Cryptography by Means of Linear Algebra and Number Theory

Ajaeb Elfadel

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the Degree of

Master of Science
in
Mathematics

Eastern Mediterranean University
February 2014
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Elvan Yılmaz
Director

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

Prof. Dr. Nazım I. Mahmudov
Chair, Department of Mathematics

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Mathematics.

Asst. Prof. Dr. Müge Saadetoğlu
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Rashad Aliyev

2. Asst. Prof. Dr. Ersin Kuset

3. Asst. Prof. Dr. Müge Saadetoğlu

ABSTRACT

This thesis focuses on the techniques of cryptography in linear algebra and number theory.

We first give the necessary review on modular arithmetic. Under Linear Algebra, Hill cipher cryptographic technique and its variations are studied. Under number theory, on the other hand, the definition of Euler function, and some important theorems in this regard are given. The cryptographic techniques such as the Caesar cipher, Exponential transformations and the Public key cryptographic techniques are explained.

Finally, some more advanced cryptographic techniques such as the Digraph transformations are given.

Keywords: Hill cipher, Euler theorem, Caesar cipher, Exponential method, Public Key method, Monoalphabetic cipher, Digraph transformations.

ÖZ

Bu yüksek lisans tezinde Lineer Cebir ve Sayılar kuramı kavramları kullanan şifreleme yöntemleri anlatılmıştır.

Tezin giriş kısmı tezde sıkça kullanılan modüler aritmetik ile ilgili ön bilgi vermektedir.Lineer cebir de Hill Şifreleme yöntemi baz alınmıştır.Sayılar kuramı bölümünde ise, Euler fonksiyonu tanıtılıp, bu fonksiyonla ilgili temel teoremler verildikten sonra, bu teoremleri kullanan şifreleme yöntemleri aktarılmıştır.Sezar Şifreleme, Üstel transformasyon ve Asimetrik şifreleme yöntemleri işlenen şifreleme yöntemlerinden bazılarıdır.

Son olarak da daha ileri derecede şifreleme imkanı sunan ‘tek sesi temsil eden iki harf’ yöntemi anlatılmıştır.

Anahtar Kelimeler: Hill Şifreleme, Euler Teoremi, SezarŞifreleme, Üstel ransform-asyon, Asimetrik şifreleme, Tek sesi temsil eden iki harf metodu.

ACKNOWLEDGEMENT

First of all, I am thankful to Allah for all the gifts He has provided me.

I would like to express my gratitude to my supervisor Müge Saadetoğlu for her encouragement, suggestions to solve the problems, valuable advice, and taking care of the preparation of this thesis.

I am especially grateful to my husband and to all my family members for their support.

Finally, many thanks go to my friends for their help and encouragement.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

Cryptography is one of the most important applications of linear algebra and number theory where the process is to change important information to another unclear one.

The main goal of cryptography is to keep the integrity and security of this information. There are many types of cryptography techniques and we will try to consider some of them in this thesis. This thesis consists of five chapters, where chapter one includes this introduction. In the second chapter, we first mention some necessary definitions, theorems and some known results that will be needed in this thesis. We show some important proofs in modular arithmetic and groups.

We review the Division algorithm theorem, study the addition and multiplication modulo n, and finally after defining the notion of a (group); we give the conditions for a set to be a group. The third chapter gives the cryptography techniques that use linear algebra. The most important type here is the Hill Cipher method, which uses the encryption algorithm:

$$C \equiv AP \mod N$$

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \bmod N$$

where C is the column vector containing the numerical values of the cipher text message and we can get the new message that is unclear by changing these values to their letters. A is called the key of the algorithm, and this key should be invertible for the decryption algorithm. P is the column vector of the plaintext numerical values and finally N is the number of letters of the alphabet used in our work. For the decryption algorithm:

$$P \equiv A^{-1}C \bmod N$$

where A^{-1} is the inverse of the matrix A. We have used 2×2 and 3×3 matrices to encode some messages in our examples. We can use matrices of higher size, where we can use computer programs to find inverses of them. In this chapter also we try to use the properties of the matrix A to make this process more complex and interesting. We can also use more than one key, where the algorithm becomes:

$$C \equiv ABP \bmod N$$

Also, we use the algorithm of affine cipher with this method, where:

$$C \equiv AP + B \bmod N .$$

In the fourth chapter, we study the number theory techniques of cryptography with some examples. Here, we define the Euler function $\phi(n)$ and revise the proof of the Euler's theorem which states:

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

where a and n are relatively prime. Also, we state and prove some theorems, lemmas and corollaries related with the Euler's theorem such as the Lagrange's theorem:

$$H \subseteq G \Rightarrow |H| \| |G|$$

where G is a finite group. Next, we talk about some codes that are based on number theory.

① Caesar cipher: In this cipher we use the encryption algorithm

$$y \equiv x + k \mod N;$$

where K is any integer and N is the number of letters of the alphabet used in the coding process. For decryption, we use the algorithm:

$$x \equiv y - k \mod N$$

② Affine cipher; in this cipher we use for encryption the algorithm $y \equiv ax + b \mod N$ where a, b are any two different integers, a being a unit modulo N.

For decryption, the algorithm is:

$$x \equiv a^{-1}(\mathrm{y} - b) \mod N$$

where a^{-1} is the inverse of the element a.

③ An exponential method; Here we choose a large prime number P and any integer e where

$$\gcd(e, P-1) = 1$$

Then, for encryption the algorithm is:

$$y \equiv x^e \mod P$$

For decryption:

$$x \equiv y^h \mod P$$

where $eh = 1 \mod (P-1)$.

④ Public key cryptographic technique; here we choose two prime number's p, q where:

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

Then, for encryption the algorithm is:

$$C \equiv M^e \mod n$$

where e is any integer that is co-prime to $\phi(n)$. For decryption:

$$M \equiv C^d \mod n$$

where $ed \equiv 1 \mod \phi(n)$.

In the last chapter, more advanced cryptographic techniques are collected and some related examples are given. First of all, we mention the mono alphabetic cipher. This method depends on using the frequency analysis for the ciphertext message and compares it with the standard frequency in the language that is used.

Also, to break the cipher which is encrypted, we use the techniques discussed in previous chapters; i.e. we use the Caesar and the affine ciphers.

Later, we study the digraph transformation method. This method depends on putting the letters of the plaintext message in pairs (x, y) and calculating

$$P = xN + y$$

where N again is the number of the letters in the alphabet. We use for encryption the algorithm:

$$C \equiv aP + b \mod N^2$$

For decryption, we use the algorithm:

$$P \equiv a^{-1}C + b' \mod N^2$$

where a^{-1} is the inverse of $a \mod N$, $b' = -a^{-1}b \mod N^2$. After that, we try to use an affine matrix transformation of pairs of digraphs.

For encryption:

$$C \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} P + \begin{pmatrix} e \\ f \end{pmatrix} \mod N^2.$$

$$C \equiv AP + B \mod N^2$$

where A is an invertible matrix mod N^2, and for decryption

$$P \equiv A^{-1}(C - B) \mod N^2$$

Finally, we use an affine matrix transformation of $P(\mathrm{x}, \mathrm{y}, \mathrm{z})$ trigraph. Here:

$$P = xN^2 + yN + z$$

And the algorithm is:

$$C \equiv \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} + \begin{pmatrix} Y \\ K \\ L \end{pmatrix} \mod N^3.$$

Chapter 2

MODULAR ARITHMETIC

In this chapter, we will consider some important facts that we need in our study. First of all we give the definition of addition modulo n and multiplication modulo n, and then we explain some facts on modular arithmetic.

2.1 The Equivalence Relation

Definition 2.1.1 We say that a and b are equivalent modulo n if and only if $n \mid (a-b)$ and we write modulo equivalent as:

$$a \equiv b \mod n .$$

Theorem 2.1.2 The relation given above is an equivalence relation on Z.

Proof. a) Reflexive: $\forall a \in Z$, $n \mid 0 = a - a \Rightarrow a \equiv a \bmod n$.

b) Symmetric: $\forall a,b \in Z,\ a \equiv b \bmod n \Rightarrow n \mid a-b$ and $n \mid b-a = -(a-b) \Rightarrow b \equiv a \bmod n$.

c) Transitive: $\forall$a,b,c $\in Z$, if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then:

$$n \mid a-b, n \mid b-c \Rightarrow n \mid a-c = (a-b)+(b-c) \Rightarrow a \equiv c \mod n .\square$$

Theorem 2.1.3 If $a \equiv b \mod n$, $c \equiv d \bmod n$ then:

a) $a+c \equiv b+d \mod n$.

b) $ac \equiv bd \mod n$.

Proof. a) Since $a \equiv b \mod n \Rightarrow n \mid a-b \Rightarrow a-b = m\,n \Rightarrow a = b+m\,n$.

$c \equiv d \mod n \Rightarrow n \mid c-d \Rightarrow c-d = k\,n \Rightarrow c = d+k\,n$.

For some $m,k \in Z$, Then

$$(a+c)-(b+d)=b+mn+d+kn-b-d=n(m+k)$$

Since

$$(m+k)\in \square \Rightarrow a+c\equiv b+d \mod n$$

b) Also $ac-bd=(b+mn)(d+kn)-bd=bd+knb+mnd+mkn^2-bd$

$$=n(kb+md+mkn).$$

Since

$$(kb+md+mkn)\in Z \Rightarrow ac\equiv bd \mod n. \square$$

Definition 2.1.4 The set $[a]$ of all integers equivalent to $a \pmod n$ is said to be the remnant class of a .

We can also denote this class by $\bar{a}$.

Example 2.1.5 Remnant classes mod 5:

[0]={….,-10,-5,0,5,10,……}, [1]={….,-9,-4,1,6,11,…….}, [2]={….,-8,-3 ,2,7,12,…….}

[3]={….,-7 ,-2 ,3,8,13,…..}, [4]={….,-6 ,-1 ,4,9,14,…..}

Definition 2.1.6 The set $Z_n=\{0,1,2,3,\ldots\ldots\ldots,(n-1)\}$ is said to be the set of the remnant classes mod n .This group is referred to as modular group.

Remark 2.1.7

Next, we can define the binary operations $(+_n)$ and $(\cdot_n)$ on Z_n , where $(+_n)$ is said to be addition modulo n and $(\cdot_n)$ is said to be multiplication modulo n .

2.2 The Addition Modulo n

Definition 2.2.1 $\forall [a]\in Z_n$ and $[b]\in Z_n$ we define the addition on Z_n as follows:

$$[a]+_n[b]=[a+b]$$

Theorem 2.2.2 $\forall [a],[b],[c] \in Z_n$:

a) $[a]+_n[b]=[b]+_n[a]$

b) $[a]+_n([b]+_n[c])=([a]+_n[b])+_n[c]$

c) $\exists\,[0] \in Z_n$ Such that $[a]+_n[0]=[a]$

d) $\exists[-a] \in Z_n$ Such that $[a]+_n[-a]=[0]$.

Proof. a) Since $\forall a,b \in Z,\ a+b=b+a$ then $[a]+_n[b]=[a+b]=[b+a]=[b]+_n[a]$.

b) Since $\forall a,b,c \in Z$, $a+(b+c)=(a+b)+c$ then

$[a]+_n([b]+_n[c])=[a]+_n[b+c]=[a+b+c]=[a+b]+_n[c]=([a]+_n[b])+_n[c]$.

c) $[a]+_n[0]=[a+0]=[a]$.

d) Since $\forall a \in Z,\ \exists\,(-a)$ such that $a+(-a)=(-a)+a=0 \Rightarrow [a]+_n[-a]=[a+(-a)]=0.$

□

Theorem 2.2.3 $\forall a \in Z_n$, the system $(\mathrm{Z}_n,+_n)$ is a group.

Proof. a) Z_n is closed under $+_n$.

b) Z_n is also associative by the theorem above.

c) $[0]$ is the identity element of this set.

d) If $[a] \in Z_n$, then its inverse is $[n-a]$, because $[a]+_n[n-a]=[a+n-a]=[n]=[0]$.

Therefore $(\mathrm{Z}_n,+_n)$ is a group. □

2.3 The Multiplication Modulo n

Definition 2.3.1 $\forall [a],[b] \in Z_n$, we define the multiplication on Z_n as follows:

$$[a]\cdot_n[b]=[a\cdot b]$$

Theorem 2.3.2 $\forall [a],[b],[c] \in Z_n$

i) $[a] \cdot_n [b] = [b] \cdot_n [a]$

ii) $[a] \cdot_n ([b] \cdot_n [c]) = ([a] \cdot_n [b]) \cdot_n [c]$

iii) $\exists\, [0] \in Z_n$ such that $[a] \cdot_n [0] = [0]$

iv) $\exists [1] \in Z_n$ such that $[a] \cdot_n [1] = [a]$.

Proof. i) Since $\forall a,b \in Z,\ a \cdot b = b \cdot a$ then $[a] \cdot_n [b] = [a \cdot b] = [b \cdot a] = [b] \cdot_n [a]$.

ii) Since $\forall a,b,c \in Z\ , a \cdot (b \cdot c) = (a \cdot b) \cdot c$ then:

$[a] \cdot_n ([b] \cdot_n [c]) = [a] \cdot_n [b \cdot c] = [a \cdot b \cdot c] = [a \cdot b] \cdot_n [c] = ([a] \cdot_n [b]) \cdot_n [c]$.

iii) $[a] \cdot_n [0] = [a \cdot 0] = [0]$.

iv) $[a] \cdot_n [1] = [a \cdot 1] = [a]$. □

Theorem 2.3.3

$\forall [a][b][c] n \in Z_n : [a] \cdot_n \{[b] +_n [c]\} = \{[a] \cdot_n [b]\} +_n \{[a] \cdot_n [c]\}$.

Proof.

since $\forall a,b,c \in Z,\ a(b+c) = (ab) + (ac)$

Then

$[a] \cdot_n \{[b] +_n [c]\} = [a] \cdot_n [b+c] = [a(b+c)] = [(ab) + (ac)]$

$= [ab] +_n [ac] = \{[a] \cdot_n [b]\} +_n \{[a] \cdot_n [c]\}$. □

Definition 2.3.4 We say that the numbers a,b are relatively prime if gcd $(a,b) = 1$.

For example, 21- 20 are relatively prime $\Longrightarrow$ because gcd (21,20)=1.

Definition 2.3.5 We say that the number $a \in Z_n$ is unit if $\exists b \in Z_n$ such that

$$ab \equiv 1 \bmod n$$

Remark 2.3.6 The set of all units in Z_n is denoted by U_n or Z_n^* for example:

$$Z_4^* = U_4 = \{[1],[3]\},\ Z_7^* = U_7 = \{[1],[2],[3],[4],[5],[6]\}$$

Theorem 2.3.7 For any $a \in Z_n$, the system $(Z_n^*, \cdot_n)$ is a group.

Proof. i) If $[a] \in Z_n^*$ and $[b] \in Z_n^*$ then, $\exists [c],[d] \in Z_n^*$ such that:

$[a] \cdot_n [c] = [1]$, $[b] \cdot_n [d] = [1] \Rightarrow [ab] \cdot_n [cd] = [abcd] = [acbd] = [ac] \cdot_n [bd] = [1]^2 = [1]$

So $[ab]$ is also a unit $\Rightarrow Z_n^*$ is a closed under $(\cdot_n)$.

ii) $\forall [a][b][c] \in Z_n^*$,

$$[a] \cdot_n ([b] \cdot_n [c]) = [a] \cdot_n [b \cdot c] = [a \cdot b \cdot c] = [a \cdot b] \cdot_n [c] = ([a] \cdot_n [b]) \cdot_n [c].$$

iii) The identity of Z_n^* is the class $[1]$, because $[a] \cdot_n [1] = [1] \cdot_n [a] = [a]$ for all $[a] \in Z_n^*$.

iv) Since for $[a] \in Z_n^*$, $\exists [b] \in Z_n^*$ such that $[a] \cdot_n [b] = [1]$ (from the definition), every element in Z_n^* has a multiplicative inverse.□

Remark 2.3.8 If n is a prime, then $Z_n^* = Z_n^* - [0]$ is a group under $(\cdot_n)$, as all the non-zero classes in this case, are units.

Theorem 2.3.9 $[a] \in Z_n$ has a multiplicative inverse $[b]$ if and only if gcd $(n, a) = 1$

Proof. $\Leftarrow$ If gcd $(a, n) = 1$, then by Euclid's algorithm $ac + nd = 1$ for some $c, d \in Z$. That is:

$$[ac + nd] = [1], [ac] +_n [nd] = [1], \{[a] \cdot_n [c]\} +_n \{[n] \cdot_n [d]\} = [1], [a] \cdot_n [c] = [1]$$

(Because $[n] = [0]$). So, $[c]$ is the multiplicative inverse of $[a]$, Let $[c] = [b] \Rightarrow$

$$[a]\cdot_n[b]\equiv[1] \bmod n$$

$\Rightarrow$ If $ab\equiv 1 \bmod n$. Then, $n|1-ab$ or $dn=1-ab$ for some $d\in Z$. Therefore:

$$ab+dn=1\Rightarrow \gcd\ (a,n)=1.\ \square$$

Definition 2.3.10 We say that, the classes $[a]$ and $[b]$ are zero divisors if $[a][b]=[0]$ but both of $[a],[b]$ are not zero classes. (This is also true for the elements; that is a non- zero element a is a zero divisor if $ab=0$ for some other non zero element b .)

Theorem 2.3.11 If a is a unit, then a is not a zero divisor.

Proof. If a is a unit $\Rightarrow a$ is invertible $\Rightarrow \exists\, c$ such that ac = 1.

Assume that a is a zero divisor. This means that $a\neq 0,\ b\neq 0$ but $ab = ba = 0$.

$$(ba)c = 0 \Rightarrow b(ac) = b = 0.$$

This is a contradiction with the fact above. Hence, a is not a zero divisor. $\square$

Chapter 3

LINEAR ALGEBRA CRYPTOGRAPHIC TECHNIQUES

In this chapter, the main cryptographic technique we will use is Hill cipher which is a method developed by the mathematician Lester Hill in 1929 [11]. Here the encryption algorithm takes plaintext letters as input, and produces $\boldsymbol{m}$ ciphertext letters for them.

3.1 Hill Cipher

3.1.1 The encryption process In fact, we can summarize the encryption which is the process of converting plaintext into ciphertext in four basic steps:

i) Choose an $(n \times n)$ matrix A which is invertible, where n here maybe depends on the length of the message that needs to be encrypted.

ii) Change each plaintext to its numerical value, by using the table below:

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
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

iii) Form the $(n \times 1)$ column vector P, having these numerical values as its entries.

iv) Get each ciphertext vector C by multiplying A with P, and convert each entry of the ciphertext vector to its letter in the alphabet. The encryption algorithm of this method is:

$$C \equiv AP \mod N .$$

where C is the column vector of the numerical values of ciphertext, P is the column vector of the numerical values of plaintext, A an $(n \times n)$ matrix, is the key of the algorithm, (this matrix must be invertible because we need the inverse of this matrix for the decryption process), and N is the number of letters of the alphabet used in the cryptography.

3.1.2 The decryption process The decryption which is the process of converting the ciphertext into plaintext could also be summarized in four basic steps:

i) Get the inverse of the matrix A; say A^{-1} .

ii) Change each ciphertext to its numerical value.

iii) Put each ciphertext in a $(n \times 1)$ column vector say C .

iv) Get each plaintext vector by multiplying A^{-1} with C, and convert each plaintext vector to its letter in the alphabet. The decryption algorithm of this method is:

$$P \equiv A^{-1}C \mod N .$$

where A^{-1} is the inverse of the matrix A.

Remark 3.1.3: In general, if $A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ and $P=\begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix}$ then, in the encryption process, we get

$$C \equiv AP \mod N$$

$$\Rightarrow \begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} \mod N.$$

Here when the size of the matrix A increases, or in other words when n increases, we will have the following advantages:

1. The cryptography process will be more complex and more difficult to decode.

2. The number of column vectors will decrease and we can encode any message consisting for example of 7 letters by using a (7×7) matrix in only one step. But there is one problem here, that is, it's not easy to get the inverse of the matrix used in the encryption process as n increases.

Below, we give several other ways of using Hill cipher technique for encryption.

3.2 Using More Than One Key in Hill Cipher

In the Hill cipher, since the key used to encode or decode any message is a matrix, we can use the associative property of matrices to make the coding process more complex and more secure. Therefore; if we have two invertible matrices A, B and a plaintext column vector P, then the general case is explained below.

Given $A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$, $B=\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$ $P=\begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix}$, the encryption algorithm is:

$$C \equiv ABP = A(BP) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} = \begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \bmod N$$

The decryption algorithm, on the other hand, is

$$P \equiv (\mathrm{AB})^{-1} C \equiv B^{-1} A^{-1} C = B^{-1}(A^{-1} C) \mod N .$$

In this way, we got a new cipher column vector C, because the matrix multiplication operation is an associative. Here, we also use the fact that $(\mathrm{XY})^{-1} = Y^{-1} X^{-1}$.

Note also that:

$(\mathrm{XY})^{-1} = Y^{-1} X^{-1} = X^{-1} Y^{-1}$ if and only if X and Y commute. Here we should be careful as matrix multiplication is not always commutative.

3.2.1 Generalizing the Above Algorithm

In this case we can use n number of invertible matrices to encode or decode any message and the steps will be the same. This means that, if we have the invertible matrices $A, B, C, ..., M$, then the encryption algorithm will be:

$$C \equiv (ABC.....M)P \bmod N$$

$$\begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \cdots\cdots \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} \bmod N$$

Hence the decryption algorithm is:

$$P \equiv (ABC.....M)^{-1} C \bmod N$$

3.3 Using The Affine Cipher Algorithm in Hill Cipher

We can use the Affine cipher technique to make the Hill cipher more complex. Encryption algorithm here is given as:

$$C \equiv AP + B \pmod N$$

$$\begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} + \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} (\text{mod } N)$$

where A is an invertible matrix and B is a column vector like the vectors C and P.

For the decryption:

$$P \equiv A^{-1}C - A^{-1}B = A^{-1}(C - B) \pmod{N}$$

3.4 Using the Affine Cipher Algorithm in Hill Cipher with More Than One Key

By using the following algorithm to encrypt any message we will get more complex process:

$$C \equiv (AB.....M)P + K \pmod{N}.$$

$$\begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \cdots\cdots \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} + \begin{pmatrix} k_{11} \\ \vdots \\ k_{n1} \end{pmatrix} (\text{mod } N)$$

The decryption here works as below;

$$P \equiv (AB....M)^{-1}(C - K) \pmod{N}.$$

Here are some examples now to illustrate the above facts.

3.5 Examples

Example 3.5.1 Encode the message (Help me) by using Hill cipher algorithm where the matrix is

$A = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$.

Solution. First use the table below to convert letters in the message to their numerical values.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Put also number 0 for the space between words. Group the plaintext letters into pairs and add 0 to fill out the last pair:

H	E	L	P		M	E	
8	5	12	16	0	13	5	0

Then:

$$C \equiv AP \mod N .$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 21 \\ 8 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 12 \\ 16 \end{pmatrix} = \begin{pmatrix} 40 \\ 12 \end{pmatrix} = \begin{pmatrix} 14 \\ 12 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 0 \end{pmatrix}=\begin{pmatrix} 10 \\ 5 \end{pmatrix} \pmod{26}$$

Now, the new message becomes: (Uhnlm je).

21	8	14	12	13	0	10	5
U	H	N	L	M		J	E

Example 2.5.2 Decode the message (Xofmnofaare sfaty mqepxeqxetd amerblfseqcoeb-bbdavxeraa), by using the Hill cipher algorithm and the inverse of the matrix:

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Solution: Since $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, by Gaussian elimination, one can show that

$$A^{-1} = \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Now, put the ciphertext into groups, where each group consists of three letters. Find the numerical value of each letter from the table above. Therefore:

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 24 \\ 15 \\ 6 \end{pmatrix}=\begin{pmatrix} 0 \\ 9 \\ 6 \end{pmatrix}.$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 13 \\ 14 \\ 15 \end{pmatrix}=\begin{pmatrix} 0 \\ -1 \\ 15 \end{pmatrix}=\begin{pmatrix} 0 \\ 25 \\ 15 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 6 \\ 1 \\ 1 \end{pmatrix}=\begin{pmatrix} -5 \\ 0 \\ 1 \end{pmatrix}=\begin{pmatrix} 21 \\ 0 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 18 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} -8 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 5 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 19 \\ 6 \\ 1 \end{pmatrix} = \begin{pmatrix} -8 \\ 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 18 \\ 5 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 20 \\ 25 \\ 0 \end{pmatrix} = \begin{pmatrix} 30 \\ 25 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 25 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 13 \\ 17 \\ 5 \end{pmatrix} = \begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 16 \\ 24 \\ 5 \end{pmatrix} = \begin{pmatrix} 27 \\ 19 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 19 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 17 \\ 24 \\ 5 \end{pmatrix} = \begin{pmatrix} 26 \\ 19 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 20 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} -12 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 14 \\ 4 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 18 \\ 2 \\ 12 \end{pmatrix} = \begin{pmatrix} -26 \\ -10 \\ 12 \end{pmatrix} = \begin{pmatrix} 0 \\ 16 \\ 12 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 6 \\ 19 \\ 5 \end{pmatrix} = \begin{pmatrix} 27 \\ 14 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 14 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 17 \\ 3 \\ 15 \end{pmatrix} = \begin{pmatrix} -26 \\ -12 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 14 \\ 15 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} -3 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 23 \\ 0 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 24 \\ 5 \end{pmatrix} = \begin{pmatrix} 21 \\ 19 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 18 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -17 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 9 \\ 0 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 9 \\ 9 \end{pmatrix} = \begin{pmatrix} -13 \\ 0 \\ 9 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \\ 9 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 16 \\ 4 \\ 4 \end{pmatrix} = \begin{pmatrix} -12 \\ 0 \\ 4 \end{pmatrix} = \begin{pmatrix} 14 \\ 0 \\ 4 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 8 \\ 21 \\ 7 \end{pmatrix} = \begin{pmatrix} 27 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 5 \\ 18 \\ 0 \end{pmatrix} = \begin{pmatrix} 31 \\ 18 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 18 \\ 0 \end{pmatrix} \pmod{26}$$

It is clear that, by changing every numerical value above to its letter in the alphabet, we get the message (If you are ready please send the plane now because I am in danger).

Example 3.5.3 Encode the following message by using the matrices $A = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$,

$B = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$, (I AM IN CYPRUS).

Solution. Put the plaintext message in pairs; change the letters to their numerical values by using the following table and put 0 instead of a space between words:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

We get $P_1 = \begin{pmatrix} 9 \\ 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 \\ 13 \end{pmatrix}$, $P_3 = \begin{pmatrix} 0 \\ 9 \end{pmatrix}$, $P_4 = \begin{pmatrix} 14 \\ 0 \end{pmatrix}$, $P_5 = \begin{pmatrix} 3 \\ 25 \end{pmatrix}$, $P_6 = \begin{pmatrix} 16 \\ 18 \end{pmatrix}$,

$P_7 = \begin{pmatrix} 21 \\ 19 \end{pmatrix}$. Here we put **0** for the space between words. Therefore:

$$C \equiv ABP \mod N .$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 9 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 27 \\ 36 \end{pmatrix} = \begin{pmatrix} 90 \\ 27 \end{pmatrix} = \begin{pmatrix} 12 \\ 1 \end{pmatrix} \text{ (mod 26).}$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 13 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 29 \\ 43 \end{pmatrix} = \begin{pmatrix} 101 \\ 29 \end{pmatrix} = \begin{pmatrix} 23 \\ 3 \end{pmatrix} \text{ (mod 26).}$$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 9 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 18 \\ 27 \end{pmatrix} = \begin{pmatrix} 63 \\ 18 \end{pmatrix} = \begin{pmatrix} 11 \\ 18 \end{pmatrix} \text{ (mod 26).}$$

$$\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}14\\0\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}42\\56\end{pmatrix}=\begin{pmatrix}140\\42\end{pmatrix}=\begin{pmatrix}10\\16\end{pmatrix} \pmod{26}.$$

$$\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}3\\25\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}59\\87\end{pmatrix}=\begin{pmatrix}205\\59\end{pmatrix}=\begin{pmatrix}23\\7\end{pmatrix} \pmod{26}.$$

$$\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}16\\18\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}84\\118\end{pmatrix}=\begin{pmatrix}286\\84\end{pmatrix}=\begin{pmatrix}0\\6\end{pmatrix} \pmod{26}.$$

$$\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}21\\19\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}101\\141\end{pmatrix}=\begin{pmatrix}343\\101\end{pmatrix}=\begin{pmatrix}5\\23\end{pmatrix} \pmod{26}.$$

Then by changing every numerical value to its letter, the ciphertext message becomes (LAWCKRJPWG FEW).

Example 3.5.4 Try to decode the message (KY JQCVMHUEVEDD) by using the inverse of the matrices:

$$A = \begin{pmatrix}-1&2&1\\0&1&1\\0&0&1\end{pmatrix}, B = \begin{pmatrix}1&0&0\\0&1&0\\-4&0&1\end{pmatrix}.$$

Solution. Since $A = \begin{pmatrix}-1&2&1\\0&1&1\\0&0&1\end{pmatrix}$, by Gaussian elimination, one can show that

$$A^{-1} = \begin{pmatrix}-1&2&-1\\0&1&-1\\0&0&1\end{pmatrix}.$$

And since $B = \begin{pmatrix}1&0&0\\0&1&0\\-4&0&1\end{pmatrix}$, by Gaussian elimination, one can show that

$B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}$. Then:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 11 \\ 25 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} 39 \\ 25 \\ 0 \end{pmatrix} = \begin{pmatrix} 39 \\ 25 \\ 156 \end{pmatrix} = \begin{pmatrix} 13 \\ 25 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 10 \\ 17 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} 21 \\ 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 21 \\ 14 \\ 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 13 \\ 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -4 \\ 5 \\ 8 \end{pmatrix} = \begin{pmatrix} -4 \\ 5 \\ -8 \end{pmatrix} = \begin{pmatrix} 22 \\ 5 \\ 18 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 21 \\ 5 \\ 22 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -33 \\ -17 \\ 22 \end{pmatrix} = \begin{pmatrix} -33 \\ -17 \\ -110 \end{pmatrix} = \begin{pmatrix} 19 \\ 9 \\ 20 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 5 \\ 4 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 0 \\ 4 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 25 \\ 0 \\ 0 \end{pmatrix} \pmod{26}.$$

Now by changing each numerical value in plaintext column vectors to its letter we get the message **(**MY UNIVERSITY).

Example 3.5.5 Try to encode (LONDON) by using the algorithm $C \equiv AP + B \pmod{26}$ where: $A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

Solution. By using the table:

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
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

L	O	N	D	O	N
11	14	13	3	14	13

Then:

$$C \equiv AP + B \pmod{N}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 11 \\ 14 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 139 \\ 64 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 141 \\ 67 \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix} \text{(mod 26).}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 13 \\ 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 83 \\ 35 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 85 \\ 38 \end{pmatrix} = \begin{pmatrix} 7 \\ 12 \end{pmatrix} \text{(mod 26).}$$

$$\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 14 \\ 13 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 148 \\ 67 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 150 \\ 70 \end{pmatrix} = \begin{pmatrix} 20 \\ 18 \end{pmatrix} \text{(mod 26).}$$

L O N D O N $\Longrightarrow$ L P H M U S.

Example 3.5.6 Try to decode the ciphertext message (LPMGKZ) by using the algorithm

$P \equiv (AB)^{-1}(C - K) \pmod{N}$,

and the inverse of the matrices $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix}$, $K = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

Solution. Since $A=\begin{pmatrix}-1 & 2 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}$, by Gaussian elimination,one can show that

$$A^{-1}=\begin{pmatrix}-1 & 2 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}.$$

And since $B=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ -4 & 0 & 1\end{pmatrix}$, by Gaussian elimination, one can show that $B^{-1}=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}$.

Since

L	P	M	G	K	Z
11	15	12	6	10	25

Then:

$$P_1\equiv B^{-1}A^{-1}(C_1-K)\equiv\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 2 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}\left[\begin{pmatrix}11\\ 15\\ 12\end{pmatrix}-\begin{pmatrix}1\\ 2\\ 3\end{pmatrix}\right]$$

$$=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 2 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}10\\ 13\\ 9\end{pmatrix}$$

$$=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}\begin{pmatrix}7\\ 4\\ 9\end{pmatrix}=\begin{pmatrix}7\\ 4\\ 37\end{pmatrix}\equiv\begin{pmatrix}7\\ 4\\ 11\end{pmatrix}\pmod{26}.$$

$$P_2\equiv B^{-1}A^{-1}(C_2-K)\equiv\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 2 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}\left[\begin{pmatrix}6\\ 10\\ 25\end{pmatrix}-\begin{pmatrix}1\\ 2\\ 3\end{pmatrix}\right]$$

$$=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 4 & 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 2 & -1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}5\\ 8\\ 22\end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix} \begin{pmatrix} -11 \\ -14 \\ 22 \end{pmatrix} = \begin{pmatrix} -11 \\ -14 \\ -22 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 12 \\ 4 \end{pmatrix} \pmod{26}.$$

(LPMGKZ) $\Longrightarrow$ (HELPME).

Chapter 4

NUMBER THEORY CRYPTOGRAPHIC TECHNIQUES

In this chapter, we give the definition of the Euler function $\phi(n)$, revise the proof of the Euler's theorem, and study the number theory techniques of cryptography with some examples.

4.1 Euler's Function

Definition 4.1.1 [7] We define $\phi(n)$, to be the number of units in $\mathbf{Z}_n$. In other words, $\phi(n) = |U_n|$.

Example 4.1.2 Compute the Euler function of n where n is the set of all integers less than or equal to 15.

Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Before we give the Euler theorem, we state and prove the Lagrange's theorem.

Theorem 4.1.3 (Lagrange's Theorem**)** If G is a finite group and H is a subgroup of G, then the order of H, divides the order of G.

Proof. Since G is a finite group, $G=\{a_1,a_2,a_3,.....,a_n\}$, and the left coset of H by a is given by $aH=\{ah_1,ah_2,.....,ah_m\}$. Two cosets are either equivalent or disjoint, so $a_iH=a_jH$ or $a_iH\cap a_jH=\phi$. Since cosets have the same size, $|aH|=|H|$ for all $a\in G$ Therefore:

$$G=\cup\, aH\Rightarrow|G|=\sum|aH|=\sum|H|=k|H|\Rightarrow|H|\|G|.\square$$

Corollary 4.1.4 If G is a group and a is an element in G, $|a|\|G|$.

Proof. Let $H\subseteq G$ be the subgroup $\langle a\rangle$. Then by Lagrange's theorem, $|H|=|\langle a\rangle|$ divides $|G|.\square$

Theorem 4.1.5 [1] (Euler's Theorem**)** If a and n are relatively prime, $a^{\phi(n)}\equiv 1 \pmod n$.

Proof. Since the system $(U_n,*_n)$ is a group and since $|U_n|$ is the number of elements in U_n, then by Lagrange's theorem $[a]^{|U_n|}=[1]$ for all $[a]\in U_n\Rightarrow a^{\phi(n)}\equiv 1 \pmod n.\square$

Example 4.1.6 1) If $n=8\Rightarrow U_8=\{[1],[3],[5],[7]\}\Rightarrow|U_8|=\phi(8)=4$.

Then: $(1)^4=1$, $(3)^4=81\equiv 1 \pmod 8$, $(5)^4=625\equiv 1 \pmod 8$, $(7)^4=2401\equiv 1 \pmod 8$.

2) If $n=9\ \Rightarrow\ \mathrm{U}_9=\{[1],[2],[4],[5],[7],[8]\}\ \Rightarrow|U_9|=\phi(9)=6.$

Then: $(1)^6=1$, $(2)^6=64\equiv 1 \bmod 9$, $(4)^6=4096\equiv 1 \bmod 9$, $(5)^6=15625\equiv 1 \bmod 9$, $(7)^6=117649\equiv 1 \bmod 9$, $(8)^6=262144\equiv 1 \bmod 9.$

Lemma 4.1.7 If a is a prime number, then $a^{n-1}\equiv 1 \pmod n$ for all $[a]\in U_n$.

Example 4.1.8 1) If $n=5\Rightarrow U_5=\{[1],[2],[3],[4]\}$.

Then: $(1)^4=1$, $(2)^4=16\equiv 1 \pmod 5$, $(3)^4=81\equiv 1 \pmod 5$, $(4)^4=256\equiv 1 \pmod 5$.

2) If $n=7\ \Rightarrow \mathrm{U}_7=\{[1],[2],[3],[4],[5],[6]\}.$

Then: $(1)^6 = 1,\ (2)^6 = 64 \equiv 1 \bmod 7,\ (3)^6 = 729 \equiv 1 \bmod 7,\ (4)^6 = 4096 \equiv 1 \bmod 7,$

$(5)^6 = 15625 \equiv 1 \bmod 7,\ (6)^6 = 46656 \equiv 1 \bmod 7.$

Corollary 4.1.9 [1]

Let p be a prime then:

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

for every integer *a*.

Example 4.1.10 1) If $n = 5$ then, $3^5 = 243 \equiv 3 \mod 5,\ 4^5 = 1024 \equiv 4 \mod 5,$

$6^5 = 7776 \equiv 6 \bmod 5.$

2) If $n = 7,$ then, $3^7 = 2187 \equiv 3 \bmod 7,\ 4^7 = 16384 \equiv 4 \bmod 7,\ 5^7 = 78125 \equiv 5 \bmod 7.$

Corollary 4.1.11 $\phi(n)$ is an even number for all $n \geq 3$.

Proof. The element $n-1$ in U_n always has order 2; so by Lagrange's theorem, $2 \mid |U_n|$ which implies that $2 \mid \phi(n)$. □

Theorem 4.1.12 [7] If $n = p^e$ where p is prime, then:

$$\phi(n) = \phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = n\left(1 - \frac{1}{p}\right).$$

Proof. $\phi(n)$ is the number of elements in $\mathbf{Z}_n$, that are relatively prime to $n = p^e$, or in other words, the number of elements that are not multiples of p. This set contains p^e elements where $p^e / p = p^{e-1}$ of them are in the form kp, so $\phi(p^e) = p^e - p^{e-1}$. □

Example 4.1.13 1) If $n = 25 = 5^2 \Rightarrow \phi(5^2) = 5^2 - 5^1 = 25 - 5 = 20$.

2) If $n = 27 = 3^2 \Rightarrow \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$.

Lemma 4.1.14 Let the set M be a complete set of residues mod n and let a and b be

two integers, where a and n are relatively prime. Then the new set:

$$Ma+b=\{ma+b: m\in M\}$$

is again a complete set of residues mod n.

Proof. $ma+b\equiv m'a+b \pmod{n} \Rightarrow ma\equiv m'a \pmod{n} \Rightarrow m\equiv m' \pmod{n} \Rightarrow m=m'.$

Since every element $(Ma+b)$ corresponds to a different congruency class in M, the set $(Ma+b)$ is again a complete set of residues mod n.□

Theorem 4.1.15 The Euler function is multiplicative. That is to say; for relatively prime numbers a and b:

$$\phi(ab)=\phi(a)\phi(b).$$

Proof. Assume that $R=ab$ where a,b are coprime .Then by the Chinese remainder theorem:

$$\gcd(n,R)=1 \Leftrightarrow \gcd(n,a)=1 \text{ and } \gcd(n,b)=1.$$

Or if:

$$A=\{t: t\equiv 1 \pmod{R}\}.$$

$$B=\{t: t\equiv 1 \pmod{a} \text{ and } t\equiv 1 \pmod{b}\}$$

Now, for any $k\in Z_+$, $k\le R$ and relatively prime with $R \Rightarrow K=\phi(R)$. But also for any pair (c,d) where $c\le a$ and relatively prime with $a \Rightarrow c=\phi(a)$, $d\le b$ and relatively prime with $b \Rightarrow d=\phi(b)$. Thus, $\phi(R)=\phi(ab)=\phi(a)\phi(b)$. □

Example 4.1.16 1) If $n=35 \Rightarrow \phi(35)=\phi(7\cdot 5)=\phi(7)\phi(5)=6\cdot 4=24.$

2) If $n=55 \Rightarrow \phi(55)=\phi(11\cdot 5)=\phi(11)\phi(5)=10\cdot 4=40.$

Corollary 4.1.17 If $n=p_1^{X_1}p_2^{X_2}...p_m^{X_m}$ where $p_1, p_2, ..., p_m$ are all primes, then:

$$\phi(n)=\prod_{j=1}^{m}(p_j^{X_j}-p_j^{X_j-1})=\prod_{j=1}^{m}p_j^{X_j}\left(1-\frac{1}{p_j}\right)=n\prod_{j=1}^{m}\left(1-\frac{1}{p_j}\right)$$

Proof. We will prove this corollary by induction, when $m=1\Rightarrow n=p^x\Rightarrow$ by a previous theorem:

$$\phi(n)=p^x-p^{x-1}=p^x\left(1-\frac{1}{p}\right)=n\left(1-\frac{1}{p}\right)$$

Now assume that the statement is true for $m-1$ and try to prove it for m .Since $n=p_1^{X_1}p_2^{X_2}...p_m^{X_m}$ and since $\phi(n)$ is multiplicative, then $\phi(n)=\phi(p_1^{x_1}...p_{m-1}^{x_{m-1}})\phi(p_m^{x_m})$

Since:

$$\phi(p_1^{x_1}...p_{m-1}^{x_{m-1}})=\prod_{j=1}^{m-1}(p_j^{X_j}-p_j^{X_j-1})\ \text{(By induction)}$$

$$\phi(p_m^{x_m})=p_m^{x_m}-p_m^{x_m-1}\ \text{(By a previous theorem)}$$

Therefore:

$$\phi(n)=\phi(p_1^{X_1}p_2^{X_2}.....p_m^{X_m})=\prod_{j=1}^{m}(p_j^{X_j}-p_j^{X_j-1})=\prod_{j=1}^{m}p_j^{X_j}(1-\frac{1}{p_j})=n\prod_{j=1}^{m}(1-\frac{1}{p_j})\ .\ \square$$

Example 4.1.18

1**)** If $n=66\Rightarrow$ then: $\phi(66)=\phi(2\cdot3\cdot11)=66\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)=66\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{10}{11}\right)=20.$

2) If $n=70\Rightarrow\phi(70)=\phi(2\cdot5\cdot7)=70\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)=70\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)=24.$

Theorem 4.1.19 The sum of the Euler functions over all positive divisors d of n is equal to the number n where $n=1,2,.....$, that is to say

$$\sum_{d|n}\phi(d)=n$$

Proof. Let $A=\{1,2,....,n\}$,and let $A_d=\{x\in A:\gcd(x,n)=\frac{n}{d}\}$ for every $(d|n)$, since

$x\in Z$ **t**hen:

$\gcd\ (x,n)=\frac{n}{d}$ for some unique $d|n$. Then $|A_{d1}|\bigcup|A_{d2}|\bigcup.....\bigcup|A_{dd}|=\sum_{d|n}|A_d|=|A|=n$.

So**,** we must prove that $|A_d|=\phi(d)$. $x\in Z\ \Leftrightarrow x\in A_d\Rightarrow 1\le x\le n,\ \gcd(x,n)=\frac{n}{d}$. Now

let $b=\frac{xd}{n}\ \forall\ x\in Z$, then $x=\frac{nb}{d}$ where $b\in Z$ with $1\le b\le d$, $\gcd(b,d)=1$. Therefore:

$$|A_d|=\phi(d)\Rightarrow\sum_{(d/n)}\phi(d)=n.\ \square$$

Example 4.1.20 If $n=8\Rightarrow(d\setminus 8)=1,2,4,8$. $\phi(1)=1,\phi(2)=1,\phi(4)=2,\phi(8)=4$.

$$\Rightarrow 1+1+2+4=8=n.$$

4.2 Applications of Euler's Theorem

We can use Euler's theorem $(a^{\phi(n)}\equiv 1 \bmod n)$ to compute simple congruences $(\bmod n)$.

Example 4.2.1 Find the least non-negative residue of 9^{1346} mod 70.

Solution:

Since 9 is relatively prime with 70, by Euler's theorem $9^{\phi(70)}\equiv 1$ mod 70**,** and since

$70=2\cdot 5\cdot 7\Rightarrow\phi(70)=\phi(2\cdot 5\cdot 7)=70(1-\frac{1}{2})(1-\frac{1}{5})(1-\frac{1}{7})=24.$

Then $9^{24}\equiv 1 \bmod 70$. Also since $1346=24\cdot 56+2$

$\Rightarrow 9^{(1346)}\equiv 9^{(24.56)}\cdot 9^2 \bmod 70\equiv 9^2 \bmod 70$.

Now, $9^2=81\equiv 11 \bmod 70$, then the least non-negative residue of 9^{1346} mod 70 is 11.

4.3 Number Theory Techniques

Now we shall talk about some codes that are based on number theory:

4.3.1 Caesar cipher, Caesar cipher uses the algorithm:

$$y = x + k \pmod{N}$$

where k is any integer. For decoding, we use:

$$x = y - k \pmod{N}.$$

Example 4.3.1.1 If $k = 3$:

x	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
y	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

For example; for $k = 3$, the plaintext message (Cyprus) becomes (FBSUXV).

Remark 4.3.1.2 This type of cryptographic technique is easy to decode because in English alphabet, there are only 25 possible keys.

4.3.2 Affine cipher

The Affine cipher is another type of cryptographic technique that uses the transformation

$$y \equiv ax + b \pmod{N}$$

Here, a and b are two different integers where a is a unit $(\text{mod } N)$. For decoding we use the transformation:

$$x \equiv a^{-1}y + b' \pmod{N}$$

where a^{-1} is the inverse of a, and $b' = -a^{-1}b$.

Example 4.3.2.1 Try to encode the message (GAUSS**)** by using the transformation $y \equiv 3x + 4 \pmod{26}$ and the numerical values $A = 0$, ..., $Z = 25$.

Solution. $G \to 3 \cdot 6 + 4 = 22 \to W$

$A \to 3 \cdot 0 + 4 = 4 \to E$

$U \to 3 \cdot 20 + 4 = 64 \equiv 12 \pmod{26} \to M$

$S \to 3 \cdot 18 + 4 = 58 \equiv 6 \pmod{26} \to G$

$S \to 3 \cdot 18 + 4 = 58 \equiv 6 \pmod{26} \to G$, Then (GAUSS) $\to$(WEMGG).

Example 4.3.2.2 Try to decode (WEMGG**)** by using the transformation

$$x \equiv a^{-1} y + b' \bmod 26$$

Solution.

Here, since $a = 3$ then $a^{-1} = 9$ because $3 \cdot 9 = 27 \equiv 1 \bmod 26$, and $b' = -36 \equiv 16 \bmod N$

The decoding transformation is $x \equiv 9y + 16 \pmod{26}$

$W \to 9 \times 22 + 16 = 214 \equiv 6 \pmod{26} \to G$

$E \to 9 \times 4 + 16 = 52 \equiv 0 \pmod{26} \to A$

$M \to 9 \times 12 + 16 = 124 \equiv 20 \pmod{26} \to U$

$G \to 9 \times 6 + 16 = 70 \equiv 18 \pmod{26} \to S$

$G \to 9 \times 6 + 16 = 70 \equiv 18 \pmod{26} \to S \Rightarrow$ (WEMGG) $\to$(*GAUSS* **)**

4.3.3 An Exponential Method

In this method we choose p to be a large prime number and e to be any integer where $\gcd(e, p - 1) = 1$. Now for the encode transformation

$$x \to x^e \pmod{p}$$

Where $0 < x < p \Rightarrow x$ is relatively prime to $p \Rightarrow x^{(p-1)} \equiv 1 \pmod{p}$ {Fermat's Little Theorem}.

For the decoding transformation, we should find h where $eh \equiv 1 \pmod{p-1}$

$\Rightarrow eh = (p-1)k + 1$ for some integer k. Then:

$$x \to y^h = (x^e)^h = x^{(p-1)k+1} = (x^{p-1})^k x \equiv x \pmod{p}$$

Example 4.3.3.1 Try to encode the message (EULER**)** by using the previous method, if $p = 31$, $e = 7$ and the numerical values $A = 0$, ..., $Z = 25$ as follows.

Since $\gcd(7, 30) = 1$, the encoding transformation is $y \equiv x^7 \pmod{31}$.

$$E \to (4)^7 = 16384 \equiv 16 \pmod{31} \to \mathrm{Q}$$

$$U \to (20)^7 = 1280000000 \equiv 18 \bmod 31 \to S$$

$$L \to (11)^7 = 19487171 \equiv 13 \bmod 31 \to N$$

$$E \to (4)^7 = 16384 \equiv 16 \bmod 31 \to \mathrm{Q}$$

$$R \to (17)^7 = 410338673 \equiv 12 \bmod 31 \to M$$

Then the word (EULER) transforms into the word (QSNQM).

Example 4.3.3.2 Try to decode (QSNQM) by using the inverse of the previous transformation.

Solution. Here, since $e = 7 \Rightarrow h = 13$ because $7 \times 13 = 91 \equiv 1 \pmod{30}$.

Then, the decoding transformation is $x \to y^{13} \pmod{31}$:

$$\mathrm{Q} \to (16)^{13} = (4^7)^{13} = 4^{91} = 4^{30 \cdot 3 + 1} = 4^{30 \cdot 3} 4 \equiv 4 \pmod{31} \to E$$

$$\mathrm{S} \to (18)^{13} = (20^7)^{13} = 20^{91} = 20^{30 \cdot 3 + 1} = 20^{30 \cdot 3} 20 \equiv 20 \pmod{31} \to U$$

$$\mathrm{N} \to (13)^{13} = (11^{7})^{13} = 11^{91} = 11^{30\cdot 3+1} = 11^{30\cdot 3}11 \equiv 11 \pmod{31} \to L$$

$$\mathrm{Q} \to (16)^{13} = (4^{7})^{13} = 4^{91} = 4^{30\cdot 3+1} = 4^{30\cdot 3}4 \equiv 4 \pmod{31} \to E$$

$$\mathrm{M} \to (12)^{13} = (17^{7})^{13} = 17^{91} = 17^{30\cdot 3+1} = 17^{30\cdot 3}17 \equiv 17 \pmod{31} \to R$$

Then $(\mathrm{QSNQM}) \Rightarrow (\mathrm{EULER})$.

4.3.4 Public Key cryptographic technique

This method depends on using two keys; referred to as the public key and the private key instead of one key used in other cryptographic techniques. Also it depends on using a one- way function $y = f(x)$ where the calculation of the function f is easy, but the calculation of the inverse function (f^{-1}) is infeasible.

4.3.4.1 The general algorithm of public key cryptography technique We use Euler's theorem to make this method more interesting. Choose two prime numbers $p,\ q$ then;

$$n = pq \ \Rightarrow\ \phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$$

Now, select a number e coprime to $\phi(n)$. The algorithm becomes:

$$C \equiv M^{e} \bmod n$$

$$M \equiv C^{d} \bmod n$$

Where:

$$ed \equiv 1 \bmod \phi(n) \Rightarrow \phi(n) \mid ed-1 \ \Rightarrow \phi(n)k+1 = ed.$$

$$M \to C^{d} = (M^{e})^{d} = M^{\phi(n)k+1} = M^{\phi(n)k}\ M = M \bmod n$$

(Euler's Theorem, where M is coprime to n).

This algorithm is called the RSA algorithm and it was developed in 1977 by Rivest, Shamir and Adleman. It is one of the oldest and most current public key cryptosystems [8].

Example 4.3.4.2 If $p = 7,\ q = 11 \Rightarrow n = pq = 77$

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) = 6 \times 10 = 60$$

Now, we select e as the smallest number satisfying $\gcd(e, 60) = 1 \Rightarrow e = 7$

$ed \equiv 1 \bmod 60 \Rightarrow d = e^{-1} \Rightarrow d = 43$ because $7 \times 43 = 301 \equiv 1 \bmod 60.$

For the message (NO):

$$M_1 = 13 \Rightarrow C_1 = M_1^e \equiv 13^7 \bmod 77 = 62 \equiv 10 \bmod 26 \Rightarrow K$$

$$M_2 = 14 \Rightarrow C_2 = M_2^e \equiv 14^7 \bmod 77 = 42 \equiv 16 \bmod 26 \Rightarrow \text{Q}$$

Now, for the decryption process:

$$C_1 = 62 \Rightarrow M_1 = C_1^d \bmod 77 = 62^{43} \bmod 77 \equiv 13 \Rightarrow \text{N}$$

$$C_2 = 42 \Rightarrow M_2 = C_2^d \bmod 77 = 42^{43} \bmod 77 \equiv 14 \Rightarrow \text{O}$$

Remark 4.3.4.3 In Public key cryptographic technique we can keep the integrity of any important message by using the signature. In the case that the sender can decode any message by using his public key and encode the result by using the receiver's public key and send it. The receiver should decode the ciphertext message by using his public key then encode the result by using the sender's public key. Here the receiver will be sure this message came from this sender and nobody else.

Chapter 5

MORE ADVANCED CRYPTOGRAPHIC TECHNIQUES

In this chapter, we'll study some other types of encryption, which are more complex than the ones discussed in previous chapters. These are Monoalphabetic ciphers, digraph transformations and the affine matrix transformations by using the digraph transformation method**.**

5.1 Monoalphabetic Cipher

This method depends on using the frequency analysis in a way that, we can easily obtain the original message from the quite long ciphertext message. The main idea here is to get the relative frequency of each letter in the ciphertext message by using the formula:

$$A = \frac{\text{the number of the letters in ciphertext}}{\text{the number of occurrences of a letter in ciphertext}} \times 100$$

Then by comparing the relative frequency of the letters in the ciphertext, with their standard frequency in the English alphabet, we can guess the original letter.

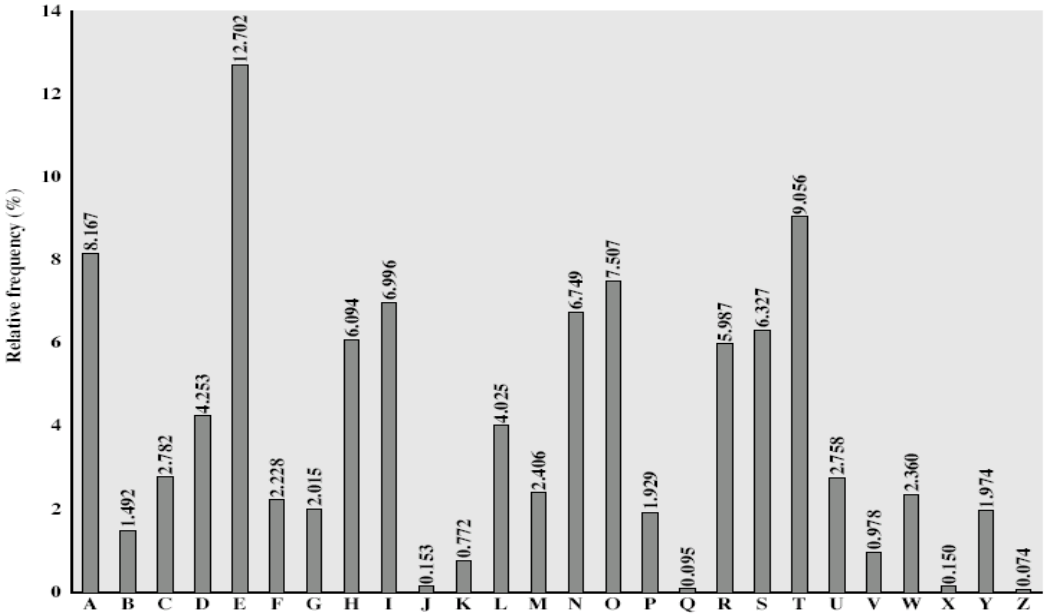

Fig 5.1: Frequency of Letters in English Alphabet [10].

As an example, if the most common letter in the ciphertext is P, then this letter should be E in the original message and so on.

Remark 5.1.1 The Monoalphabetic method is much easier than other types of cryptographic techniques and it is very useful for us to break the ciphertext that is encrypted by using the Caesar cipher and the Affine cipher.

i) The Caesar cipher: In this method, the algorithm used is:

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

where P is the numerical value of the plaintext letter, and K is the key used to encode the original message. Now by using the Monoalphabetic cipher we can find the most common letter in the ciphertext message, and this letter will correspond to the letter E in English alphabet. Hence, we can get the key of the previous algorithm. For example, if the most frequently occurring letter in a ciphertext message encrypted by using Caesar

cipher is M, then this letter corresponds to the letter E in the original message, hence by using the numerical value of these letters, we can find the key K: $M = 12$, $E = 4 \Rightarrow M = E + K \pmod{26} \Rightarrow 12 = 4 + K \pmod{26} \Rightarrow K = 8 \pmod{26}$.

ii) The Affine cipher: The algorithm used in this method is:

$$C \equiv a\,P + b \pmod{N}$$

$$P \equiv a^{-1}C - a^{-1}b = a^{-1}C + b' \pmod{N}$$

where P is the numerical value of the plaintext letter, a and b are the keys used to encode the original message, a^{-1} is the multiplicative inverse of the element a and $b' = -a^{-1}b$. Again, by using the Monoalphabetic cipher we can discover the first and second most common letters in the ciphertext message, and these letters will agree with the letters E and T in English alphabet. Now, by solving these two congruencies:

$$P_1 \equiv a^{-1}C_1 + b' \pmod{N}$$

$$P_2 \equiv a^{-1}C_2 + b' \pmod{N}$$

we can get the keys of the previous algorithm. For example, if we have the part (QAOOYQQEVHEQV) from the cipher text message and if the first most frequently occurring letter in a cipher text message encrypted by using the Affine cipher is Y, and the second most frequently occurring letter is V, then these letters correspond to the letters E and T in the original message. Finally, by using the numerical value of these letters, we can find the keys: $Y = 24$, $E = 4$, $V = 21$, $T = 19$.

$$24a^{-1} + b' \equiv 4 \pmod{26}$$

$$21a^{-1} + b' \equiv 19 \pmod{26}$$

$$3a^{-1} \equiv -15 \pmod{26} \Rightarrow a^{-1} = -5 \equiv 21 \pmod{26} \Rightarrow a = 5.$$

$$b' \equiv 4 - 24a^{-1} \pmod{26} = -500 \equiv 20 \pmod{26} \Rightarrow b = 4$$

Now we can decode the following parts:

$$Q \rightarrow 16(21) + 20 = 356 \equiv 18 \pmod{26} \rightarrow S$$

$$A \rightarrow 0(21) + 20 = 20 \pmod{26} \rightarrow \mathrm{U}$$

$$O \rightarrow 14(21) + 20 = 314 \equiv 2 \pmod{26} \rightarrow C$$

$$E \rightarrow 4(21) + 20 = 104 \equiv 0 \pmod{26} \rightarrow A$$

$$H \rightarrow 7(21) + 20 = 167 \equiv 11 \pmod{26} \rightarrow L$$

Therefore (QAOOYQQEVHEQV) becomes (SUCCESS AT LAST).

5.2 Digraph Transformations

This method depends on putting the letters of the plaintext message in pairs (x, y), and then using the algorithm:

$$C \equiv a\ P + b \pmod{N^2}$$

where:

$$P = x\ N + y$$

Here x is the numerical value of the first letter and y is the numerical value of the second letter in P. N is the number of the letters in the alphabet, a is relatively prime with N^2, and b is a random number. For the decryption process, the algorithm is:

$$P \equiv a'C + b' \pmod{N^2}$$

where:

$$C = x'\ N + y',\ a' = a^{-1} \pmod{N^2},\ b' = -a^{-1}b \pmod{N^2}.$$

Example 5.2.1 Find the ciphertext for plaintext BE, by using the digraph transformation, where $a = 79,\ b = 50.$

Solution:

If P is (BE), then $P = 1 \times 26 + 4 = 30$. Then, if $a = 79,\ b = 50$

$C \equiv 79\ (30) + 50\ (\text{mod}\, 676) \equiv 2420 \equiv 392\ (\text{mod}\, 676) \Rightarrow 392 = 15 \times 26 + 2 \Rightarrow (PC)$.

Example 5.2.2 We encode the message (HELP ME PLEASE), by using the digraph transformation cryptographic technique where $a = 451$, $b = 60$.

Solution:

The algorithm here is:

$$C \equiv a\ P + b\ (\text{mod}\, N^2)$$

where

$$P = x\ N + y,\ \ N = 26$$

Now

$$P_1(HE) \Rightarrow 7 \times 26 + 4 = 186$$

$$P_2(LP) \Rightarrow 11 \times 26 + 15 = 301$$

$$P_3(ME) \Rightarrow 12 \times 26 + 4 = 316$$

$$P_4(PL) \Rightarrow 15 \times 26 + 11 = 401$$

$$P_5(EA) \Rightarrow 4 \times 26 + 0 = 104$$

$$P_6(\text{SE}) \Rightarrow 18 \times 26 + 4 = 472$$

Then

$$C_1 = 451 \times 186 + 60 = 83946 \equiv 122 \,\text{mod}\, 676 \Rightarrow 122 = 4 \times 26 + 18 \Rightarrow C_1(\text{ES})$$

$$C_2 = 451 \times 301 + 60 = 135811 \equiv 611 \,\text{mod}\, 676 \Rightarrow 611 = 23 \times 26 + 13 \Rightarrow C_2(\text{XN})$$

$$C_3 = 451 \times 316 + 60 = 142576 \equiv 616 \,\text{mod}\, 676 \Rightarrow 616 = 23 \times 26 + 18 \Rightarrow C_3(\text{XS})$$

$$C_4 = 451\times 401+60 = 180911 \equiv 419 \bmod 676 \Rightarrow 419 = 16\times 26+3 \Rightarrow C_4(\text{QD})$$

$$C_5 = 451\times 104+60 = 46964 \equiv 302 \bmod 676 \Rightarrow 302 = 11\times 26+16 \Rightarrow C_5(\text{LQ})$$

$$C_6 = 451\times 472+60 = 212932 \equiv 668 \bmod 676 \Rightarrow 668 = 425\times 26+18 \Rightarrow C_6(\text{ZS})$$

Therefore, the original message becomes (ESXNXSQDLQZS).Now, for decryption, we use the algorithm:

$$P = a^{-1}C - a^{-1}\text{b} \pmod{N^2}$$

Since

$$a = 451 \;\Rightarrow\; a^{-1} = 3 \text{ because } (3\times 451) = 1353 \equiv 1 \text{ mod } 676$$

Also

$$a^{-1}b = 3\times 60 = 180$$

$$P_1 = 3\times 122 - 180 = 186 \bmod 676$$

$$P_2 = 3\times 611 - 180 = 1653 \equiv 301 \bmod 676$$

$$P_3 = 3\times 616 - 180 = 1658 \equiv 316 \bmod 676$$

$$P_4 = 3\times 419 - 180 = 1077 \equiv 401 \bmod 676$$

$$P_5 = 3\times 320 - 180 = 780 \equiv 104 \bmod 676$$

$$P_6 = 3\times 668 - 180 = 1824 \equiv 472 \bmod 676$$

Finally:

$$P_1 = 186 = 7\times 26+4 \Rightarrow (HE)$$

$$P_2 = 301 = 11\times 26+15 \Rightarrow (LP)$$

$$P_3 = 316 = 12\times 26+4 \Rightarrow (ME)$$

$$P_4 = 401 = 15\times 26+11 \Rightarrow (PL)$$

$$P_5 = 104 = 4 \times 26 + 0 \Rightarrow (EA)$$

$$P_6 = 472 = 18 \times 26 + 4 \Rightarrow (SE)$$

So, we get the original message (HELP ME PLEASE).

Remark 5.2.3 If the message has numbers, we can modify the alphabet so that it is suitable for this kind of message. For example; if we have the message (GIVE ME 1530\$), the letters $A-Z$ take the numerical values $0-25$, numbers $0-9$ take the values $26-35$ and finally \$ sign takes the value 36. Here, we can use the same process with mod 37 and now to encode the previous message by using the Caesar cipher with $K = 15$, the algorithm is:

$$C \equiv P + 15 \mod 37$$

$G = 6 \Rightarrow C_1 = 6 + 15 \bmod 37 = 21 \Rightarrow \text{V}$, $I = 8 \Rightarrow C_2 = 8 + 15 \bmod 37 = 23 \Rightarrow \text{X}$

$v = 21 \Rightarrow C_3 = 21 + 15 \bmod 37 = 36 \Rightarrow \$$, $E = 4 \Rightarrow C_4 = 4 + 15 \bmod 37 = 19 \Rightarrow \text{T}$

$M = 12 \Rightarrow C_5 = 12 + 15 \bmod 37 = 27 \Rightarrow 1$, $1 = 27 \Rightarrow C_6 = 6 + 15 \bmod 37 = 5 \Rightarrow \text{F}$

$5 = 31 \Rightarrow C_7 = 31 + 15 \bmod 37 = 9 \Rightarrow \text{J}$, $3 = 29 \Rightarrow C_8 = 29 + 15 \bmod 37 = 7 \Rightarrow \text{H}$

$0 = 26 \Rightarrow C_9 = 26 + 15 \bmod 37 = 4 \Rightarrow \text{E}$, $\$ = 36 \Rightarrow C_{10} = 36 + 15 \bmod 37 = 14 \Rightarrow \text{O}$

Then the original message becomes $(\text{VX\$T1FJHEO})$, therefore we can use this method in all types of cryptographic techniques.

5.3 The Affine Matrix Transformations by Using the Digraph Transformation Method

We can use the digraph transformation method in the affine matrix transformations. Here the algorithm is:

$$C \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} P + \begin{pmatrix} e \\ f \end{pmatrix} \bmod N^2$$

$$\Rightarrow C \equiv A\,P + B \bmod N^2 .$$

where: $0 \le a,b,c,d \le N^2$, $ad - bc$ is must be unit mod N^2, P is a column vector of two plaintext digraphs $p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ $P_i = x_i N + y_i$, x is the numerical value of the first letter in P, y is the numerical value of the second letter in P, and N is the number of the letters in the alphabet.

Remark 5.3.1 The most important condition here is that, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ must be invertible mod N^2. That it has no common factor with N for the decryption process. The decryption algorithm is:

$$P \equiv A^{-1}C - A^{-1}B \equiv A^{-1}(C - B) \bmod N^2$$

Example 5.3.2 If we have $P_1(\mathrm{NO})$, $\mathrm{P}_2(BE)$, $A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 100 \\ 53 \end{pmatrix}$ then we can endode them as follows: $P_1(\mathrm{NO}) = 13 \times 26 + 14 = 352,\ P_2(BE) = 1 \times 26 + 4 = 30,\ N = 26 \Rightarrow N^2 = 676$

$$C \equiv \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 352 \\ 30 \end{pmatrix} + \begin{pmatrix} 100 \\ 53 \end{pmatrix} = \begin{pmatrix} 1941 \\ 794 \end{pmatrix} + \begin{pmatrix} 100 \\ 53 \end{pmatrix} = \begin{pmatrix} 2040 \\ 847 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 171 \end{pmatrix} \bmod 676$$

$$\Rightarrow C_1 = 12 = 0 \times 26 + 12 \Rightarrow AM.$$

$$C_2 = 171 = 6 \times 26 + 15 \Rightarrow GP$$

Now, for the decryption:

$$P = A^{-1}C - A^{-1}B \equiv A^{-1}(C - B) \bmod 676$$

Since $A^{-1} = \dfrac{1}{\det A}\begin{pmatrix} 3 & -6 \\ -2 & 5 \end{pmatrix} \bmod 676$, $\det A = 3 \Rightarrow \dfrac{1}{\det A} = \dfrac{1}{3} = 3^{-1} \Rightarrow 3^{-1} = 451 \bmod 676$

$$\Rightarrow A^{-1} = 451\begin{pmatrix} 3 & -6 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} 1353 & -2706 \\ -902 & 2255 \end{pmatrix} \equiv \begin{pmatrix} 1 & 674 \\ 450 & 227 \end{pmatrix} \bmod 676$$

Now:

$$P \equiv \begin{pmatrix} 1 & 674 \\ 450 & 227 \end{pmatrix}\left[\begin{pmatrix} 12 \\ 171 \end{pmatrix} - \begin{pmatrix} 100 \\ 53 \end{pmatrix}\right] \equiv \begin{pmatrix} 1 & 674 \\ 450 & 227 \end{pmatrix}\begin{pmatrix} -8 \\ 118 \end{pmatrix} = \begin{pmatrix} 79444 \\ -12814 \end{pmatrix} \equiv \begin{pmatrix} 352 \\ 30 \end{pmatrix} \bmod 676$$

$\Rightarrow P_1 = 352 = 13 \times 26 + 14 \Rightarrow (NO)$, $P_2 = 30 = 1 \times 26 + 4 \Rightarrow (BE)$.

Remark 5.3.3 We can use a (3×3) matrix in the previous method, again by setting

$P = xN + y$

Example 5.3.4 We try to encode the message (HELP ME PLEASE) by using the digraph transformation with

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix}$$

Solution. Here, since

$$P_1(HE) \Rightarrow 7 \times 26 + 4 = 186$$

$$P_2(LP) \Rightarrow 11 \times 26 + 15 = 301$$

$$P_3(ME) \Rightarrow 12 \times 26 + 4 = 316$$

$$P_4(PL) \Rightarrow 15 \times 26 + 11 = 401$$

$$P_5(EA) \Rightarrow 4 \times 26 + 0 = 104$$

$$P_6(SE) \Rightarrow 18 \times 26 + 4 = 472$$

We use the algorithm $C \equiv AP + B \bmod N^2$, $P = \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$, $N = 26$, then:

$$C_i \equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 186 \\ 301 \\ 316 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} \bmod 676$$

$$\equiv \begin{pmatrix} 732 \\ 617 \\ 316 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} = \begin{pmatrix} 894 \\ 836 \\ 639 \end{pmatrix} \equiv \begin{pmatrix} 218 \\ 160 \\ 639 \end{pmatrix} \bmod 676$$

$$C_{ii} \equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 401 \\ 104 \\ 472 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} \bmod 676$$

$$\equiv \begin{pmatrix} 279 \\ 576 \\ 472 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} = \begin{pmatrix} 441 \\ 795 \\ 795 \end{pmatrix} \equiv \begin{pmatrix} 441 \\ 119 \\ 119 \end{pmatrix} \bmod 676$$, Therefore:

$218 = 8 \times 26 + 10 \Rightarrow C_1(\text{IK})$

$160 = 6 \times 26 + 4 \Rightarrow C_2(\text{GE})$

$639 = 24 \times 26 + 15 \Rightarrow C_3(\text{YP})$

$441 = 16 \times 26 + 25 \Rightarrow C_4(\text{QZ})$

$119 = 4 \times 26 + 15 \Rightarrow C_6(\text{EP})$

$119 = 4 \times 26 + 15 \Rightarrow C_6(\text{EP})$, Finally, the ciphertext message is (IKGEYPGZEPEP).Now, for the decryption we use the inverse of the matrix A, and the algorithm works as below:

$$P \equiv A^{-1}(C - B) \bmod N^2,\ A^{-1} = \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

Then:

$$P_i \equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\left[\begin{pmatrix} 218 \\ 160 \\ 639 \end{pmatrix} - \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix}\right]$$

$$\equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 56 \\ -59 \\ 316 \end{pmatrix} = \begin{pmatrix} -490 \\ -375 \\ 316 \end{pmatrix} \equiv \begin{pmatrix} 186 \\ 301 \\ 316 \end{pmatrix} \mod 676$$

$$P_{ii} \equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \left[\begin{pmatrix} 441 \\ 119 \\ 119 \end{pmatrix} - \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} \right]$$

$$\equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 279 \\ -100 \\ -204 \end{pmatrix} = \begin{pmatrix} -275 \\ 104 \\ -204 \end{pmatrix} \equiv \begin{pmatrix} 401 \\ 104 \\ 472 \end{pmatrix} \mod 676.$$ Therefore:

$186 = 7 \times 26 + 4 \Rightarrow P_1(HE)$

$301 = 11 \times 26 + 15 \Rightarrow P_2(LP)$

$316 = 12 \times 26 + 4 \Rightarrow P_3(ME)$

$401 = 15 \times 26 + 11 \Rightarrow P_4(PL)$

$104 = 4 \times 26 + 0 \Rightarrow P_5(EA)$

$472 = 18 \times 26 + 4 \Rightarrow P_6(SE)$, we can get the original message (HELP ME PLEASE).

Remark 5.3.5 We can use the previous method with (x, y, z) that is with $P = xN^2 + yN + z$, where x, y and z are the numerical values of the letters of P.

Example 5.3.6 Try to encode the message (HELP ME NOW) by using the previous method where:

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix}$$

Solution. Here, we have $P_1(HEL)$, $P_2(PME)$, $P_3(NOW)$.

$\Rightarrow P_1 = 7 \times 26^2 + 4 \times 26 + 11 = 4847$

$P_2 = 15 \times 26^2 + 12 \times 26 + 4 = 10456$

$P_3 = 13\times 26^2 + 14\times 26 + 22 = 9174$, Then, by using the algorithm:

$$C \equiv AP + B \bmod N^3$$

$$C \equiv \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 4847 \\ 10456 \\ 9174 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} = \begin{pmatrix} 25239 \\ 19630 \\ 9174 \end{pmatrix} + \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix} = \begin{pmatrix} 25401 \\ 19849 \\ 9497 \end{pmatrix} \equiv \begin{pmatrix} 7825 \\ 2273 \\ 9497 \end{pmatrix} \bmod 26^3$$

Now:

$7825 \bmod 26^3 = 11\times 26^2 + 14\times 26 + 25 \Rightarrow (\text{LOZ})$.

$2273 \bmod 26^3 = 3\times 26^2 + 9\times 26 + 11 \Rightarrow (\text{DJL})$.

$9497 \bmod 26^3 = 14\times 26^2 + 1\times 26 + 7 \Rightarrow (\text{OAH})$.

Therefore, the message becomes (LOZDJLOAH). Finally, for decryption the algorithm is:

$$P \equiv A^{-1}(C - B) \bmod N^3$$

Then

$$P \equiv \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\left[\begin{pmatrix} 7825 \\ 2273 \\ 9497 \end{pmatrix} - \begin{pmatrix} 162 \\ 219 \\ 323 \end{pmatrix}\right] = \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 7663 \\ 2054 \\ 9174 \end{pmatrix} = \begin{pmatrix} -12729 \\ -7120 \\ 9174 \end{pmatrix} \equiv \begin{pmatrix} 4847 \\ 10456 \\ 9174 \end{pmatrix} \bmod 26^3$$

where $4847 = 7\times 26^2 + 4\times 26 + 11 \Rightarrow (\text{HEL})$

$10456 = 15\times 26^2 + 12\times 26 + 4 \Rightarrow (\text{PME})$

$9174 = 13\times 26^2 + 14\times 26 + 22 \Rightarrow (\text{NOW})$.In this way, we can get the original message (HELP ME NOW).

Remark 5.3.7 We can use this method with a $(n\times n)$ matrix, if we can find the inverse of the matrix used in the encryption algorithm.

$$C \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \bmod N^n$$

For example, if $(x,\mathrm{y},\mathrm{z},\mathrm{h})$ with $P = xN^3 + yN^2 + zN + h$, or if (x, y, z, d) with $P = xN^3 + yN^2 + zN + hN + d$. The previous process will be more difficult and the numbers will be very big but this makes the cryptographic technique more secure and interesting.

Chapter 6

CONCLUSION

From this study, we emerged some points, the most definite one that, the cryptography techniques which use linear algebra are easier than the others which use number theory to implement. But, on the other hand the first type is easy to break and decreases the privacy and the integrity of the information that is encoded. We can improve the security of this technique by using matrices of higher size where we can use computer programs to find inverses of them.

Another point is that, the cryptographic techniques that use number theory are more difficult to calculate and hence are more private. But, also, in this type, it's not easy to determine the inverse of a big prime number modulo n.

Another problem with this type is that, there are many situations where one wants to know if a large number e is a prime.

Finally, there is another type of cryptography technique that uses a one-way function in its coding. There is no known algorithm to decode these and as an example one could use a non-invertible matrix as a key.

REFERENCES

[1] Charles C. Pinter, A Book of Abstract Algebra, Second Edition, QA162.P56, 1990.

[2] I. H. Sheth, Abstract Algebra, 2002.

[3] Joseph. A. Gallian, Contemporary Abstract Algebra, Sixth Edition, 2006.

[4] Howard Anton-Chris Rorres, Elementary Linear Algebra Applications Version, Seven Edition, 1994.

[5] P. B. Bhattacharya-S. K.Jain-S. R. Nagpaul, First Course in Linear Algebra, 1983.

[6] N. S. Gopalakrishnan, University Algebra, Second Edition, June 1998.

[7] Gareth A. Jones and J. Mary Jones, Elementary Number Theory, QA241, J62, 1998.

[8] Neal. Koblitz, A Course in Number Theory and Cryptography, second Edition, 1991.

[9] Lecture Note by Victor, Adamchik, Full 2005.

[10] Lecture Note in Network Data Security by Rza, Bashirov.

[11] Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol.36, June–July 1929, pp. 306–312