CHAPTER I

INTRODUCTION TO CRYPTOGRAPHY

Cryptography is a science in which any message can be written in a disguised form such that only recepient can read the message written by sender foundations of this subject were developed even in 14 12. It is not the such subject took birth recently but rapid developments of this subject were started recently in the second half of 20th century. Mainly, It got a milestone by the appearence of W.Diffie and M.E. Hellman's paper "Newdirections in Crypto graphy" in 1976. With this paper cryptology has gained an enaromous popularity in the academic world for that reasons are mentioned as two folds. Firstly, They proved that it is possible to exchange data over a public channel in a secureway. Secondaly, It is a foundation for coustructing public key crypto systems.

PLAINTEXT :

The message which can be read as soon as we see the message is said to be in plain text.

CIPHER TEXT :

The message which is written in disguised form and can not be read as soon as we see the message is said to be in cipher text.

ENCIPHERING :

Transformation from plain text to cipher text is said to be enciphering. We use some key denoted by K_E to encipher the message.

DECIPHERING :

Transformation from ciphertext to plain text is to be deciphering we use some key denoted by K_D to decipher the message.

CRYPT ANALYSIS :

The analysis to break the cipher text is said to be crypt analysis.

CRYPTO SYSTEM :

The system which is needed to set up enciphering of message is said to be crypto system :

PRIVATE KEY :

The key which is assigned to a person or party and which is to be kept secret from other is said to be private key.

PUBLIC KEY :

The key which is made public is said to be public key.

Actually in this cryptography, we see two types of crypto systems.

1.Classical Cryptosystems

2. Public Key Crypto Systems.

CLASSICAL CRYPTO SYSTEMS :

Firstly to find crypto system of any message, we have to label the all possible plaintext message units and all possible cipher text message units. We suppose as follows

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

M	N	O	P	Q	R	S	T	U	V	W
12	13	14	15	16	17	18	19	20	21	22

X	Y	Z
23	24	25

In some other situations, one might want to label message units using other mathematical objects besides integers. For example, vectors or points on some curve but for the duration of this section, we use only integers. For example we consider a cryptosystem suppose we are using the 26 - letter alphabet A-Z with numerical equivalents between 0-25. Let the letter $P \in \{0, 1, \ldots 25\}$ Stand for a plain text message units. Let $f : P \to C$ be defined by $f(P) = C = P+3 \mod 26$ then encipher the message "YES".

We have

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

ENCIPHERING OF 'Y'

$$C = f(P) = P + 3 \mod 26$$

C = 24 + 3 mod 26, P = 24 Since Y is at 24 th place in plain text

C = 27 mod 26

= 1

= B

Y = B

ENCIPHERING OF Y = B

ENCIPHERING OF E :

C = P +3 mod 26 since E is at 4th place in plain text, P = 4

C = 4 + 3 mod 26

= 7

= H

Enciphering of C = H

ENCIPHERING OF S.

C = P + 3 mod 26

C = 18 + 3 mod 26 since S is at 18 th place in plantext

= 21

= V

enciphering of C = V then completely enciphering of

YES = BHV

Above method can be generalized as follows. suppose, we are using N - letter alphabet with numerical equivalents 0, 1, 2, . . ., N-1. Let b be a fixed integer by a shift transformation, we may define enciphering function f : P $\rightarrow$ C by C = f (P) = P + b mod N.

When we decipher, then we get C $\in$ {0, 1,2, . . . N-1}

and C = P + b => P = C - b mod N.

Example : we suppose we are given a message "ZKB" to decipher the a crypto system where single letter message units are allowed and letters are. 26 with numerical equivalents same as above and as well as enciphering function.

"Z K B"

25 10 1

To decipher Z :

We have P = C -3 mod 26

P = 25 - 3 mod 26

= 22

= W

deciphering of Z = W

To decipher K

We P = C - 3 mod 26

= 10 - 3 mod 26

= 7 mod 26

= H.

enciphering of K = H

To decipher S :

P = C -3 mod 26

= 1 - 3 mod 26

P = -2 mod 26

= -2 + 26 mod 26

= 24 mod 26

P = 24.

= Y.

So we have CIPHERTEXT : ZKB

if P = 24, C = 7.24+12 mod 26 = 24

if P = 12, C = 7. 12 + 12 mod 26 = 18

if P = 4, C = 7.4+12 mod 26 = 25

if P = 14, C = 7.14+12 mod 26 = 6

if P = 22, C = 7.22 + 12 mod 26 = 10

C : 13 14 24 18 14 25 6 10

Cipher text : N M Y S O G K

DIGRAPH TRANSFORMATION :

We now assure that our plaintext and cipher text message units are two letter blocks which are called digraphs. i.e. when we are asked to use digraphs we have to split the entire message into two letter blocks i.e. into digraphs. if there are odd number of letters, add any new letter such that another digraph can be possible and assign numerical equivalent to that letter.

We suppose that we are using only N letters in plaintext, then we can have the numerical equivalents between O to N^2-1. if we want to encipher the plaintext we find $P = Nx + y$ where x is numerical equivalent of first letter in digraph, while y is the numerical equivalent of second letter.

In this system we have a simplest crypto system $C = aP + b \mod N^2$ where a and b are parameters and a is never be a factor of N

$P = 9C + 18 \bmod 26$

Example : We suppose that we are working with 26 letter alphabet and single letter message units. we are given the affine mapping $C = aP+b \bmod N$ where $a = 7$, $b = 12$ and $N = 26$. then encipher the message " PAYME NOW".

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

Plaintext :	P	A	Y	M	E	N	O	W
p :	15	0	24	12	4	13	14	22

$C = 7p + 12 \bmod 25$

if $P = 15$, $c = 7.15 + 12 \bmod 26 = 13$

if $P = 0$, $C = 7.0 + 12 \bmod 26 = 12$

if $P = 24$, $C = 7.24+12 \bmod 26 = 24$

if P = 12, C = 7. 12 + 12 mod 26 = 18

if P = 4, C = 7.4+12 mod 26 = 25

if P = 14, C = 7.14+12 mod 26 = 6

DIGRAPH TRANSFORMATION :

We now assure that our plaintext and cipher text message units are two letter blocks which are called digraphs. i.e. when we are asked to use digraphs we have to split the entire message into two letter blocks i.e. into digraphs. if there are odd number of letters, add any new letter such that another digraph can be possible and assign numerical equivalent to that letter.

We suppose that we are using only N letters in plaintext, then we can have the numerical equivalents between O to N^2-1. if we want to encipher the plaintext we find $P = Nx + y$ where x is numerical equivalent of first letter in digraph, while y is the numerical equivalent of second letter.

In this system we have a simplest crypto system $C = aP + b \bmod N^2$ where a and b are parameters and a is never be a factor of N and as well as of N^2.

We use here modulo N^2 because of we work with N letter alphabet and 2 block Message units, then we can have N^2 distinct message units whose numerical equivalents are less than N^2.

To decipher if we are given cipher text, then we have

$C = aP + b \bmod N^2$

$aP = C - b \bmod N^2$

$a^{-1}(aP) = a^{-1}(C-b) \bmod N^2$

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

$P = a^{1}C + b^{1} \bmod N^2$ where $a^{1} = a^{-1}$ and

$$b^{1} = -a^{-1}b$$

this enciphering transformation is said to be affine transformation.

For an examle, we consider if we are given to use a crypto system with 27 letter alphabet, in which A-Z have numerical equivalents 0 - 25 and blank = 26 each digraph then corresponds to an integer between 0 and $728 = 27^2-1$ according to the rule that, if the two letters in the digraph have numerical equivalents x and y, then the digraph has numerical equivalent Nx+y as explained earlier.

Suppose that a study of a large sample of cipher text reveals that the most frequently occuring digraphs are (in order) "ZA", "IA" and "IW". suppose that the most common digraphs in the english language (for text written in our 27 letter alphabet) are "E" (i.e, "E blank"), "S", "T". you know that the crypto system uses an affine enciphering transformation modulo 729 find the deciphering key and read the message "NDXBHO".

We have

CIPHER TEXT	"ZA"	"IA"	"IW"
C =	27.25+0=675	27.8+0 = 216	27.8+22=238
PLAINTEXT	"E "	"S "	" T"
P =	27+26 = 134	27.18+26=51	27.26+19 = 121

Then substitute above Cand p in

$$P = a^{1}c + b^{1} \bmod 729$$

$$675\ a^{1} + b^{1} = 134 \bmod 729 \qquad (1)$$

$$216\ a^{1} + b^{1} = 512 \bmod 729 \qquad (2)$$

$$238\ a^{1} + b^{1} = 721 \bmod 729 \qquad (3)$$

by subtracting (3) from (1), we get

$675\ a^{1}+b^{1} = 134 \bmod 729$

$238\ a^{1}+b^{1} = 721 \bmod 729$

$437\ a^{1}=142 \bmod 729$

$437^{-1}(437)a^{1} = 437^{-1}.\ 142 \bmod 729$

$a^{1} = 362\text{-}142 \bmod 729$

$a^{1} = 374 \bmod 729$

from (1)

$675\ a^{1}+b^{1} = 134 \bmod 729$

$b^{1} = 134\text{-}675.374 \bmod 729$

$b^{1} = 647 \bmod 729$

then

$P = a^{1}C+b^{1} \bmod 729$

$P = 374\ C + 647 \bmod 729$

Deciphering key $(a^{1}, b^{1}) = (374, 647) \bmod 729$

"ND XB HO"

C = ND = 27.13+3 = 354

P = 374 C + 647 mod 29

= 374.354 + 647 mod 729

= 365 mod 729

= 13.27 + 14mod 29

= NO

ND = NO

C = HO

= 27.7+14 mod 29

= 203

P = 374C+647mod 729

= 374.203+647 mod 729

= 24

= 0.27+24 mod 729

= AY

HO = AY