1-1

Cryptography

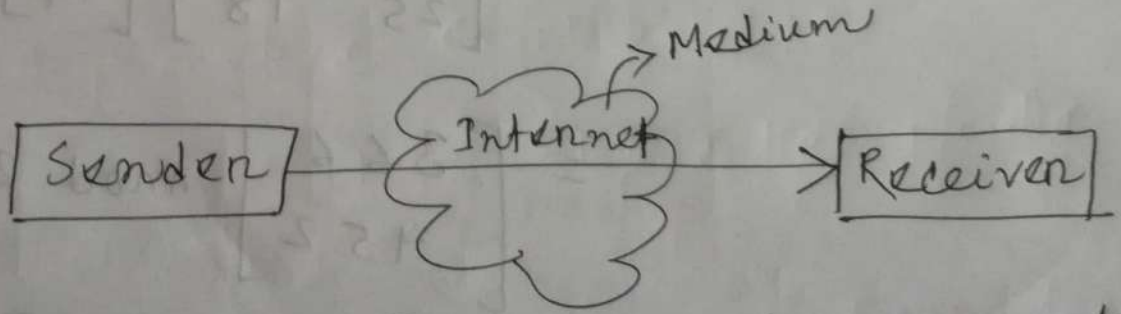
* The art of Protecting information by transforming it into an unreadable format.

OR

* Method of Protecting information and communications through the use of codes so that only those for whom the information is intended can read and Process it.

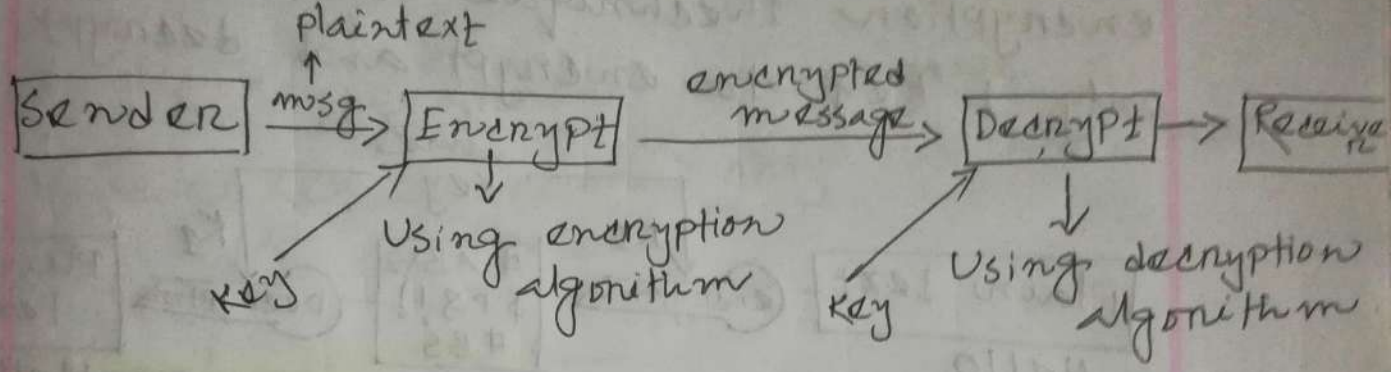
More generally Cryptography is about constructing and analyzing Protocols that prevent third parties or the Public from reading Private messages.

General process of a data communication



But it is not secure because attacker or 3rd party may corrupt/change our data.

Thus, to provide security and protect the valuable information, we can use cryptography.



case 1: If Keys are same, that is Symmetric cryptography.

case 2: If Keys are different, that is Asymmetric cryptography.

Encryption: Process of transforming information from readable to unreadable format.

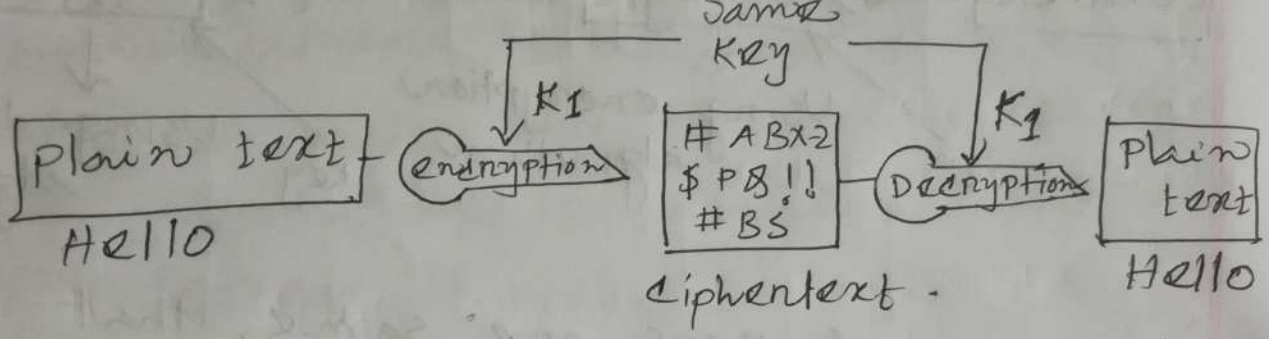
Decryption: Process of transforming data from unreadable to readable format.

Key: String of bits used by cryptographic algorithms to transform plain text to cipher text and vice versa.

Types of Cryptography

Symmetric cryptography :-

It is the simplest kind of encryption technique that involves only 1 key to encrypt and decrypt.



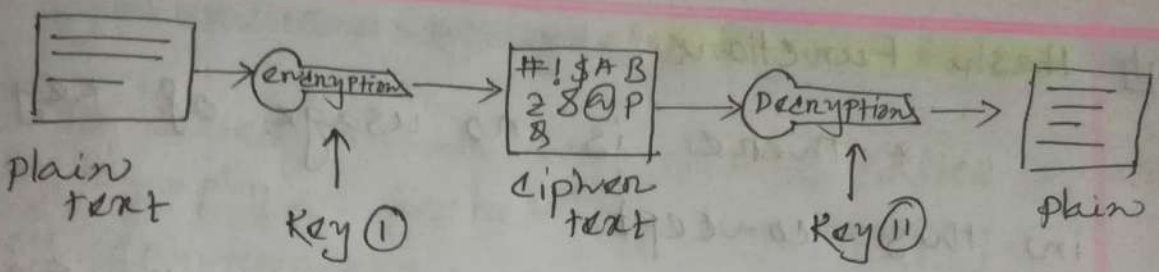
* It is also called Secret key cryptography or Private key cryptography.
* The most popular symmetric key cryptography is DES (Data Encryption Systems).

Asymmetric cryptography :-

* It is also called public key cryptography.
* It uses two keys for encryption and decryption.

L-2

04



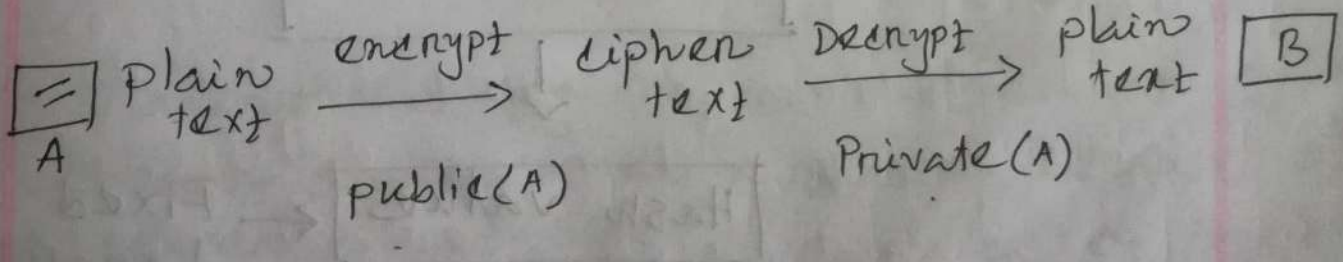
public Key → Known to everyone.

Private Key → Known only to that particular Person.

Important Note:—

~~A Message~~ A message that is encrypted using a public Key, can only be decrypted using a Private Key, while also, a message encrypted using Private Key can be decrypted using public Key.

popular asymmetric Key algorithms → RSA, DSA, Elliptic curve etc

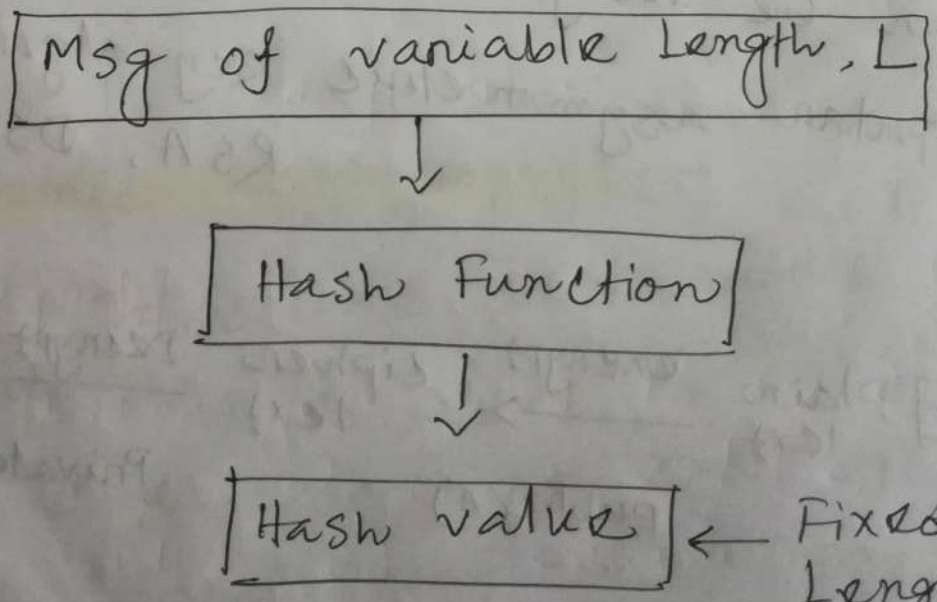


Hash Functions :—

* There is no usage of key in this concept.

* Takes variable length size message and gives fixed size output → Hash code / Hash value.

* Hash code makes it impossible for the contents of plaintext to be recovered.
* Many OS use hash functions to encrypt passwords.



Symmetric Cryptography	Asymmetric Cryptography
• Also called Private Key Cryptography or secret Key Cryptography.	• Also called public Key Cryptography.
• Only one Key is used for encryption and decryption.	• TWO different Keys are used for encryptio and decryption.
• Symmetric Key algorithms are faster in execution.	• Slower in executio
• Less complex and less computational power is required.	• More complex and more computationa power needed.
• Used for the transfer of bulk data (because it executes faster.	• Used for secret exchanging the se ret Key.
• Sharing the Key in between Sender and receiver is not safe.	• NO Problem of sharing because o Private Key concer
• commonly used algorithms → DES, AES, RC4, 2DES,	• Algorithms → RS Deffie Hellman, DS etc.

Security Goals.

(i) confidentiality :—

* It is the most common aspect of information security. It allows authorized users to access sensitive and Protected data.

* The data sent over the Network should not be accessed by unauthorized users.

* Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data, so that even if the attacker gains access, he or she will not be able to decrypt it.

(ii) Integrity :—

* changes need to be done only by the authorized entities and through authorized mechanisms, and nobody else should modify our data.

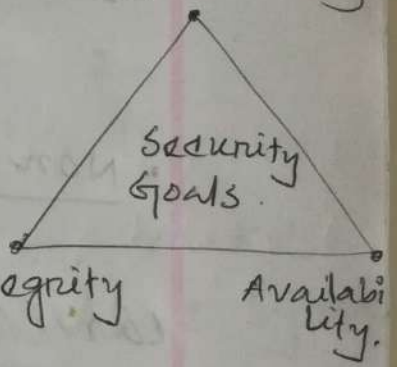
For example, In a bank, when we deposit / withdraw money, the balance needs to be maintained.

(iii) Availability :—

* Data must be available to the authorized user.

* Information is useless if we can not access it.

CIA Triad



Security Services :-

- Data confidentiality
  - Protect data from attackers.
- Data Integrity
  - Protecting data from unauthorized modification.
- Authentication
  - verifying actual person.
- Non repudiation
  - Assurance that someone can not deny the validity of something.
  - It is a service which Provides Proof of the origin of the data and the integrity of the data.

1-4-5

- Access control

- To whom the access should be given can be decided.

- This service controls who can have access to our information under what condition.

Security Attacks

- Active attack.
- Passive attack.

Passive attack:

* It attempts to learn or make use of the information from the system but does not affect the system resource. The attacker will only see the data, He will not modify it.

* We can prevent it using better encryption techniques.

Two types of passive attack

(i) Release of message content

- The attacker/hacker will easily be able to understand the data.

(ii) Traffic analysis

- If we have encryption protection, an attacker might still be able to observe the pattern of these messages.

- The attacker could determine the location and the identity of communication hosts and could observe the frequency and the length of the message.

- These information might be helpful in guessing the nature of communication that was taking place.

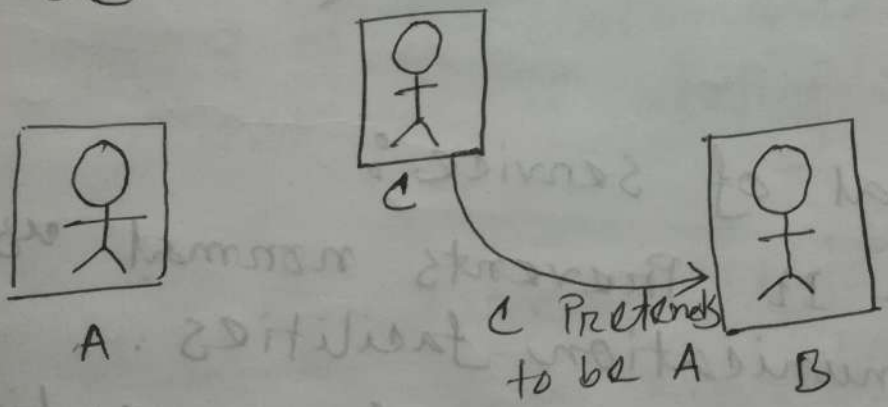
* Passive attack is difficult to detect because they do not involve any alteration of data.

Active attack:

* It attempts to alter system resources.

(i) Masquerade:

- When one entity pretends to be another entity.

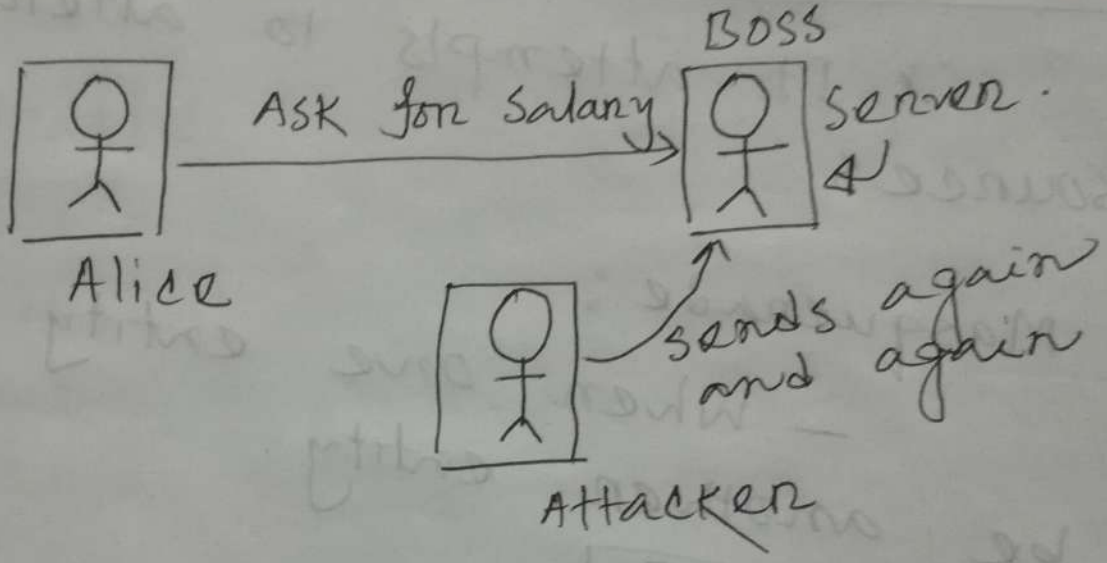


(ii) Modification of messages:

- Some portion of the message is altered or the message is delayed or reordered to produce an unauthorized effect.

(iii) Replay :

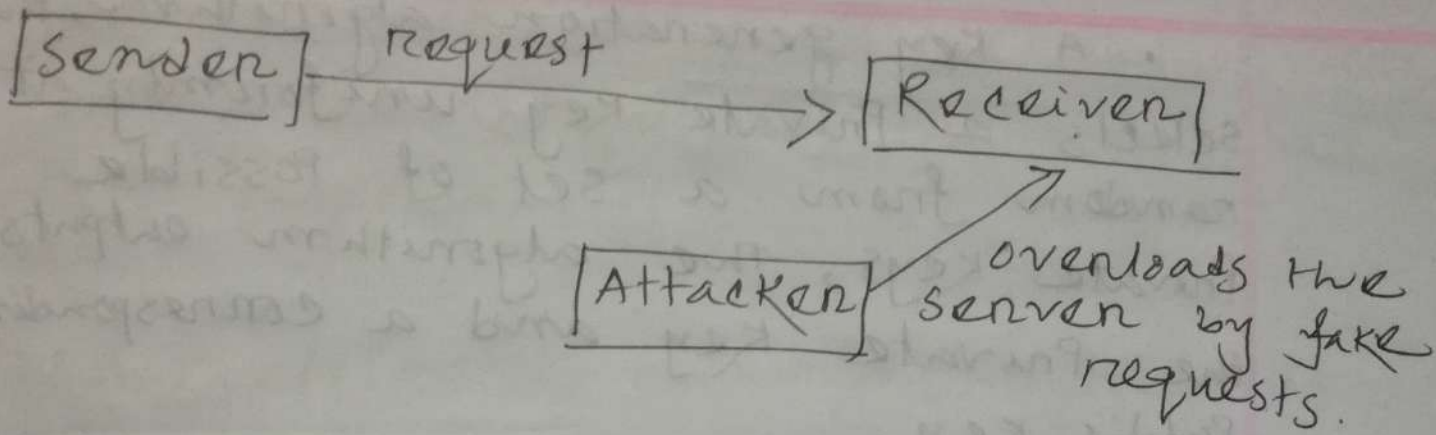
* Involves passive capture of a message and its subsequent retransmission to produce an unauthorized effect.



(iv) Denial of service :

* It Prevents normal use of communication facilities.

example - disruption of an entire network whether by disabling the network or by overloading it by messages so as to degrade performance.



Security Mechanisms:

Security mechanisms are used to Provide security.

(i) Encipherment → The use of mathematical algorithms to transform data into a form that is not readily intelligible.

(ii) Digital signature → It is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
A digital signature scheme typically consists of three algorithms.

- A Key generation algorithm, that selects a Private Key uniformly at random from a set of Possible Private Keys, The algorithm outputs the Private Key and a corresponding Public Key.

- A Signing algorithm, given a message and a Private Key, Produces a Signature.

- A Signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the messages claim to authenticity.

(iii) Data Integrity → this mechanism appends to the data a short check value that has been created by a specific Process from the data itself. The receiver creates a new check value from the received data and compares the newly created check value with the

received one. If both the values are same, the integrity of the data has been preserved.

(iv) Authentication exchange:→ In this, two entities exchange some messages to prove their identity to each other. eg→ bluetooth, shareit.

(v) Routing control:→ Means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from eavesdropping on a particular route.

(vi) Access control:→ This method prove that a user has access right to the data.

(viii) Notarization: Means selecting a third trusted Party to control the communication between two entities. This can be done to prevent repudiation.

Classical encryption techniques:

Symmetric encryption also referred to as conventional encryption is of 2 types.

(i) Substitution Techniques.

(ii) Transposition Techniques.

Substitution Technique:

It is the one in which the letters of the plaintext are replaced by other letters or by Number or Symbols.

N E T W O R K → O F U X P S L

Transposition Technique:

Performing some sort of permutations on the plaintext letters.

N E T W O R K → N T R K W E O

OR, T K R N E O W

Transposition cipher

- Keyless
- Keyed.

Transposition ciphers

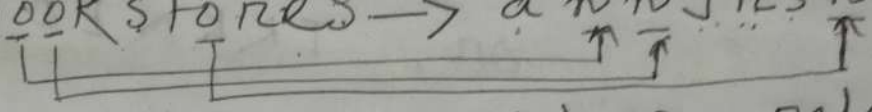
- Rail fence.
- columnar Transposition
- Double Transposition

Substitution Techniques

- ceasen cipher
- Monoalphabetic cipher.
- polyalphabetic cipher
  - vigenere cipher
  - vernam cipher.
- playfair cipher.
- Hill cipher.
- one time pad.

(I) Monoalphabetic Substitution cipher :-

A single cipher alphabet for each plaintext alphabet is used throughout the process.

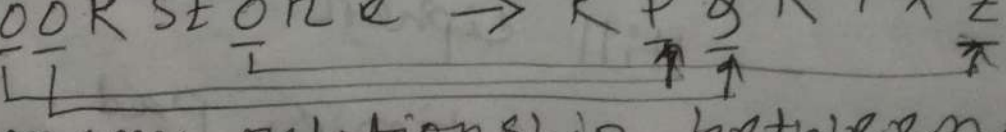
i.e. BOOKSTORES → 

In monoalphabetic cipher, relation between a character in the plaintext to a symbol in cipher text is always one to one.

(II) polyalphabetic Substitution cipher :

* there is no fixed substitutions.

* Each occurance of a character may have a different substitute. We can use more than one substitution for the same letter.

e.g. BOOKSTORE → 

one to many relationship between plaintext and ciphertext.

TRANSPOSITION TECHNIQUES

(i) No replacement of character.

(ii) We will ~~replace~~ rearrange the character's position. We will apply some sort of permutation on the plaintext letters.

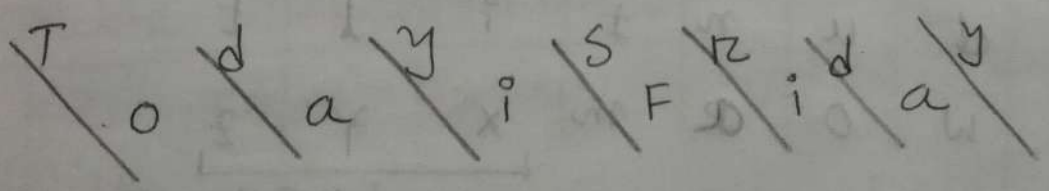
(i) Rail Fence Technique:

In this the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

e.g.

"Today is Friday" → plaintext

To encrypt this with a rail fence of depth 2, we write the following.



encrypted message is "TDYSRDYOAIFIA"

* Used for short messages
* Easy to break ~~th~~ by attacker.

(11) Row Transposition cipher

We write the message in a rectangle, row by row and read the message off, column by column, but permute the order by column.

Key → integer value (unique digits from 0 to 9)

eg. 45312

C R Y P T O
1 4 6 3 5 2

plain → attack postponed until two am

Key →	4	3	1	2	5	6	7
	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	q	m	x	y	z

↳ Extra/Dummy bit.

ciphertext →
TTNA APTM TSUO AODW COIX KNLY PETZ

Problem → can easily be understood by the attacker.

Used for short messages only.

It can be made more secure by performing more than 1 stage of transposition, so the result will be more complex Permutations

Key →

4	3	1	2	5	6	7
t	t	n	a	a	P	t
m	t	S	u	O	a	O
d	W	C	O	i	x	K
n	l	y	P	R	t	Z

ciphertext →

NSCY AUOP TTWL TMDN AOIE PAXT TOKZ

Double Transposition:

* Columnar Transposition / Row transposition applied Twice.
* The key can be same / different.

Note: Key → STRIPE
564231

Caesar Cipher

* It is also called Shift cipher or additive cipher.

* Each letter in the plaintext is replaced by a letter corresponding to a number of shifts in the alphabet.

* It is a monoalphabetic caesar cipher.

Note → Julias Caeser used an additive cipher to communicate with his officers. He used a key of 3 for communication.

eg plain → call me
cipher → FDOO PH
K = 3.

Ciphertext

$$C = E(K, P) = (P + K) \bmod 26$$

For Decryption

$$P = D(K, C) = (C - K) \bmod 26.$$

if (C-K) is -ve, add 26 to it.

Numerical value is assigned to each letter.

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

* If the cryptanalyst/attacker knows a ciphertext, then he can apply brute force technique to find the plaintext by using all possible 25 keys.

* Since it is a part of Symmetric encryption, same key is used for encryption and decryption. $1 \leq K \leq 25$.

eg Message → hello ; let, Key = 4

$C(h) = (P+K) \bmod 26$
$= (7+4) \bmod 26 = 11 \bmod 26 = 11 = L$

$C(e) = (4+4) \bmod 26 = 8 = I$

$C(l) = (11+4) \bmod 26 = 15 = P$

$C(o) = (14+4) \bmod 26 = 18 = S$

Ciphertext → LIPPS

Decryption

Cipher, C = LIPPS.

Now, $P = (C - K) \bmod 26$.

$P(L) = (11 - 4) \bmod 26 = 7 = h$

$P(I) = (8 - 4) \bmod 26 = 4 = e$

$P(P) = (15 - 4) \bmod 26 = 11 = l$

$P(S) = (18 - 4) \bmod 26 = 14 = o$

∴ plaintext → hello.

Playfair cipher Algorithm

* It was invented in 1854 by Charles Wheatstone, but was named after Lord playfair, who promoted the use of cipher.

Algorithm

(i) Create 5x5 matrix that is called grid of letters.

(ii) The matrix is made by inserting the values of key and remaining alphabets into the matrix (row wise from left to right), where letter I and J will be combined together.

(iii) Convert the text into pairs of alphabet.

eg Mina → Mi na.

(a) pair can not be made with same letters, break the letters in single and add 'x' to the previous letter.

eg Hello → He lx lo

Helloe → He lx lo e

e alone problem

(b) If the letter is standing alone in the process of pairing, then add 'z' with the letter.

eg Helloe → He lx lo ez

Hexxoe → He xz xo ez

(iv) code will be formed using 3 rules.

(a) If both the alphabets are in the same row, replace them with alphabets to their immediate right.

(b) If both alphabets are in same column, replace them with alphabets immediately below them.

(c) If not in same row/column, replace them with alphabets in the same row respectively, but at other pair of corners.

Key → EBRAHIM

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

Same Row

MD → CF

LO → NG

Same column

KW → QB

CS → LX

Horizontal

RW → BX

AK → BN

Vernam cipher

(i) used for encrypting alphabetic text.

(ii) Simply a type of substitution cipher.

In this we assign a number to each character of plain text. like

(a = 0, b = 1, c = 2, d = 3, ... x = 23, y = 24, z = 25)

Length of the key = length of plaintext.

Plaintext → RAMSWARUPK

Key → RANCHOBABA

plain text →	17	0	12	18	22	0	17	20	15	10
key →	17	0	13	2	7	14	1	0	1	0
(P + K)	34	0	25	20	29	14	18	20	16	10
	8	0	25	20	3	14	18	20	16	10

Ciphen → IAZUDOSUSK

Cipher → IAZUDOSUBK.

NOW, for decryption,

Cipher →	8	0	25	20	3	14	18	20	16	10
Key →	17	0	13	2	7	14	1	0	1	0
C - K	-9	0	12	18	-4	0	17	20	15	10
	17	0	12	18	22	0	17	20	15	10

plaintext → RAMSWARUPK.

L-12

Vigenere cipher

(i) Designed by Blaise De vigenere (16th century French mathematician)

(*) It is a polyalphabetic Substitution cipher.

The encryption is done using a (26x26) matrix.

Method (1) → vigenere Table.

plain text = GIVE MONEY

Key = LOCK

Solution

G I V E M O N E Y

L O C K L O C K L.

→ Repeat the letters of the key so that the number of letters in P and K (plain text and Key) becomes equal.

Cipher → R W X O X C P O J.

For Decryption

Cipher → R W X O X C P O J
Key → L O C K L O C K L
Plain Text → G I V E M O N E Y

Method (II), When the table is not given.

Encryption, $E_i = (P_i + K_i) \text{ Mod } 26$

Decryption, $D_i = (E_i - K_i) \text{ Mod } 26$

plaintext → She is Listening
Key → PASCAL

∴ Key Stream → 15, 0, 18, 2, 0, 11.

The Key Stream is the repetition of this initial Key Stream (as many times needed).

$\Rightarrow -x \bmod 26$

$= (-x + 26) \bmod 26$

* $E_i = (P_i + K_i) \bmod 26$
* $D_i = (E_i - K_i) \bmod 26$

33

13

Plain Text	S	h	e	i	s	l	i	s	t	e	n	i	n	g
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key Stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Cipher Text	H	H	W	K	S	W	X	S	L	G	N	T	C	G
plain value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Plain Text	S	H	E	I	S	L	I	S	T	E	N	I	N	G

HILL CIPHER

- Developed by Lester Hill in 1929.
- Encrypts a group of letters called polygraph.

To encrypt, $C = KP \bmod 26$.

K = Key, P = plaintext.

Step 1: Choose a key. (Key matrix must be a square matrix)

We can take any key.

Example: $VIEW = \begin{bmatrix} V & I \\ E & W \end{bmatrix} = \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$

$$QUICKNESS = \begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix} = \begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}$$

Let, A Given plaintext, P = ATTACK.

and key, $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Since the key is a 2×2 matrix, plaintext should be converted into vectors of length 2.

So, $\begin{bmatrix} A \\ T \end{bmatrix}$ $\begin{bmatrix} T \\ A \end{bmatrix}$ $\begin{bmatrix} C \\ K \end{bmatrix}$

NOW encryption begins

$$\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}, \quad K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

$C = KP \bmod 26$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2\times0+3\times19 \\ 3\times0+6\times19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

Corresponding Alphabets = $\begin{bmatrix} F \\ K \end{bmatrix}$

$\therefore \begin{bmatrix} A \\ T \end{bmatrix}$ becomes $\begin{bmatrix} F \\ K \end{bmatrix}$ $\therefore AT \rightarrow FK$

Now, second vector is $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$C = KP \bmod 26$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2\times19+3\times0 \\ 3\times19+6\times0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$

Corresponding Letters will be $\begin{bmatrix} M \\ F \end{bmatrix}$.

$\therefore$ TA becomes MF.

Next is $\begin{bmatrix} C \\ K \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$$C = KP \bmod 26 = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

corresponding Letters will be $\begin{bmatrix} I \\ O \end{bmatrix}$

∴ CK becomes IO

∴ Plaintext → ATTACK

ciphertext → FKMFIO

Hill cipher Decryption

To encrypt, $C = KP \bmod 26$.

To decrypt, find inverse of key matrix K^{-1}

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

Here, Cipher, C = FKMFIO

Key, $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Determinant of Matrix, $d = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$

$$d = |ad - bc|$$

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

L-15

38

Here,

$$d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3.$$

∴ determinant value, $d = 3$.

Now, find multiplicative inverse of determinant

i.e $d d^{-1} \equiv 1 \mod 26$.

So, $3 * d^{-1} \equiv 1 \mod 26$.

$\therefore d^{-1} = 9$

So, Till now, determinant, $d = 3$.

$d^{-1} = 9$.

Now, we will find adjoint of the matrix,,

Let, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

then $adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Here,

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \quad \therefore \text{adj}(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

Before decryption, we have to reduce negative values (add 26 to -ve values)

$$\therefore \text{adj}(K) = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

Now, $K^{-1} = \frac{1}{|K|} \text{adj}(K)$

$$\therefore K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$$

Now, Find its modulo 26

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$\therefore K^{-1} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now we will decrypt.

ciphen = FK MF IO

$$C = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

plaintext, $P = K^{-1} C \bmod 26$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26$$

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

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

Similarly,

$$C = \begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$

$$\therefore P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26$$

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

Again, $C = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$

$$\therefore P = K^{-1} C \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 2$$

$$= \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

$\therefore$ Plaintext = ATTACK (Answer)

Hill Cipher (3×3) Matrix Example

Let,

Plaintext = "SAFEMESSAGES"

Key = "CIPHERING"

$$K = \begin{bmatrix} C & I & P \\ H & E & R \\ I & N & G \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$$

Since key is a 3×3 Matrix, plaintext should be converted into column vectors of length 3. i.e (3×1) matrices.

So, we get,

$$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \begin{bmatrix} E \\ M \\ E \end{bmatrix} \begin{bmatrix} S \\ S \\ A \end{bmatrix} \begin{bmatrix} G \\ E \\ S \end{bmatrix}$$

Encryption $C = KP \bmod 26$

$$P \rightarrow \begin{bmatrix} S \\ A \\ F \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2\times18 + 8\times0 + 15\times5 \\ 7\times18 + 4\times0 + 17\times5 \\ 8\times18 + 3\times0 + 6\times5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} H \\ D \\ S \end{bmatrix}$$

Next is, $P = \begin{bmatrix} E \\ M \\ E \end{bmatrix} = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}$

$$C = KP \bmod 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} I \\ O \\ E \end{bmatrix}$$

Next is, $P = \begin{bmatrix} S \\ S \\ A \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}$

$$C = KP \bmod 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} = \begin{bmatrix} Y \\ Q \\ O \end{bmatrix}$$

Again, $P = \begin{bmatrix} G \\ E \\ S \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} C \\ A \\ A \end{bmatrix}$$

~~∴ SAFENESS~~

∴ SAFEMESSAGES → HDSIOEYBOCAA

HILL CIPHER Decryption (3×3 Matrix)

Cipher → HDSIOEYBOCAA

Key, K = CIPHERING = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

Decrypt — $P = K^{-1} C \bmod 26$

NOW, we need K^{-1} ; $\boxed{K^{-1} = \frac{1}{|K|} adj(K)}$

(1) finding determinant value of K

$$d = \begin{vmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{vmatrix}$$

$= 2(24 - 13\times17) - 8(42 - 17\times8) + 15(13\times7 - 32$

$= 1243$

Now, we will find the multiplicative inverse of the determinant.

i.e $\boxed{d\,\bar{d}^{-1} \equiv 1 \bmod 26}$

$$(d \cdot \bar{d}^{-1}) \bmod 26 = 1$$

So,

$$1243(\bar{d}^{-1}) \equiv 1 \bmod 26$$

$$\therefore \bar{d}^{-1} = 5$$

$\bar{d}^{-1} = 5$

$(1243 \times 5) \bmod 26$

$= 6215 \bmod 26$

$= 1$

Now, we will find adjoint (K)

$$K = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$$

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

For 1st element

$4 \times 6 - 17 \times 13$

$= -197$

For 2nd element

$7 \times 6 - 8 \times 17$

$= -94$

47

For 3rd element

$$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} = 7\times13 - 8\times4$$

$$= 59$$

And so on...

After solving all we get.

$$\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}$$ ← cofactor matrix

NOW, we will do transpose

$$adj(K) = \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$$

NOW Removing the Negative Signs

$$adj(K) = \begin{bmatrix} -197+26(n) & 147 & 76 \\ \downarrow & & \\ 94 & 7 \quad -108+26(n) & 71 \\ & \downarrow & \\ & 5 & \\ 59 & 38 & -48+26(n) \\ & & \downarrow \\ & & 2 \end{bmatrix} = \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$$

Now,

$$adj(K) = \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$$

$$K^{-1} = |d^{-1}| \cdot adj(K)$$

$$= .5 \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix}$$

Find its modulo to simplify.

$$\begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \leftarrow K^{-1}$$

NOW, the Decryption Formula.

$$P = K^{-1} C \mod 26$$

Cipher → HDS IOE YQO CAA.

$$P = K^{-1} C \mod 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 330 \\ 338 \\ 447 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} = \begin{bmatrix} S \\ A \\ F \end{bmatrix}$$

Again.

$$P = K^{-1} C \mod 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 186 \\ 168 \\ 264 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ M \\ E \end{bmatrix}$$

50

Again For $\begin{bmatrix} Y \\ S \\ O \end{bmatrix} \rightarrow \begin{bmatrix} 24 \\ 18 \\ 14 \end{bmatrix}$

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \cdot \begin{bmatrix} 24 \\ 18 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} = \begin{bmatrix} S \\ S \\ A \end{bmatrix}$$

For $\begin{bmatrix} C \\ A \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}$

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} G \\ E \\ S \end{bmatrix}$$

SO, HDSIOEYBOCAA becomes

SAFEMESSAGES.

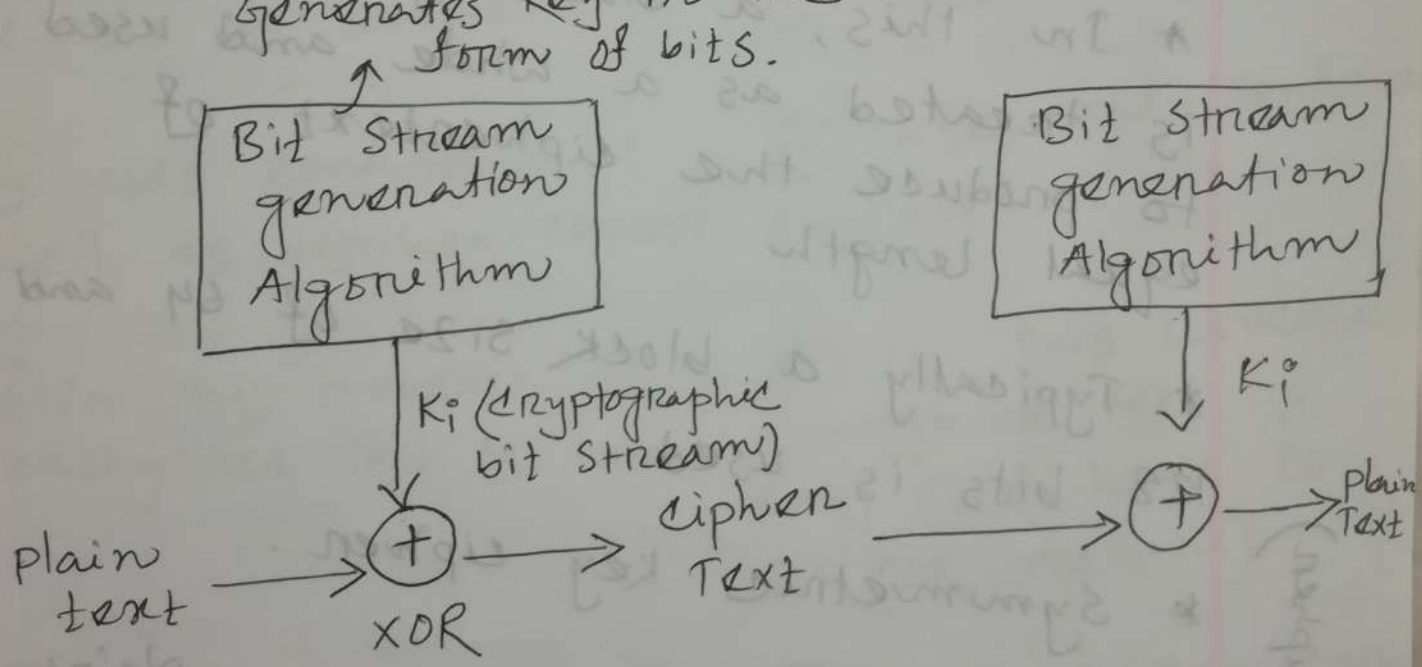
Stream and Block cipher.

* Used to convert plaintext → cipher text.

① Stream cipher

* It is the one that encrypts a digital data stream one bit or one byte at a time.

* It is a Symmetric key cryptography.



eg

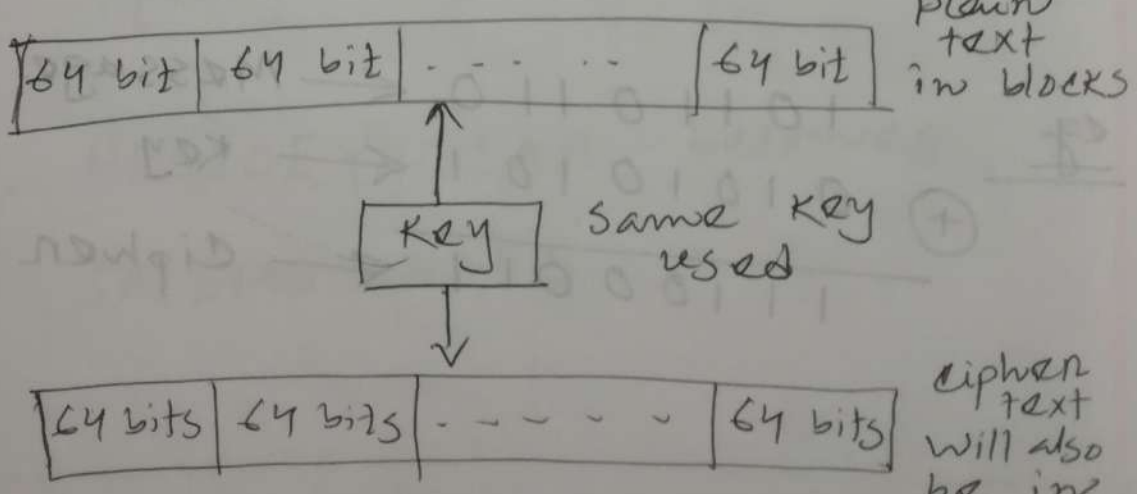
```
  10110110   ← Message to sent
⊕ 01010101   ← key
----------
  11100011   ← cipher.
```

To Decrypt

```
  11100011  ← ciphen
⊕ 01010101  ← key
----------
  10110110  ← plain text.
```

(ii) Block ciphen

* In this, a block of plain text is treated as a whole and used to produce the ciphentext of equal length.
* Typically a block size of 64 and 128 bits is used.
* Symmetric key ciphen.



Example
DES (64 bit block ciphen)

Block cipher	Stream cipher
(i) Plain → cipher text by taking plain texts block at a time.	(i) 1 bit or 1 byte of plain text → cipher text.
(ii) It uses 64 bits or more.	(ii) It uses 8 bits.
(iii) Complexity of block cipher is simple.	(iii) While stream cipher is more complex.
(iv) uses confusion as well as defusion concept.	(iv) uses only confusion concept.
(v) In this reverse encrypted text is hard.	(v) In this reverse encrypted text is easy (we have to do XOR again).
(vi) uses ECB (Electronic code Book) and CBC (cipher Block chaining) algorithm modes.	(vi) uses CFB (cipher feedback) and OFB (output feedback) algorithm modes.

Shannon's Theory of confusion and Diffusion.

1. The terms confusion and diffusion were introduced by Claude Shannon.

2. Shannon's concern was to prevent crypt analysis, based on statistical analysis. This reason is as follows—

* Assume that attacker has some knowledge of the statistical characteristics of the plaintext (eg- in a message, the frequency distribution of the various letters may be known)

* If these statistics are in any way reflected in the ciphertext, the cryptanalist may be able to deduce the encryption key.

Thus Shannon suggested 2 methods to frustrate the attackers:

(i) confusion
(ii) Diffusion.

Diffusion

→ In simple words, if a symbol in the plain text is changed, several or all symbols in the cipher text will also change.

→ The idea of diffusion is to hide the relationship between the cipher text and plain text.

→ Diffusion means that if we change a single bit of plain text, then half of the bits in the cipher text should change and similarly -

If we change 1 bit of cipher-text, then at least one half of the plain text bits should change.

→ Diffusion implies that each symbol in the cipher text is dependent on some or all the symbols in the plain text.

5th

Confusion

→ It hides the relationship between cipher text and the key.

→ If a single bit in the key is changed then rest / all bits of the cipher text will also be changed.

→ Confusion means that each bit of the cipher text should depend on several parts of the key, obscuring the connection between the two.

Fiestel Cipher Structure.

* Most of the block cipher technique follows this structure.

① The plain text is processed in two equal halves (L_0 and R_0). ← divided

→ The 2 halves of the data pass through n rounds of processing and then combine to produce the cipher-text block.

→ on the right half, we apply a function and in the f_n we will use a subkey generated from the master key.

→ The output of this is XORed with the left half, and then their output will be swapped.

*** This is one single round.

→ We will have n rounds (Depends on algorithm). All rounds will have same structure.

→ We devide the plain text in 2 halves and apply the function on RHS and XOR it with LHS and the output is swapped then, that algorithm follows fiestel structure.

(i) Block size → Langer block size, more security.

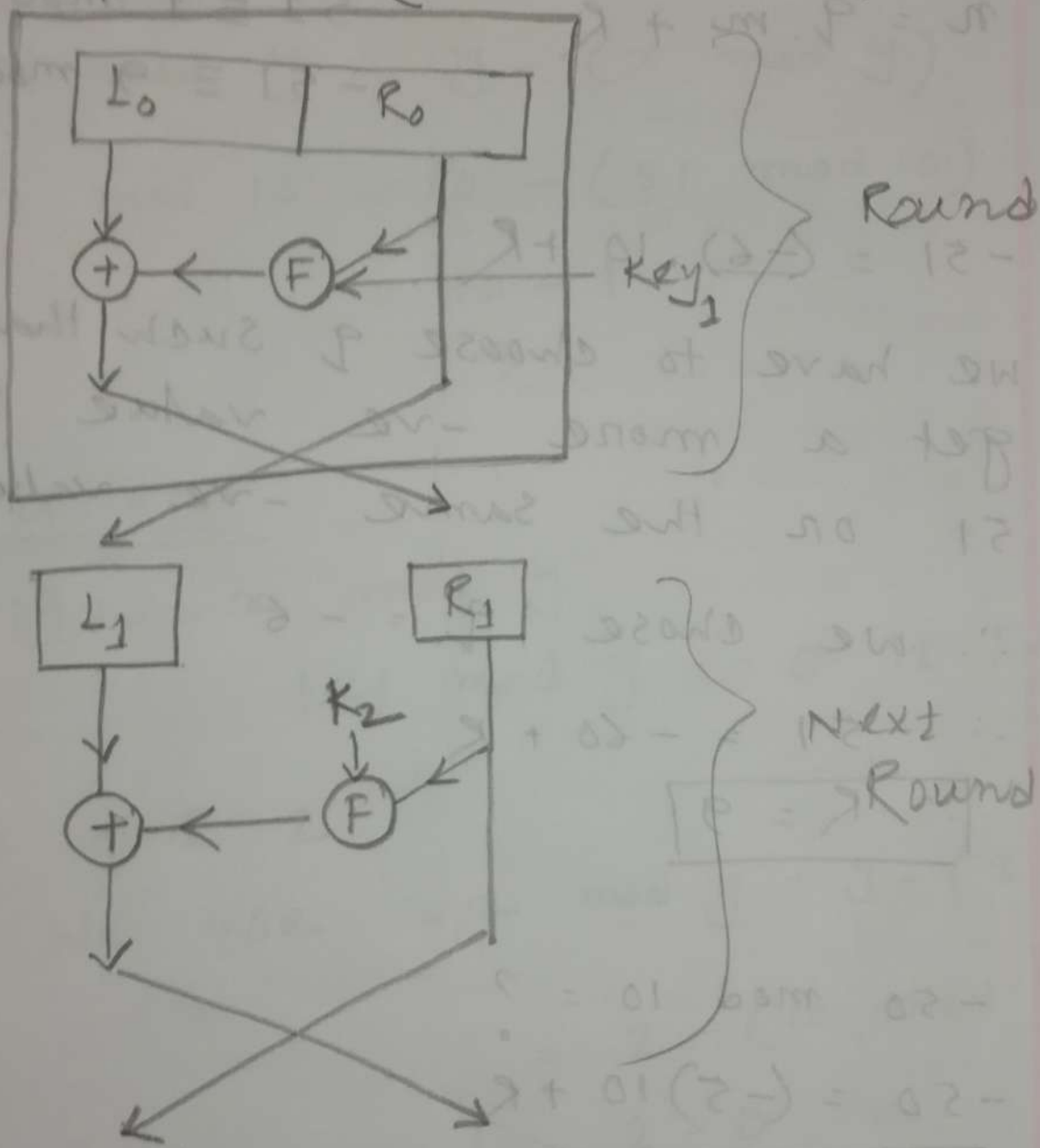
(ii) Key size → Langer Key size means more security (but may decrease the speed of encryption/ decryption)

(iii) NO of Rounds → More rounds, more secure.

(iv) Subkey generation algo → More complex algo, harder for attacker to steal data.

(v) Function / Round Function → More complex function, harder for the crypt analyst to attack.

plain text (Divided in 2 equal halves)



Modulus of -ve Number.

$n = q.m + R$

$51 \equiv 1 \mod 10$

$-51 \equiv 9 \mod 10$

* $-51 = (-6).10 + R$

We have to choose q such that we get a more -ve value than 51 or the same -ve value.

$\therefore$ we chose $q = -6$

$\therefore -51 = -60 + R$

$\boxed{\therefore R = 9}$

* $-50 \mod 10 = ?$

$-50 = (-5)10 + R$

$\boxed{\therefore R = 0}$ Here we chose q such that the no. becomes the same.

* $-37 \mod 5$

$-37 = (-8).5 + R$

$\boxed{\therefore R = 3}$

Method 2

$-x \bmod y = y - (x \bmod y)$

$-51 \bmod 10 = 10 - (51 \bmod 10)$

$= 10 - 1$

$= 9.$

Exception

If in $-x \bmod y$,

$|x| \bmod y == 0$ it Fails.

$-10 \bmod 2$

if we use $-x \bmod y = y - (x \bmod y)$

$= 2 - (10 \bmod 2)$

$= 2 - 0$

$= 2$

which is wrong.

So, if in $-x \bmod y$, $|x| \bmod y == 0$.

remainder = 0

So, $-10 \bmod 2 = 0$

as $|-10| \bmod 2 = 0$

Method 3

* $-23 \mod 7$

$= (-23 + 28) \mod 7$

$= 5$

* $-6 \mod 4$

$= (-6 + 8) \mod 4$ [add multiple of 4 to make it +ve or 0]

$= 2 \mod 4$

$= 2$

* $-10 \mod 2$

$= (-10 + 10) \mod 2$

$= 0$

Modular Arithmetic

$7 \bmod 4 = 3$

$-11 \bmod 7 = 3$

$-x \bmod y$

$= y - (x \bmod y)$

$7 - (11 \bmod 7)$

$= 7 - 4$

$= 3$

if $|x| \bmod y \neq 0$; it works

if $|x| \bmod y = 0$; it fails.

This Formula may fail in some cases i.e. $-10 \bmod 2$

Congruent Modulo

Two integers a and b are said to be congruent modulo n if

$$(a \bmod n) = (b \bmod n)$$

This is written as

$$a \equiv (b \bmod n) \quad \text{or} \quad b \equiv (a \bmod n)$$

eg $73 \equiv (4 \bmod 23)$ means

$$73 \bmod 23 = 4 \bmod 23.$$

Properties of congruence

(i) $a \equiv b \pmod{n}$; if $n/(a-b)$

(ii) $a \equiv b \pmod{n}$ implies

$b \equiv a \pmod{n}$

(iii) if $a \equiv b \pmod{n}$ and

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

Modular Arithmetic operations

(i) $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

(ii) $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

(iii) $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

** Let, $a = 11$, $b = 15$, $n = 8$

$(11 \times 15) \bmod 8$

$= 165 \bmod 8$

$= 5$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8$

$= (3 \times 7) \bmod 8$

$= 5$

Note → Exponention is performed by repeated multiplication

$11^7 \bmod 13$

$11^2 = 121 \equiv 4 \bmod 13 = 4$

$11^4 = (11^2)^2 \equiv 4^2 \bmod 13 \equiv 3 \bmod 13 = 3.$

$11^7 = 11^2 \times 11^4 \times 11$

$= (4 \times 3 \times 11) \bmod 13$

$= 132 \bmod 13$

$= 2$

(iv) if $x \equiv y \bmod n$, $a \equiv b \bmod n$;
then $\boxed{(x+a) \equiv (y+b) \bmod n}$

eg $17 \equiv 4 \bmod 13$, $42 \equiv 3 \bmod 13$
$59 \equiv 7 \bmod 13$; which is true.

(v) if $x \equiv y \bmod n$ and $a \equiv b \bmod n$
then $\boxed{(x-a) \equiv (y-b) \bmod n}$

$42 \equiv 3 \bmod 13$ and $14 \equiv 1 \bmod 13$
then, $28 \equiv 2 \bmod 13$.