choice is X = e, and therefore the first key is 19 = t.

He now looks at the 2nd, 6th, 10th, ... letters and he finds

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	3	4	6	7	2	0	2	2	4	0	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	0	0	0	4	3	3	5	7	1	3	4	8

The most frequent is Z, F and V occure 7 times. The best choice is V = e, hence the second key is 17 = r.

He looks at the 3rd, 7th, 11th, ... letters and he has

A	B	C	D	E	F	G	H	I	J	K	L	M
4	5	4	2	2	0	0	0	3	2	3	3	9

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	1	2	3	1	0	6	3	6	6	0	0	0

The most occurrence letter is M, though W, T, V are close behind. The best choice is M = e, and therefore the third key is 8 = i.

Finally, he looks at the 4th, 8th, 12th, ... letters and he obtains

A	B	C	D	E	F	G	H	I	J	K	L	M
3	2	3	4	0	1	4	3	8	5	0	3	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	5	1	4	4	10	2	1	2	4	0	0

T occures 10 times and I occures 8 times. The best choice is T = e, and so the fourth key is 15 = p.

Finally, Bob finds out the key { 19,17,8,15} and deciphers the ciphertext using the key . He obtains

"Clactonisasmallquietandbeautifulvillageinsoutheastoflondonclactonisntcrowdedwevisitedhorwichipswichcambridgecalchesterlondonandcanterburyinenglandinlondonwewenttomadammetussadswheretherewereremummiesoffamouspeoplewehadatourofthethamesriverwewentpobigbenandcambridgeuniversity".

4.2 ENCIPHERING MATRICES

Assume that we use a cryptosystem in which we have an alphabet of *N*-letter and message units are digraphs. Numerical equivalents of digraphs are elements of Z/N^2Z. Each digraph can also be defined as a vector such that $xy \to \begin{pmatrix} x \\ y \end{pmatrix}$ where x and y are element of Z / *NZ*. To illustrate, in 26-letter alphabet A-Z correspond to 0-25 then KL corresponds to vector $\begin{pmatrix} 10 \\ 11 \end{pmatrix}$.

Let *P* be plaintext digraph vector, *C* be ciphertext digraph vector, *B* be a constant vector, and *A* be $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z / NZ$.

Shift transformation is $C \equiv P + B \bmod N$. In otherwords,

$$C = \left[\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \right] \bmod N = \begin{pmatrix} x+e \\ y+f \end{pmatrix} \bmod N \ .$$

Linear transformation is $C \equiv AP \bmod N$. In other words,

$$C = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right] \bmod N = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \bmod N$$

Afine transformation is $C = AP + B \bmod N$. In otherwords,

$$C = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \right] \bmod N = \begin{pmatrix} ax+by+e \\ cx+dy+f \end{pmatrix} \bmod N$$

Enciphering transformation is a permutation of vectors such that $Av + b \bmod N$ where A is an invertible $n \times n$ matrix, b and v are vectors. A is defined on Z / NZ. The following equivalences can be proved easily;

A is invertible(Encrypted message can be decrypted if A is invertible) $\Leftrightarrow$ Determinant of A is coprime to N $\Leftrightarrow$ A is one-to-one and onto.

A matrix A has an inverse if and only if

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\det A = ad - cd$

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\det A)^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

For $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{23} & a_{33} \end{pmatrix}$,

$$\det A = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{12} \\ a_{33} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ \begin{vmatrix} a_{23} & a_{21} \\ a_{33} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{11} \\ a_{23} & a_{21} \end{vmatrix} \\ \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{11} \\ a_{32} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{bmatrix}$$

In general, inverse of $n \times n$ matrix can be obtained by Gaussian elimination or LU decomposition or Gauss-Jordan elimination.

Example1:

To find inverse of $A = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \in M_2(Z/29Z)$, we first find determinant of A.

$\det A = 21.18 - 22.19 = -40 \equiv 18 \bmod 29$. A has an inverse since $\gcd(18,29) = 1$ and $18^{-1} \equiv 21 \bmod 29$. Hence,

$$A^{-1} \equiv \begin{pmatrix} 21.18 & 21.(-19) \\ 21.(-22) & 21.21 \end{pmatrix} \equiv \begin{pmatrix} 378 & -399 \\ -462 & 441 \end{pmatrix} \equiv \begin{pmatrix} 1 & 7 \\ 2 & 6 \end{pmatrix} \bmod 29$$

4.2.1 Linear Transformation

Let plaintext message unit P will be $\begin{pmatrix} x \\ y \end{pmatrix}$ and ciphertext message unit C be $\begin{pmatrix} x' \\ y' \end{pmatrix}$.

Let enciphering matrix be $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M^2(Z/NZ)$ with $\gcd(\det A, N) = 1$. The relationship $C \equiv AP \bmod N$ is used to encrypt message. In otherwords,

$$C \equiv \begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N .$$

For deciphering, we need to know inverse of A. Linear transformation $P \equiv A^{-1}C \bmod N$ is used to convert ciphertext into plaintext. In otherwords,

$$P \equiv \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} (\det A)^{-1}.d & -(\det A)^{-1}.b \\ -(\det A)^{-1}.c & (\det A)^{-1}.a \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N$$

Example2:

Assume that we use Turkish letter alphabet with 29-letter. We encipher the message "şifrekırıldı" by linear transformation. Numerical equivalents of Turkish letter are

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	27	28

"şifrekırıldı" corresponds to the sequence of vectors $\begin{pmatrix} 22 \\ 11 \end{pmatrix}, \begin{pmatrix} 6 \\ 20 \end{pmatrix}, \begin{pmatrix} 5 \\ 13 \end{pmatrix}, \begin{pmatrix} 10 \\ 20 \end{pmatrix}, \begin{pmatrix} 10 \\ 14 \end{pmatrix}, \begin{pmatrix} 4 \\ 10 \end{pmatrix}$.

We can write this vectors as columns of a 2×6 -matrix which denotes plaintext.

Applying linear transformation $C \equiv AP \bmod 29$ using the matrix $A = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}$, we obtain

$$C \equiv \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}\begin{pmatrix} 22 & 6 & 5 & 10 & 10 & 4 \\ 11 & 20 & 13 & 20 & 14 & 10 \end{pmatrix} \equiv \begin{pmatrix} 4 & 13 & 4 & 10 & 12 & 13 \\ 15 & 28 & 25 & 0 & 8 & 7 \end{pmatrix} \bmod 29$$

= “DMKZDÜIAJĞKG”

Example3:

Suppose that two cryptosystems are used to encrypt vectors. First apply the matrix $\begin{pmatrix} 3 & 2 \\ 8 & 7 \end{pmatrix}$ working modulo 26 and apply the matrix $\begin{pmatrix} 13 & 4 \\ 7 & 24 \end{pmatrix}$ working modulo 27. Plaintext is on single letter in the 26-letter alphabet in which A-Z correspond to 0-25 and ciphertext is on single letter in the 27-letter alphabet in which A-Z correspond to 0-25 and blank = 26. Alice wants to encipher the message “contactwithtom”. Apply the two rules:

$$I \equiv A_1 P \bmod 26$$

$$C \equiv A_2 I \bmod 27$$

She obtains

$$I \equiv \begin{pmatrix} 3 & 2 \\ 8 & 7 \end{pmatrix}\begin{pmatrix} 2 & 13 & 0 & 19 & 8 & 7 & 14 \\ 14 & 19 & 2 & 22 & 19 & 19 & 12 \end{pmatrix} \equiv \begin{pmatrix} 8 & 25 & 4 & 23 & 10 & 7 & 24 \\ 10 & 3 & 14 & 20 & 15 & 7 & 6 \end{pmatrix} \bmod 26$$

$$C \equiv \begin{pmatrix} 13 & 4 \\ 7 & 24 \end{pmatrix}\begin{pmatrix} 8 & 25 & 4 & 23 & 10 & 7 & 24 \\ 10 & 3 & 14 & 20 & 15 & 7 & 6 \end{pmatrix} \equiv \begin{pmatrix} 9 & 13 & 0 & 1 & 1 & 11 & 12 \\ 26 & 4 & 13 & 20 & 25 & 1 & 15 \end{pmatrix} \bmod 27$$

= ”J NEANBUBZLBMP”.

Alice sends this message to Bob. And Bob deciphers the message by applying the following two rules:

$$I \equiv A_2^{-1} C \bmod 27$$

$$P \equiv A_1^{-1} \operatorname{Im} od 26$$

First, Bob computes inverse of $A_1 \bmod 26$ and $A_2 \bmod 27$ such that

$$A_1^{-1} \equiv \begin{pmatrix} 17 & 10 \\ 14 & 11 \end{pmatrix} \bmod 26 \text{ and } A_2^{-1} \equiv \begin{pmatrix} 21 & 19 \\ 13 & 26 \end{pmatrix} \bmod 27$$

then Bob has

$$I \equiv \begin{pmatrix} 21 & 19 \\ 13 & 26 \end{pmatrix}\begin{pmatrix} 9 & 13 & 0 & 1 & 1 & 11 & 12 \\ 26 & 4 & 13 & 20 & 25 & 1 & 15 \end{pmatrix} \equiv \begin{pmatrix} 8 & 25 & 4 & 23 & 10 & 7 & 24 \\ 10 & 3 & 14 & 20 & 15 & 7 & 6 \end{pmatrix} \bmod 27$$

$$P \equiv \begin{pmatrix} 17 & 10 \\ 14 & 11 \end{pmatrix}\begin{pmatrix} 8 & 25 & 4 & 23 & 10 & 7 & 24 \\ 10 & 3 & 14 & 20 & 15 & 7 & 6 \end{pmatrix} \equiv \begin{pmatrix} 2 & 13 & 0 & 19 & 8 & 7 & 0 \\ 14 & 19 & 2 & 22 & 19 & 19 & 12 \end{pmatrix} \bmod 26$$

Converting back vectors to letters, Bob obtains the message “contactwithtom”.

4.2.2 Affine transformation

Let plaintext message unit P be $\begin{pmatrix} x \\ y \end{pmatrix}$ and ciphertext message unit C be $\begin{pmatrix} x' \\ y' \end{pmatrix}$.

Let enciphering matrix be $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M^2(Z/NZ)$ with $\gcd(\det A, N) = 1$ and a constant vector B be $\begin{pmatrix} e \\ f \end{pmatrix}$. The enciphering transformation is $C \equiv AP + B(\bmod N)$. In other words, $\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \bmod N$. The deciphering transformation is $P \equiv A^{-1}C - A^{-1}B \equiv A' + \mathrm{B}' \bmod N$ where $A' = A^{-1}C$ and $\mathrm{B}' = -A^{-1}B$.

Example4:

Assume that you want to encrypt the message “tom was killed yesterday” using affine transformation in the 27-letter alphabet with A-Z correspond to 0-25 and blank = 26. You use the encryption matrix $A = \begin{pmatrix} 13 & 4 \\ 7 & 24 \end{pmatrix}$ working modulo 27^2 and constant vector $\begin{pmatrix} 121 \\ 153 \end{pmatrix}$. Numerical equivalents of digraphs are the integer $x = 27x_1 + x_2$.

First, you divide plaintext into digraphs and then compute their numerical equivalents such that

“to” = 27.19 + 14 = 570

“wa” = 27.22 + 0 = 594

“ki” = 27.10 + 8 = 278

“ed” = 27.4 + 3 = 111

“es” = 27.4 + 18 = 126

“m ” = 27.12 + 26 = 350

“s ” = 27.18 + 26 = 512

“ll” = 27.11 + 11 = 308

“ y” = 27.26 + 24 = 726

“te” = 27.19 + 4 = 517

"rd" = 27.17 + 3 = 462 "ay" = 27.0 + 24 + 24

using enciphering transformation $C \equiv AP + B(\mathrm{mod}\, N^2)$, you obtain that

$$C \equiv \begin{pmatrix} 13 & 4 \\ 7 & 24 \end{pmatrix}\begin{pmatrix} 570 & 594 & 278 & 111 & 126 & 462 \\ 350 & 512 & 308 & 726 & 517 & 24 \end{pmatrix} + \begin{pmatrix} 121 \\ 153 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 183 & 414 & 593 & 94 & 182 & 391 \\ 150 & 561 & 14 & 126 & 321 & 318 \end{pmatrix} \mathrm{mod}\, 27^2$$

converting back to letters, you have

183 = 27.6 + 21 = "GV" 150 = 27.5 + 15 = "FP"

414 = 27.15 + 9 = "PJ" 561 = 27.20 + 21 = "UV"

593 = 27.21 + 26 = "V " 14 = 27.0 + 14 = "AO"

94 = 27.3 + 13 = "DN" 126 = 27.4 + 18 = "ES"

182 = 27.6 + 20 = "GU" 321 = 27.11 + 24 = "LY"

391 = 27.14 + 13 = "ON" 318 = 27.11 + 21 = "LV"

Hence the ciphertext is "GVFPPJUVV AODNESGULYONLV".

Example5:

Alice sent to ciphertext "KIMDZWP NEUITR. CXUXBNHKJ" to Bob. Alice used an enciphering matrix $A = \begin{pmatrix} 1 & 3 & 13 & 5 & 6 \\ 16 & 5 & 7 & 9 & 7 \\ 10 & 20 & 6 & 5 & 8 \\ 10 & 0 & 24 & 8 & 9 \\ 10 & 0 & 25 & 17 & 1 \end{pmatrix}$ working modulo 29 and enciphering vector $B = \begin{pmatrix} 24 \\ 3 \\ 9 \\ 17 \\ 5 \end{pmatrix}$. Alice and Bob use a single letter with 29-letter alphabet in which 0-25 correspond to A-Z, blank = 26, ',' = 27, '.' = 28. First Bob computes inverse of A modulo 29 and obtains $A^{-1} \equiv \begin{pmatrix} 27 & 17 & 12 & 19 & 3 \\ 13 & 0 & 1 & 16 & 2 \\ 7 & 13 & 16 & 21 & 14 \\ 27 & 0 & 9 & 11 & 15 \\ 24 & 27 & 23 & 26 & 4 \end{pmatrix} \mathrm{mod}\, 29$.

Bob uses deciphering transformation $P \equiv A'C + B' \bmod 29$. Bob finds out

$$B' \equiv \begin{pmatrix} 15 \\ 6 \\ 5 \\ 24 \\ 8 \end{pmatrix} \bmod 29 \quad \text{and} \quad A'C \equiv \begin{pmatrix} 15 & 28 & 6 & 11 & 27 \\ 8 & 6 & 27 & 2 & 24 \\ 25 & 21 & 21 & 13 & 15 \\ 3 & 16 & 13 & 24 & 16 \\ 11 & 0 & 5 & 21 & 20 \end{pmatrix} \bmod 29.$$ Hence Bob finds out

$$P \equiv \begin{pmatrix} 1 & 14 & 21 & 26 & 13 \\ 14 & 12 & 4 & 8 & 1 \\ 1 & 26 & 26 & 18 & 20 \\ 27 & 11 & 8 & 19 & 11 \\ 19 & 8 & 13 & 0 & . \end{pmatrix} \bmod 29 \ .$$

Finally, converting back to letters, he obtains “Bob,Tom live in Istanbul.”

CHAPTER 5

PUBLIC KEY CRYPTOGRAPHY

5.1 THE IDEA OF PUBLIC KEY CRYPTOGRAPHY

In public key cryptosystems, enciphering and deciphering keys are different from each other. Enciphering key is public whereas deciphering key is kept secret. Public key cryptosystem is also called asymmetric key cryptosystem. The most significant point in public key cryptosystems is that deciphering the ciphertext is very hard by using the ciphertext and enciphering key. Asymetric-key algorithms depend on the number theory. Enciphering transformation is a mapping f from P, the set of plaintext message units, to C, the set of ciphertext message units. The mapping f is one to one correspondence and Z_n to Z_n. Calculating inverse of f is too difficult without knowing private key, K_D. F is called *trapdoor* function which means that computing inverse of a function without additional information is infeasible.

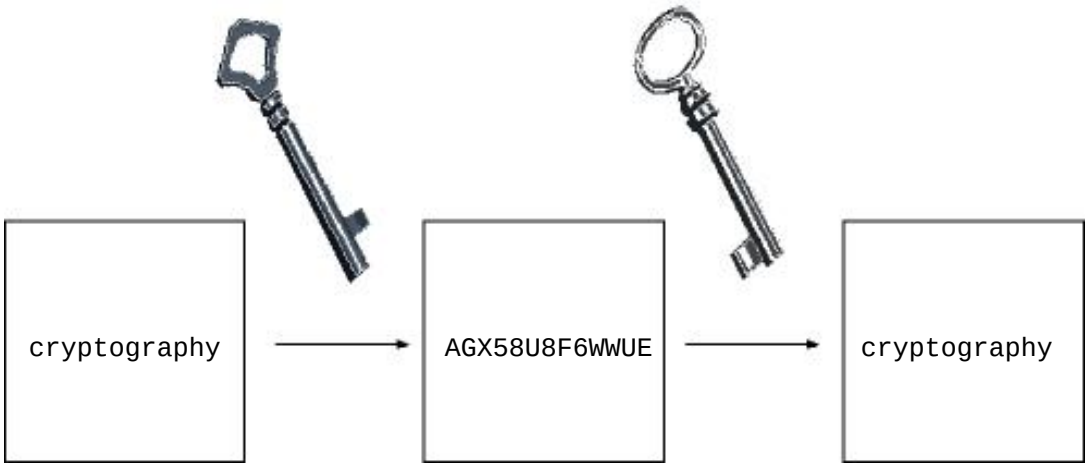


Figure 3 – Public Key Cryptography

In 1976, Diffie and Hellman invented public key cryptosystem. Their asymetric key algorithm depends on discrete logarithm. Then, in 1977, RSA was discovered by Ron Rivest, Adi Shamir and Leonard Adleman. RSA is based on factoring extremely large numbers. In 1985, T. El Gamal invented El Gamal cryptosystem. It depends on the discrete logarithm.

5.2 RSA

RSA is one of the most common public key cryptosystem that is based on factoring extremely large integers. Ron Rivest, Adi Shamir and Leonard Adleman invented RSA in 1977. In RSA algorithm, modular arithmetic, primality, factorization, Chinese remainder theorem, Fermat and Euler theorem are used.

Now we describe RSA algorithm. Let Alice and Bob work in N-letter alphabet. Assume that plaintext message units are blocks of k letters and ciphertext message units are blocks of l letters where $k < l$.

To begin with, Bob generates two distinct extremely large prime integers p and q to form $n = p.q$ where n is between N^k and N^l. p and q are elements of Z/NZ. We compute k and l using the condition

$$k \leq [\ log_N(n)\ ] < l$$

In other words, we obtain $k < log_N(n) < l$ from $N^k < n < N^l$ and this implies

$$k \leq [\ log_N(n)\ ] < l.$$

By maple

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

Next Bob computes $\varphi(n) = (p\text{-}1)(q\text{-}1)$ which is Euler phi function.

By maple

- phi(n);

Then he chooses a number e, relatively prime to $\varphi(n)$ and between 1 and $\varphi(n)$. e is called enciphering exponent. n and e form enciphering key. Bob publishes n, e and

keeps p, q private. Alice enciphers her message, P, by using the equation $C \equiv P^e \bmod n$. P is an element of $\{ 0,1,2,3,\ldots\ldots,N^k\text{-}1 \}$.

By maple
➢ C : = P &^ e mod n;

Enciphering transformation is Z/NZ *to* Z/NZ. Alice sends the ciphertext to Bob. Bob needs to know decryption exponent d in order to decipher the ciphertext. He computes d by computing inverse of e modulo $\varphi(n)$ such that

$$d\,e \equiv 1 \bmod ((p\text{-}1)(q\text{-}1))$$

$$d \equiv e^{-1} \bmod ((p\text{-}1)(q\text{-}1))$$

By maple
➢ d : = (1 / e) mod $\varphi(n)$;

Consequently, Bob decrypts the message C by solving

$$P \equiv C^d \bmod n$$

This systems works because

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

since ed-1 is a multiple of $\varphi(n)$, ed-1 = $k\varphi(n)$. It implies that

$$C^d \equiv P^{ed} \equiv P^{1+k\varphi(n)} \equiv P^1 P^{k\varphi(n)} \equiv P(1)^k \equiv P \bmod n$$

Decryption transformation is Z/NZ *to* Z/NZ.

5.2.1 Summary of RSA Algorithm

- Bob selects two distinct extremely large prime integers p and q to form $n = p.q$ where n is between N^k and N^l.
- Bob chooses e between 1 and $\varphi(n)$ with coprime to $\varphi(n)$.
- Bob makes n and e public.
- Alice encrypts her message P using $C \equiv P^e \bmod n$.
- Alice sends C to Bob.
- Bob computes inverse of e modulo $\varphi(n)$.
- Bob deciphers C using $P \equiv C^d \bmod n$.

5.2.2 RSA Signature Scheme

As it is stated above, public key is pairs of (*n, e*) and the secret key is pairs of (*n,d*). The signature is $P \equiv C^d \bmod n$ and verification of signature is $P \equiv C^e \bmod n$.

Example 1:

Plaintext and ciphertext letters are written in 26-letter alphabet. Plaintext message units are digraphs and ciphertext message units are trigrahs. In other words, $k = 2$, $l = 3$ and $26^2 < n < 26^3$ for all n. We wish to encrypt the message "arrestmike". Let's choose p and q to form n between 26^2 and 26^3. Let p be 61, q be 37 and e be 133. Enciphering key (*n,e*) is (2257, 133). Now, we find numerical equivalents of plaintext blocks.

"ar" = 17 + 0.26 = 17

"re" = 4 + 17.26 = 446

"st" = 19 + 18.26 = 487

"mi" = 8 + 12.26 = 320

"ke" = 4 + 10.26 = 264

Applying $P^e \bmod n$, we obtain

$17^{133} \equiv 96 \bmod 2257$

$446^{133} \equiv 1574 \bmod 2257$

$487^{133} \equiv 487 \bmod 2257$

$320^{133} \equiv 809 \bmod 2257$

$264^{133} \equiv 1351 \bmod 2257$

Converting back to letters, we have

$96 = 0.26^2 + 3.26 + 18$ = "ADS"

$1574 = 2.26^2 + 8.26 + 14$ = "CIO"

$487 = 0.26^2 + 18.26 + 19$ = "AST"

$809 = 1.26^2 + 5.26 + 3$ = "BFD"

$1351 = 1.26^2 + 25.26 + 25$ = "BZZ"

Hence, the ciphertext is "ADSCIOASTBFDBZZ"

Example 2:

Suppose that Alice and Bob use a 40-letter alphabet in which A-Z correspond to 0-25, "blank" = 26, "." = 27, "? "= 28, ", "= 29, the numerals 0-9 correspond to 30-39 for both plaintext and ciphertext. Bob chooses two distinct primes, p = 123456811 and

q = 427419669163, to form n = 52767869313539019193. k and l are calculated using $k \leq log_N n < l$. k = 12 and l = 13. Next, he generates a number e = 9507029 , relatively prime to $\varphi(n)$ = 52767868885995893 220 .

Alice wishes to send her message to Bob. Her message is "Ron Rivest,Adi Shamir and Leonard Adleman found RSA in 1977.". To encrypt, Alice first divides her message into 12-blocks such that

"Ron Rivest,A" , "di Shamir an" , "d Leonard Ad" , "leman found " , "RSA in 1977.".

Next, she computes numerical equivalents of plaintext message units.

"Ron Rivest,A" = 7280698525809823560

"di Shamir an" = 1349112136930409613

"d Leonard Ad" = 1533833105451753603

"leman found " = 4658825404965140946

"RSA in 1977." = 7319232240312316707

Applying $P^e \equiv C \ mod \ n$, she obtains

3449976683012239796 1, 10891019001444304501, 9639793540902248331, 21689606995749800046, 2222086672149204714.

Converting back to letters, she obtains ciphertext

"CCKGGZ6KQWS,BAZ8Z7YZ59HKMVAW9M50T747ZILBL?TLPH740ZBGAFL6XU?7?LM74".

Alice sends the ciphertext to Bob. For deciphering, Bob calculates $d \equiv e^{-1} \ mod \ \varphi(n)$ and $d \equiv 22954230467328982169 \bmod 52767868885995893220$.

Breaking ciphertext into 13-blocks and computing their numerical equivalents, he obtains

"CCKGGZ6KQWS,B" = 34499766830122397961

"AZ8Z7YZ59HKMV" = 10891019001444304501

"AW9M50T747ZIL" = 9639793540902248331

"BL?TLPH740ZBG" = 21689606995749800046

"AFL6XU?7?LM74" = 2222086672149204714

Using $C^d \bmod n$ and converting back to letters, he obtains the original message "Ron Rivest,Adi Shamir and Leonard Adleman found RSA in 1977.".

Example 3:

Eve wishes to decipher the encrypted message "ADY.INFKNZSIP,QZWYWI.IMQCTLIKNALHHUPG,ESRZMQB,BEQKVRRGW'blank'NRIOAAWFQWDTJ'blank'JODNBCIV'blank'XIVFK.YDKCSACGZ'blank'KTEYS'blank'J,'blank'MH'blank'ONCQJ,TPFTYNWAGZZCHATNXG'blank'GPJPIM'blank'SXTRFGZFFGQAVFDVRJPENTZMUS.APBGKABUGKJBAPASG,'blank'DNSQBNPWWDUL'blank'VHCJIGOWJHNXAKNQISMKDUMJJPMRXVSKYANLVJ'blank'JLG". Eve knows that the enciphering keys are n = 248424769256545978817475999014399348294046 7 and e = 675184119179267202659. A 29-letter alphabet in which A-Z correspond to 0-25, "blank" = 26, "," = 27, and "." = 28 is used. First, Eve calculates plaintext and ciphertext message units using the condition $k \leq [\ log_N (n)\ ] < l$ and finds out k = 29 and l = 30. As the ciphertext message unit is 30-block, she divides the disguised message into 30-blocks and computes their numerical equivalents such that

C_1 = "ADY.INFKNZSIP,QZWYWI.IMQCTLIKN" = 341876482091204619012279086537592963553529.

C_2 = "ALHHUPG,ESRZMQB,BEQKVRRGW NRIO" = 99613334045663862667441731836473904398305.

C_3 = "AAWFQWDTJ JODNBCIV XIVFK.YDKCS" = 6775621821028728226779371437414173928 9495.

C_4 = "ACGZ KTEYS J, MH ONCQJ,TPFTYNW" = 19812834748560408912073114504502583263 7917.

C_5 = "AGZZCHATNXG GPJPIM SXTRFGZFFGQ" = 6102139271053534044075607428547786857 98124.

C_6 = "AVFDVRJPENTZMUS.APBGKABUGKJBAP" = 1875018859584794313209880227593807653148984.

C_7 = "ASG, DNSQBNPWWDUL VHCJIGOWJHNX" = 1614992437664252218209508354779268780466837.

C_8 = "AKNQISMKDUMJJPMRXVSKYANLVJ JLG" = 9268156049878222861142849969276883275024 46.

She needs to know deciphering exponent d, p and q. She finds p = 565713850319 10524108581 and q = 43913503110524108407 by factoring n = 248424769256545 97881747599901439934829404 67. Then, she computes $d \equiv e^{-1} \bmod \varphi(n)$ and $d \equiv 18$

637807894463090482085934777389600080448 99 mod 248424769256545978811874599901439934829404 67 691608972434723480. Next, she uses $C^d \bmod n$ to decrypt the message such that

$C_1^{18637807894463090482085934777389600080448 9}$ = 170416657198058224850620430979705449 2017966 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “The pyramid of Giza, the Hangi”.

$C_2^{18637807894463090482085934777389600080448 9}$ = 117210968017442486513509176251000690 0467385 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “ng Gardens of Babylon,The Sta”.

$C_3^{18637807894463090482085934777389600080448 9}$ = 174533104236445073311595418414162638 4346301 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “tus of Zeus at Olympia,The Co”.

$C_4^{18637807894463090482085934777389600080448 9}$ = 101865678469700309404722686581804523 6543313 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “lossus of Rhodes,The Temple o” .

$C_5^{18637807894463090482085934777389600080448 9}$ = 522150121127696445713936945856846652 551535 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “of Artemis at Ephesus,The Maus”.

$C_6^{18637807894463090482085934777389600080448 9}$ = 127365244947423915198144870424438634 5313506 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “oleum at Halicarnassus and Th”.

$C_7^{18637807894463090482085934777389600080448 9}$ = 434733018135420554759942988701176180 838025 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “e Lighthouse of Alexandria ar” .

$C_8^{18637807894463090482085934777389600080448 9}$ = 435457324227160099204791087923411069 588149 mod 248424769256545978811874599901439934829404 67.

Converting back to letters she obtains “e seven wonders of the world.”.

Hence the original message is “The pyramid of Giza,The Hanging Gardens of Babylon, The Status of Zeus at Olympia,The Colossus of Rhodes,The Temple of Artemis at Ephesus,The Mausoleum at Halicarnassus and The Lighthouse of Alexandria are seven wonders of the world.”.

5.3 DISCRETE LOGARITHM

Discrete logarithm is very significant for public key that is used in Diffie-Hellman key exchange, El Gamal cryptosystem, the Massey-Omura cryptosystem for message transformation and the Digital Signature Algorithm.

Definition: Let G be a multiplicative group. Let a be a generator of G and β be an element of $< a >$. Then discrete logarithm of β to the base a is finding unique exponent x such that $\beta = a^x$.

We work in Fq^*. Let a be a generator of Fq^* and β be in $< a >$. The goal of discrete logarithm is to find out x, $0 \leq x < q$ such that $\beta = a^x \pmod q$.

Example 1: Let q be 17 and 5 be generators of F_{17}^*. 4 is the discrete logarithm of 13 to the base 5.

Example 2: In F_8^*, let a be a root of $x^3 + x + 1$. The discrete logarithm of 1 to the base a is 7.

5.4 EL GAMAL

To begin with, Bob chooses an extremely large finite field F_q and a primitive element g in F_q. Alice wants to send her message to Bob. She converts her message to numerical equivalents P in F_q.

If P is greater than q then Alice breaks P, $0 \leq P \leq q$-1, into blocks. Bob chooses a secret integer x, $0 \leq x \leq q$-1, in order to compute $y = g^x \bmod q$. Bob makes (q, g, y) public but keeps x private. Alice generates a secret integer k at random to compute $r \equiv g^k \bmod q$ and $s \equiv y^k P \bmod q$. k is in the interval [$0, q$-1]. Next, Alice sends the pair (r, s) to Bob. Bob decrypts ciphertext by solving the equation $P = s.r^{-x} \bmod q$. As $r^{-x} = (g^k)^{-x} = (g^x)^{-k} = y^{-k} \bmod q$, $s.r^{-x} = y^{-k}.P$. $y^{-k} \equiv P \bmod q$.

Finding P is very hard by only knowing s and r. If somebody knows x, he / she can find P. Hence, the most significant point in El Gamal cryptosystem is keeping x secret since computing discrete logarithm is infeasible.

5.4.1 The El Gamal Signature Scheme

Let Alice wants to sign a message. Key generation is same as for El Gamal encryption. First, Alice generates very large finite field F_q and a primitive element g in F_q. Next, she selects a random integer x , $1 \leq x < q$-1 and calculates $y = g^x \bmod q$. x is

private key and y is public key. She makes q, g, y public. Numerical equivalents of plaintext message units, P, is in the range $0 \leq P \leq q\text{-}1$.

For signing message, Alice generates an integer k in the interval (1, q-1) at random with $gcd(k, q\text{-}1) = 1$. Next, she computes $r \equiv g^k \bmod q$. Finally, she solves the equation $g^P \equiv g^{xr} g^{ks} \bmod q$ or $P \equiv xr + ks \pmod{q\text{-}1}$ or $s \equiv (P - xr)k^{-1} \bmod q\text{-}1$ if and only if $gcd(k, q\text{-}1) = 1$. Therefore, signature is the pair (r, s) for P. In order for Bob to verify the signature, Bob checks whether $1 < r < q$ and $g^P \equiv y^r r^s \bmod q$ since $g^P \equiv g^{xr} g^{ks} \bmod q$.

5.5 DIFFIE-HELLMAN KEY EXCHANGE

The aim of algorithm is that two users shares their keys securely. Diffie-Hellman assumption is based on discrete logarithm. Assume that we work in F_q. Let g be a generator of F_q^*. $g \bmod q$, $g^2 \bmod q$, $g^3 \bmod q$, ……, $g^{q-1} \bmod q$ are all distinct and correspond to an integer from 1 to q-1. q and g are public. Alice selects a random number α between 1 and q-1, and computes $Y_{\text{Alice}} \equiv g^{\alpha} \bmod q$. Bob chooses a random number β between 1 and q-1, and computes $Y_{\text{Bob}} \equiv g^{\beta} \bmod q$. Alice and Bob keep α and β private and make Y_{Alice} and Y_{Bob} public. Alice can calculate the key such that

$$(Y_{\text{Bob}})^{\alpha} \bmod q = (g^{\beta})^{\alpha} \bmod q = (g^{\alpha})^{\beta} \bmod q = (Y_{\text{Alice}})^{\beta} \bmod q.$$

Moreover, Bob can calculate the key by following the same procedure;

$$(Y_{\text{Alice}})^{\beta} \bmod q = (g^{\alpha})^{\beta} \bmod q = (g^{\beta})^{\alpha} \bmod q = (Y_{\text{Bob}})^{\alpha} \bmod q.$$

It is a known fact that for large primes, calculating discrete logarithms is very hard. This makes Diffie-Hellman key exchange secure.

5.6 MASSEY-OMURA CRYPTOSYSTEM FOR MESSAGE TRANSMISSION

Massey-Omura cryptosystem depends on discrete logarithm and Shamir three-pass protocol.

Shamir three-pass protocol works as follows:

Bob and Alice choose a finite field F_q. It is fixed and public. Alice selects a secret integer e_A, encryption exponent, in the range, $1 \leq e_A \leq q\text{-}1$, with $gcd(e_A, q - 1) = 1$. Bob generates a private integer e_B in the range, $1 \leq e_B \leq q\text{-}1$, such that $gcd(e_B, q - 1) = 1$. Alice calculates d_A, decryption exponent, such that $e_A\, d_A \equiv 1 \pmod{q - 1}$ by using

the Euclidean algorithm. Bob computes d_B such that $e_B d_B \equiv 1 \bmod q - 1$. Assume that P is the plaintext message unit.

1) Alice calculates P^{eA} and sends it to Bob.
2) Bob raises P^{eA} to e_B and returns $(P^{eA})^{eB}$ to Alice. Next Alice raises $(P^{eA\ eB})$ to d_A which becomes $(P^{eA\ eB})^{dA} = P^{eB}$ and sends to Bob.
3) Finally, Bob raises P^{eB} to d_B and obtains the message P.

As you see, there is no public key in this system.

5.7 DIGITAL SIGNATURE

Digital signature provides to understand whether Alice sent message or not. There are exactly two process of digital signature; the signing and verification. For key generation

1) Alice chooses 512 bit prime p and 160 bit prime q which is divisor of p-1.
2) Alice generates a generator g of F_p^*. Order of g is q.
3) Alice chooses an integer x at random in the range, $1 \leq x \leq q$-1.
4) Alice computes $y = g^x \bmod p$. y is the public key and x is the private key. Alice makes (p, q, y, g) public.

To sign message;

1) Alice converts her message to numerical equivalents m, $0 \leq m \leq q$-1.
2) Alice chooses a random integer k, $1 < k < q$, with $gcd(k, q) = 1$.
3) Alice computes $r \equiv (g^k \bmod p) \bmod q$.
4) Alice computes s by solving the equation $s \equiv (m + xr)k^{-1} \bmod q$.

Signature is the pair (r, s).

For verification of the signature, Bob computes $w = s^{-1} \bmod q$ and $v = (g^{mw} y^{rw} \bmod p) \bmod q$. If $v = r$, it means that Alice sent the message.

CHAPTER 6

PRIMALITY TEST

Let a be a positive integer. If n is not prime, a is relatively prime to n, and $a^{n-1} \equiv 1 (\text{mod } n)$, then n is called a *pseudoprime* to the base a. For example,there are three pseudoprime to the base 2 below 1000. 341 ia a pseudoprime to the base 2 as $2^{340} \equiv 1 \pmod{341}$, 561 is a pseudoprime to the base 2 as $2^{560} \equiv 1 \pmod{561}$ and 645 is a pseudoprime to the base 2 as $2^{644} \equiv 1 \pmod{645}$.

A composite positive integer n is called *carmichael* number if n satisfies the condition

$b^{n-1} \equiv 1 \pmod{n}$ for all integers b coprime to n.

Theorem6.1(*Koblitz, Neal.)***:** Let n be odd and positive integer. n is charmichael number if and only if n is square-free and $p-1 \mid n-1$ for all prime divisors p of n.

For example: $1729 = 7.13.19$ and $6 \mid 1728, 12 \mid 1728, 18 \mid 1728$.

$41041 = 7.11.13.41$ and $6 \mid 41040$, $10 \mid 41040$, $12 \mid 41040$, $40 \mid 41040$.

An odd composite positive integer n is said to be an *Euler pseudoprime* to base a, if $\gcd(a,n) = 1$ and $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n$ where $\left(\frac{a}{n}\right)$ is the Jacobi symbol.

Theorem6.2(*Koblitz, Neal.)***:** If n is an Euler pseudoprime to the base a, then n is a pseudoprime to the base a.

But every pseudoprime is not always an Euler pseudoprime.

Theorem6.3(*Koblitz, Neal.***):**If n is a strong pseudoprime to the base a then n is an Euler pseudoprime to base a.

For example, 5461 is a pseudoprime to the base 2 since $2^{5461} \equiv 2 (\text{mod } 5461)$. However, 5461 is not an Euler pseudoprime. Because

$$2^{\left(\frac{5461-1}{2}\right)} \equiv \left(\frac{2}{5461}\right) \bmod 5461$$

$$1 \not\equiv -1 \bmod 5461$$

561 is an Euler pseudoprime to the base 2, because

$$2^{\left(\frac{561-1}{2}\right)} \equiv \left(\frac{2}{561}\right) \bmod 561$$

$$1 \equiv 1 \bmod 561.$$

561 is also a pseudoprime to the base 2 as $2^{561} \equiv 2 \bmod 561$.

Generating extremely large primes is very significant in cryptographic algorithms. A primality test is an algorithm to reveal if a given number is prime or composite. Probabilistic tests are the most famous one. It relies on some equalities which is true for prime numbers. Now we present the *Miller-Rabin primality test* which is the most popular probabilistic test. Assume that n is an odd prime. We write $n\text{-}1 = 2^s.d$ where s is an positive integer and d is odd positive integer. Next, we choose an integer $a \in (Z/nZ)^*$. n is prime if one of the following condition is satisfied:

$$a^d \equiv 1 \pmod{n} \qquad (1)$$

or

$$a^{2^r d} \equiv -1 \pmod{n}, \quad 0 \le r \le s \qquad (2)$$

If n is composite and satisfies the above conditions (1) and (2) then n is said to be a strong pseudoprime to the base a.

The *Fermat Primality test* is a probabilistic test. We say a number n is prime, if $\exists$ a such that $\gcd(a,n) = 1$ and $a^{n-1} \equiv 1 \pmod{n}$. It is enough to look at the integer a such that $1 \le a \le n$.

Another probabilistic test is *Solovay-Strassen Primality test* . Let n be a positive odd integer.We choose k integers $a_1, a_2, \ldots, a_k$ where $0 < a_i < n$, $1 \le i \le k$

$\left(\frac{a_i}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$ where $\left(\frac{a_i}{n}\right)$ is Jacobi symbol. If the equality does not hold for all a_i, then n is composite.

APPENDIX A

PUBLIC KEY ALGORITHMS BY MAPLE

A.1 RSA ALGORITHM BY MAPLE

- with(linalg): with(numtheory): with(StringTools):

Alphabet and the numeric equivalences of symbols of the alphabet

- indx:=table(["a"=0,"b"=1,"c"=2,"d"=3,"e"=4,"f"=5,"g"=6,"h"=7,"i"=8,"j"=9,"k"=10,"l"=11,"m"=12,"n"=13,"o"=14,"p"=15,"q"=16,"r"=17,"s"=18,"t"=19,"u"=20,"v"=21,"w"=22,"x"=23,"y"=24,"z"=25,"#"=26,"."=27,"?"=28,","=29,"0"=30,"1"=31,"2"=32,"3"=33,"4"=34,"5"=35,"6"=36,"7"=37,"8"=38,"9"=39]):
- symb:=table([0="a",1="b",2="c",3="d",4="e",5="f",6="g",7="h",8="i",9="j",10="k",11="l",12="m",13="n",14="o",15="p",16="q",17="r",18="s",19="t",20="u",21="v",22="w",23="x",24="y",25="z",26="#",27=".",28="?",29=",",30="0",31="1",32="2",33="3",34="4",35="5",36="6",37="7",38="8",39="9"]):

Conversion a block of text into decimal representation and vice versa

Suppose we are given a sequence of symbols (plaintext). Many enciphering algorithms before encryption the text convert the text into the convenient for enciphering representation. This is usually done by fragmentation the plainttext into *k*-blocks and conversion these blocks into decimal fragmentation. For example, suppose we are given the text "*cryptography*". Let *k* =3. Then 3-blocks are:

"*cry*", "*pto*", "*gra*", "*phy*".

Let the letters in the text are drawn from 26-letter alphabet. Thus each 3-block cab be regarded as a 3-digit base-26 number. For instance, the decimal representations of "*cry*"

is 1818. Conversely, we can compute the 3-digit base-26 representation of a decimal number *d* as long as *d* is less than 26^3. Functions *itoa* and *atoi* can be used for conversion a block of text into decimal representation and vice versa.

converting letter blocks to numerical equivalents

This procedure converts a sequence of alphabets to an integer base *N*. Let *N* be a size of the alphabet. Then any sequence $a_1,a_2,\ldots..,a_k$ of symbols drawn from the alphabet whose length is less than or equal to *n* can be thought as a number base *N* and hence can be uniquely mapped onto the range 0...N^n-1 as following $\partial(a_1) + \partial(a_2)\, N + \ldots.. + \partial(a_k)\, N^{k-1}$, where $\partial(a_i)$ is the numeric eqivalence of the symbol a_i.

For example, let $N = 40$, then "*hello*" is mapped to $7 + 4.40 + 11.40^2 + 11.40^3 + 14.40^4 + 14.40^5 = 18194054$

- atoi:=proc(txt,N)
- local i,res,t;
- res:=0; t:= LowerCase(Reverse(txt)); t:=SubstituteAll(t," ", "#");
- for i from 1 while i<= length(t) do
- res := res + indx[substring(t,i)]*(N^(i-1));
- end do;
- return (res);
- end:

for example

- atoi("yasemin",40);

98350355533

converting numbers back to letters

This procedure converts the integer *m* from decimal representation into *N*-base representation having *k* digits. *k* must be greater than or equal to $[\log_n m]$ otherwise an error message is displayed.

- itoa:=proc(m,k,N)
- local res,len,i,lst;
- lst := convert(m,base,N);
- res:=[];
- len := nops(lst);
- for i from 1 while i<= k do

- res := [op(res),0];
- end do;
- for i from 1 while i<= len do
- res[i] := lst[i];
- end do;
- for i from 1 while i<= k do
- res[i] := symb[res[i]];
- end do;
- return Reverse((Implode(res)));
- end:

for example

- itoa(98350355533,7,40);

"yasemin"

encryption for RSA algorithm

- encrypteRSA:=proc(ptxt,N,n,e)
- local i,k,l,ctext,m,r,blocknumber,ptext;
- k:=round(evalf(log[N](n)));
- l:=k+1;ptext:=ptxt;
- printf("From %d -blocks of letters into %d -blocks of letters\n",k,l);
- printf("Plaintext: %s\n",ptext);
- r := length(ptext) mod k;
- if r > 0 then
- for i from 1 while i <= k-r do
- ptext := cat(ptext,"#");
- end do;
- end if;
- blocknumber:=length(ptext)/k; ctext:="";
- for i from 1 while i <= blocknumber do
- m:=atoi(substring(ptext,(i-1)*k+1..i*k),N);
- m:= m&^e mod n;
- ctext := cat(ctext,itoa(m,l,N));
- end do;

- printf("Ciphertext: %s\n",ctext);
- end:

decryption for RSA algorithm

- decrypteRSA:=proc(ctxt,N,n,d)
- local i,k,l,ptext,m,txtlen,blocknumber,ctext;
- k:=round(evalf(log[N](n)));
- l:=k+1;ctext:=ctxt;
- printf("From %d -blocks of letters into %d -blocks of letters\n",l,k);
- printf("Ciphertext: %s\n",ctext);
- txtlen := length(ctext);
- blocknumber:=txtlen/l; ptext:="";
- for i from 1 while i <= blocknumber do
- m:=atoi(substring(ctext,(i-1)*l+1..i*l),N);
- m:= m&^d mod n;
- ptext := cat(ptext,itoa(m,k,N));
- end do;
- ptext:=SubstituteAll(ptext,"#", " ");
- printf("Plaintext: %s\n",ptext);
- end:

for example

- encrypteRSA("muberragurel",40,52767869313539019193,9507029);

From 12 -blocks of letters into 13 -blocks of letters

Plaintext: muberragurel

Ciphertext: b2j,5u2vml5vt

- decrypteRSA("b2j,5u2vml5vt ",40,52767869313539019193,9507029);

From 13 -blocks of letters into 12 -blocks of letters

Ciphertext: b2j,5u2vml5vt

Plaintext: muberragurel

- encrypteRSA("Ron Rivest,Adi Shamir and Leonard Adleman found RSA in 1977.",40,52767869313539019193,9507029);

From 12 -blocks of letters into 13 -blocks of letters

Plaintext: Ron Rivest,Adi Shamir and Leonard Adleman found RSA in 1977.

Ciphertext:
cckggz6kqws,baz8z7yz59hkmvaw9m50t747zilbl?tlph740zbgafl6xu?7?lm74

- decrypteRSA("cckggz6kqws,baz8z7yz59hkmvaw9m50t747zilbl?tlph740zbgafl6xu?7?lm74",40,52767869313539019193,22954230467328982169);

From 13 -blocks of letters into 12 -blocks of letters

Ciphertext:
cckggz6kqws,baz8z7yz59hkmvaw9m50t747zilbl?tlph740zbgafl6xu?7?lm74

Plaintext: ron rivest,adi shamir and leonard adleman found rsa in 1977.

A.2 DIFFIE-HELLMAN KEY EXCHANGE SYSTEM BY MAPLE

- with(numtheory):with(LinearAlgebra:-Modular):with(StringTools):

Alphabet and the numerical equivalences of symbols of the alphabet

- N:=40: #size of the alphabet
- indx:=table(["a"=0,"b"=1,"c"=2,"d"=3,"e"=4,"f"=5,"g"=6,"h"=7,"i"=8,"j"=9,"k"=10,"l"=11,"m"=12,"n"=13,"o"=14,"p"=15,"q"=16,"r"=17,"s"=18,"t"=19,"u"=20,"v"=21,"w"=22,"x"=23,"y"=24,"z"=25,"#"=26,"."=27,"?"=28,"$"=29,"0"=30,"1"=31,"2"=32,"3"=33,"4"=34,"5"=35,"6"=36,"7"=37,"8"=38,"9"=39]):
- symb:=table([0="a",1="b",2="c",3="d",4="e",5="f",6="g",7="h",8="i",9="j",10="k",11="l",12="m",13="n",14="o",15="p",16="q",17="r",18="s",19="t",20="u",21="v",22="w",23="x",24="y",25="z",26="#",27=".",28="?",29="$",30="0",31="1",32="2",33="3",34="4",35="5",36="6",37="7",38="8",39="9"]):

converting letter blocks to their numerical equivalents

- atoi:=proc(txt,N)
- local i,res,t;
- res:=0; t:= LowerCase(Reverse(txt)); t:=SubstituteAll(t," ", "#");
- for i from 1 while i<= length(t) do
- res := res + indx[substring(t,i)]*(N^(i-1));
- end do;
- return (res);
- end:

converting numbers back to letters

This procedure converts the integer *m* from decimal representation into *N*-base representation having *k* digits. *k* must be greater than or equal to $[log_n m]$ otherwise an error message is displayed.

- itoa:=proc(m,k,N)
- local res,len,i,lst;
- lst := convert(m,base,N);
- res:=[];
- len := nops(lst);
- for i from 1 while i<= k do
- res := [op(res),0];
- end do;
- for i from 1 while i<= len do
- res[i] := lst[i];
- end do;
- for i from 1 while i<= k do
- res[i] := symb[res[i]];
- end do;
- return Reverse((Implode(res)));
- end:

Generating a key using the Deffie-Hellman key exchange system

This procedure generates a pair of a secret and public keys for a single user based on Deffie-Hellman algorithm.

- DeffieHellman:=proc(galf,gnr)
- local q, X, Y,lst;
- lst:=[];
- q:=galf[size]():
- randomize():
  #generate keys
- X:=rand() mod q: lst:=[op(lst),X]: #keep it secret
- Y:=gf[output](gf[`^`](gnr,X)): lst:=[op(lst),Y]: #make it public

- printf("Your secret key (X) is:%d\n",X);
- printf("Your public key (Y) is:%d\n",Y);
- return lst;
- end proc:

Suppose two users want to agree on a public key. They choose a finite field, for example, *GF*(7,20) and compute the primitive element of the field.

- gf:=GF(11,20):g:=gf[PrimitiveElement]():

and the first user generates a pair of keys and anounces his/her public key

- KEY:=DeffieHellman(gf,g);

Your secret key (X) is:889109933313

Your public key (Y) is:512807151746229471124

KEY:=[889109933313, 512807151746229471124]

- XA:=KEY[1];YA:=KEY[2];

XA:= 889109933313

YA:= 512807151746229471124

then the second user generates a pair of keys and anounces his/her public key

- KEY:=DeffieHellman(gf,g);

Your secret key (X) is:743949271486

Your public key (Y) is:550730814315003042959

KEY:=[743949271486, 550730814315003042959]

- XB:=KEY[1];YB:=KEY[2];

XB:= 743949271486

YB:= 550730814315003042959

The following computations show that the users have agreed on a common public key**:**

- SKEY:=gf[output](gf[`^`](gf[input](YB),XA));

SKEY:=202810007682204043917

- SKEY:=gf[output](gf[`^`](gf[input](YA),XB));

SKEY:=202810007682204043917

- SKEY:=SKEY mod N^12;

SKEY:=1483415682204043917

- k:=convert(SKEY,base,N^2);

k:=[717, 1527, 1260, 431, 751, 141]

- A:=<<k[1],k[2]>|<k[3],k[4]>>;Ai:=Inverse(N^2,A);

$$A := \begin{matrix} 717 & 1260 \\ 1527 & 431 \end{matrix}$$

$$Ai := \begin{matrix} 833 & 620 \\ 839 & 131 \end{matrix}$$

- B:=<<k[5],k[6]>>;Bi:=-B; #additive inverse

$$B := \begin{matrix} 751 \\ 141 \end{matrix}$$

$$Bi := \begin{matrix} -751 \\ -141 \end{matrix}$$

Affine Encryption

- encrypteAffine:=proc(ptxt,N,M,V) # ptxt is plaintext, N is base, M is encryption matrix and V is encryption vector
- local i,k,ctext,x,y,r,blocknumber,ptext,P,C;
- k := 2; #because of diagraph
- ptext:=ptxt;
- printf("Plaintext: %s\n",ptext);
- r := length(ptext) mod 2*k;
- if r > 0 then
- for i from 1 while i <= 2*k-r do
- ptext := cat(ptext,"#");
- end do;
- end if;
- blocknumber:=length(ptext)/(2*k); ctext:="";
- for i from 1 while i <= blocknumber do
- x:=atoi(substring(ptext,(i-1)*2*k+1..(i-1)*2*k+2),N);
- y:=atoi(substring(ptext,(i-1)*2*k+3..(i-1)*2*k+4),N);
- P:= <<x,y>>; C:=AddMultiple(N^2,Multiply(N^2,M,P),V);
- ctext := cat(ctext,itoa(C[1,1],2,N));ctext := cat(ctext,itoa(C[2,1],2,N));
- end do;

- printf("Ciphertext: %s\n",ctext);
- end:

Affine Decryption

- decrypteAffine:=proc(ctxt,N,Mi,Vi)
- local i,k,ptext,x,y,blocknumber,ctext,P,C;
- k := 2; #because of diagraph
- ctext:=ctxt;
- printf("Ciphertext: %s\n",ctext);
- blocknumber:=length(ctext)/(2*k); ptext:="";
- for i from 1 while i <= blocknumber do
- x:=atoi(substring(ctext,(i-1)*2*k+1..(i-1)*2*k+2),N);
- y:=atoi(substring(ctext,(i-1)*2*k+3..(i-1)*2*k+4),N);
- C:=<<x,y>>; P:=Multiply(N^2,Mi,AddMultiple(N^2,Vi,C));
- ptext := cat(ptext,itoa(P[1,1],2,N));ptext := cat(ptext,itoa(P[2,1],2,N));
- end do;
- ptext:=SubstituteAll(ptext,"#", " ");printf("Plaintext: %s\n",ptext);
- end:

Now, the users comunicate

- encrypteAffine("when are you comming?",40,A,B);

Plaintext: when are you comming?

Ciphertext: h0i3g15za91j4zzhphuxt38j

- decrypteAffine("h0i3g15za91j4zzhphuxt38j",40,Ai,Bi);

Ciphertext: h0i3g15za91j4zzhphuxt38j

Plaintext: when are you comming?

A.3 EL GAMAL BY MAPLE

- with(numtheory):with(LinearAlgebra:-Modular):with(StringTools):

Alphabet and the numerical equivalences of symbols of the alphabet

- N:=40: #size of the alphabet
- indx:=table(["a"=0,"b"=1,"c"=2,"d"=3,"e"=4,"f"=5,"g"=6,"h"=7,"i"=8,"j"=9,"k"=10,"l"=11,"m"=12,"n"=13,"o"=14,"p"=15,"q"=16,"r"=17,"s"=18,"t"=19,"u"=20

,"v"=21,"w"=22,"x"=23,"y"=24,"z"=25,"#"=26,"."=27,"?"=28,"$"=29,"0"=30,"1"=31,"2"=32,"3"=33,"4"=34,"5"=35,"6"=36,"7"=37,"8"=38,"9"=39]):

- symb:=table([0="a",1="b",2="c",3="d",4="e",5="f",6="g",7="h",8="i",9="j",10="k",11="l",12="m",13="n",14="o",15="p",16="q",17="r",18="s",19="t",20="u",21="v",22="w",23="x",24="y",25="z",26="#",27=".",28="?",29="$",30="0",31="1",32="2",33="3",34="4",35="5",36="6",37="7",38="8",39="9"]):

converting letter blocks to numerical equivalents

- atoi:=proc(txt,N)
- local i,res,t;
- res:=0; t:= LowerCase(Reverse(txt)); t:=SubstituteAll(t," ", "#");
- for i from 1 while i<= length(t) do
- res := res + indx[substring(t,i)]*(N^(i-1));
- end do;
- return (res);
- end:

converting numbers to letters

- itoa:=proc(m,k,N)
- local res,len,i,lst;
- lst := convert(m,base,N);
- res:=[];
- len := nops(lst);
- for i from 1 while i<= k do
- res := [op(res),0];
- end do;
- for i from 1 while i<= len do
- res[i] := lst[i];
- end do;
- for i from 1 while i<= k do
- res[i] := symb[res[i]];
- end do;
- return Reverse((Implode(res)));
- end:

Users agree upon a fixed large finite field.

- q:=3355685403029:Randomize():rnd:=rand(q-1):
- gf:=GF(q,1):g:=gf[PrimitiveElement]():

Each user generates a key and makes it public.

For example let a user A performs his/her computation as following:

- a:= rnd(); PK:=gf[`^`](g,a);# PK means public key

##

Now we want to send A a message.

a:=3269645449646

PK:=2576936998293 mod 3355685403029

- text := "sos":textlength:=length(text):
- P:=atoi(text,N): y:=gf[input](P);

Warning: the value of *P* must be between 1 and *q*-1 .To send the message to the user, we choose a random integer

y:=29378 mod 3355685403029

- k:=rnd();

and send the following pair of elements of GF(q) to A:

k:=1482676938101

- mes := [gf[`^`](g,k), gf[`*`](y,gf[`^`](PK,k))]; # (r,s)

A encryptes the message as following:

mes:=[2180885012773 mod 3355685403029, 1107371752052 mod 3355685403029]

- mask:=gf[`^`](mes[1],a);

mask:=2751932742240 mod 3355685403029

- imask:=gf[inverse](mask);

imask:=1173959117360 mod 3355685403029

- y:=gf[`*`](mes[2],imask);

y:=29378 mod 3355685403029

- P:=gf[output](y);

P:=29378

- itoa(P,textlength,N);

“sos”

A.4 MASSEY-OMURA BY MAPLE

- with(numtheory):with(LinearAlgebra:-Modular):with(StringTools):

Alphabet and the numeric equivalences of symbols of the alphabet

- N:=40: #size of the alphabet
- indx:=table(["a"=0,"b"=1,"c"=2,"d"=3,"e"=4,"f"=5,"g"=6,"h"=7,"i"=8,"j"=9,"k"=10,"l"=11,"m"=12,"n"=13,"o"=14,"p"=15,"q"=16,"r"=17,"s"=18,"t"=19,"u"=20,"v"=21,"w"=22,"x"=23,"y"=24,"z"=25,"#"=26,"."=27,"?"=28,"$"=29,"0"=30,"1"=31,"2"=32,"3"=33,"4"=34,"5"=35,"6"=36,"7"=37,"8"=38,"9"=39]):
- symb:=table([0="a",1="b",2="c",3="d",4="e",5="f",6="g",7="h",8="i",9="j",10="k",11="l",12="m",13="n",14="o",15="p",16="q",17="r",18="s",19="t",20="u",21="v",22="w",23="x",24="y",25="z",26="#",27=".",28="?",29="$",30="0",31="1",32="2",33="3",34="4",35="5",36="6",37="7",38="8",39="9"]):

Functions *itoa* and *atoi* can be used for conversion a block of text into decimal representation and vice versa.

converting letter blocks to numerical equivalents

- atoi:=proc(txt,N)
- local i,res,t;
- res:=0; t:= LowerCase(Reverse(txt)); t:=SubstituteAll(t," ", "#");
- for i from 1 while i<= length(t) do
- res := res + indx[substring(t,i)]*(N^(i-1));
- end do;
- return (res);
- end:

for example

- atoi("rr",40);

697

- atoi("cry",26);

1818

converting numbers to letters

- itoa:=proc(m,k,N)
- local res,len,i,lst;

- lst := convert(m,base,N);
- res:=[];
- len := nops(lst);
- for i from 1 while i<= k do
- res := [op(res),0];
- end do;
- for i from 1 while i<= len do
- res[i] := lst[i];
- end do;
- for i from 1 while i<= k do
- res[i] := symb[res[i]];
- end do;
- return Reverse((Implode(res)));
- end:

for example

- itoa(18194054,5,40);

"hello"

Suppose two users want to communicate. They choose a finite prime field.

- q:=164328833:Randomize():rnd:=rand(q-1):gf:=GF(q,1):

The first user generates a secrete key

- eA:= rnd();igcd(q-1,eA);

eA:= 30047783

1

- igcdex(q-1,eA,'u','dA'):if dA<0 then dA:=dA+q-1: end if:dA:=dA;

dA:= 20236311

The second user generates a secrete key

- eB:= rnd();igcd(q-1,eB);

eB:= 119743093

1

- igcdex(q-1,eB,'u','dB'):if dB<0 then dB:=dB+q-1: end if:dB:=dB;

dB:= 41811421

##

- text := "hello":textlength:=length(text):

Warning: the value of *P* must be between 1 and *q*-1

- P:=atoi(text,N); y:=gf[input](P);

P := 18194054

y:= 18194054 mod 164328833

now *A* sends *B* the element y^{eA} .

- **y**:= gf[`^`](y,eA);

y:= 75197608 mod 164328833

B recieves y^{eA} , raises it to the power *eB* and sends it back to *A*

- y:= gf[`^`](y,eB);

y:= 49265163 mod 164328833

A recieves $y^{(eAeB)}$, raises it to the power *dA* and sends the result back to *B*

- y:= gf[`^`](y,dA);

y:= 141767915 mod 164328833

Finally, *B* unravels the message by raising the element to the power *dB*

- y:= gf[`^`](y,dB);

y:= 18194054 mod 164328833

- P:=gf[output](y);

P:= 18194054

- itoa(P,textlength,N);

"hello"

APPENDIX B

FINITE FIELDS BY MAPLE

Let us start with creating a finite field. As we know for any prime p and nonnegative integer n, there exists a Galois field GF(p, n) with p^n elements. Let p be 3 and n be 2. GF (2,3) is created as following:

- **G1:=GF(2,3):**

Another way of creating a finite field is to use an irreducible polynomial over a prime field (see. Kronecker's Theorem). Let us choose an irreducible polynomial of degree 2 over the prime field F_3.

- **P1:=x^2 + x + 2:**

To be sure that this polynomial is irreducible over the prime field try to factorize it using the following command:

- **Factor(P1) mod 3;**

$x^2 + x + 2$

This polynomial is irreducible over F_3. Now we are ready to create an extesion field of F_3: $F_3[x]/<x^2+x+2>$

Type the following:

- **G2:=GF(3,2,alpha^2+alpha+2):**

Let us start with choosing an element randomly from a finite field.

- **a:=G2[random]();**

a:= (2a + 2) mod 3

The size (number of elements) of the field is computed as following:

- **G2[size]();**

9

As we know if α is algebraic over F and F (α) is an extension of the field F then the basis of the F (α) is { 1,α , ..., α^{n-1}} and any element of the field F (α) can be written as $a_0+a_1\alpha + ... + a_{n-1}\ \alpha^{n-1}$, so to display the elements of the field in this form we can use operator *ConvertOut*:

- **x:=G2[ConvertOut](a);**

x:= 2a + 2

To convert back to a field element we use *ConvertIn*:

- **G2[ConvertIn](x);**

(2a + 2) mod 3

Let F be a finite field of characteristic *p* and alpha is algebraic over F. Then there is a correspondence between the elements of the field F(α) and the range of integers {0, ..., p^n-1}, where [F [α] : F] = n.

To find correspondence between elements of the field F(α) and the range of integers {0, ..., p^n-1} we use operators *output* and *input*:

- **G2[output](a);**

8

- **G2[ConvertOut](G2[input](8));**

2a + 2

- **G2[ConvertOut](G2[input](100));**

$a^4 + 2a^2 + 1$

Another well-known fact is that nonzero elements of a finite field F_q is finite group with respect to multiplication with q-1 elements. This group has a generator that is called a *primitive element*. To get a primitive element type:

- **PrimElem:=G2[PrimitiveElement]();**

PrimElem:= (2a + 2) mod 3

Now, let us see how to do arithmetic in a finite field. The general format of operations is as following:

<*Field Name*>[`<*operation*>`](*parameter1*, *parameter2*) or

<*Field Name*>[`<*operation*>`](*parameter1*).

- **a:=G2[random](); b:=G2[random]();**

a:= (a + 2) mod 3

b:= a mod 3

Addition:

- **G2[`+`](a,b);**

(a + 2) mod 3

Subtraction:

- **G2[`-`](a,b);**

2 mod 3

Multiplication:

- **G2[`*`](a,b);**

(a + 1) mod 3

Division:

- **G2[`/`](a,b);**

2a mod 3

Inverse of an element:

- **InverseOfa:=G2[inverse](a);**

InverseOfa:= (2a + 1) mod 3

It easy to check that we obtained the inverse of *a* by multiplication of *a* and it inverse:

- **G2[`*`](a,InverseOfa);**

1 mod 3

Power of an element is computed as following:

- **G2[`^`](a,5);**

(a + 2) mod 3

- **G2[`^`](PrimElem,5);**

(a + 1) mod 3

The order of a nonzero element in the field can be found by typing:

- **G2[order](a);**

4

- **G2[order](PrimElem);**

8

Zero and identity elements are obtained using the operators *zero* and *one*.

- **G2[zero];**

0 mod 3

- **G2[one];**

1 mod 3

Given an element of a finite field, to find out whether this elemnt is primitive or not we use operator *isPrimitiveElement*

- **a;G2[isPrimitiveElement](a);**

(a + 2) mod 3

false

- **b;G2[isPrimitiveElement](b);**

a mod 3

true

- **PrimElem;G2[isPrimitiveElement](PrimElem);**

(2a + 2) mod 3

true

REFERENCES

- **Fraleigh, John B.,** *Abstract Algebra*, **Addison-Wesley, 1999.**
- **Koblitz, Neal,** *A Course in Number Theory and Cryptography*, **2nd ed., Springer-Verlag, New York, 1994.**
- **Rosen, Kenneth H.,** *Elementary Number Theory and its applications*, **4th ed., Addison Wesley Longman, United State of America, 2000.**
- **Gardner, Martin,** *Codes,Ciphers and Secret Writing*, **Dover publications, Inc. New York, 1984.**
- **Washington, Lawrence C.,** *Elliptic Curves Number Theory and Cryptography*, **Chapman&Hall/CRC, USA, 2003.**
- **Schneier, Bruce,** *Applied Cryptography*, **2nd ed., John Willey & Sons,Inc., Canada, 1996.**
- **Washington, Lawrence C. and Trappe, Wade,** *Introduction to Cryptography with Coding Theory,* **Prentice Hall, New Jersey, 2002.**
- **Stallings, William,** *Cryptography and Network Security*, **3rd ed., Printice Hall, New Jersey, 2003.**
- **Stinson, Douglas R.,** *Cryptography Theory and Practice*, **2nd ed., Chapman&Hall/CRC, United States of America, 2002.**
- **Spillman, Richard J.,** *Classical and Contemporary Cryptology*, **Pearson Prentice Hall, New Jersey, 2005.**
- **Koblitz, Neal,** *Algebraic Aspects of Cryptography*, **Springer-Verlag, New York, 1999.**
- **Niederreiter, Harald and Lidl, Rudolf,** *Introduction to finite fields and their applications*, **Revised ed., Cambridge University Pres, Great Britain, 1994.**
- **Apostol, Tom M.,** *Introduction to Analytic Number Theory*, **Springer-Verlag, United States of America, 1976.**

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