CLASSICAL ENCRYPTION TECHNIQUES

Cryptography :-

Process of converting plain text to cipher text.
→ enciphering. Reverse process is called - deciphering.
Study of encryption techniques - Cryptography.

Encryption → has secret key + encryption process

- Symmetric
  - ↓
  - both encryption + decryption done using same keys
- Asymmetric
  - ↓
  - Encryption and decryption is done by two different keys.

Attack on encryption

↓ → breaking of code.

→ Cryptanalysis → Reveals properties of encryp. algo.

→ Brute force attack → Trying all possible keys.

Transposition cipher :-

→ Substitutes text into cipher text.

Rotor machines :-

H/w device which performs substitution ciphers.

Stegnography :-

hiding secret message into image.

Conventional Encryption.

Plain text → Encryption algorithm → (Using secret Shared key) → Transmitted cipher text → Decryption algorithm → (Using secret shared key) → plain text

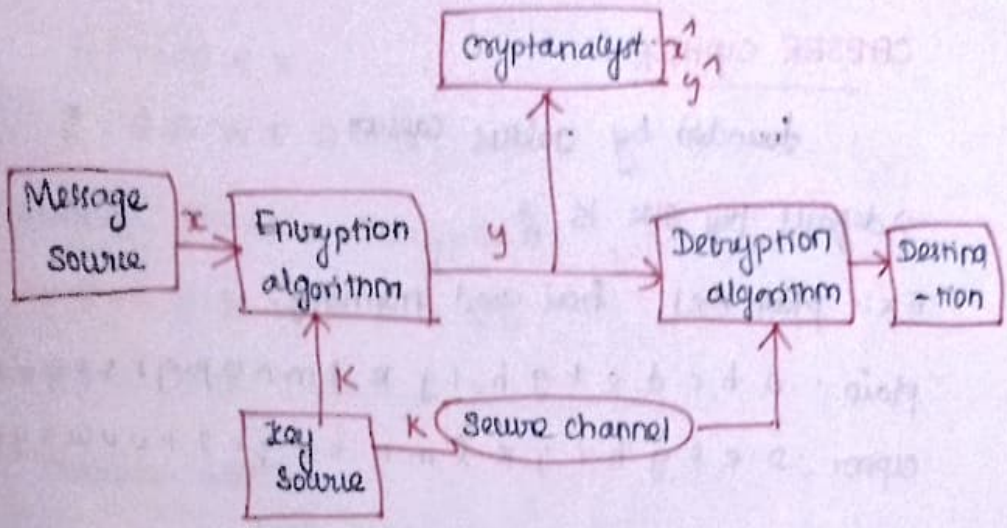


Fig :. Conventional cryptosystem.

3 dimensions of cryptography :.

-> Transforming plain text to cipher text
-> Numbers of keys used
-> way in which plaintext is processed.
↓
Block cipher - one block at a time
Stream cipher - takes i/p element continously

Types of attacks :.

Cryptanalyst
-> cipher text only -> En. algo
-> known plaintext -> one or more plain text, ciphertext pair
-> chosen plaintext -> plaintext by cryptanalyst, secret key
-> chosen ciphertext
↳ ciphertext by cryptanalyst.
-> chosen text
↳ Both encrypted and decrypted text

SUBSTITUTION TECHNIQUES :.

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or by symbols.
↓
Encryption is unconditionally secure when cipher text is strong enough which cannot be predicted.
-> Computation secure. -> when cost of breaking exceeds value & lifetime of cipher text.

CAESER CIPHER:

founded by julius caesar.

→ default key size is 3.

Ex: plain text hai good morning.

plain : 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

cipher : 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

a to z = 0 to 25 number equivalent.

Algorithm:

$C = E(3, p) = (p+3) \bmod 26$ $E = E(p+k) \bmod 26$ $D = c(c-k) \bmod 26$

but it can be any key between 1 to 25.

25 keys are possible for brute force attack.

MONO ALPHABETIC CIPHER

Since there is no security for caeser apher.

Playfair cipher:

Multiple letter encryption.

mono alphabetic example:-

↓

It is a substitution cipher in which for a given key the cipher aphabet for each plain alphabet is fixed

Ex: D is replaced by A means. Its for all ourence in the plain text.

If key = 3, then 3! = 6 combinations are possible

Ex: PT = NETWORK

key = hello how are you.

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

h e l o w a r y u a b c d f g i j k m n p q s t v y z

NETWORK

g · SBWEDGD

Reverse process - Decryption.

CT - SBWEDGD

PT - NETWORK.

Possible attacks

One A is replaced by E, means every occurence is replaced by E.

PLAYFAIR CIPHER:

This is the best known Multiple letter encryption and this treats plaintext as single units and translates the units into ciphertext diagrams.

->Based on 5x5 matrices using keywords.

Rules: Ex: Occurence.

-> No repeating letters eg: ocuren

->Create a table

↳ either left to right or top to bottom

↳ I/J should be in same box

PT- fall treos
keyword: occurence.

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

Prepare message:-

→ Split the PT into plain txt

→ If there is duplication of letters by separating by 'x'.

→ If there is odd number of letters. add 'x' at end.

Tall trees → Ta lx lt re es.

This can be done - same pa
means have to insert 'x'.

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

Ta = DF Rule 3

Lx - IZ

LT - TZ Rule 1

RE - EO Rule wrap round

ES - RT

CT - PFIZTZEORT.

Ad:-

→ It difficult to particular diagram

→ Freq analysis is very difficult.

Disod:-

→ Easy to break

→ Sufficient No of ciphertext is small.

HILL CIPHER:

Developed by mathematician Lester Hill 1929.

Basic mode calculation:-

27 mod 26

$$26 \overline{)27}\ (1$$
$$\underline{26}$$
$$1$$

have to take remainder. 1.

Inverse of mod operation:-

1) $9^{-1} \bmod 26$

$9x? \bmod 26 = 1$ -> have to do get 1 as remainder.

$9 \times 1 \bmod 26 = 9 \bmod 26 = 9$

$9 \times 2 \bmod 26 = 18 \bmod 26 = 18$

$9 \times 3 \bmod 26 = 27 \bmod 26 = 1$

hence $9^{-1} \bmod 26 = 3$.

Similarly $444^{-1} \bmod 26 = 11$

$441 \times 25 \bmod 26 = 1$

hence $441^{-1} \bmod 26 = 25$

Hill cipher:-

Plain Text = HELP

key $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Cipher text $C = Kp \bmod 26$

Split the plain text into two-two letters as 'HE' 'LP'

$P = HE = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$ -> as 7 and 4 are numbers to H and E.

hence $C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 21 & 12 \\ 14 & 20 \end{bmatrix} \bmod 26$ have to odd

$$\begin{bmatrix} 38 \\ 94 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 37 \\ 364 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 7 \\ 8 \end{bmatrix} \Rightarrow \begin{bmatrix} H \\ I \end{bmatrix}$$

Next $P = 2P = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$

$C = KP \bmod 26$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 33 & 45 \\ 22 & 75 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 78 \\ 97 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

Hence Cipher Text: HELP = HIAT

Decryption:-

Plain Text $P = K^{-1}C \bmod 26$

$$K^{-1} = \frac{1}{|K|} \text{adj } K$$

$$|K| = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = 15 - 6 = 9 \qquad \text{adj } K = \begin{bmatrix} 3 & -3 \\ -2 & 3 \end{bmatrix}$$ (change sign)

$$K^{-1} = \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 5(9)^{-1} & (-3)9^{-1} \\ (-2)9^{-1} & (3)9^{-1} \end{bmatrix}$$ we know $9^{-1} \bmod 26 = 3$.

$$\Rightarrow \begin{bmatrix} 5(3) & (-3)(3) \\ (-2)(3) & (3)(3) \end{bmatrix}$$

$$= \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26$$

$-9 \bmod 26$

$\Rightarrow -9+26 = 17$.

$$= 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$$

$-3+26 = 23$

$-2+26 = 24$

$$= 3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$$ additional step

$$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Hence $P = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 105 & 89 \\ 140 & 72 \end{bmatrix}$

$$= \begin{bmatrix} 241 \\ 212 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \Rightarrow \begin{bmatrix} H \\ E \end{bmatrix}$$

Similarly for AT

$$P = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 323 \\ 171 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ P \end{bmatrix}$$

hence HELP.

H/w:

Playfair - keyword monarchy

P.T- Balloon

Caesar cipher - PT- meet me after the toga party

key = 3.

Hill cipher :- "pay more money" - PT

key $\begin{bmatrix} 17 & 7 & 5 \\ 21 & 19 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

Ex: 2 PT. Hillcipher

key = $\begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix}$. HCRZSSXNSP .

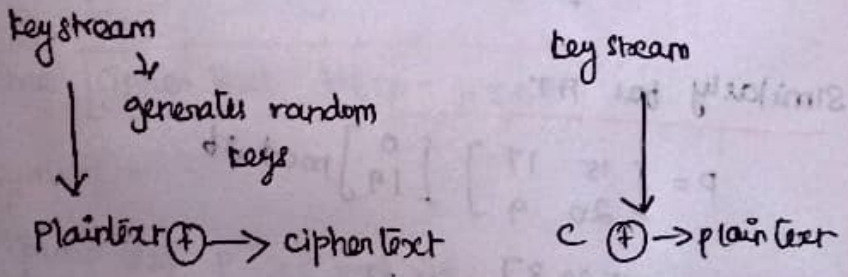
VERNAM CIPHER

It is a poly aplphabetic cipher.

-> main aim of cryptanalysis is to choose a keyword.

-> This was introduced by AT & T engineer Gilbert Vernam in 1918.

->This works on binary data rather than letters.



$C_i = P_i \text{ Xor } k_i$

P_i - binary digit of plaintext

k_i - binary digit of key.

C_i - binary digit of cipher text.

Ex:- Vernam cipher also called OTP (one time pad).

plain text : HELLO

key - any random key where PT & key length should same.

Key :- NCBTA

Encryption :-

P :	H	E	L	L	O	
	7	4	11	11	14	
K :	N	C	B	T	A	(+)
	13	2	1	19	0	
	20	6	12	30	14	
				-26		
				4		

→ There are only 26 alphabets. Hence we have to subtract 26 from 30

cipher text : U G M E O

Decryption :- C - K

C :	U	G	M	E	O
	20	6	12	4	0
	20	6	12	30	0

→ Add 26 to avoid negative result

K :	N	C	B	T	A
	13	2	1	19	0
	7	4	11	11	14

P : H E L L O → hence plain text

Ques :- PT :- WORLD
key : tejas.
find CT.

Adv :-

→ The key is used for encryption and decryption and then that key can be discarded.

→ One time pad - is unbreakable.

→ There is no statistical relationship b/w PT, hence there is no simple way for breaking the code :-

Polyalphabetic cipher:

Another way for improving simple monoalphabetic technique called polyalphabetic cipher.

→ vigenere

↳ auto key system where key word is concatenated with plaintext to provide running key.

Ex:- attack at dawn

key: lemon.

a t t a c k a t d a w n
l e m o n l e m o n l e

ciphertext:- L X F O P V E F R N H R.

l e m o n l e m o n l e

a t t a c k a t d a w n.

Method II:

Using key table.

key: deceptivedeceptivedeceptive -> has to repeat the keyword.

PT: we are discovered y save yourself.

CT:. ZICVTWQNGRZGVTWAVZHCQYGLMGJ.

key:

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22

have to add key and PT

key	8	21	4	3	4	2	4	15	19	8	21	4
PT	18	0	21	4	24	14	20	17	18	4	11	5
CT	25	8	25	7	2	16	24	6	10	12	6	9

CRYPTANALYSIS:

This vigenere cipher is unbreakable, due to the use of 26 different cipher alphabets.

Disadvantage:

-> If the key length is smaller than plaintext length, then key will be repeated.. due to repeating nature of key.

-> This is computationaly secured.