Cryptography and Network security

→ cryptography is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand and process it inorder to prevent unauthorized access

→ The term cryptography means: crypt → hidden
graphy → writting

security Attacks

Attack: A violation on system security that derives from an intelligent threat

security Attack: Any action that comprimises the security of information owned by an organisation

There are 2 types of attacks

i) Passive Attacks ii) Active Attacks

Passive Attacks

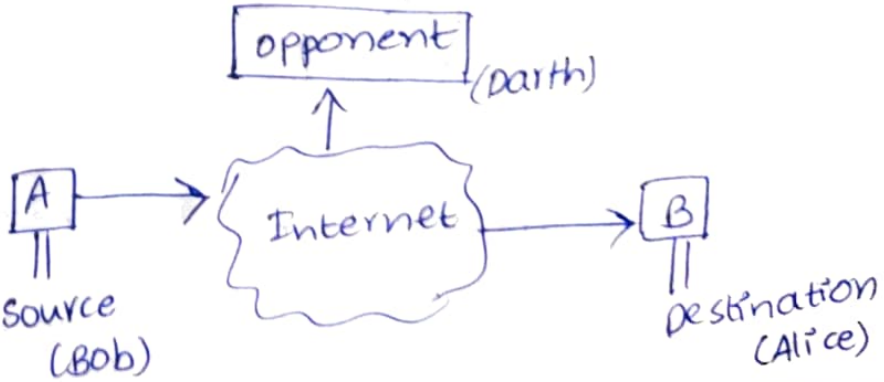
these are the attacks in which the goal of the opponent is to obtain information that is being transmitted.

The types of passive attacks are

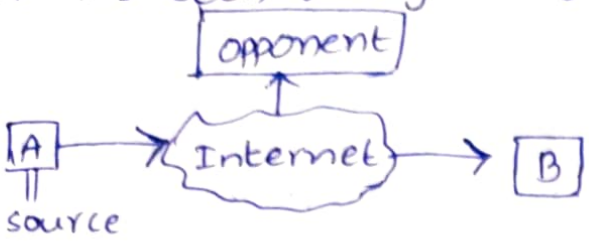
1) Release of message contents

2) Traffic Analysis.

1) Release of message contents: The contents of the message will be released to the opponent while transmitting from source to destination via some network.



2) Traffic Analysis: The traffic b/w the sender and receiver has been analyzed by the opponent



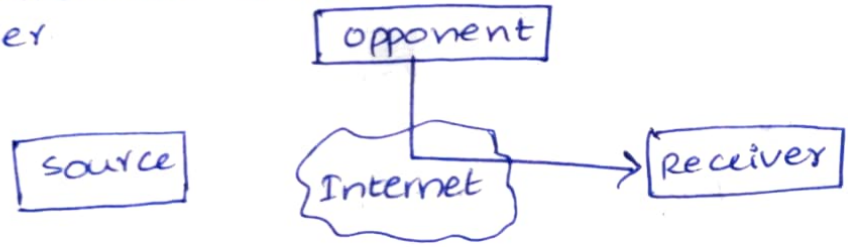
Active Attack

An active attack attempts to alter system resources or effect their operation, it involves some modification of the data stream or the creation of the false stream.

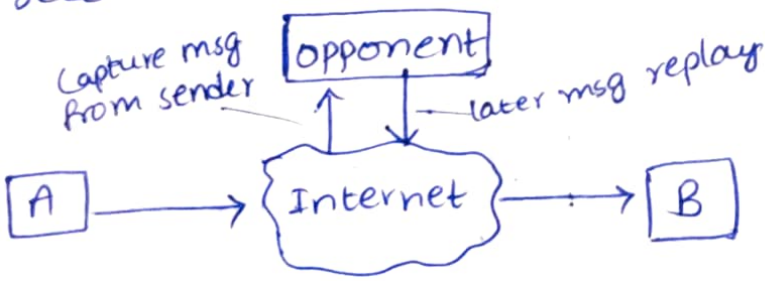
The various types are

1) Masquerade
2) Replay
3) Modification of messages
4) Denial of service

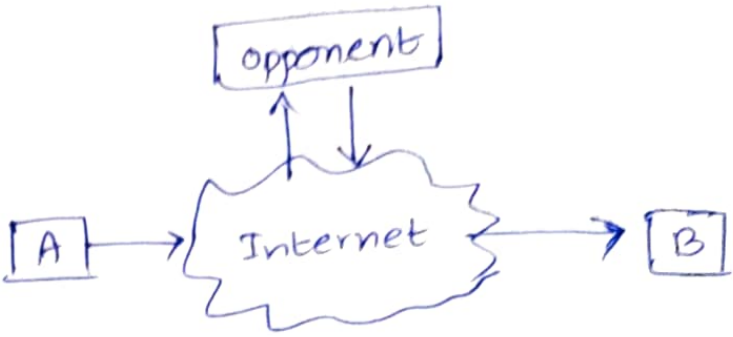
1) Masquerade :- The opponent person acts as alleged (or) authorized sender and transmit data to the receiver



2) Replay :- when the data is going to be transmitted b/w the sender and receiver the opponent capture the messages and later transmitts the same message to the receiver as authorised sender.



3) modification of message: when the message is transmitted from the sender it is received by the opponent and opponent modifies the message and transmits to the receiver



4) Denial of service

when the services are going to be provided by the server the opponent disrupts all the services from the server.

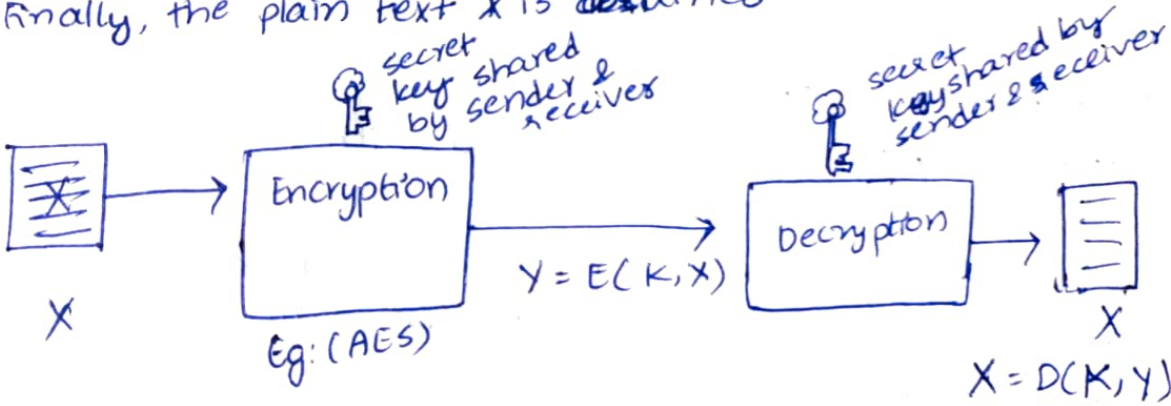
Symmetric Cipher Model:

In this model, the plain text X goes into encryption algorithm and gives the output Y

In the encryption algorithm the transmitted cipher text will be $Y = E(K, X)$

Now the Y is received by the receiver and fed into decryption algorithm and the final output is X. $X = D(K, Y)$

Finally, the plain text X is obtained



Security Services

The various services provided to the data in order to acheive security are

1) Authentication
2) confidentiality
3) Integrity
4) Access control
5) Non-Repudation
6) Availability

1) Authentication

This service is considered with assuring that a

communication is authenticate It also ensures that the end users are authorized The 2 categories of authentication are:

1) Peer entity authentication.
2) Data origin authentication

2) Confidentiality

It is a protection of transmitted data from passive attacks. The various types of confidentiality

1) connection
2) connection-less
3) selective field
4) Traffic flow

Classical Encryption Techniques

There are 2 techniques that are used for encryption in the early days of cryptography

1) substitution cipher 2) Transposition cipher

1) Substitution cipher

In this technique one letter is replaced with another letter or symbol

Ex: CSE + 1 = DTF

2) Transposition cipher

Here the plain text is converted with permutations. of the letters of plain text

permutations are nothing but combinations of the finite set of elements in the plain text

Ex: let PT = CSE

(Plain Text)

Now the combinations for CSE are

CSE
SCE
SEC
ESC
ECS
CES

The cipher text can be one of the combinations from the above permutations.

The various techniques in substitution cipher are

1) ceaser/ shift cipher
2) Hill cipher
3) playfair cipher
4) mono alphabetic cipher
5) poly alphabetic cipher
6) one time pad

① ceaser cipher

1) letters are replaced by the other letters or symbols
2) Earlier this is used by the mathematician Julius ceaser
3) Replacing the each letter of the plain text with 3 places down the alphabet.
4) In Encryption $C = E(P, K) \% 26$ (or)

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

$$C = (P + K) \% 26$$

$$\boxed{C = (P + K) \% 26}$$

5) In decryption $P = D(C, K) \% 26$

$$= (C - K) \% 26$$

$$\boxed{P = (C - K) \% 26}$$

Ex:
①

$P = \overset{2}{C}\ \overset{18}{S}\ \overset{4}{E}$

A	B	C	D	. . .	Z
0	1				25

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

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

$= (2+3) \bmod 26, \quad (18+3) \bmod 26, \quad (4+3) \bmod 26$

$= 5 \bmod 26 \quad = 21 \quad = 7 \bmod 26$

$= 5 \quad = 7$

$C = (5\ 21\ 7)$

$C = F\ V\ H$

Decryption

$P = D(C, K) \% 26$

$= (C - K) \% 26$

$= (5-3) \% 26, \quad (21-3) \% 26, \quad (7-3) \% 26$

$= 2 \qquad = 18 \qquad = 4$

$P = (2 \ 18 \ 4)$

$= C \ S \ E$

(2) Find the cipher text for the given plain text

SAVE WATER

$P = \overset{18}{s}\ \overset{0}{a}\ \overset{21}{v}\ \overset{4}{e}\ \overset{22}{w}\ \overset{0}{a}\ \overset{19}{t}\ \overset{4}{e}\ \overset{17}{r}$

$C = (P + k) \bmod 26$

$= (18+3) \bmod 26, \quad (0+3) \bmod 26, \quad (21+3) \bmod 26,$

$= 21 \qquad = 3 \qquad = 24$ ~~$(4+3) \bmod$~~

$(4+3) \bmod 26 \qquad (22+3) \bmod 26 \qquad (0+3) \bmod 26$

$= 7 \qquad = 25 \qquad = 3$

$(19+3) \bmod 26 \qquad (4+3) \bmod 26 \qquad (17+3) \bmod 26$

$= 22 \qquad = 7 \qquad = 20$

$C = (21 \ 3 \ 24 \ 7 \ 25 \ 3 \ 22 \ 7 \ 20)$

$C = (V \ D \ Y \ H \ Z \ D \ W \ H \ U)$

Disadvantage

can be easily cracked ie the opponent can easily retrieve the PT upon watching the paltern of CT

(2) Hill cipher

1) It is multiletter cipher
2) Deveioped by Lester Hill in 1929
3) Encrypt a group of letters:

digraph, trigraph or polygraph.

4) key is a square matrix

5) If it is 2x2 matrix then 2 letters of PT will be encrypted at the same time

If it is 3x3 matrix then 3 letters of PT will be encrypted at the same time

If it is 4x4 matrix then 4 letters of PT will be encrypted at the same time

6) Matrix Arithmetic modulo 26 is involved

7) For Encryption $C = (K, P) \bmod 26$

8) For Decryption $P = (CK^{-1}) \bmod 26$ $\quad K \rightarrow$ matrix

Example:

1) Find the cipher text for the given PT Hello world with key value $K = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$

A) Hello world

divide into two letters as it is 2x2 matrix

C_1 C_2 C_3 C_4 C_5

He | ll | ow | or | ld

$C = KP \bmod 26$

(C1) $\overset{7\ 4}{He} = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 18 \\ 37 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 18 \\ 11 \end{bmatrix}$ (i.e. 18 mod 26, 37 mod 26)

$C_1 = \begin{bmatrix} S \\ L \end{bmatrix}$

(C2) $= KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 33 \\ 77 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 \\ 25 \end{bmatrix} \bmod 26$

$C_2 = \begin{bmatrix} H \\ Z \end{bmatrix}$

(C3) $C_3 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 22 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 50 \\ 130 \end{bmatrix} \bmod 26$

$C_3 = \begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$

(C4) $C_4 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 13 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 45 \\ 110 \end{bmatrix} \bmod 26$

$C_4 = \begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$

Decryption

$P = D(C, K) \% 26$

$= (C - K) \% 26$

$= (5-3) \% 26, \quad (21-3) \% 26, \quad (7-3) \% 26$

$= 2 \qquad = 18 \qquad = 4$

$P = (2 \quad 18 \quad 4)$

$= C \; S \; E$

② Find the cipher text For the given plain text

SAVE WATER

$P = {}^{18}\,0\;21\;4\;22\;0\;19\;4\;17$

$P = s\,a\,v\,e\;w\,a\,t\,e\,r$

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

$= (18+3) \bmod 26, \quad (0+3) \bmod 26, \quad (21+3) \bmod 26,$

$= 21 \qquad = 3 \qquad = 24$ ~~$(4+3) \bmod$~~

$(4+3) \bmod 26 \qquad (22+3) \bmod 26 \qquad (0+3) \bmod 26$

$= 7 \qquad = 25 \qquad = 3$

$(19+3) \bmod 26 \qquad (4+3) \bmod 26 \qquad (17+3) \bmod 26$

$= 22 \qquad = 7 \qquad = 20$

$C = (21 \;\; 3 \;\; 24 \;\; 7 \;\; 25 \;\; 3 \;\; 22 \;\; 7 \;\; 20)$

$C = (V\,D\,Y\,H\,Z\,D\,W\,H\,U)$

Disadvantage

can be easily cracked ie the opponent can easily retrieve the PT upon watching the paltern of CT

(2) Hill cipher

1) It is multiletter cipher
2) Developed by Lester Hill in 1929
3) Encrypt a group of letters:

Digraph, trigraph or polygraph.

4) Key is a square matrix

5) If it is 2x2 matrix then 2 letters of PT will be encrypted at the same time

If it is 3x3 matrix then 3 letters of PT will be encrypted at the same time

If it is 4x4 matrix then 4 letters of PT will be encrypted at the same time

6) Matrix Arithmetic modulo 26 is involved

7) For Encryption $C = (K, P) \bmod 26$

8) For Decryption $P = (CK^{-1}) \bmod 26$ $\quad K \rightarrow$ matrix

Example:

1) Find the cipher text for the given PT Hello world with key value $K = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$

A) Hello world

divide into two letters as it is 2x2 matrix

C_1 C_2 C_3 C_4 C_5

He | ll | ow | or | ld

$C = KP \bmod 26$

(1) $He = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 18 \\ 37 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 18 \\ 11 \end{bmatrix}$ (i.e. 18 mod 26, 37 mod 26)

$C_1 = \begin{bmatrix} S \\ L \end{bmatrix}$

(2) $C_2 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 33 \\ 77 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 \\ 25 \end{bmatrix} \bmod 26$

$C_2 = \begin{bmatrix} H \\ Z \end{bmatrix}$

(3) $C_3 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 22 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 50 \\ 130 \end{bmatrix} \bmod 26$

$C_3 = \begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$

(4) $C_4 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 45 \\ 110 \end{bmatrix} \bmod 26$

$C_4 = \begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$

(5) $C_5 = KP \bmod 26$

$= \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 11 \\ 3 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 25 \\ 45 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 25 \\ 19 \end{bmatrix}$

$C_5 = \begin{bmatrix} Z \\ T \end{bmatrix}$

$C = C_1\ C_2\ C_3\ C_4\ C_5$

$= SL\ HZ\ YA\ TG\ ZT$

Decryption

$P = CK^{-1} \bmod 26$

$K^{-1} = D^{-1}\, adj(K)$

$D = |2 \times 4 - 1 \times 3|$

$= 5$

$DD^{-1} = 1 \bmod 26$

$5 \times D^{-1} = 1 \bmod 26$

$5D^{-1} \bmod 26 = 1$

$5 \times 21 \bmod 26 = 1$

$D^{-1} = 21$

$adj(K) = \begin{bmatrix} 4 & -1 \\ -3 & 2 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 4 & 25 \\ 23 & 2 \end{bmatrix}$

$K^{-1} = D^{-1}\, adj(K)$

$= 21 \begin{bmatrix} 4 & 25 \\ 23 & 2 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 84 & 525 \\ 483 & 42 \end{bmatrix} \bmod 26$

$-1 \bmod 26$

$= -(1 \bmod 26)$

$= -1$

$= 26 - 1$

$= 25$

$-3 \bmod 26$

$= -(3 \bmod 26)$

$= 23$

$$K^{-1} = \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix}$$

$$PI = C1\ K^{-1} \bmod 26$$

$$= \begin{bmatrix} 18 \\ 11 \end{bmatrix} \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18\times6 + 11\times5 \\ 18\times5 + 16\times11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 \\ 4 \end{bmatrix} \text{ mod 26}.$$

$$= \begin{bmatrix} H \\ e \end{bmatrix}$$

Similarly find the plain text for P2, P3, P4, P5

2) Find the cipher text for the given plain text ATTACK with key 2x2 matrix $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

A) $C_1\ C_2\ C_3$
AT/TA/CK

$$C_1 = KP \bmod 26$$

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

$$= \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$$

$$C_2 = KP \bmod 26$$

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

$$= \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

$$C_3 = KP \bmod 26$$

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

$$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

$C = C_1\ C_2\ C_3$
$= FKMFIO$

1
38
19
57
38
26
12

Decryption

$P = CK^{-1} \bmod 26$

$K^{-1} = D^{-1} \text{adj } K$

$D = |12 - 9| = 3$

$DD^{-1} = 1 \bmod 26$

$3D^{-1} \bmod 26 = 1$

$\boxed{D^{-1} = 9}$

$3 \times 9 \bmod 26 = 1$

$$\text{adj } K = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$K^{-1} = D^{-1} \text{adj } K = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$P1 = C1\, K^{-1} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5\times2 + 25\times10 \\ 25\times5 + 10\times18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

$$P2 = C2\, K^{-1} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

$$P3 = C3\, K^{-1} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 360 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

(3) Playfair cipher

1) This algorithm is used by british army during the world war I
2) The secret key is made of 25 alphabet letters arranged in 5x5 matrix in which i and j letters are considered as same while encrypting
3) Different arrangements of the letters in the matrix can create many different secret key

Example:

RAM

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

5x5

4) The cipher uses 3 rules for encryption

i) If the 2 letters in pair of a plain text are placed in same row of the secret key, the corresponding encrypted character for each letter is the next letter to the right in the same row (with wrapping to the beginning of the row. If the plain text letter is the last character in the row)

|→| Right

ii) If the two letters in a pair are located in the same column of the secret key, the corresponding encrypted character for each letter is the letter beneath it in the same column (with wrapping to the beginning of the column. If the plain text letter is the last character in the row)

|↓| beneath

iii) If the pair of plaintext letters doesnot locate in same row or same column then the corresponding encrypted character for each letter is a letter that is in its own row but in the same column as the other letter

|⇄| swap

Example

(1) Find the cipher text for the given plain text SUNRISE with the key MONARCHY

A) P= SU/NR/IS/E.
K= MONARCHY

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

5×5

SU NR IS EX

C= LX AM SX JU

(2) P= He/ll/o wo/rl/d

K= MONARCHY

A)

He ll ow or ld

CF PP NV NM TC

Note :-

1) In this technique the key stream and the cipher stream are the same. This means that the rules that are mentioned can be thought of rules for creating the key stream.

2) The key stream depends on the position of the characters of a particular keyword.

3) The cipher text is actually the key stream

4) For encryption $CI = KI$

For Decryption $PI = KI$

(4) Mono Alphabetic Cipher

1) The cipher line can be any permutation of the 26 alphabet characters.

2) This would seem to be eliminating brute-force attack for crypt analyst (hacker/ Attacker)

Playfair cipher

Ex: (2) Find the cipher text for the given plain text Hello using key = MONARCHY

A) P = HE/LL/OX

K = MONARCHY

C = HE LL OX

CF PP AV.

when two letters in plain text are repeated, a filling character 'X' is placed between them.

C = HE LX LO

CF SU PM

C = CFSUPM

5) The main disadvantage of this cipher is nature of plain text is known.

4) this cipher needs 26! attempts to break the key

5) key is not fixed

Example

① PT = sunrise / college / VVIT

key = +2 +4 +1

CT = uwptkug / gsppiki / wwju

⑤ Poly Alphabetic cipher

1) A set of related mono-alphabetic substitution rules are used
2) A key determines which particular rule is choosen for a given transformation
3) This is of 2 types
   i) vigenese cipher
   ii) vernam cipher

i) vigenere cipher

→ It consists of 26 ceaser ciphers with shifts of 0 through 25 (0-25)

→ For encryption $CI = PI + KI \bmod 26$

→ For decryption $PI = CI - KI \bmod 26$

Eg: Find the cipher text for the given plain text

We are discovered save yourself and the key is deceptive

A)

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

(22+3) mod 26 = 25 mod 26 = 25

(4+4) mod 26 = 8

0 + 2 = 2

17 + 4 = 21

4 + 15 = 19

3 + 19 = 21

8 + 8 = 16

18 + 21 = 39

C1 = zicwqngrzgvt

(2) Find the cipher text for plaintext college with key vvit

A)

P =	c	o	l	l	e	g	e
k =	v	v	i	t	v	v	i
C =	x	j	t	e	z	b	m

C = xjtezbm

ii) vernam cipher

→ Gilvert vernam, an AT ~~and~~ T Engineer in year 1918

→ This cipher works on binary bits rather than letter.

→ The length of the keyword should be equals to length of the plain text.

→ The XOR operation will be performed on plain text and the key for encryption and cipher text and key for decryption

→ $C_I = P_I \oplus K_I \quad (C_i = P_i \oplus k_i)$

$P_I = C_I \oplus K_I \quad (P_i = C_i \oplus K_i)$

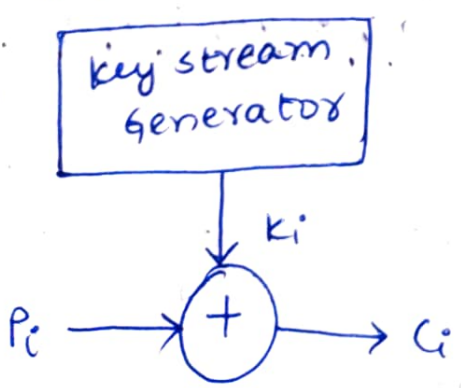
where P_i = ith binary of the plain text

k_i = ith binary of the ~~cipher~~ ~~key~~

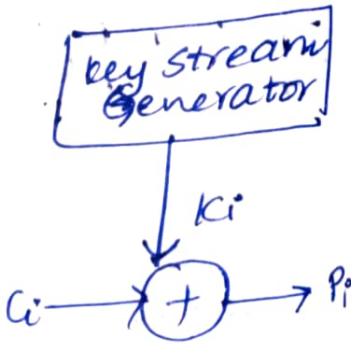
C_i = ith binary of the cipher text

$\oplus$ = XOR operation

vernam cipher Encryption



vernam cipher Decryp



Ex① Find the cipher text for the given plain text cat and key value and

A) P = cat
K = and

P = 00010 00000 10011
K = 00000 01101 00011

00010 01101 10000

C = c n q

② Find the cipher text for the given plain text Hello and key value nebct

Encryption:	+	(>25) substract from 26
Decryption:	−	(-venum) Add to 26

A) P = H e l l o
k = n e b c t

P = 0111 100 1011 1011 0110
k = 1101 100 0001 0010 10011

10100 1000 1100 1101 100001

C = u t m n h

Encryption

P = 7 4 11 11 14
+ 13 4 1 2 19

C = 20 8 12 13 33(7)
u i m n h

Decryption

C = 20 8 12 13 7
− 13 4 1 2 19
---
7 4 11 11 −12(14)
H e l l o

(6) One time pad

1) It is the improvement to the vernam cipher
2) Random key is generated as long as the message
3) One key is used only once in the encryption i.e. for a single message, one key is used and discarded
4) It produces random output!!
5) The code is unbreakable
6) The security of this cipher is entirely due to the randomness of the key.
7) The 2 fundamental difficulties of this technique is
   i) The pratical problem of making large quantities of random keys
   ii) Protecting and key distribution
8) The same technique is used for encryption and decryption ie. XOR (⊕) operation.

(2) Transposition cipher

In transposition cipher the set of permutation can be taken out as the cipher text.

There are 2 techniques in this cipher

1) Rail Fence
2) Row column

1) Rail Fence

In this cipher the plain text is returned in the following format.

 with given depth value

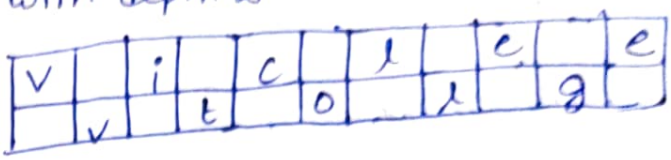
Ex① Find the cipher text for the plain text 'Hello' for depth 2

A)

H		l		o
	e		l	

c = Hloel

(2) Find cipher text for plain text vvit college with depth 2



c = vicleevtolg

2) Row column transposition cipher

→ In this technique the plain text can be written as row by row and it is read as column by column

→ It creates a rectangle, that can be of any dimension

→ key is order of the column

→ It is a more complex scheme

Eg

① Find the cipher text for the given plain text

VVIT COLLEGE NAMBUR CSE SECTION A B

The key is 241356

(A) 5×6

2	4	1	3	5	6
V	V	I	T	C	O
L	L	E	G	E	N
A	M	B	U	R	U
E	E	E	E	E	E
T	I	D	M	A	B

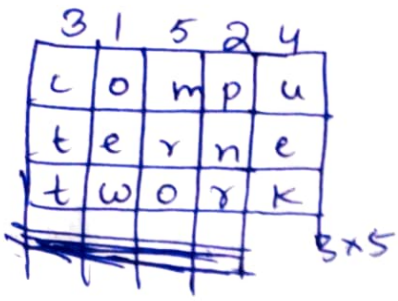
6×6

CT: Iebeovlacttgusnvlmsicereaonucb

② Find the cipher text for the given plain text

COMPUTER NETWORK with the key layer

A)



LAYER
3 1 5 2 4

CI: oewpnrcttuekmro
3 1 5 2 4

Mathematics of cryptography

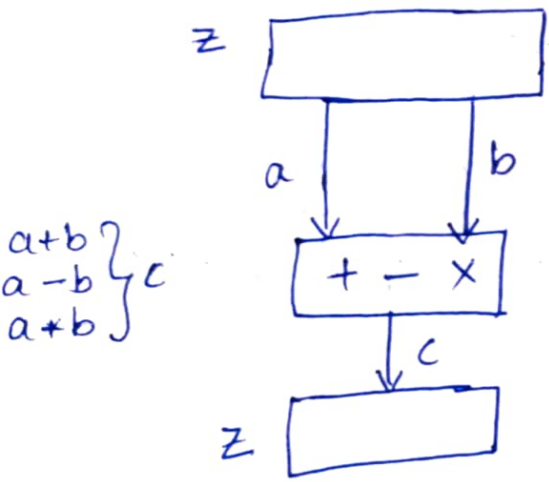
1) Integer Arthematic

It has set of integers denoted by Z that contains all integral numbers from $-\infty$ to $+\infty$

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

2) Binary operations

In cryptography 3 operations that are used namely, addition, subtraction, multiplication



Addition:
$5+9 = 14$
$-5+9 = 4$
$5+(-9) = -4$
$-5+(9) = -14$

Subtraction:
$5-9 = -4$
$-5-9 = -14$
$-5-(-9) = 4$
$5-(-9) = 14$

Multiplication:
$5*9 = 45$
$-5*9 = -45$
$5*(-9) = -45$
$-5*(-9) = 45$

Add:	5+9	-5+9	5+(-9)	-5+(-9)
Sub:	5-9	-5-9	5-(-9)	-5-(-9)
Mul:	5*9	-5*9		

3) Integer Division

In integer arithematic, if we divide 'a' by 'n' we get q and r. The relationship between these 4 integers is

$$a = q * n + r$$

where q is quotient, r is remainder, a is dividend, n is divisor

Ex:

Let $a = 255$ and $n = 11$

$$\begin{array}{r} 23 \leftarrow q \\ 11 \overline{)255} \\ 22 \\ \hline 35 \\ 33 \\ \hline 2 \leftarrow r \end{array}$$

$q = 23$, $r = 2$

Here there are 2 restrictions

i) $n > 0$

ii) $r \geq 0$

Divisibility

If a is not zero and $r = 0$ in the division relation then $a = q * n$ where a is divisible by n. It can be written as $a \mid n$

'a pipen'

where the remainder value is zero $r = 0$

If the remainder is not zero then the notation is $a \nmid n$ $r \neq 0$

The various properties for this notation is

Property - 1

if $a|1$ then $a = \pm 1$

property - 2

if $a|b$ and ~~b|a then~~ $b|c$ then $a|c$

property - 3

if $a|b$ and $b|a$ then $a = \pm b$

property - 4

if $a|b$ and $a|c$ then $a|((m*b)+(n*c))$

where m and n are arbitary integers

Euclidean

~~Euclidean~~ Algorithm

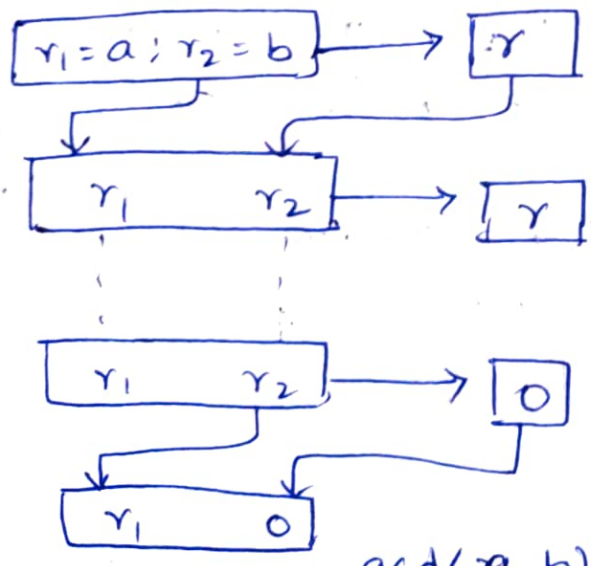
A mathematician euclid developed an algorithm that can find gcd of 2 integers. It is based on 2 facts

Fact 1 : $gcd(a,0) = a$

Fact 2 : $gcd(a,b) = gcd(b,r)$

where r is the remainder of dividing a by b

Procedure:



gcd(a,b) = r1

Algorithm

```
r1 ← a; r2 ← b;
while (r2 > 0)
{
    q = r1 / r2;
    r = r1 - q * r2;
    r1 ← r2; r2 ← r;
}
gcd(a, b) ← r1;
```

Problems

① Find gcd(12,33)

sol:-

q	r_1	r_2	r
2	33	12	9
1	12	9	3
3	9	3	0
X	3	0	X

∴ gcd(3,0) = 3

gcd(12,33) = 3

② Find gcd(750,900)

q	r_1	r_2	r
1	900	750	150
3	750	150	0
X	150	0	X

gcd(750, 900)

= 150

③ Find gcd(252,105)

sol:-

q	r_1	r_2	r
2	252	105	42
2	105	42	21
2	42	21	0
X	21	0	X

gcd(252,105) = 21

④ Find gcd(2740, 1560)

q	r_1	r_2	r
1	2740	1560	1180
1	1560	1180	380
3	1180	380	40
9	380	40	20
2	40	20	0
X	20	0	X

gcd(2740,1560) = 20

Extended Euclidean Algorithm - EED Algorithm

→ Given 2 integers a and b, 2 more integers 's' and 't' need to be find out such that

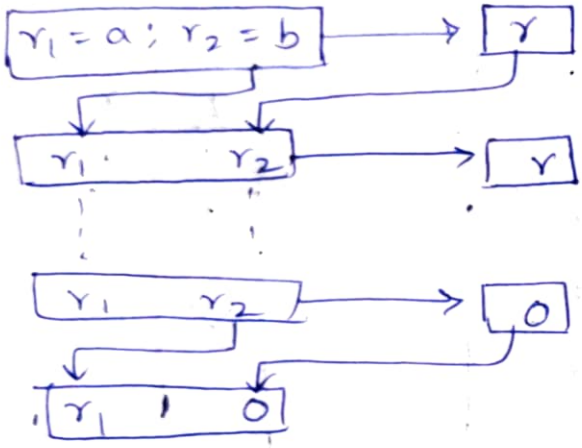
$$s * a + t * b = gcd(a, b)$$

→ This algorithm can calculate both gcd(a, b) and s and t values at the same time

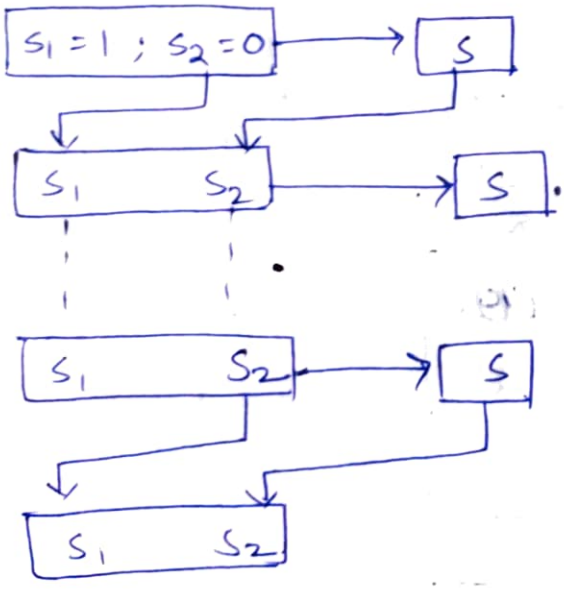
→ Here 3 sets of calculations and exchanges are used.

The 3 sets of variables are r's, s's, t's

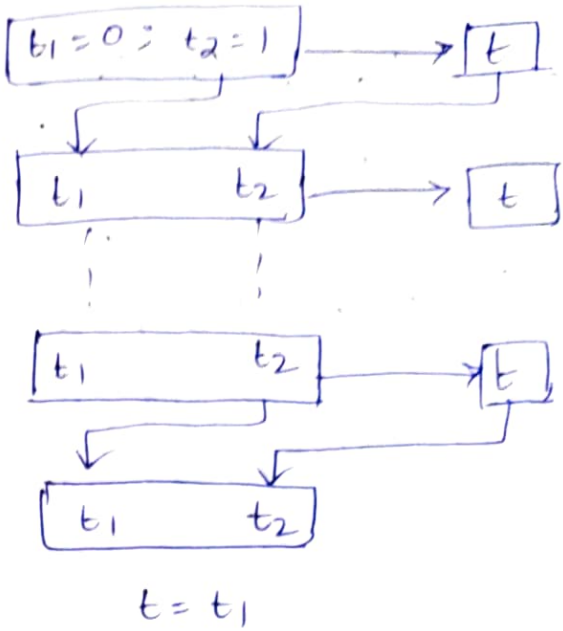
Process:-



$gcd(a, b) = r_1$



$s = s_1$



$t = t_1$

Algorithm:

```
r1 ← a; r2 ← b;
s1 ← 1; s2 ← 0;
t1 ← 0; t2 ← 1;
while (r2 > 0)
{
    q = r1 / r2;
    r = r1 − q * r2;
    r1 ← r2; r2 ← r;        } updating r's
    s = s1 − q * s2;
    s1 ← s2; s2 ← s;        } updating s's
    t = t1 − q * t2;
    t1 ← t2; t2 ← t;        } updating t's
}
gcd(a, b) ← r1;
s ← s1;
t ← t1;
```

Problems

① Find the gcd(12,33) using EED

A)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	33	12	9	1	0	1	0	1	-2
1	12	9	3	0	1	-1	1	-2	3
3	9	3	0	1	-1	4	-2	3	-11
X	3	0	X	-1	4	X	3	-11	X

$s = s_1$, $t = t_1$

$s = -1$, $t = 3$

$$gcd(a,b) = s \times a + t \times b$$

$$gcd(33,12) = -1 \times 33 + 3 \times 12$$
$$= -33 + 36$$
$$= 3$$

$$gcd(12,33) = 3$$

② Find the gcd(161, 28) using EED

A)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	23
X	7	0	X	-1	4	X	6	23	X

$s = s_1$ $t = t_1$

$s = -1$ $t = 6$

$$gcd(a,b) = s \times a + t \times b$$

$$gcd(161,28) = -1 \times 161 + 6 \times 28$$
$$= -161 + 168$$
$$= 7$$

$$gcd(161,28) = 7$$

steganography:

It word with origin in greek means "covered writting" which means that conseling the message itself by covering it with something else.

Security Mechanisms

These are used to provide the security services. The various mechanisms are

1) EN cipherment
2) Data Integrity
3) Digital Signature
4) Authentication Exchange
5) Traffic Padding
6) Routing control
7) Notarization
8) Access Control

Q) Find the cipher text for the given plain text engineering to the following techniques

1) ceaser cipher
2) Hill cipher → key = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
3) Playfair cipher → key = COLLEGE
4) Mono alphabetic cipher
5) Poly alphabetic cipher
   - vigenere cipher key = CSE
   - vernam cipher key = HELLO WORLLD
6) One time pad

1) ceaser cipher

$C = (P + K) \% 26$

$= (ENGINEERING + 3) \% 26$

$= (4|13|6|8|13|4|4|17|8|13|6 + 3) \% 26$

$= (7|16|9|11|16|7|7|20|11|16|9) \% 26$

~~Unit 2~~ :-

C = HQJLQHHULQJ

2) Hill cipher

P = EN/GI/NE/ER/IN/GX

$C_1 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 \\ 13 \end{bmatrix}$

$= \begin{bmatrix} 30 \\ 64 \end{bmatrix} \bmod 26$

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

$C_2 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 6 \\ 8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 22 \\ 50 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 22 \\ 24 \end{bmatrix} = \begin{bmatrix} W \\ Y \end{bmatrix}$

$C_3 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 13 \\ 4 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 21 \\ 55 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 21 \\ 3 \end{bmatrix} = \begin{bmatrix} V \\ D \end{bmatrix}$

$C_4 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 38 \\ 80 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 12 \\ 2 \end{bmatrix} = \begin{bmatrix} M \\ C \end{bmatrix}$

$C_5 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 34 \\ 76 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 8 \\ 24 \end{bmatrix} = \begin{bmatrix} I \\ Y \end{bmatrix}$

$C_6 = KP \bmod 26$

$= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 6 \\ 23 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 52 \\ 110 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 6 \end{bmatrix} = \begin{bmatrix} A \\ G \end{bmatrix}$

C = EMWYVDMCIYAG

3) Playfair cipher

key = COLLEGE

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

P = ENGINEERING

[EN] [GI] [NE] [ER] [IN]

FT CP TF OT KP

[GX]

LZ

C = FTCPTFOTKPLZ

4) Monoalphabetic cipher

Let the key be ~~k = +1, +2, +3, +4, ...~~

k = +5

P: E N G I N E E R I N G

\+ 5

C: J S L N S J J W N S L

5) Poly Alphabetic cipher

→ Vigenere cipher - key = CSE

P =	E	N	G	I	N	E	E	R	I	N	G
K =	C	S	E	C	S	E	C	S	E	C	S
C =	G	F	K	K	F	I	G	J	M	P	Y

C: GFKKFIGJMPY

→ vernam cipher - key = HELLO WORLDD

P =	E	N	G	I	N	E	E	R	I	N	G
K =	H	E	L	L	O	W	O	R	L	L	D
C =	L	R	R	T	B	A	S	I	T	Y	J

6) One-time Pad

P: E N G I N E E R I N G

K: h e L o w ϑ d c s m i

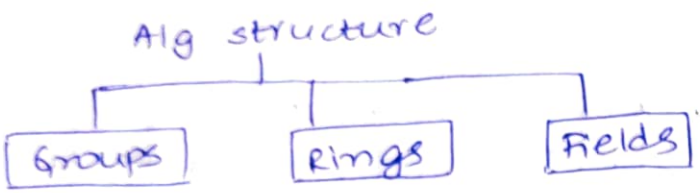
100 111	1011 0100	0110 1011	1000 1110	01101 10110	00100 10001	100 011	10001 00010	01000 10010	1101 1100
011	1111	1101	0110	11011	10101	111	10011	11010	0001
d	p	n	g	b	v	h	t	z	b

0110
1000
1110
0

Unit 2:- Mathematics of Symmetric key Cryptography

The main algebraic structures that are used in cryptography are

1. Groups 2. Rings 3. Fields



Groups:-

A group G denoted by $\{G, \cdot\}$ is a set under some operation $(\cdot)$ and if it satisfies CAIN properties

CAIN ⇒ 1. closure → if $a, b \in G$ then $a \cdot b \in G$

2. Associativity → $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\forall a, b, c \in G$

3. Identity → $a \cdot e = e \cdot a = a \quad \forall a, e \in G$

4. Inverse → $a \cdot a^{-1} = a^{-1} \cdot a = e \quad \forall a, e \in G$

Abelian group:-

It is a group which satisfies one more property that is commutative

commutative → $a \cdot b = b \cdot a \quad \forall a, b \in G$

Example:- Is $\{Z, +\}$ a group?

1. closure

$\{\ldots -\infty \ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$(a \cdot b) \in Z$

$5 + 4 = 9 \in Z$ ✓

2. Associativity

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$2 \cdot (-3 \cdot 1) = (2 \cdot -3) \cdot 1$

$-6 = -6 \in Z$ ✓

3) Identity

$a \cdot e = e \cdot a = a$

$5 + 0 = 0 + 5 = 5$

$e = 0 \in Z$

$a = 5 \in Z$ ✓

4) Inverse

$a \cdot a^{-1} = a^{-1} \cdot a$

$5 + (-5) = (-5) + 5 = 0$

$e = 0, \ a = 5 \in Z$ ✓

5) commutative

$a \cdot b = b \cdot a$

$5 \cdot 2 = 2 \cdot 5$ ✓

∴ The given $\{Z, +\}$ is a group as well as an abelian group.

Rings :-

A ring R denoted by $\{R, +, *\}$ is a set of elements with two binary operations addition and multiplication such that $\forall a, b, c \in R$ should follow the properties.

1) Group (a_1 to a_4), abelian group (a_5)

2) closure under multiplication (M1)

→ if $a, b \in R$ then $ab \in R$

3) Associativity of multiplication (M2)

→ $a(bc) = (ab)c \quad \forall a, b, c \in R$

(OR)

$a * (b * c) = (a * b) * c$

4) Distributive laws (M3)

→ $a * (b + c) = ab + ac \quad \forall a, b, c \in R$

$(a + b)c = ac + bc \quad \forall a, b, c \in R$

Commutative ring:-

It is a ring which satisfies commutative of multiplication property also (M4)

$$ab = ba$$

Note:-

For subtraction and division the addition and multiplication operators are used

Eg:-

$$a - b = a + (-b)$$

$$a/b = a\,b^{-1}$$

Fields:-

A field F denoted by $\{F, +, *\}$ is a set of elements with two operations addition and multiplication such that $\forall a, b, c \in F$ if it satisfies the properties

1) a1 - m6 (a_1 - a_4 → group, a_5 → abelian group; m_1 - m_3 → ring, m_4 → commutative ring)

2) Multiplicative inverse → for each a in F, except 0 there is an element a^{-1} in F such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Examples for fields are: Rational number, Real numbers, complex numbers.

Integral Domain:-

It is a commutative ring that satisfies the properties.

1) Multiplicative identity (M5): There is an element $1 \in R$ such that

$$a \times 1 = 1 \times a = a \quad \forall a \in R$$

2) No zero divisors (m_6):

If $a, b \in R$ and $a * b = 0$ then either $a = 0$ or $b = 0$

Finite Fields

→ It is a field with finite number of elements

→ Galois showed that for a field to be finite the number of elements should be p^n where p is a prime number and n is a positive integer

→ The finite fields are usually called galois field and is denoted by $GF(p^n)$

Example: GF(2) with a set $\{0, 1\}$

GF(2) field is

0	1	+, *

Addition

⊕	0	1
0	0	1
1	1	0

multiplication

⊗	0	1
0	0	0
1	0	1

Additive inverse

a	0	1
−a	0	1

(where the 0 occurs it is considered as additive inverse)

Multiplicative inverse

a	0	1
a^{-1}	−	1

Q)

Find the additive inverse and multiplicative inverse of GF(5)

Sol:

$GF(5) = \{0, 1, 2, 3, 4\}$

Addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

multiplication

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Additive Inverse

a	0	1	2	3	4
-a	0	4	3	2	1

multiplicative Inverse

a	0	1	2	3	4
a^{-1}	-	1	3	2	4

if bit format - ⊕ & ⊗

Polynomials

→ Used to work with 'n' bit words

→ A polynomial of degree n-1 is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

where x^i is called the ith term and a_i is called coefficient of the ith term.

→ To represent an n-bit word by a polynomial the rules to be followed are.

1) The power of x defines the position of the bit in the n-bit word ie. the left most bit is at position 0 and right most bit is at position n-1

2) The coefficient of the terms define the value of the bits because a bit can have only a value of 0 or 1 and polynomial can have 0 or 1 coefficient as well.

Ex:-

1) show how can we represent the 8-bit word 10011001 using polynomial.

polynomial ⇒ $x^7 + x^4 + x^3 + 1$

2) write 8-bit word related to the polynomial $x^5 + x + 1$

since it is 8 bit the f(x) should start with x^7 so the 8 bit word is 00100011

Operations

polynomials involve 2 operations

→ Addition and multiplication on

a) Operations on coefficients

b) operations on polynomials

→ Two fields should be defined to perform operations

1) GF(2) for coefficients

2) GF(2^n) for polynomials

→ for the sets of polynomials in GF(2^n) a group of polynomials of degree 'n' is defined as the modulus.

→ These modulus are called <u>irreducable polynomial</u>

Degree	Irreducable polynomial
1	$x+1$, x
2	x^2+x+1
3	x^3+x^2+1, x^3+x+1
4	$x^4+x^3+x^2+x+1$, x^4+x^3+1, x^4+x+1
5	x^5+x^2+1, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^2+x+1$

Eg:-

$GF(2^2)$

Find the addition & multiplication for the polynomial terms

4 bit words with size of 2

$\{00, 01, 10, 11\} = \{0, 1, x, x+1\}$

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

$01 \rightarrow 1 \times 1 = 1$

$= 01$

10×01

$x \times 1 \rightarrow x = 10$

$(x+1)x = x^2+x$

$= 01$

$x^2+x+1 \overline{)\, x^2+x\,(\,1}$

x^2+x+1

(1)

$(x+1)(x+1) = x^2+2x+1$

$= x$

$= 10$

$x^2+x+1 \overline{)\, x^2+2x+1\,(\,1}$

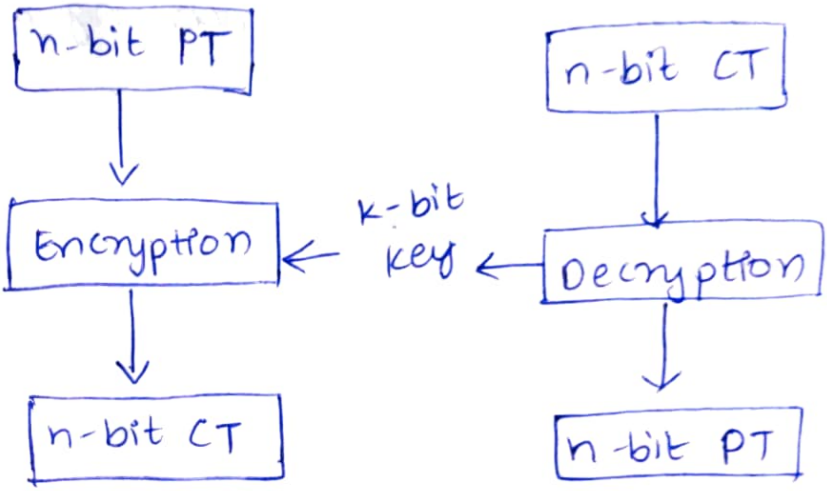
x^2+x+1

(x)

Modern Block Ciphers

In symmetric key cryptography, Modern Block ciphers encrypt 'n'-bit block of plain text and decrypts n-bit block of cipher text.

Encryption and Decryption algorithm uses same k-bit key i.e. the decryption algorithm must be the inverse of encryption algorithm and both uses same secret key.



If the message has fewer than n-bits then padding must be added to make it n-bit block

The value of n can be 64, 128, 256 or 512

Eg:-

How many padding bits must be added to a message of 100 characters if 8 bit ASCII is used for encoding and the block cipher accepts the blocks of 64 bit

Sol:

$m = 100$

8-bit ASCII

$n = 64$

P = ?

100 x 8 = 800 bits

M + P = 0 mod 64

P = −800 mod 64

= −(32)

= 64 − 32

P = 32

Total Blocks : 13

Q) Find the no of padding bits for 200 characters if 16 bit ASCII is used for encoding with 64 bit block.

A) m = 200

16 bit ASCII

n = 64

P = ?

200 x 16 = 3200 bits

M + P = 0 mod 64

P = −3200 mod 64

= −(0)

= 64 − 0

P = 64 bits

Total Blocks : 51

Components of Block cipher

The various components that are used are

1) P-Box / D-Box
   - ↓ Permutation → Diffusion
2) S-Box (substitution)
3) Product ciphers

1) P-BOX / D-BOX

This is normally keyless and is of 3 types

1. Straight P-box
2. Expansion D-box
3. Compression D-box

2) S-BOX

Inputs	00	01	10	11
0	00	10	01	11
1	10	00	11	01

3) Product cipher

Combination of substitutions, transpositions XOR, circular shift operations.

It works on 2 properties 1. Diffusion
2. confusion

Diffussion :- Hides relationship b/w CT & PT

confusion :- Hides ~~del~~ relationship between CT & key

Feistel Ciphers - stage 1, stage 2, stage 3(✓)

Design principles of modern block ciphers

1. No. of rounds
2. Round function
3. key scheduling algorithm

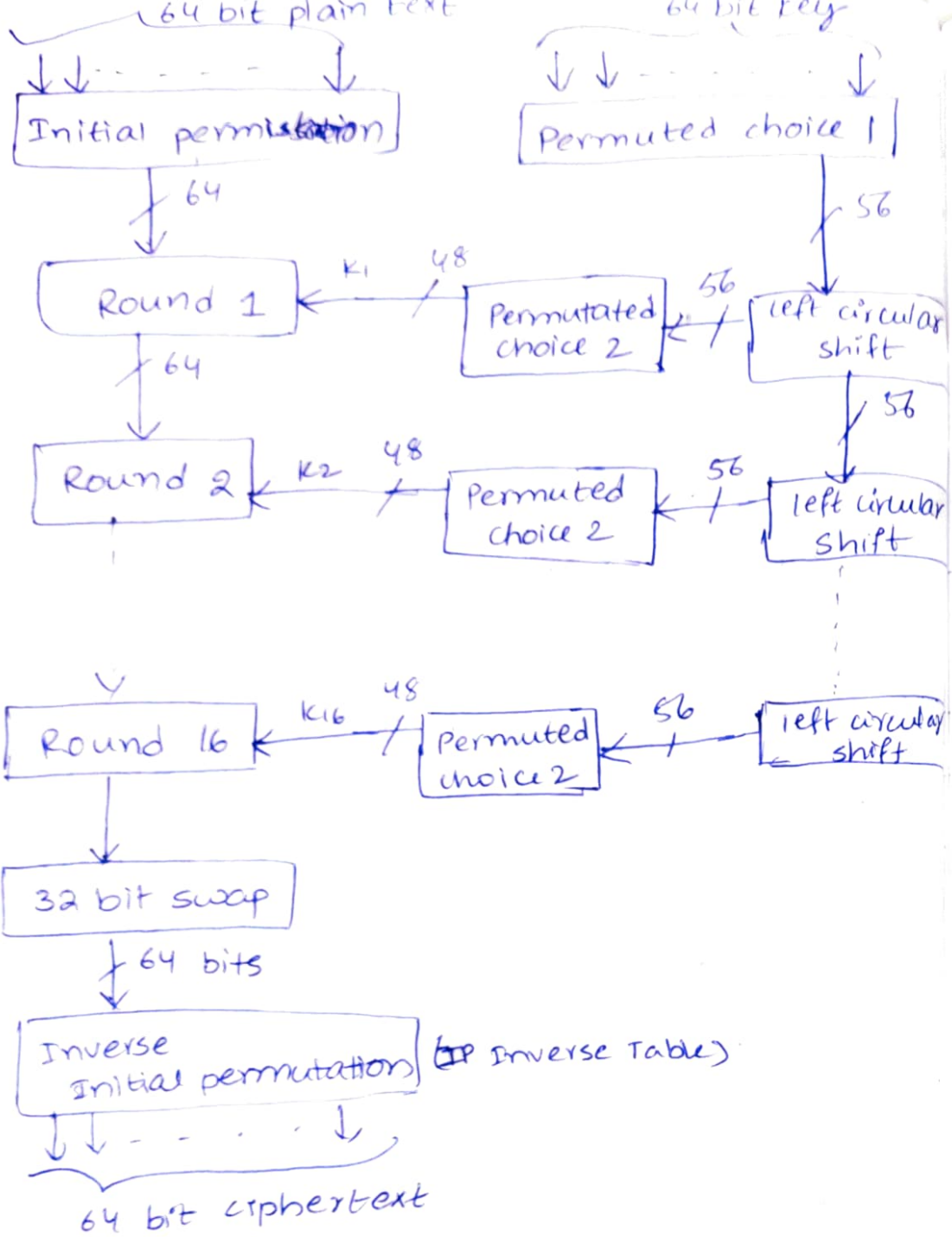
Non-Feistel cipher

→ It uses only invertible components

→ NO compression, no expansion are allowed

1) DES (Data Encryption Standards)

* This is adopted by NIST (National Institutes of Standard Technology) in year 1977
* It works on 64 bit blocks and key is 56 bits



Single Round of DES

Overall processing at each round is

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

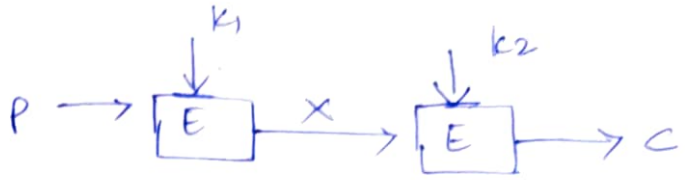
Strength of DES

1) Avalanche Effect
2) completeness.
3) use of 56 bit key.

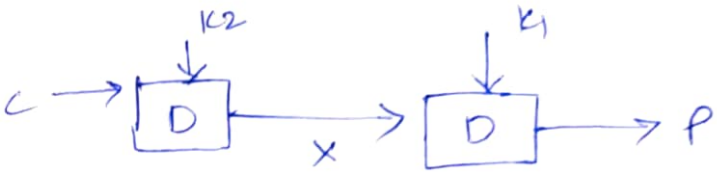
Trying to break the ciphers with all possible ways of keys - Brute force attack.

Double DES

In this algorithm, the encryption takes place for 2 times.



Encryption



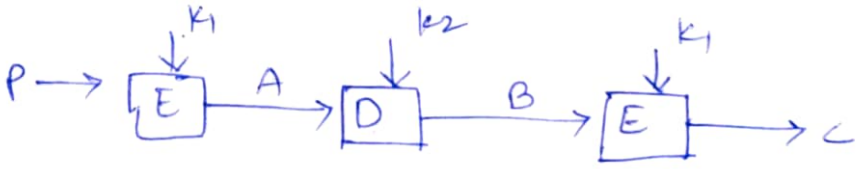
Decryption

$C = E(K_2, E(K_1, P))$

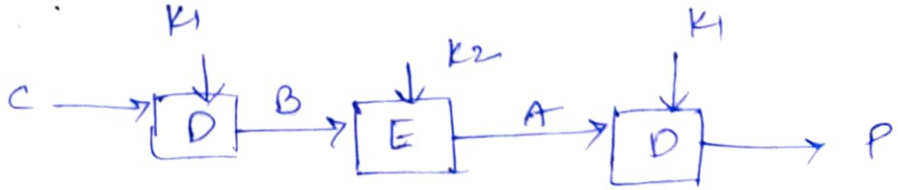
$P = D(K_1, D(K_2, C))$

Key = 56 x 2
= 112 bits.

Triple DES



Encryption.



Decryption.

$C = E(K_1, D(K_2, E(K_1, P)))$

$P = D(K_1, E(K_2, D(K_1, P)))$

2) AES (Advanced Encryption Standard)

* It is developed in year ~~1999~~ 2001 by NIST
* It performs 4 transformations in each and every round except last round
* The plain text is 128 bits
* The key size

No of rounds	key size (bits)
10	128
12	192
14	256

No of round keys = no of rounds + 1

Data units:

In this algorithm 4 data units are used

1. byte – 8 bits of data that can be represented as row matrix or column matrix
2. word
3. block
4. state

1) byte

Byte → $[b_0\ b_1\ b_2\ b_3 \cdots b_7]$ → $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b \\ \vdots \\ b_7 \end{bmatrix}$

b b b

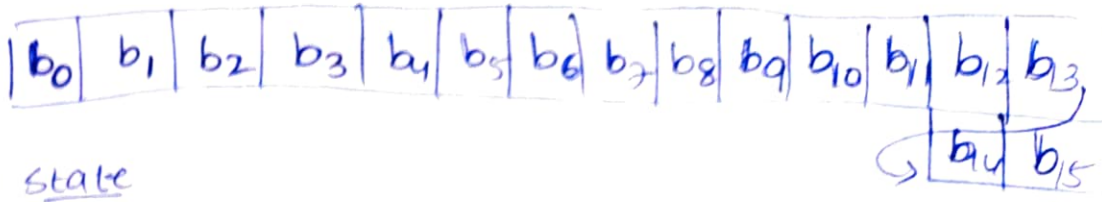
2) word - It is of 4 bytes and can be represented as row matrix & column matrix.

word → $[B_0\ B_1\ B_2\ B_3]$ → $\begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{bmatrix}$

w w w

3) Block - Each block consist of 16 bytes of data

Note:
(b) Bold - byte
(b) Not bold - bit.



4) State

The block is represented in state as 4x4 matrix when the data is transforming from one stage to another stage. The intermediate data is represented as state.

For Example, the plain text AES use matrix if the plaintext is less than 16 characters then refilling characters must be placed

Eg:-

A E S U S E S A M A T R I X Z Z

0 4 18 20 18 4 18 0 12 0 19 17 8 23 25 25

00 04 12 14 12 04 12 00 0E 00 19 11 08 23 19 19

↓

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}_{4\times4}$$

Structure of Each Round

Note-

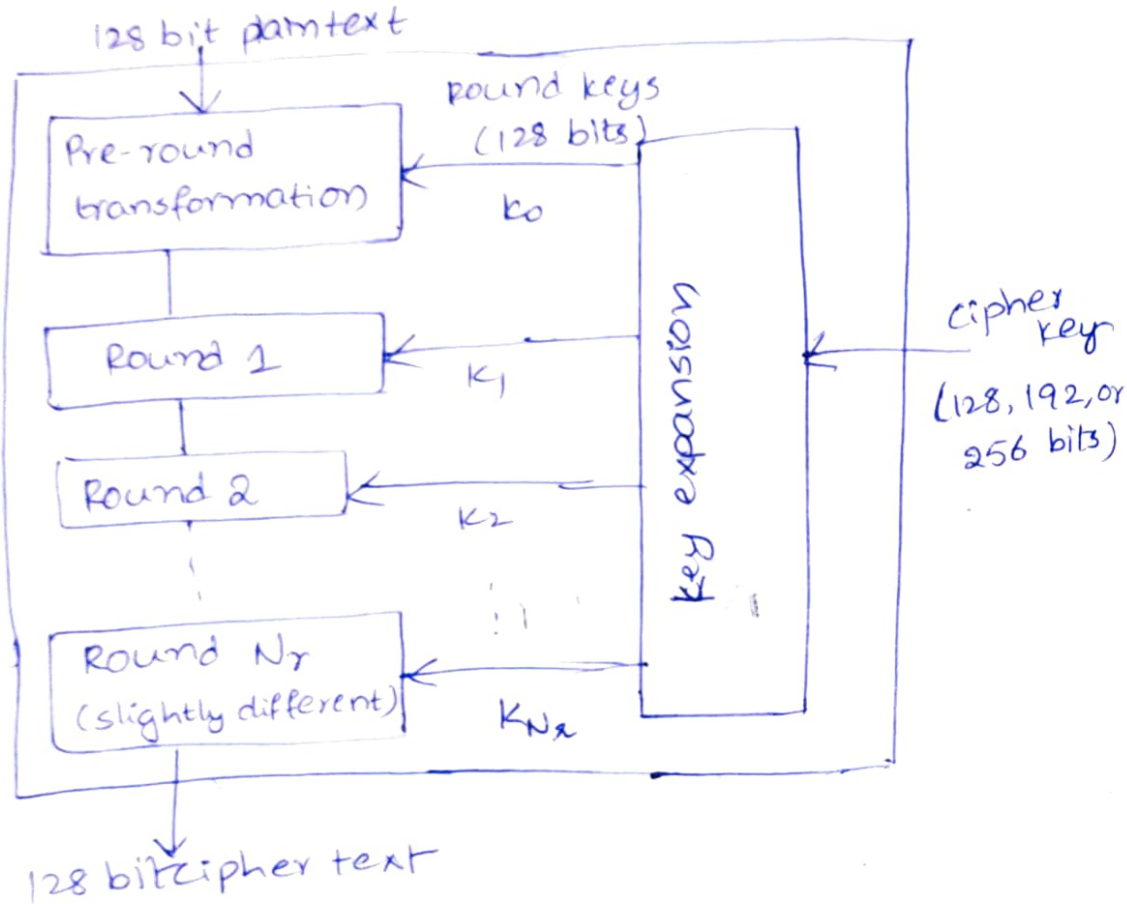
1) One AddRoundKey is applied before the first round

2) The third transformation is missing in the last round (Mix Columns) not there in last round.

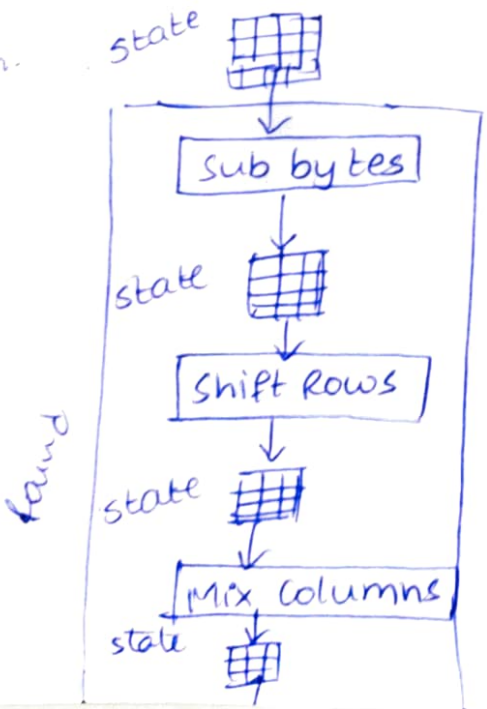
The 4 transformations are

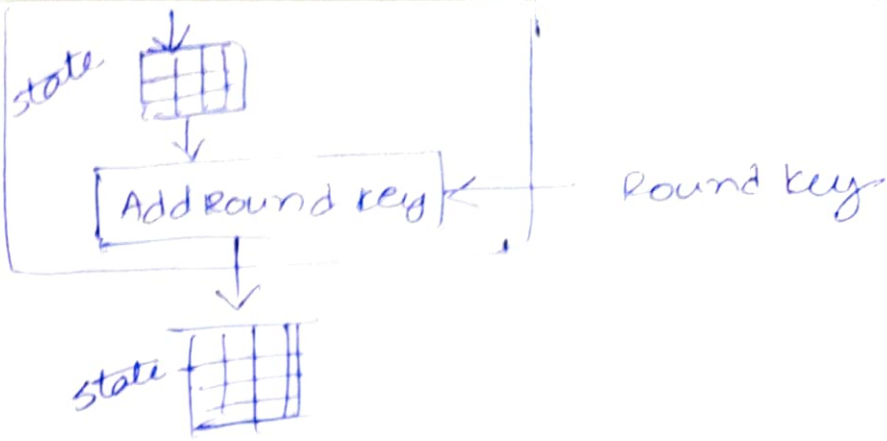
1) Substitute Bytes
2) Shift Rows
3) Mix columns
4) Add Round Key

Structure of AES



Structure of Each round :-





1) Substitution Bytes

In this transformation the bytes are substituted according to the pre-defined table. In the state array. First byte of each element represents row and second byte of each element represents column.

Eg:
$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 63 & 26 \\ C9 & C9 & 7D & D4 \\ FA & 63 & 82 & D4 \end{bmatrix}$$

According to the sub bytes table

2) Shift Rows:

In this the rows of the state matrix will be shifted as left circular manner according to the index. i.e. 0th row - 0 bytes shifts
1st row - 1 byte left shift
2nd row - 2 bytes left shift
3rd row - 3 bytes left shift.

Eg:
$$\begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 63 & 26 \\ C9 & C9 & 7D & D4 \\ FA & 63 & 82 & D4 \end{bmatrix} \rightarrow \begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & 63 & 26 & F2 \\ 7D & D4 & C9 & C9 \\ D4 & FA & 63 & 82 \end{bmatrix}$$

3) Mix Columns:

In this the columns are multiplied with Pre-defined matrix and placed in state array/ matrix.

d)
$$\begin{bmatrix} 63 & C9 & PE & 30 \\ F2 & 63 & 26 & F2 \\ 7D & 04 & C9 & C9 \\ D4 & FA & 63 & 82 \end{bmatrix}$$

↓

$$\begin{bmatrix} 63 \\ F2 \\ 7D \\ D4 \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 62 \\ CF \\ 0C \\ 99 \end{bmatrix}$$

↓

$$\begin{bmatrix} 62 & 02 & 27 & 26 \\ CF & 92 & 91 & 0D \\ 0C & 0C & F4 & D6 \\ 99 & 18 & 30 & 74 \end{bmatrix}$$

4) Addround key:

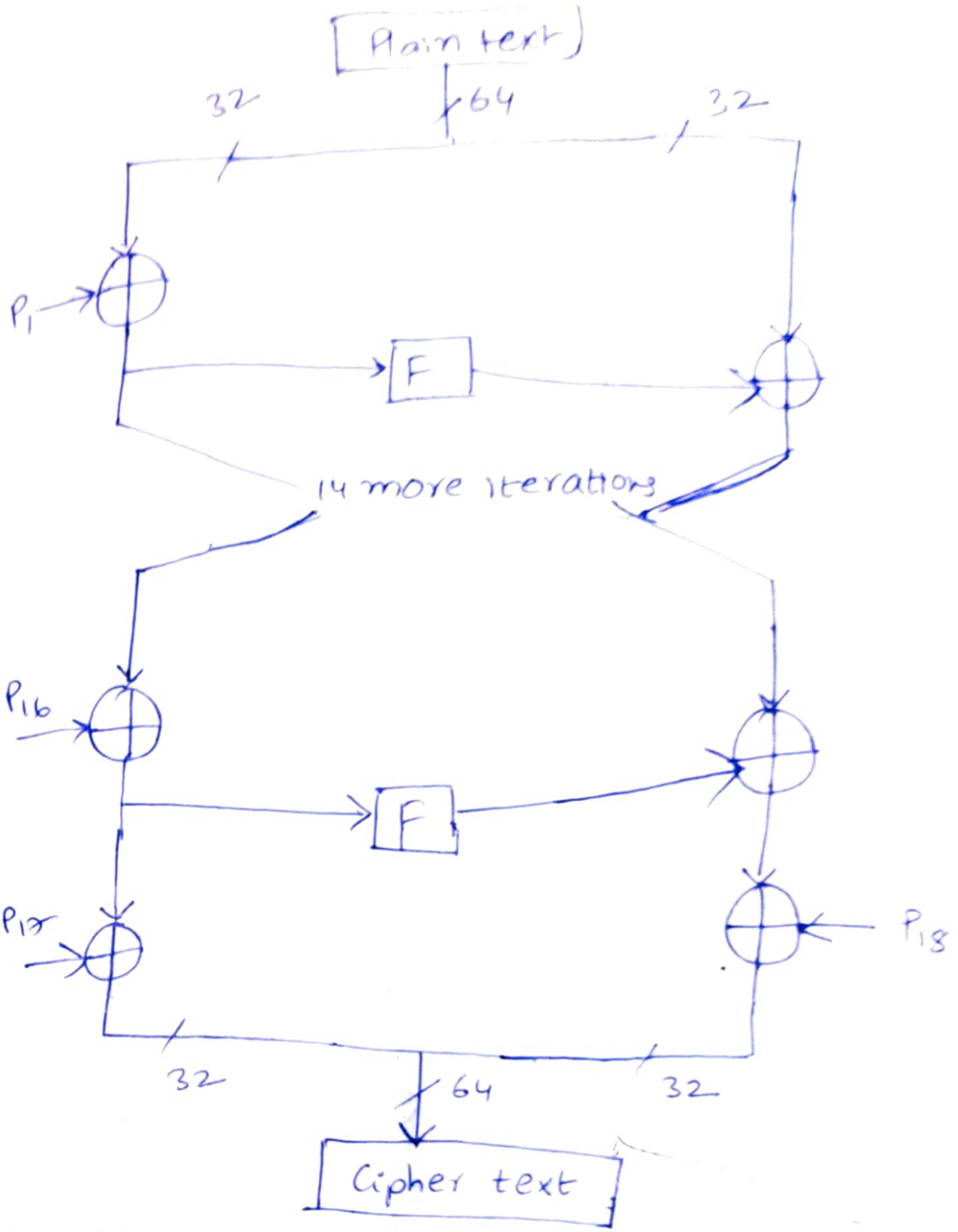
The round key with each column operates on bitwise addition and produces the updated column.

3) Blowfish Algorithm

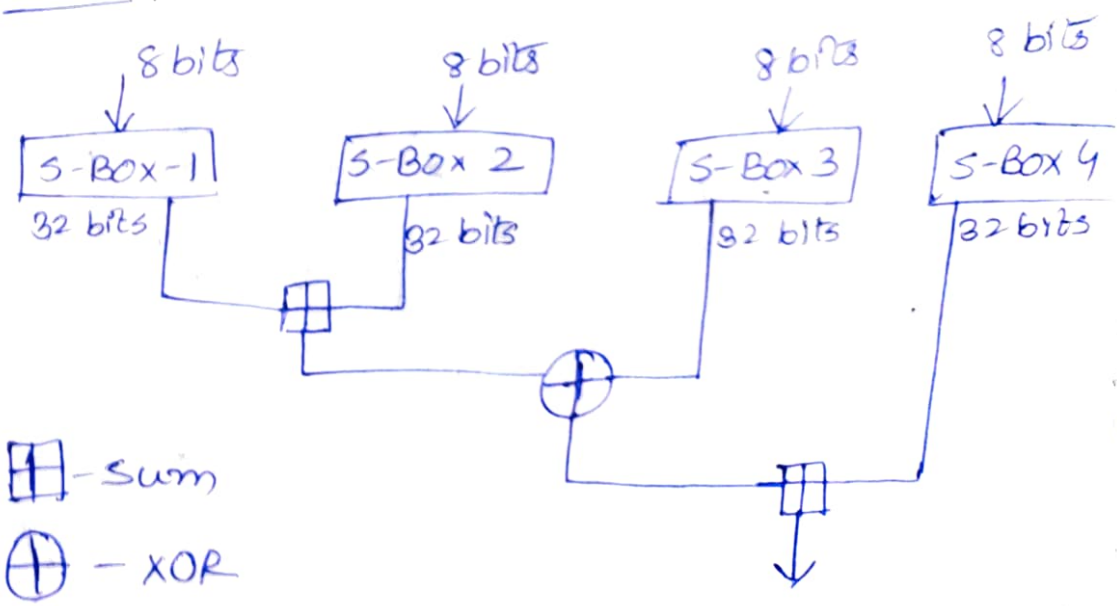
* Designed by Bruce Schneier in 1993
* faster than DES
* It uses feistel cipher structure
* 64 bit plain text key bits varies from 32 bits to 448 bits (Default key = 128 bits)
* No of rounds = 16
* 18 sub keys of size 32 bits are stored in P-array. Eg: P[0], P[1], . . P[17]

It uses 4 S-boxes which takes 8 bit input and produces 32 bit output

Encryption:



Function:



Advantages:

- It is very fast compared to DES and IDEA
- Highly secured
- Best in terms of execution time, avalanche effect and memory usage.

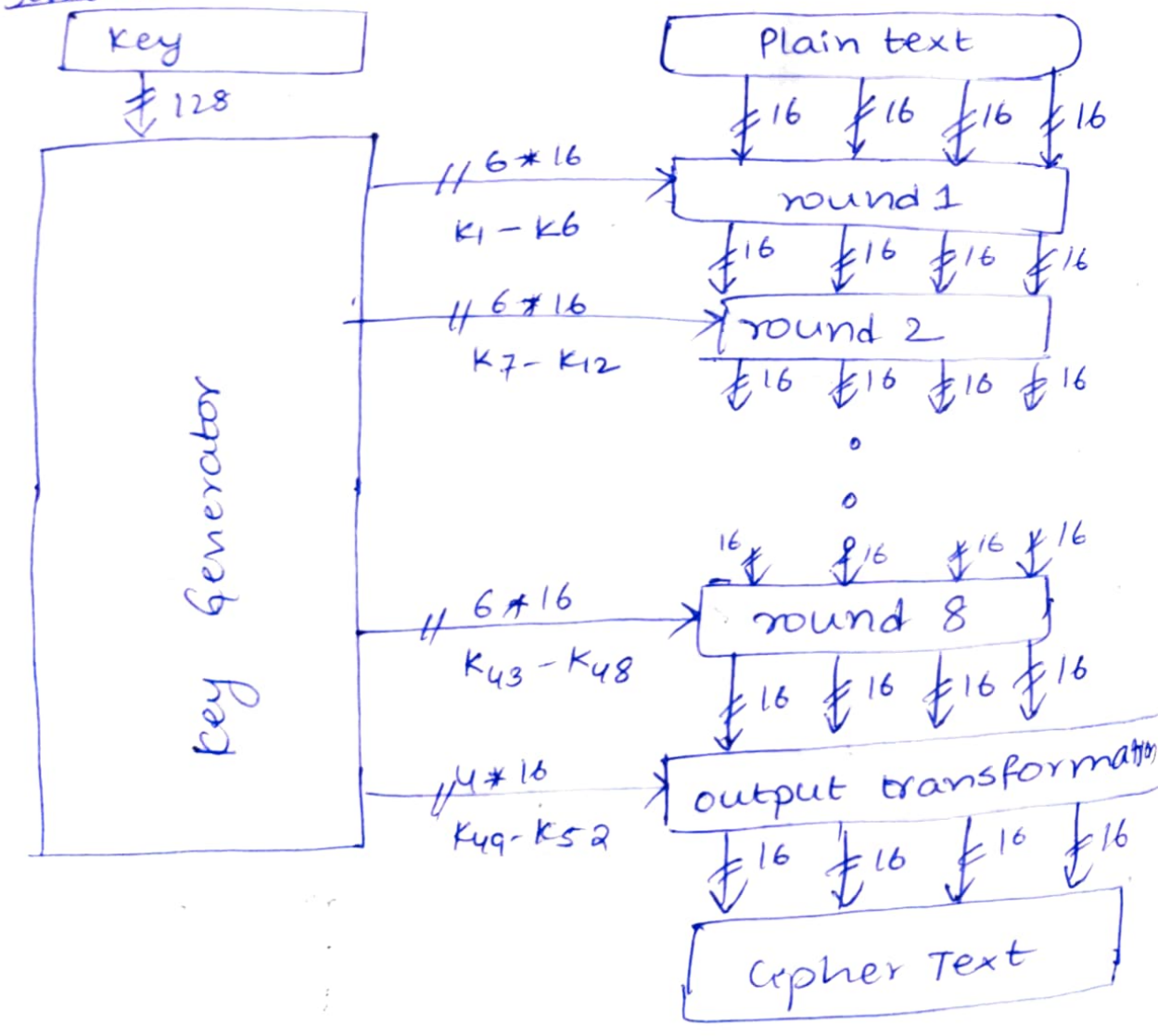
Applications:-

- Password Management (encrypt userid and password).
- Linux uses Blowfish algorithm to keep its file secure

4) IDEA (International Data Encryption Algorithm)

* It uses Feistel cipher structure with 64 bits plaintext and 128 bit key. *
* It has 8 rounds and 6 keys are used in each round

Structure:-



structure

~~4) CAST-128~~

5) CSAT-128

* Symmetric key block cipher and uses feistel structure
* Plain text - 64 bits, key size - 40 to 128 bits (increment of 8 bits)
  Eg: 40, 48, 56, ... 128
* No of rounds = 16
* Two keys used in each round
  1) Kmi (32 bits)
  2) Kri (5 bits)
* It performs 4 operations
  1) Addition (modulo 2^{32})
  2) Subtraction (modulo 2^{32})
  3) EX-OR
  4) circular Left shift operation (<<<)

- Encryption

  Loll R_0 = Plaintext

  for i=1 to 16 do

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus F_i[R_{i-1}, Km_i, Kr_i]$;

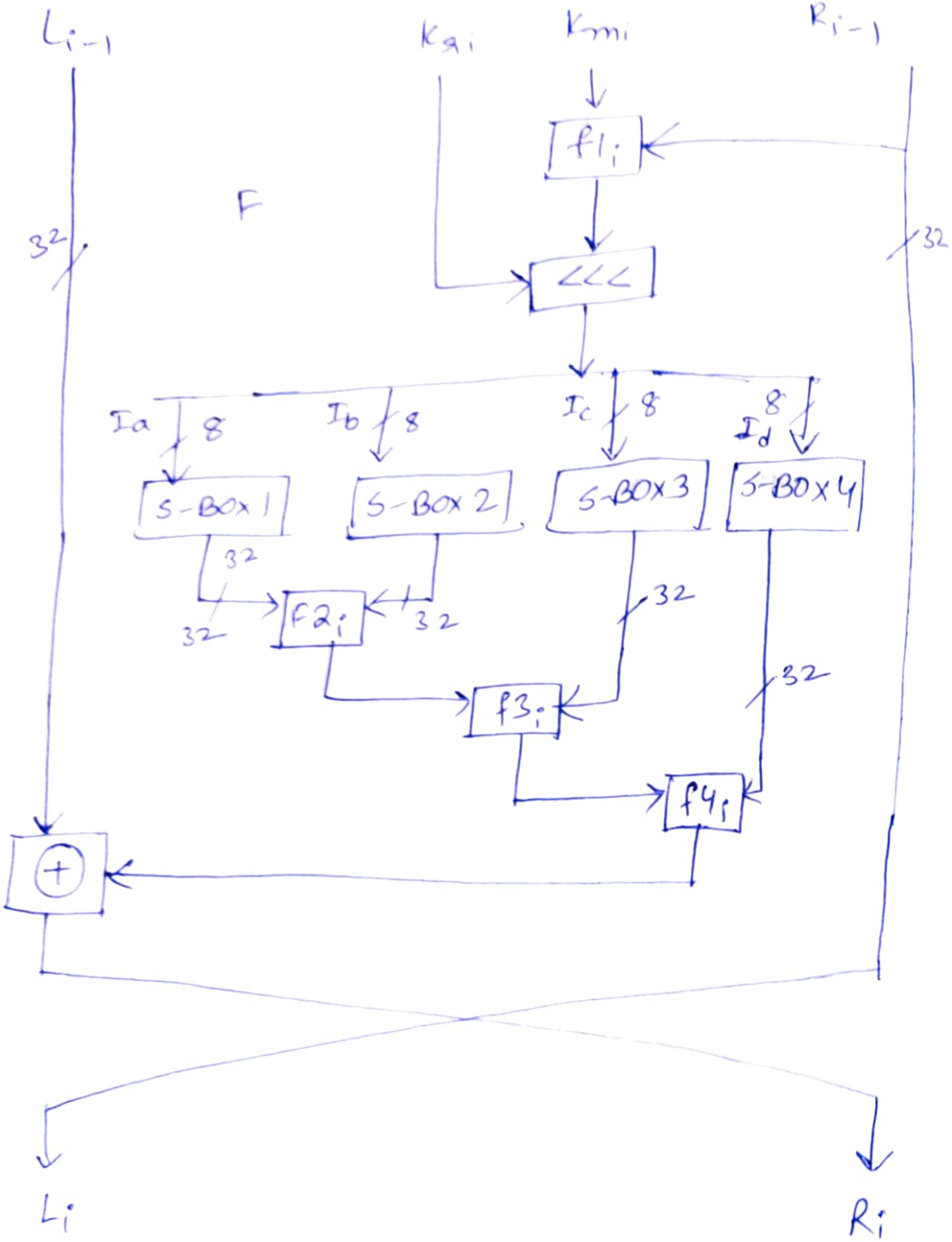
  Ciphertext = $L_{16} \| R_{16}$

- Decryption:
  Same as encryption with keys applied in the reverse order

Feistel Network structure:

64 bit iterated block cipher

12 to 16 rounds


L_{i-1}
K_{ai}
K_{mi}
R_{i-1}
$f1_i$
F
32
<<<
32
I_a 8
I_b 8
I_c 8
I_d 8
S-BOX 1
S-BOX 2
S-BOX 3
S-BOX 4
32
32
32
$F2_i$
32
32
32
$f3_i$
$f4_i$
+
L_i
R_i

The function f and i value varies from set of rounds to set of rounds ~~for rounds 1, 4, 7, 10~~,

FOR Rounds 1, 4, 7, 10, 13, 16

$$I = ((k_{m_i} + R_{i-1}) <<< k_{g_i})$$

$$F = ((((S_1[I_a] \oplus S_2[I_b]) - S_3[I_c]) + S_4[I_d])$$

Rounds 2, 5, 8, 11, 14

$$I = ((k_{m_i} \oplus R_{i-1}) <<< k_{g_i})$$

$$F = ((((S_1[I_a] - S_2[I_b]) + S_3[I_c]) \oplus S_4[I_d])$$

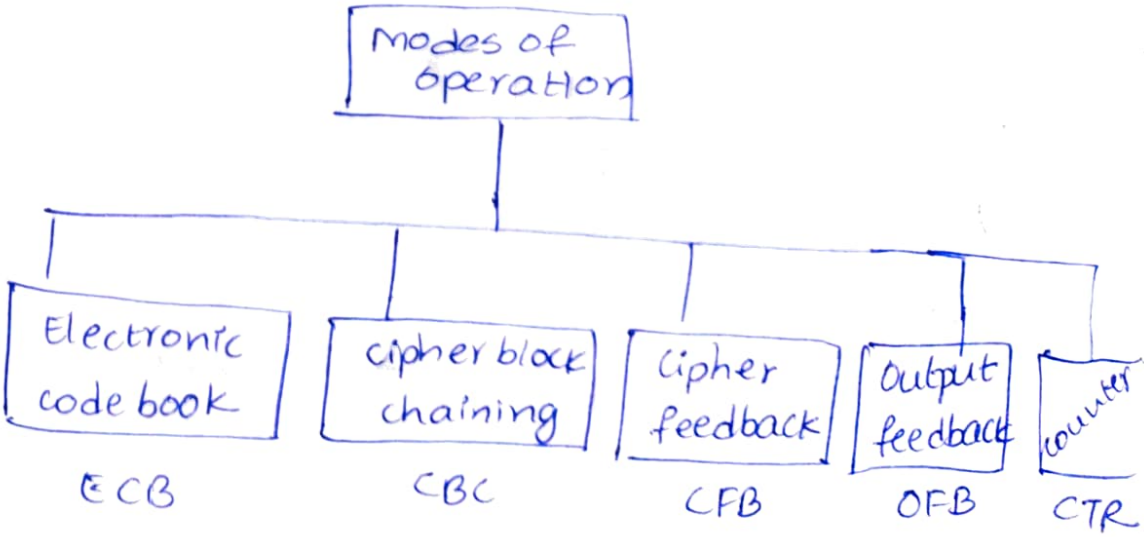
Rounds: 3, 6, 9, 12, 15

$$I = ((k_{m_i} - R_{i-1}) <<< k_{g_i})$$

$$F = [(((S_1[I_a] + S_2[I_b]) \oplus S_3[I_c]) - S_4[I_d])$$

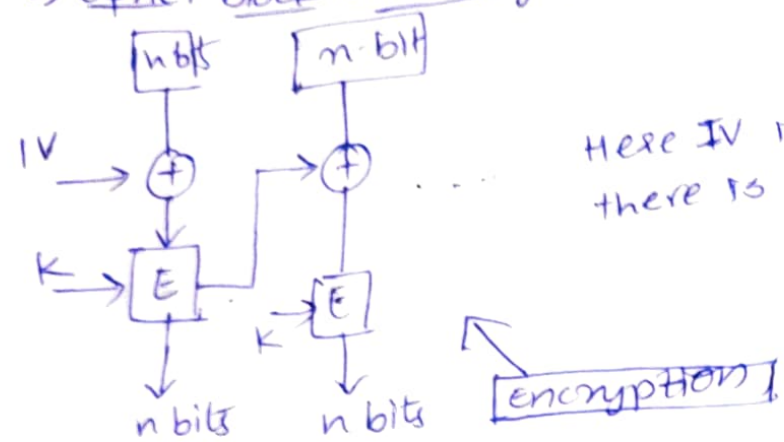
Modes of operations of Block cipher

There are 5 types of modes in block cipher to perform various operations on encryption algorithms.



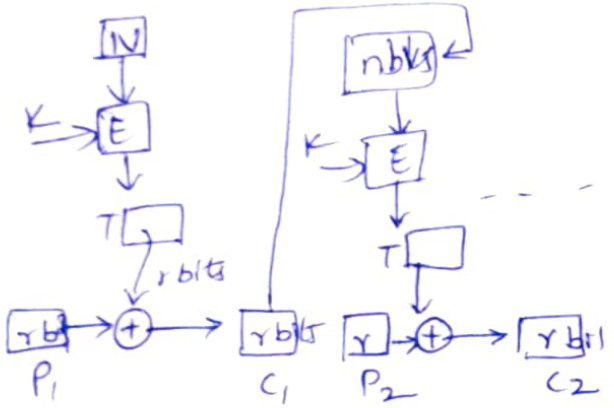
1) Electronic codebook mode (ECB):
symmetric cipher → same key is used for encryption and decryption

2) cipher block chaining (CBC):

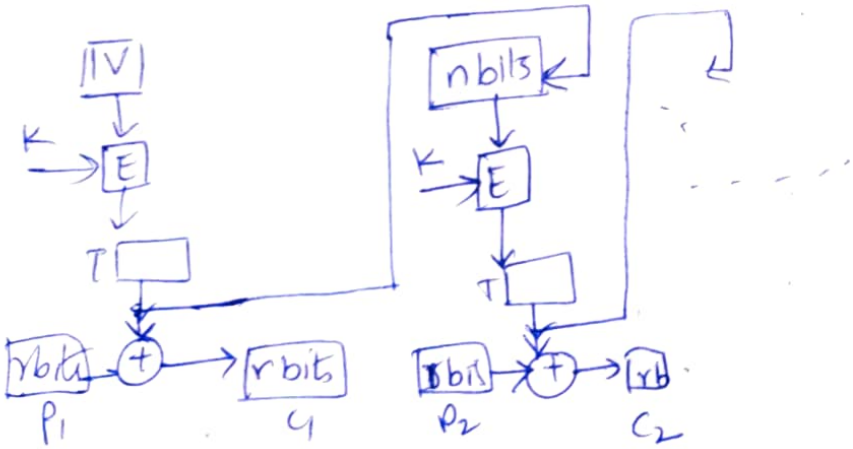


Here IV is initial vector. there is table prefined

3) cipher feedback Mode (CFB)



4) Output Feedback



5) Counter

Based on counter encryption is done.

Unit:3 Mathematics of assymetric key cayptography

Paime numbers

The positive numbers are divided into 3 categories.
1. Number with 1 divisor
2. Numbers with 2 divisors (paimes)
3. Numbers with more than 2 divisors. (composite numbers)

A paime number is a number that is divisible by 1 and itself

Relatively Paime (co-paime) numbers

Two positive integers **a** and **b** are said to be relatively paime if $gcd(a, b) = 1$

Membeas in Z_n^* are co-paimes with number n

Euler's Totient Function / Euler's Phi function [$\phi(n)$]

$\phi(n)$:- This function finds the no.of integers that are smaller than n and relatively prime to n

Let Z_n^* that contains all integers which are less than n and relatively paime to n so $\phi(n)$ represents no.of integers in Z_n^*

Eg:-

Z_{10}^* → Find the $\phi(n)$ for Z_{10}^*

A) $Z_{10}^* = \{1, 3, 7, 9\}$

$\therefore \phi(10) = 4$

→ Find $\phi(n)$ for Z_7^*

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$\phi(7) = 6$

$\rightarrow Z_{13}^{*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$\phi(13) = 12$

Finding the value of $\phi(n)$

1) $\phi(1) = 0$

2) $\phi(p) = p-1$, if p is a prime.

3) $\phi(m \times n) = \phi(m) \times \phi(n)$ If m & n are co-primes.

4) $\phi(p^e) = p^e - p^{e-1}$ If p is a prime.

Example:

① Find the value of $\phi(240)$

A) $\phi(240) = 2^4 \times 3^1 \times 5^1$

$= (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)$

$= 8 \times 2 \times 4$

$= 64$

② Find the value of $\phi(49)$

A) $\phi(49) = 7^2$

$= 7^2 - 7^1$

$= 49 - 7$

$= 42$

Note:

* The difficulty in finding $\phi(n)$ depends on the difficulty of finding the factorisation of n

Modular Arithmetic

In cryptography congruency ($\equiv$) is used and the notation is $a \equiv b \mod n$

Eg: $7 \equiv 1 \mod 2$

when we divide 7 by 2 gives remainder 1

Fermat's Little Theorem

- If p is a prime and a is an integer such that p doesnot divide a then $a^{p-1} \equiv 1 \bmod p$

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

- version 2:

If p is paime and a is integer then

$$\boxed{a^p \equiv a \bmod p}$$

Eg:

① Find the value of $6^{10} \bmod 11 = 1$

$\because (a^{p-1} \bmod p = 1)$

② Find the result of $3^{12} \bmod 11$

A) $3^{12} \bmod 11 = [3^{10} \bmod 11 \times 3^2 \bmod 11] \bmod 11$

$= (3^{10} \times 3^2) \bmod 11 = 1 \times 9 \bmod 11$

$= (3^{10} \bmod 11 \times 3^2 \bmod 11) \bmod 11$

$= (1 \times 9 \bmod 11) \bmod 11$

$= 9 \bmod 11$

$= 9$

③ Find the value of $2^{15} \bmod 17$

The intresting application of this theorem is finding the multiplicative inverse quickly. If the modulus is a prime.

If 'p' is a prime and 'a' is an integer such that p doesnot divide a then

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

Eg1) Find the value of $4^{-1} \bmod 11$.

A)
$$4^{-1} \bmod 11 \equiv 4^{11-2} \bmod 11$$
$$\equiv 4^9 \bmod 11$$
$$= 3$$

Eg2) Find $5^{-1} \bmod 23$

$5 \times 5^{-1} \equiv 1 \bmod$

A)
$$5^{-1} \bmod 23 = 5^{23-2} \bmod 23$$
$$= 5^{21} \bmod 23$$
$$= 14$$

Euler's Theorem

The modulus in Euler's theorem is an integer. It has 2 versions

1) If a and n are co-prime then

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

2) If $n = p \times q$, $a < n$ and 'k' an integer then

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

Eg: (1) prove euler's theorem hold true for $a=3$ and $n=10$

Sol: $\phi(n) = \phi(10) = 4$ $\quad Z_{10}^{*} = \{1,3,7,9\}$

$3^4 \equiv 1 \bmod 10$

$81 \equiv 1 \bmod 10$ (✓)

∴ Euler's theorem holds true for $a=3, n=10$

Eg (2) $a=2$, $n=10$

~~$\phi(n) = \phi(10) = 4$~~

~~$2^4 \equiv 1 \bmod 10$~~

Here 2, 10 are not co-primes

∴ Algorithm doesnot hold true.

Chineese Remainder Theorem

It is used to solve a set of congruent equations with one variable but different moduli. which are relatively prime.

$x \equiv a1 \bmod m1$

$x \equiv a2 \bmod m2$ and so-on

$x \equiv ak \bmod mk$

CRT states that these equations have a unique solution if the moduli are relatively prime.

The steps for finding solution

1) Find $M = m_1 m_2 \cdots m_k$
2) Find $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $\cdots$ $M_k = \frac{M}{m_k}$
3) Find the multiplicative inverse of $M_1, M_2, \cdots M_k$
4) The solution to the simultaneous equation is

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots a_k M_k M_k^{-1}) \bmod M$$

Eg: (1) Find the value of x for the given equations

$x \equiv 2 \mod 3$
$x \equiv 3 \mod 5$
$x \equiv 2 \mod 7$

Sol:

a_1	a_2	a_3	m_1	m_2	m_3	M	M_1	M_2	M_3	M_1^{-1}	M_2^{-1}	M_3^{-1}
2	3	2	3	5	7	105	35	21	15	2	1	1

$M = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$ $\quad M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$ $\quad M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 \times M_1^{-1} \equiv 1 \mod m_1$

$35 \times M_1^{-1} = 1 \mod 3$

$\boxed{M_1^{-1} = 2}$

$M_2 \times M_2^{-1} \equiv 1 \mod m_2$

$21 \times M_2^{-1} = 1 \mod 5$

$\boxed{M_2^{-1} = 1}$

$M_3 \times M_3^{-1} \equiv 1 \mod m_3$

$15 \times M_3^{-1} = 1 \mod 7$

$\boxed{M_3^{-1} = 1}$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \mod 105$

$= (140 + 63 + 30) \mod 105$

$= 233 \mod 105$

$\boxed{x = 23}$

Verification:

$23 \equiv 2 \mod 3$ (✓)
$23 \equiv 3 \mod 5$ (✓)
$23 \equiv 2 \mod 7$ (✓)

140
93
233
105
210
23

(2) Find the value of x for the given equations

$4x \equiv 5 \mod 9$
$2x \equiv 6 \mod 20$

Sol:

$x \equiv a \mod m$

$4x \equiv 5 \mod 9$

$4 \times 4^{-1} x = 4^{-1} (5 \bmod 9)$

$x = 4^{-1} \bmod 9 \times 5 \bmod 9$

$= 7 \times 5 \bmod 9$

$= 35 \bmod 9$

$x \equiv 8 \bmod 9$

$2x \equiv 6 \bmod 20$

$2 \times 2^{-1} x = 2^{-1} (6 \bmod 20)$

$x = 2^{-1} \bmod 20 \times 6 \bmod 20$

$= 2^{-1} \bmod 20 \times 2 \bmod 20 \times 3 \bmod 20$

$x \equiv 3 \bmod 20$

a_1	a_2		M_1	M_2	M_1^{-1}	M_2^{-1}	m_1	m_2
8	3	180	20	9	5	9	9	20

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$20 \times M_1^{-1} = 1 \bmod 9$

$\boxed{M_1^{-1} = 5}$

$M_2 \times M_2^{-1} \equiv 1 \bmod m_2$

$9 \times M_2^{-1} \equiv 1 \bmod 20$

$\boxed{M_2^{-1} = 9}$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$x = ((8 \times 20 \times 5) + (3 \times 9 \times 9)) \bmod 180$

$= (1043) \bmod 180$

$x = 143$

Assymetric key Cryptography

It is also known as public key cryptography in which 1 key is used for encryption and another key is used for decryption.

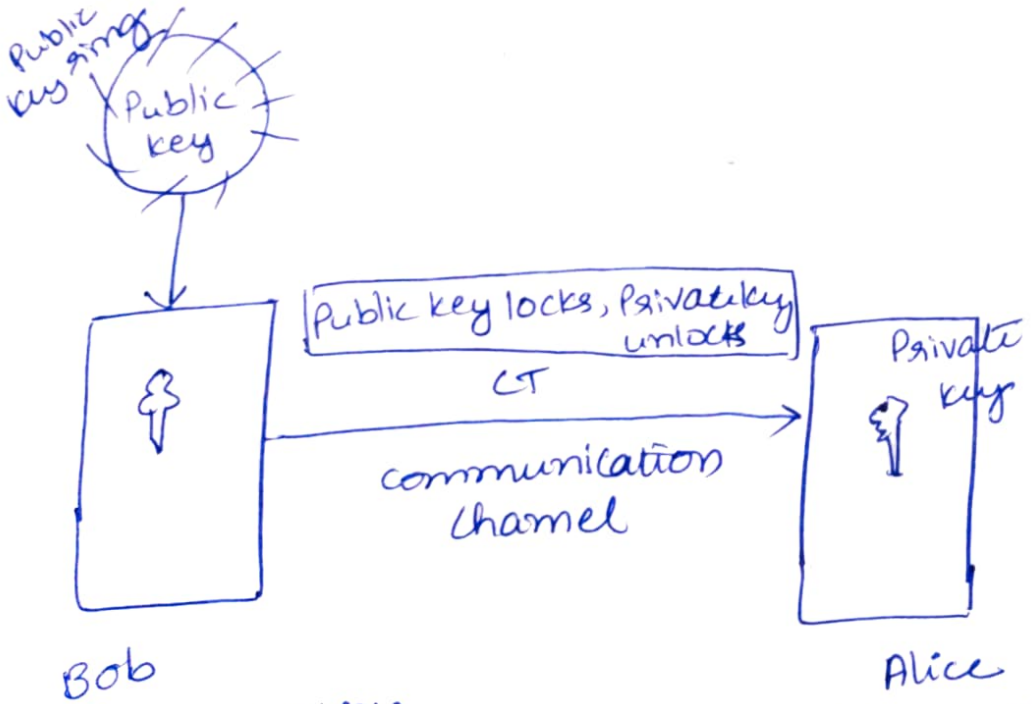
The important characteristics in assymetric key crypto system are

1. Plain text
2. Encryption Algorithm
3. Public key
4. Private key
5. Decryption Algorithm
6. cipher text

Public key:-
This is the key which is shared publicly ~~with~~ to all users in the communication network

Private key:-
Private key is the key that is kept secret.

Public key Cryptosystem



There are 2 approaches for encrypting data in public key cryptosystem.

Approach-1

If Bob(sender) wants to send secret message to Alice. Alice generates pair of keys that is public key and private key (PU_a & PR_a), the public key is shared to Bob through public key distribution sender/channel (KDC)

Now Bob uses Alice Public key to encrypt the plaintext X and produces the cipher text Y

$$Y = E(PU_a, X)$$

upon receiving the cipher text Alice uses her own private key PR_a and decrypts the ciphertext

$$X = D(PR_a, Y)$$

Approach-2

In this approach Bob generates a pair of keys PU_b and PR_b, shares the public key to Alice through KDC

The plain text is encrypted using private key of Bob and produces the cipher text

$$Y = E(PR_b, X)$$

upon receiving the cipher text Alice decrypts the cipher text using public key of Bob

$$X = D(PU_b, Y)$$

1) RSA Algorithm

Rivest, Shamir and Adleman proposed this algorithm in the year 1977

It is based on public key cryptosystem.

The various steps involved in this algorithm are

1. Consider 2 prime numbers p, q
2. Compute $n = p \times q$
3. Compute $\phi(n) = (p-1)(q-1)$
4. Find the value of e such that $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$
5. Consider the plaintext M and encrypt it to produce the ciphertext C

$$C = M^e \bmod n$$

6. For Decryption, compute the value d such that

$$d = e^{-1} \bmod \phi(n) \quad \text{or} \quad d * e \bmod \phi(n) = 1$$

7. After finding value of d cipher text c can be decrypted by

$$M = C^d \bmod n$$

Examples

1) Use RSA algorithm to encrypt the plain text M = 15 and P = 3, Q = 11

A)

$n = 3 \times 11 = 33$

$\phi(n) = 2 \times 10 = 20$

$\gcd(20, e) = 1$ let us take $e = 3$

$C = 15^3 \bmod 33$

$C = 9$

$d = e^{-1} \bmod \phi(n)$ or $d * 3 \bmod 20 = 1$

$d = 7$

$M = C^d \bmod n$

$= 9^7 \bmod 33$

$= 15$

2) Find the cipher text for the given plaintext VVIT by using the values p = 3, q = 11.

A) V V I T

22 22 9 20

$n = 3 \times 11 = 33$

$\phi(n) = 2 \times 10 = 20$

$\gcd(20, e) = 1$ Let us take $e = 3$

$c = 22^3 \bmod 33$ $\quad c = 9^3 \bmod 33$ $\quad c = 20^3 \bmod 33$

$= 22$ $\quad = 3$ $\quad = 14$

∴ Cipher text = 22 22 3 14

V V C N

2) Diffie - Hellman key Exchange Algorithm

→ This is not an encryption algorithm.

→ Used to exchange secret key between sender and receiver by using assymetric key Encryption

→ This algorithm uses public key and private key to generate the secret key

Algorithm:-

Step 1:-

Assume or consider prime number q

Step 2:-

Select α such that α is a primitive root of q, $\alpha < q$.

* Let a is primitive root of P. If $a \bmod p$, $a^2 \bmod p$, $a^3 \bmod p$ and so on $a^{p-1} \bmod p$ gives distinct results from 1 to p-1

Step 3:-

Assume x_A (Private key), $x_A < q_{x_A}$

Step 4:-

calculate y_A (Public key) of user A, ~~$y_A =$~~

~~$y_A = \alpha^{x_A} \bmod q$~~

$y_A = \alpha^{x_A} \bmod q$

Step5:- Assume x_B (private key) $x_B < q$

Step6:- Calculate y_B (Public key)

$$y_B = \alpha^{x_B} \bmod q$$

Note:-
Public key and private key of A = KR_A, KU_A

Public key and private key of B = KR_B, KU_B

Key Generation

A

$$k = y_B^{x_A} \bmod q$$

B

$$k = y_A^{x_B} \bmod q$$

Note:
The values of k at A and B should be same the only we can say that the key exchange is successfu

Example:
Find the secret key at both sides with $q = 11$ using Diffie-Hellman key exchange Algorithm

Sol:

$q = 11$

$\alpha = 2$

Let $x_A = 8$

$y_A = 2^8 \bmod 11$

$y_A = 3$

Let $x_B = 4$

$y_B = 2^4 \bmod 11$

$y_B = 5$

$q = 11$

	1	2	3	4	5	6	7	8	9	10
1										
2	2	4	8	5	10	9	7	3	6	1
3										
4										
5										
6										
7										
8										
9										
10										

A

$k = 5^8 \bmod 11 = 4$

B

$k = 3^4 \bmod 11 = 4$

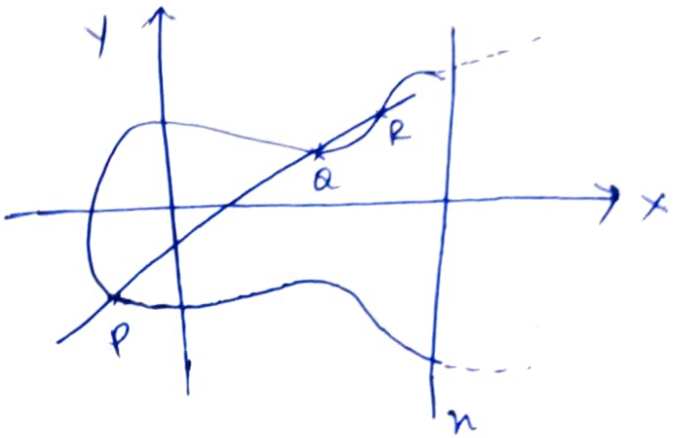
The Encryption and Decryption is done with key value 4.

3) Eliptic curve cryptography (ECC)

→ It is asymmetric ~~key~~ public key cryptography

→ It provides equal security with smaller key size (with 512 bits)

→ It makes use of eliptic curves with cubic equation



$$y^2 = x^3 + ax + b$$

→ It is symmetric to x-axis

→ Let $E_p(a, b)$ be the eliptic curve and consider the equation $Q = kP$ ~~where~~ where k and P are points on the curve and $k < n$

→ If k and P are given it is easy to find Q, but if Q and P are given it is very difficult and complex to find the value of k which is called "discrete logarithm problem" (trapdoor function)

ECC Key Exchange

1) Global public elements

* $E_q(a, b)$ → Eliptic curve with parameters a and b along with prime number 'q'. (or) Integer of the form 2^m

* G → It is a point on the curve whose order is larger value of n

2) User A key generation

1) Select private key $n_A < n$

2) Calculate public key $P_A = n_A \cdot G$

3) User B key generation

1) select private key $n_B < n$

2) Calculate public key $P_B = n_B \cdot G$

4) Calculation of secret key by A

$$K = n_A \cdot P_B$$

5) calculation of secret key by B

$$K = n_B \cdot P_A$$

ECC encryption

1. Let the message be M
2. This message is encoded in the form of point P_M
3. choose a random positive integer k such that cipher point $C_m = \{kG, P_m + kP_B\}$

ECC Decryption

* There are 2 steps in decryption process

1) Multiply 1st point in the pair with receiver's private key

$$kG * n_B$$

2) subtract the result from second point

$$= P_m + kP_B - (kG * n_B)$$

$$= P_m + kP_B - kP_B$$

$$= P_m$$

Ex: Let $E_q(a, b) = E_{11}(1, 6) - y^2 = x^3 + ax + b$

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

y	$y^2 \bmod p$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

x	$(x^3+ax+b) \bmod p$	
0	6	$(0^3+1\times0+6) \bmod 11$
1	8	$(1^3+1\times1+6) \bmod 11$
2	5	
3	3	
4	8	
5	4	
6	8	
7	4	
8	9	
9	7	
10	4	

∴ The points $E_1(1,6)$ are

$(5,2)$ $(7,2)$ $(10,2)$ $(8,3)$ $(8,8)$ $(2,4)$ $(2,7)$ $(3,5)$ $(3,6)$

1) Elliptic curves over real numbers

Eliptic curves is not ellipse but it uses a cubic equation such as

$$y^2 = x^3 + ax + b$$

To plot a curve for this equation, y should be computed

$y = \sqrt{x^3+ax+b}$ for all a and b it gets positive and negative values

Rules for addition

1. In the given curve, if any 3 points are joined by a straight line then sum of 3 points is 0

Therefore, $P+O = P$

2. If point P is (x_p, y_p) then negative of P is represented as $-P = (x_p, -y_p)$

2) Eliptic curve over prime numbers (Z_p)

In this the curve is also called as prime curve and the cubic equation contains set of

variables and coefficients with values 0 to p-1 and calculations are performed with mod p operation

The cubic equation is

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

Rules for addition

1. $P + O = P$, where O is additive identity
2. $P = (x_p, y_p)$ and $-P = (x_p, -y_p)$
3. $P + (-P) = O$

3) Eliptic curve over GF (Galois feeld) 2^m

Elements are upto 2^m and cubic equation is

$$y^2 + xy = x^3 + ax^2 + b$$

Rules for addition

1. $P + O = P$
2. $P = (x_p, y_p)$, $-P = (x_p, x_p + y_p)$

(4) Elgamal Encryption

→ It is an asymmetric key encryption and is based on discrete logarithm problem

→ It was proposed by the scientist Elagam in the year 1985

→ If p is a large prime, e_1 is primitive root in the group $G = \langle Z_p^*, X \rangle$ is an integer then $e_2 = e_1^a \bmod p$ and is easy to compute but if e_2 is given with p, it is infeasible to calcula a. where,

$e_1 = \log_{e_1} e_2 \bmod p$

→ This is mainly used in Digital Signatures

Key Generation

1. Select a large prime no p
2. select d a member of set of all primes with multiplication operation $G = \langle Z_p^*, \times \rangle$, such that $1 < d < p-2$.
3. select e_2 primitive root in G
4. calculate $\boxed{e_2 = e_1^d \bmod p}$

Public key = $\{e_1, e_2, p\}$

Private key = $\{d\}$

Encryption

1. Select a random integer r in $G = \langle Z_p^*, \times \rangle$
2. $C_1 = e_1^r \bmod p$
3. $C_2 = (PT \times e_2^r) \bmod p$ then

Cipher text is C_1 and C_2

Decryption

1. $PT = \left[C_2 (C_1)^d)^{-1}\right] \bmod p$

Security of Elgamal Algorithm

1. Low modulus attack
2. known plain text attacks

Example

Find the cipher text for the given prime number $p = 11$, $d = 3$, $r = 4$ and $PT = 7$

Sol:-

Step 1:- $p = 11$

Step 2:- $d = 3$

Step 3:- $e_1 = 2$

Step 4:-

$$e_2 = e_1^d \bmod p$$

$$= 2^3 \bmod 11$$

$$e_2 = 8$$

Public key: {2, 8, 11}

Private key: {3}

Encryption

$PT = 7$

$r = 4$

$$C_1 = e_1^r \bmod p$$

$$= 2^4 \bmod 11$$

$$C_1 = 5$$

$$C_2 = (PT)\, e_2^r \bmod p$$

$$= (7 \times 8^4) \bmod 11$$

$$= 28 \bmod 11$$

$$= 6$$

Decryption

$$PT = \left[C_2 (C_1^d)^{-1} \right] \bmod p$$

$$= \left[6 (5^3)^{-1} \right] \bmod 11$$

$$= \left[6 \times 125^{-1} \right] \bmod 11$$

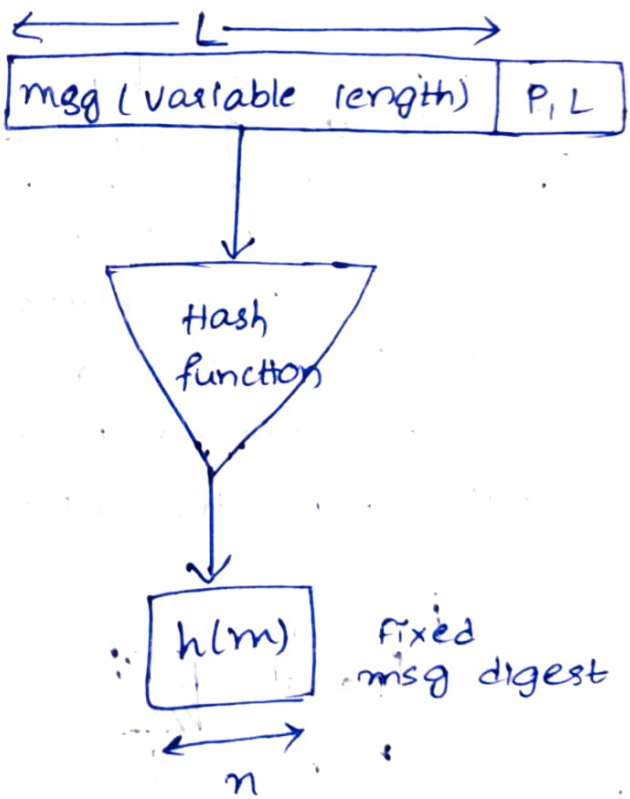
$$= [6 \times 3] \bmod 11$$

$$= 18 \bmod 11$$

$$= 7$$

Unit 4 :- Hash Function

- A cryptographic hash function is an algorithm in which it takes a message of variable length and creates a message digest of fixed length.
- A hash function H accepts a variable length block of data M as input and produces a fixed size hash value $h = H(M)$
- Services provided by Hash function are Data Integrity and Authentication.
- The input for cryptographic hash function is padded out to an integer multiple of some fixed length (1024 bits) and the padding includes the value of the length of the original message in bits.



- The two services that are going to be provided through the hash function are.
  1. Message Authentication
  2. Message Integrity.

1. Message Authentication:

It is a mechanism or services that ensure that the data has been sent by the authenticated user.

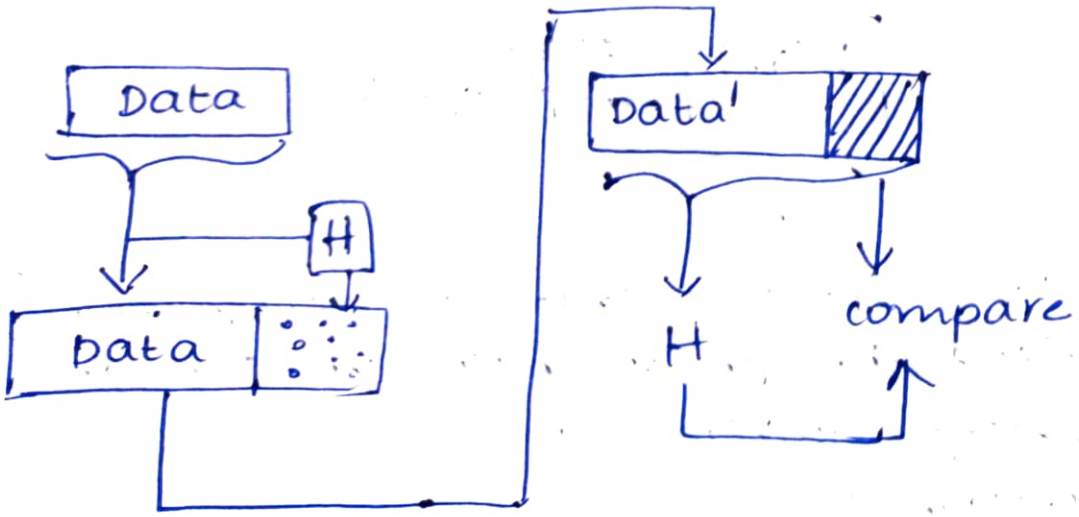
When a hash function is used to provide message authentication, the hash function value is reffered as message digest

~~The ha~~

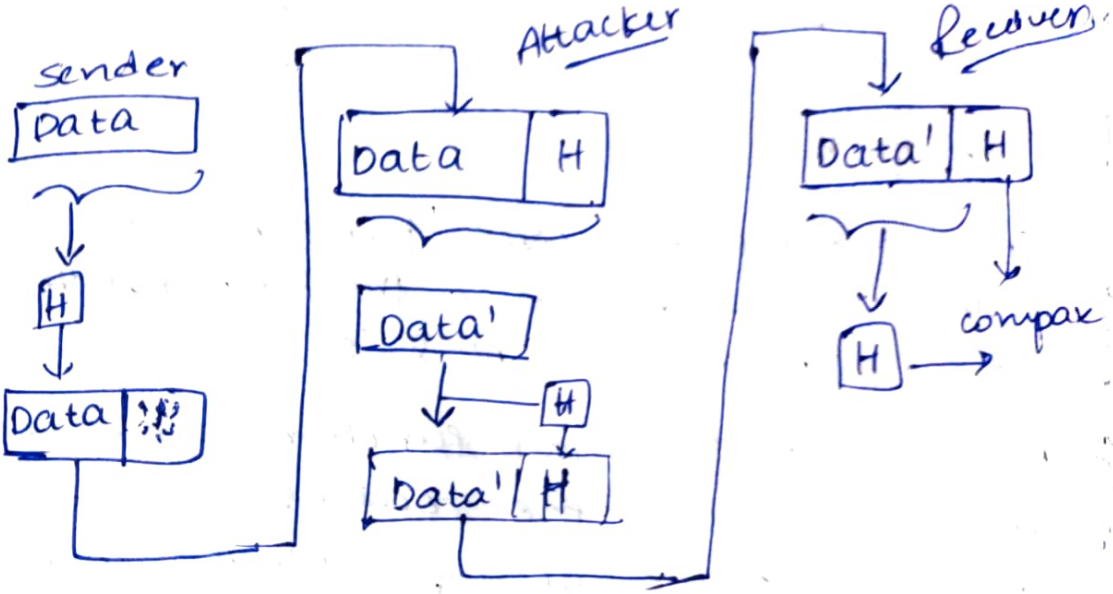
2. Message Integrity:

The hash function provides message Integrity which ensures that the data is not altered or modified by any other users in the transmission.

Let sender A computes the hash value and concatenates to the original ~~string~~ message and transmits to the receiver B. Now the receiver computes hash function upon receiving the data and compares to the received hash functi If mismatch takes place, the data has modified



The hash value must be transmitted in a secure manner because there are high chances for the attack called man-in-middle attack in which the attacker receives the data (in the middle of the transmission), modifies the data and computes the new H value, in order to fool the receiver

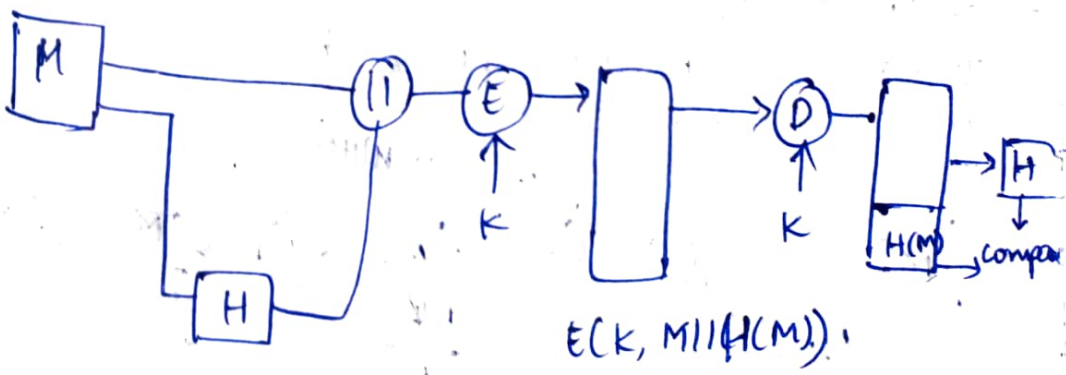


The no. of ways to ~~provide~~ protect the hash code from various attacks are

1st approach

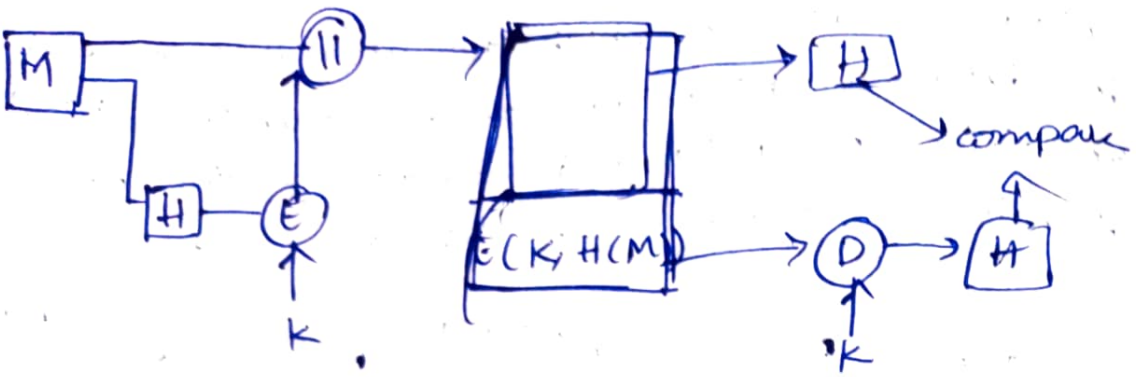
the msg and hash code are encrypted using symmetric key encryption.

~~Only the hash value is encrypted using the key encryption~~



2nd approach

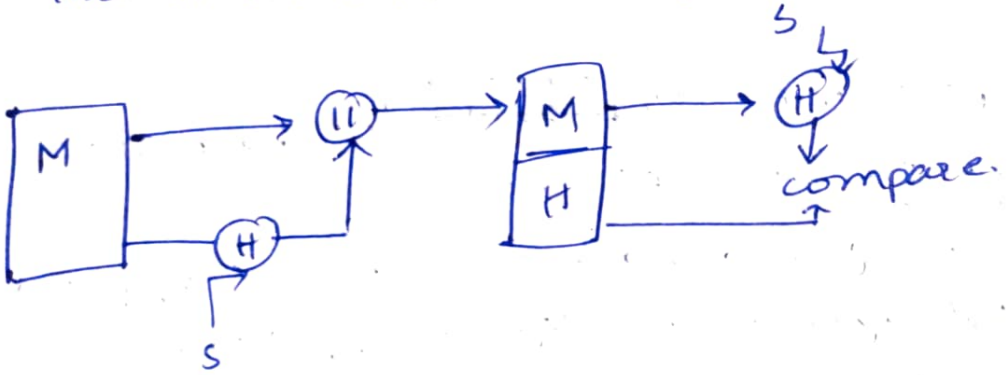
- only the hash value is encrypted using the key encryption



3rd approach

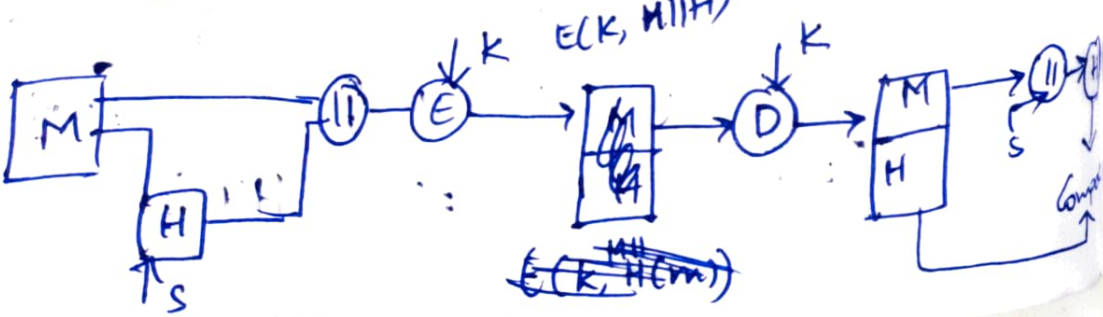
→ The sender and receiver shares a secret value 's' and performs the hash function along with message 'M' & 's'

- After computing hash function sends to the receiver and the receiver computes the h with the message received ands



4th approach

- Confidentiality can be added to the approach of method c by encrypting the entire message + hashcode



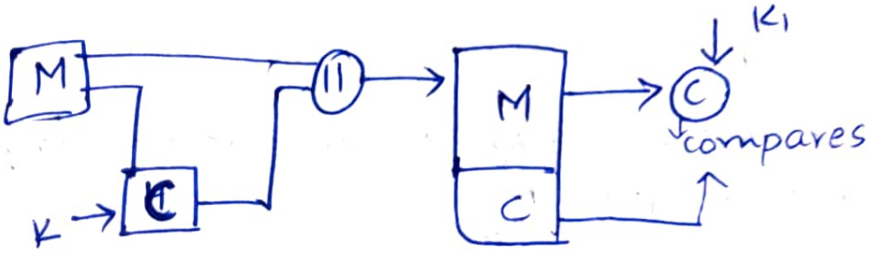
Message Authentication Code:

or,

Data Authentication code: (MAC or DAC)

This is one of the approaches for providing authentication. It acts as an authenticator the input for MAC is variable length message M and secret key K. The output of MAC is cryptographic check sum C

$$MAC = C(K, M)$$



Here, authentication is acheived but not confidentiality ie. No security of Data.

Therefore, encrypting the message using symmetric key encryption

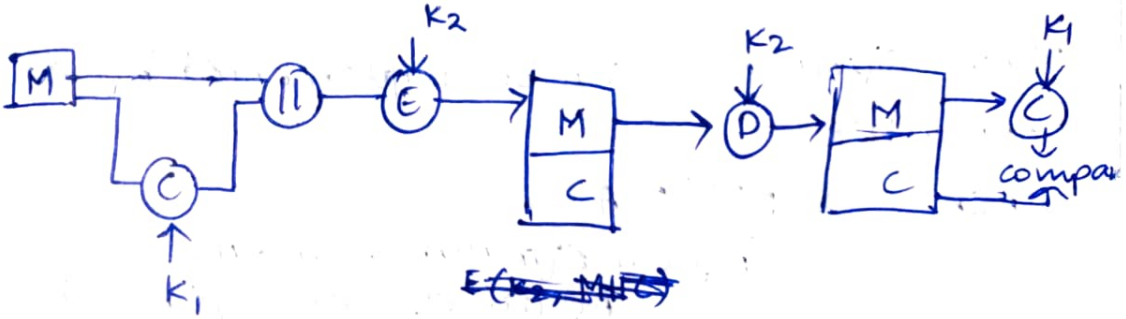
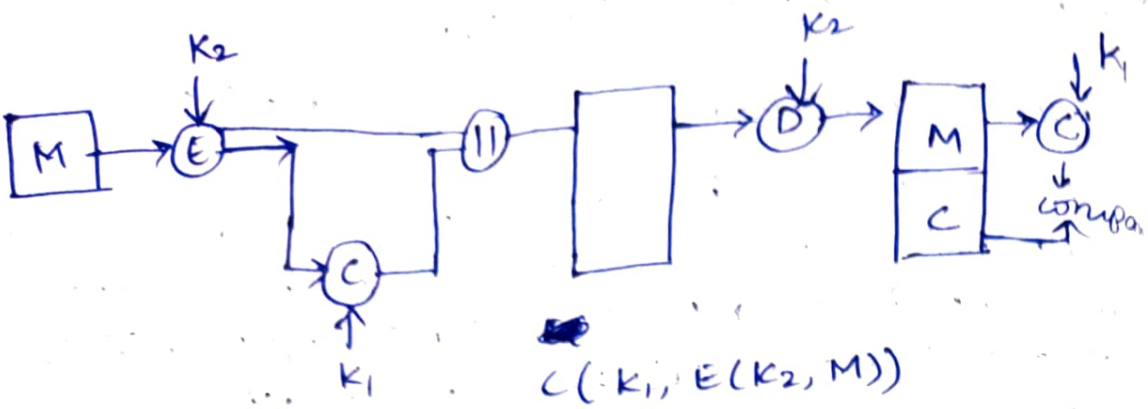


figure: Authentication and confidentiality tier 2 plain text.

3rd approach

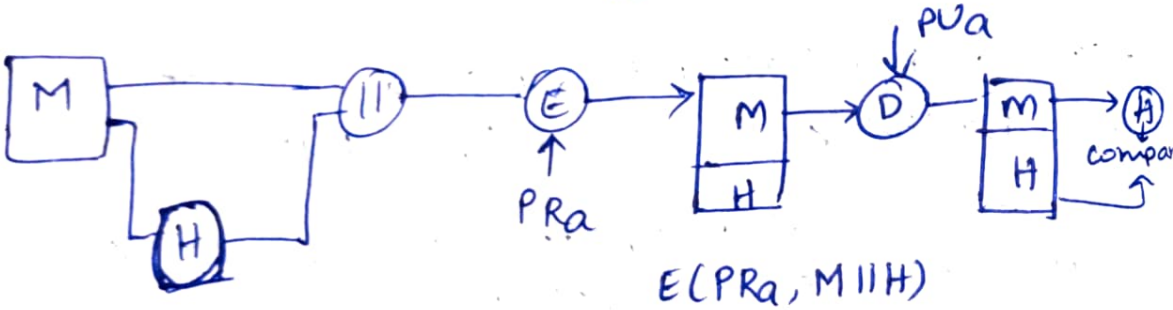
Authentication and confidentiality Tier 2 Cipher text



The application of hash function is "Digital signature"

Digital Signature

The part of the message is encrypted using sender's private key (PR_a)

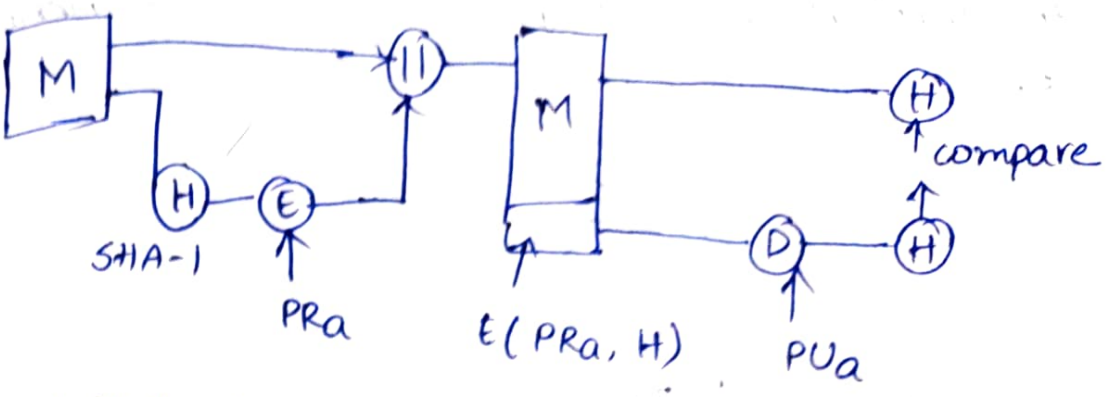


Digital signatures can be implemented by 2 approaches

1) RSA 2) DSS/DSA
(Digital signature standard/
Digital signature Algorithm)

Digital signature through RSA

The hash function has been applied to the message by using SHA algorithm and then it is encrypted using RSA algorithm and finally concatenated to the message, transmits to receiver



Digital signatures through DSA/DSS -

In this algorithm the message M and the hash function H is ~~retri~~ computed by using some hash functions and produces the hash code 'm'

This algorithm has 2 important components namely, signing and verifying.

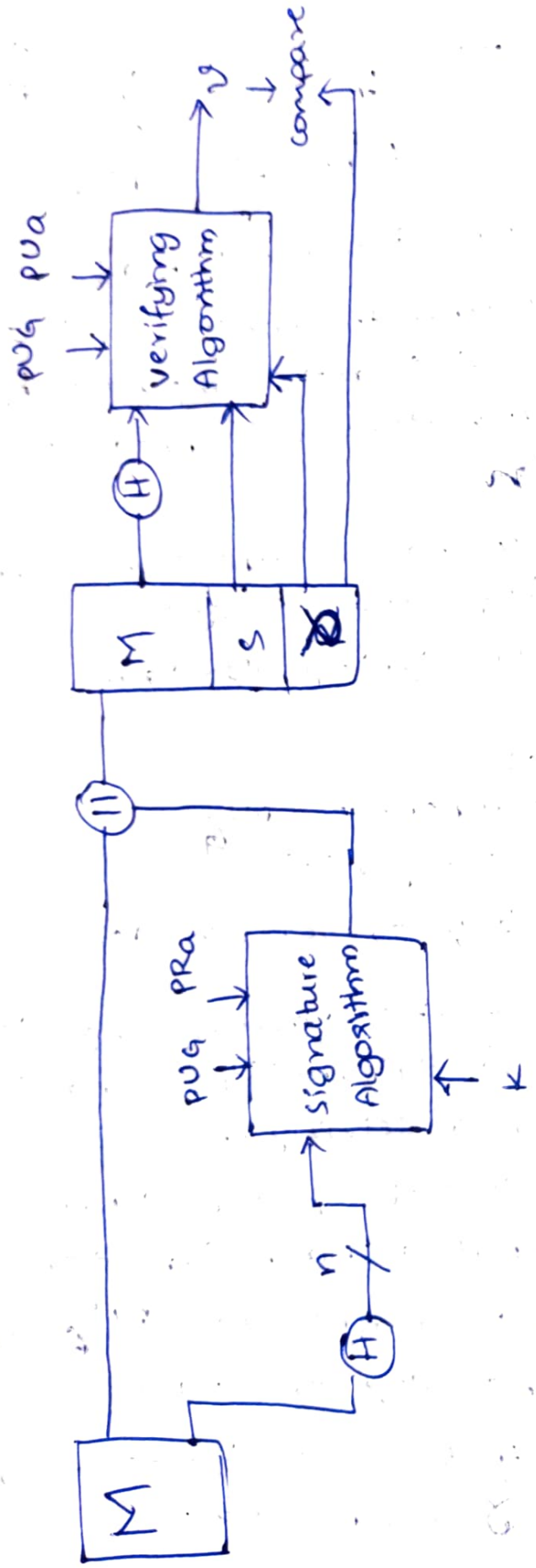
The input to signing algorithm or signature algorithm is

1) Hash code
2) Public component (PU_q)
3) Random integer (k)
4) Private key of sender (PRa)

The output of the signature algorithm is concatenated to the message and sends to receiver, upon receiving the receiver implements verifying algorithm with inputs 1) computed hash function (H)

2) Public component (PU_q), ~~Public~~
3) Public key of sender
4) Output of the signature algorithm - S, ~~S~~ components.

After implementing the verifying algorithm the output V is compared with component R.



Global
Public
key components

p - A prime number where $2^{L-1} < p < 2^L$ with $512 < L < 1024$ bits where L is a multiples of 64

q - A prime divisor of p-1 where $2^{159} < q < 2^{160}$ bit length of 160 bits

$g = h^{(p-1)/(q)} \bmod p$,
h is any integer with $1 < h < p-1$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private key

x - a random or pseudo random integer with $0 < x < q$

User's Public key

$y = g^x \bmod p$

User's per message session Value / Secret Value

k - random or pseudo random integer with $0 < k < q$

Signing Algorithm

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1}(H(M) + xr)] \bmod q$

Signature = (r, s)

Verifying Algorithm

$w = (s')^{-1} \bmod q$

$u_1 = [H(M').w \bmod q] \bmod q$

$u_2 = [(r')w] \bmod q$

$v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$

TEST $v = r$

Secure Hash Algorithm (SHA)

Developed by NIST, also called as SHS

The various versions of this algorithm are

SHA-1, SHA-256, SHA-512, etc...

~~SHA-256, SH~~

SHA-512

The input is processed as 1024 bits at a time in order to produce message digest of 512 bits

Let the message M with length L bits is not multiple of 1024 bits then padding takes place

Let M be the message and P be the padding bits then

$$|M|+|P|+128 = 0 \bmod 1024$$

$$|P| = (-|M| - 128) \bmod 1024$$

Ex:

Find the no of padding bits for the message of length 2590

A)

$M = 2590$

$P = ?$

$$P = (-M - 128) \bmod 1024$$

$$= (-2590 - 128) \bmod 1024$$

$$= -2718 \bmod 1024$$

$$= -670$$

$$= 1024 - 670$$

$$= 354 \text{ bits.}$$

1) The message M should be multiples of 1024 bits

2) It has 8 buffers/registers with 64 bit each. (Hexadecimal)

3) In this algorithm a word is considered with 64 bits from the message M

4) Each round uses additive constant k_t, where $0 <= t <= 79$ indicates one of the 80 rounds.

MD_5

This is one of the hashing algorithms. In which it produces 128 bit message digest

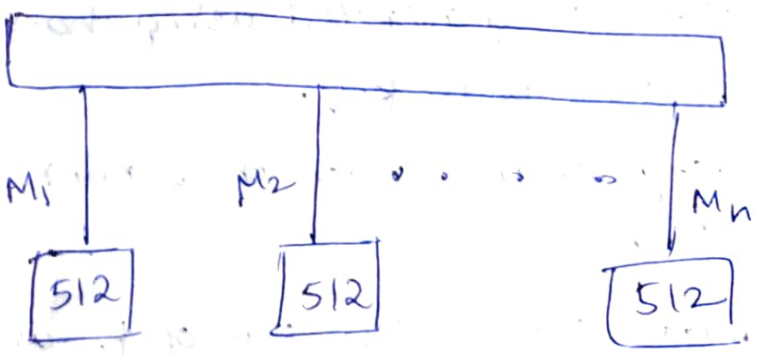
Developed by Rivest

Working of MD_5

1. Padding: padding up of bits in order to make multiples of 512

2. Appending the original length of the message before padding

3. Dividing: Dividing each block into 512 bits



4. Initializing: Four chaining variables A, B, C, D with predefined values

5. Divide 512 bit blocks into 16-32 bit blocks

Has 4 rounds in which every round has the input of additive constant K, four variables A to D and 16 blocks in every round A, B, C, D values are calculated

RIPEMD (Race Integrity Primitives Evaluation Message Digest)

- Designed by Open research community in year 1996. It
- has various versions namely RIPEMD 128, RIPEMD-160, 256 bit etc..

- Block size is 512 bit
- No of rounds = 8

Various algorithms in MAC

MAC can be implemented through 2 algorithms

1) Hash based MAC (HMAC)
2) CMAC (Cipher Message Authentication Code)

1) HMAC

The checksum is generated using hash algorithm along with key.

K - The key shared between sender and receiver

K^+ - padds 0's on left side of K until the length becomes 'b' bits

b - no. of bits in a block. this algorithm has 2 predefined bits namely

ipad - 00110110 (36 in Hexadecimal)
opad - 01011100 (5C in Hexadecimal)
predefined

Samanvita

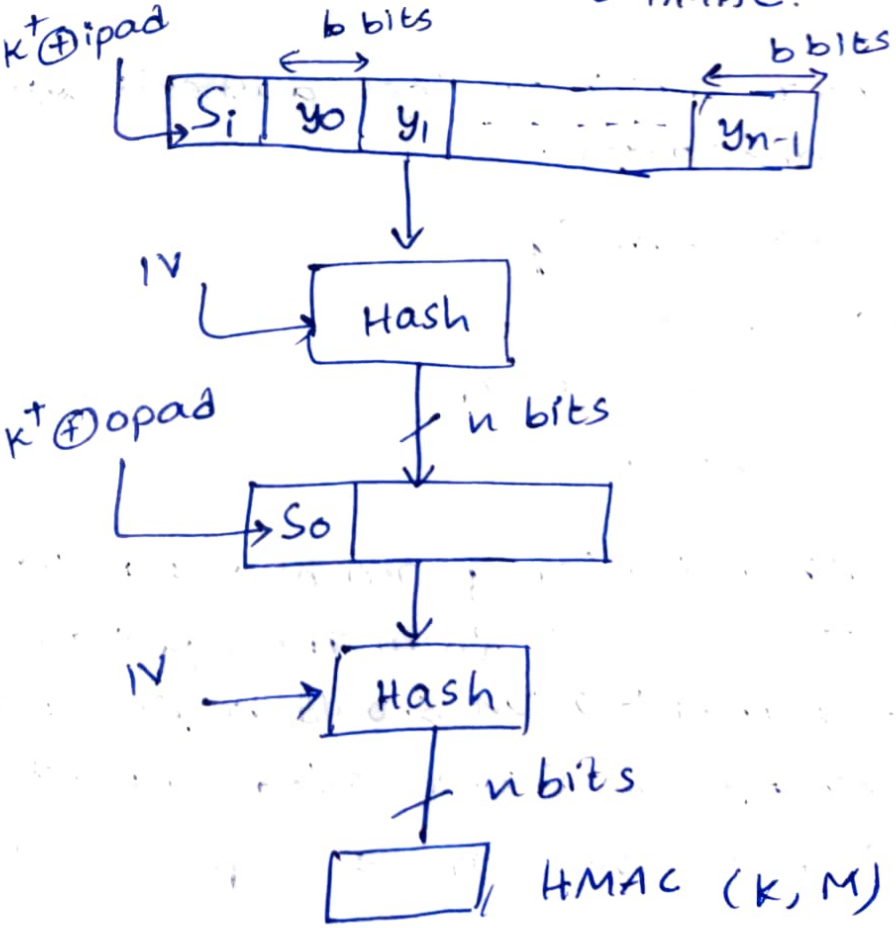
$S_i = K^+ \oplus$ ipad (b-bits)

Step1: The message is divided into blocks with b bits each and S_i is appended before the message.

Step2: The entire message will goes to hash function along with initial vector IV. The output of hash function 'n' bits goes to another procedure along with S_o

where $S_o = K^+ \oplus$ opad.

The output of the procedure will again go to its hash function with initial vector (IV) and produces output of 'n' bits. which is the final checksum of HMAC.

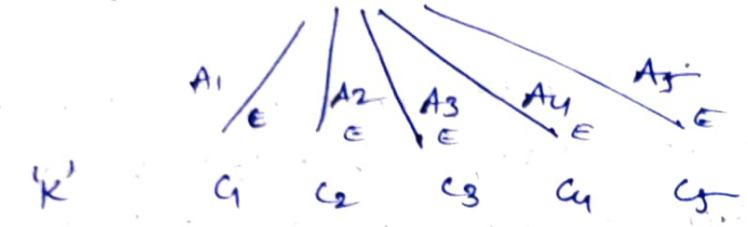


2) CMAC

In this it has limited message size and is based on block ciphers.

Message is divided into equal nos of blocks and encrypted each block seperately.

Eg:- Let message M = 10111



$C_1 = E(K, A_1)$

$C_2 = E(K, A_2 \oplus C_1)$

$C_3 = E(K, A_3 \oplus C_2)$

$C_n = E(K, A_n \oplus C_{n-1})$

KERBEROS

It is a server which provides authentication to users in a workstation.

It has 3 servers namely

1. Authentication Server
2. Ticket Granting server,
3. Application Server.

A simple authentication protocol. If a client wants to access services from the application server. The authentication should be provided to the client by the server called authentication seover. Therefore the various steps involved

between the client and application server are

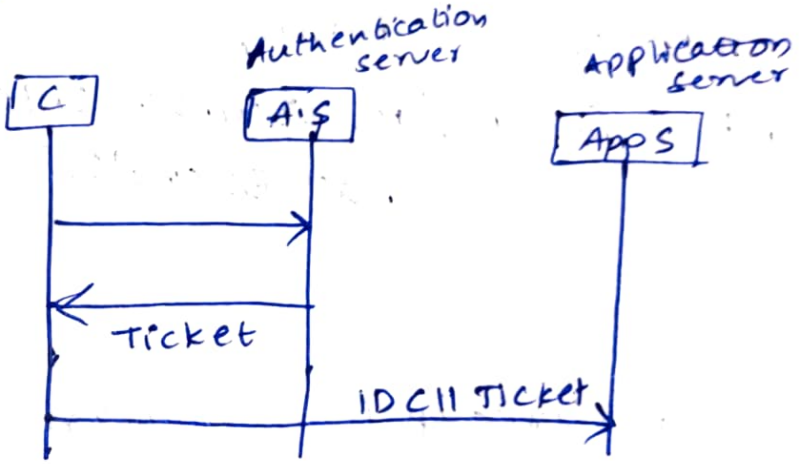
1) The client sends request to authentication server, in the form of ~~ID_c || P_c || ID_B concatenated~~

~~$ID_c || P_c || ID_B$~~

$ID_c || P_c || ID_v$

2) Now the authentication server issues the ticket to the client

3) After receiving the ticket, the client sends the ticket to the application server ID



Unit 5:- Email Security

The various agents that are involved in email services are

1) User Agent (UA)
2) Message transfer agent (MTA)
3) Message access agent (MAA)

To provide various services for e-mail, there are 2 protocols that are used are

1) PGP (Pretty Good Privacy)
2) S/MIME (Secure/Multipurpose Internet Mail Extension)

1) PGP:

It was developed by Phill Zimmermack provides various services to email.

It is an open source and freely available software for email security.

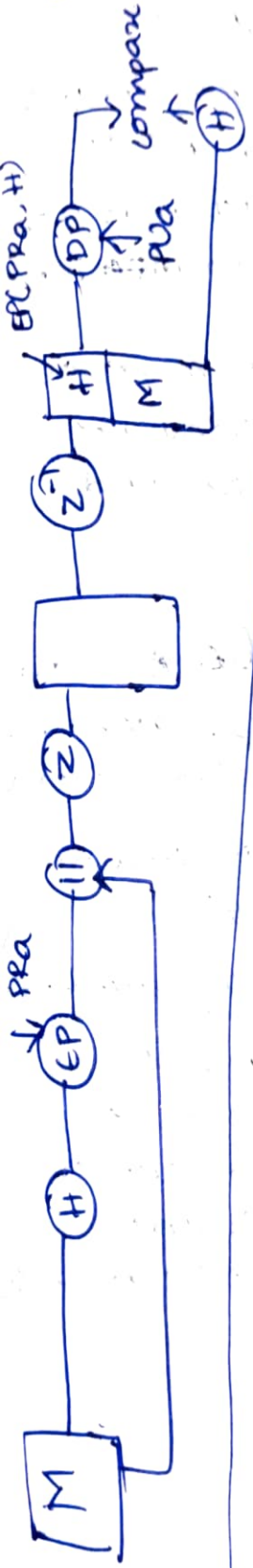
The various services provided by PGP are

i) Authentication
ii) Confidentiality
iii) Compression
iv) Email compatibility
v) Digital signature

1) Authentication:

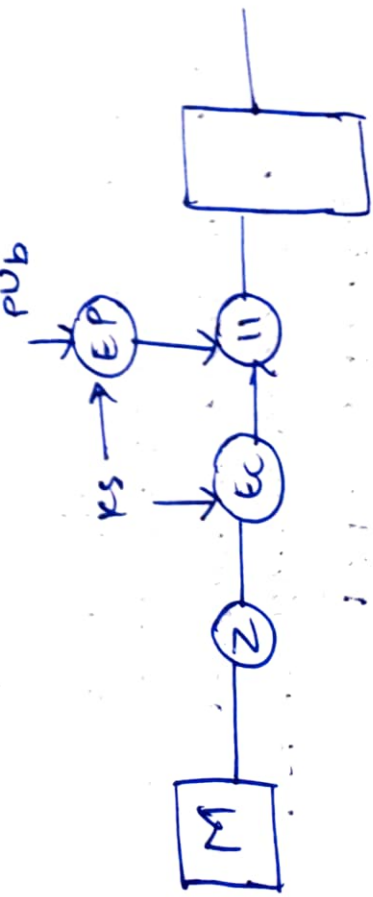
The message M is concatenated with encrypted Hash code and then compressed

and finally sent to the receiver. The encryption is done with private key of the sender upon receiving the compressed message will be decompressed, computes the hash function, decrypts the received hash function and finally compares both.



ii) Confidentiality

The message M is compressed and encrypted using (conventional encryption) session key K_s and concatenated to encrypted ~~public~~ session key ~~of the~~ by ~~receiver~~. using receiver's public key. (Public key encryption) send to the receiver and the receiver performs the entire reverse process of sender side.



2) MIME

Proposed by Bell communications in 1991 in order to expand the limited capabilities of E-mail.

It can send different types of files on the Internet such as audio, video, images etc...

The working of MIME, the message transmitted from user agent UA in the form of non-ASCII format this protocol converts this format into 7 bit NBT-ASCII format and sends to ~~MDA~~ MTA.

This MDA sends this format to MT of receiver side. Again the MIME Protocol converts the ASCII data to non-ASCII data and transmits to UA

Features of MIME:- 1) Able to send multiple attachme with a single mess

2) Unlimited mess length

3) Binary attachme

4) It provide support for various content types and multipart messa

iii) Combination of Authentication and confidentiality

PGP - Advantages

1. It is almost impenetrable. or difficult to break the code
2. can be sent to group of users securely.

PGP - Disadvantages

1. PGP is complicate
2. Issues with compatibility

S/MIME

It is a security enhancement of MIME which provides encryption to ensure the email authentication.

Extension of MIME Protocol which provides security for the mail i.e. transferring.

IPsecurity (IPsec)

Provides services to the packets that are transmitting over IP. The various functionalities of IPsec are

1) Authentication
2) confidentiality
3) key management

This procedure provides 2 algorithms/ Protocols for authentication and confidentiality

ESP - Encapsulation Security Payload
AH - Authentication Header

ESP -

This protocol provides encryption to that packets that are transmitting over IP. It consists of various encryption algorithms.

AH -

It provides authentication to the packets and has various authentication algorithm

2) Key Management

Generates various keys that are transmitting over IP

The IP packets are associated with the mechanism called SA

Security Association (SA)

SA is one way logical connection b/w sender and receiver or client and server.

The various parameters that are used to identify SA

1) SPI
2) IP Destination Address
3) Security Protocol Identifier

1) Security Parameter Index (SPI)

A unique identifier that is assigned to each SA

2) IP Destination Address

Address of Destination

3) Security Protocol Identifier

It specifies which protocol is going to be used

All the SA's are stored in the database called SAD

The various entries to this database are

1) SPI
2) Sequence number counter
3) Sequence counter overflow
4) Anti-replay window
5) AH Information
6) ESP information
7) Lifetime of this security Association
8) IPsec protocol Mode
9) Path MTU

The various addresses that an IP packet contains are

i. Remote IP address
ii. Local IP address
iii. Next Layer Protocol: IPv4 or IPv6
iv. Name: User Identifier from Operation System
v. Local & Remote ports.

The various elements that an IP packet consists of are

i. Encapsulating security Payload (ESP)
ii. Authentication Header (AH)
iii. Internet key Exchange (IKE)

The key management is used to exchange keys between 2 ends. The various key management protocols are:

1) OAKLEY
2) ISAKMP

These 2 are the key management Protocols that interchanges keys between SA's

These protocols introduces a mechanism called cookies to be used against attacks. and also introduces/uses nonce to be used against replay.