Network Security

OSI Security Architecture.

Threat - It is a possible danger that might exploit a vulnerability.

Attack - It is an deliberate attempt to evade security servic and violate the security policy of system.

OSI security Architecture

1) Security attack - Action that compromises security.

2) Security mechanism - Detect, prevent or recover from security attack

3) Security service - Enhance the security, counter security attack and provide servic.

Security attack

- Active
  - Involve modification of data stream or creation of false stream
  - Masquerade (using someone credentials)
  - Replay - (A → H → B)
  - modification of messages. — A → H → B
  - Denial of servic → H → server (busy server)
- Passive (Attempt to obtain information being transmitted)

Active	Passive
Hard to prevent	Hard to detect.
Difficult to prevent	Encription prevents.

Security services -

Implement security polices and are implemented by security mechanisms.

Authentication - Right entity are communating.

Acess control - control access by giving controlled access.

Data confidentiality - Data should remain private.

Data integrity - sent message = received message.

Non repudiation - Denial of msg should be handled.

Security mechanism -

Encipherment - conversion of text to encripted text i.e cipher text

Digital Signature - signature to prove identity of source. It is hidden code. It provide both authentication and integrity.

Access control - Giving access rights.

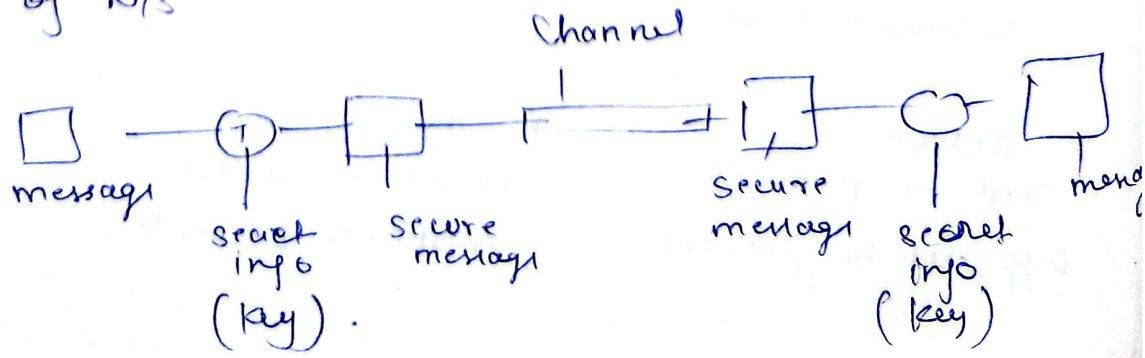
Data integrity - Data remain consistent.

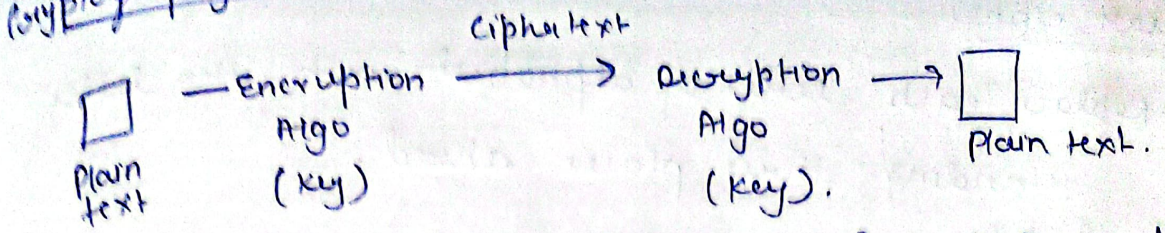
Authentication - (Right identity verification)

Routing control - Providing a specific route.

Notarization - Third party to make sender receiver secure.

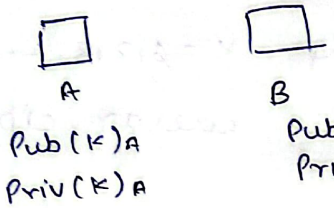
model of N/S





Cryptography is technique of securing information and communication using code so that only sender and receiver can understand.

1) Symmetric cryptography (Private key cryptography)
   Encryption and decryption algo have same key.
2) Asymmetric cryptography (Public key cryptography)
   Different key for encryption & decryption.



A encrypt with Pub (K)B

Cryptanalysis - Attacker try to know key to convert code ~~breaking~~ cipher text to plain text.

Brute force attack - Try all the key to decrypt message.

Classical Encryption techniques -

→ Substitution Techniques - (letters are replaced)
→ Transposition Techniques (letters are repositioned)

10

Caesar cipher

- Replace each letter of alphabet with the letter standing three places ahead.
- simple.

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

$C = E(p, k) \bmod 26 = (p + k) \bmod 26$

$p = D(c, k) \bmod 26 = (c - k) \bmod 26$.

P = NESO

C = QHVR

Shift cipher - similar to caesar cipher but here K can be anything $K = 0, 1, 2, 3 \ldots$

shift cipher with $K = 3$ it is caesar cipher.

Monoalphabetic cipher - it can be any permutation of 26 alphabetic characters.

Plain txt - N E S O → map these letter to any letter. (used letter can not be used again)

↓ ↓ ↓ ↓

D U L A

Better techniques but are easy to break because they reflect frequency data of original alphabet.

Prone to guessing.

Playfair cipher - multiple letter encryption techniques. In this d can be m or some occurence it can be x or y anything.

5×5 matrix

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

Repeating letter = Filler letter.

Same column → |↓| go down.

Same row → |→| go right

Rectangle - then swap (⇄)

Ex- Balloon.

Ba lx lo on

Ex- attack

at ta ck

RS SR DE

mosque

mo sq ue

ON TS ML

Hill cipher - It is also multi letter cipher.

~~Encrypt~~ Encrypt group of letter.

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

$$D = D(K, C) = CK^{-1} \bmod 26$$

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

$$c_1 c_2 c_3 = (P_1 P_2 P_3) \begin{pmatrix} K \cdots K_{13} \\ ; \\ K_{31} \cdots K_{33} \end{pmatrix}_{3\times3} \bmod 26.$$

Encrypt "pay more money" by hill cipher.

$$\text{key} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}_{3\times3}$$

we can encrypt 3 letter at a time.

15 0 24

$$[15\ 0\ 24)\begin{bmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{bmatrix} \bmod 26$$

$$C_1\ C_2\ C_3 = \begin{bmatrix}303 & 303 & 331\end{bmatrix} \bmod 26.$$

$$C_1\ C_2\ C_3 = [17\ 17\ 11]$$

$$= (17\ 17\ 11]$$

$$= [R, R, L]$$

PAY → RRL To this for all.

Decryption

$$P = D(K)C = C \times K^{-1} \bmod 26$$

$$K = \begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix} \bmod 26.$$

$$17(18\times19 - 2\times21) - 17(21\times19 - 21\times2) + 5(21\times2 - 18\times$$

$$17(300) - 17(357) + 5(6)$$

$$= -939 \bmod 26.$$

$$= -3 \bmod 26$$

$$= 23$$

find inverse matrix..

$$\text{adj } K = \begin{bmatrix}300 & -313 & 267\\ -357 & 313 & -252\\ 6 & 0 & -51\end{bmatrix} = \begin{bmatrix}14 & -1 & 7\\ -19 & 1 & -18\\ 6 & 0 & -25\end{bmatrix}$$

$$= \begin{bmatrix}14 & 25 & 7\\ 7 & 1 & 8\\ 6 & 0 & 1\end{bmatrix}$$

$$K^{-1} = \frac{1}{23} \times \begin{bmatrix}14 & 25 & 7\\ 7 & 1 & 8\\ 6 & 0 & 1\end{bmatrix} \bmod 26$$

pay

15 0 24

$$[15\ 0\ 24)\begin{bmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{bmatrix} \bmod 26$$

$$c_1\ c_2\ c_3 = \begin{bmatrix}303 & 303 & 331\end{bmatrix} \bmod 26.$$

$$c_1\ c_2\ c_3 = [17\ 17\ 11]$$

$$= (17\ 17\ 11]$$

$$= [R, R, L]$$

PAY → RRL To this for all.

Decryption

$$P = D(K, C) = C \times K^{-1} \bmod 26$$

$$K = \begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix} \bmod 26.$$

$$17(18\times19 - 2\times21) - 17(21\times19 - 21\times2) + 5(21\times2 - 18\times2$$

$$17(300) - 17(357) + 5(6)$$

$$= -939 \bmod 26.$$

$$= -3 \bmod 26$$

$$= 23$$

find inverse matrix..

$$\text{adj } K = \begin{bmatrix}300 & -313 & 267\\ -357 & 313 & -252\\ 6 & 0 & -51\end{bmatrix} = \begin{bmatrix}14 & -1 & 7\\ -19 & 1 & -18\\ 6 & 0 & -25\end{bmatrix}$$

$$= \begin{bmatrix}14 & 25 & 7\\ 7 & 1 & 8\\ 6 & 0 & 1\end{bmatrix}$$

$$K^{-1} = \frac{1}{23} \times \begin{bmatrix}14 & 25 & 7\\ 7 & 1 & 8\\ 6 & 0 & 1\end{bmatrix} \bmod 26$$

$$K^{-1} = 23^{-1} \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$= 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$P = [R\ R\ L] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$= [17\ 17\ 14] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$$

$$= [15\ 0\ 24]$$

$$= P\ A\ Y$$

Polyalphabetic cipher -
Develop to improve monoalphabetic letter.

Vigenere cipher - consist 26 caesar ciphers with shift 0 to 25.

$$C_i = (P_i + K_{i \bmod 26}) \bmod 26$$

$$P_i = (C_i - K_{i \bmod 26}) \bmod 26$$

Key = deceptive deceptive deceptive
Plain text = we are discovered save yourself.

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

autokey - A keyword is preodic so we need to eliminate to have better.

Vernam cipher -

Vernam cipher works on binary bits rather than letters.

The system can be expressed as →

$$C_i = P_i \oplus K_i$$

P_i = ith binary of plain text

C_i " " cipher text

$\oplus$ = XOR

K_i = " " key.

Encryption - $(P_i \oplus K_i)$

Decryption - $(C_i \oplus K_i)$

One time pad - Improvement to vernam cipher.

One key is used to ~~encrypt~~ encrypt and decrypt and then discarded. It is difficult to break one time pad.

It offers best level of security.

Transposition - letters are repositioned.

Rail fence technique - Plain text written down as sequence of diagnol and then read off as sequence of row.

Plain t = Neso Academy is best

depth = 2.

N	S	A	A	C	Y	S	H	B	S
E	O	C	D	M	I	T	E	E	T

Cipher text = NSAACYSHBSEOCOMITEET

Row column transposition

more complex technique to encrypt.

Encrypt - Kill corona virus at twelve am tomorrow.

4 3 1 2 5 6 7 ← key taken.

→

K	I	L	L	C	O	R
O	N	A	V	I	R	U
S	A	K	T	W	E	L
V	E	A	M	T	O	M
O	R	R	O	W	X	X

ciphex text → IATAR LUTMO ----

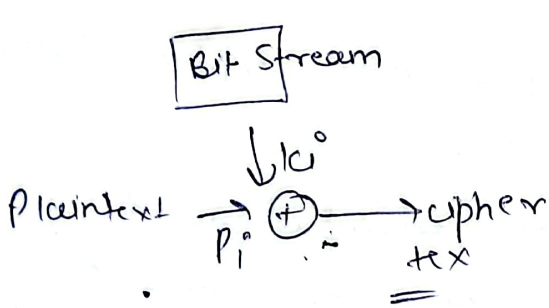
Steganography - conceals the existence of message or hiding the message.

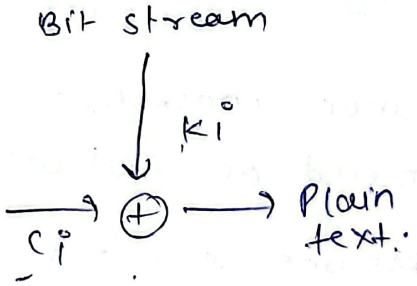
It is not an encryption technique.

Example- Sending hidden message with image.

Stream cipher and block cipher -

Stream cipher - It is the one that encrypt a digital data stream one bit or byte at a time.





eg - 10110110

01010101

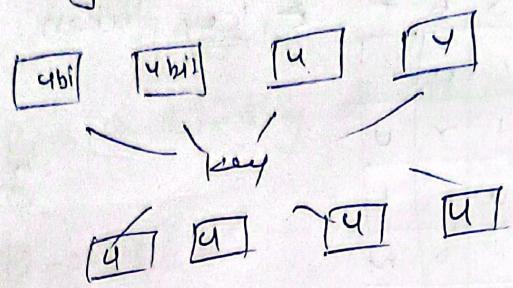
11100011 — cipher text

01010101

10110110 — plain text

Block cipher -

In this a block of plain text is treated as whole and used to produce cipher text of equal length.



Block cipher	stream cipher
Plain text is taken in block at a time	1 byte. 1 bit or more is taken at a time
Uses 64 bit or more	Use 8 bits.
complexity is simple	more complex
Uses confusion as well as diffusion concept	Uses only confusion concept.
Reverse encrypted text is hard.	Reverse encrypted text is easy.

Shanon theory of confusion and diffusion -

- Shanon concern was to prevent cryptanalysis based on statical analysis.
- Assume attacker has some knowledge of statistical characteristic of plain text (eg. frequency distribution) then he will be able to deduce key.

He suggested two methods -

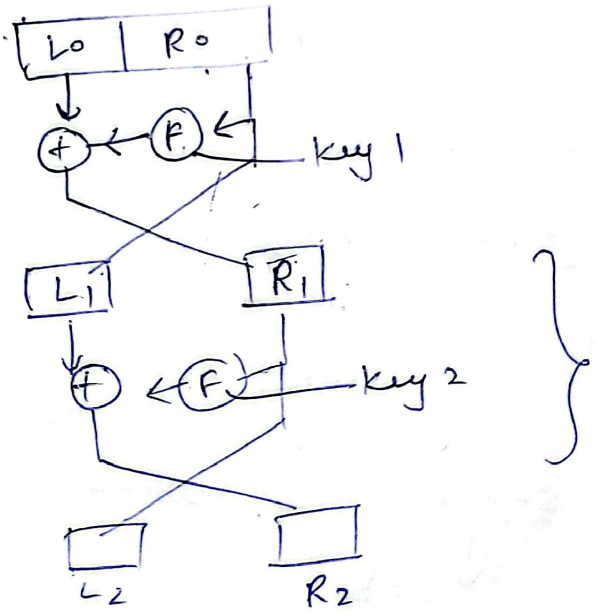
1) confusion
2) Diffusion.

diffusion - In simple ... symbol in plain text is changed several or all symbol in cipher text will also change.

The idea of diffusion is to hide relation b/w ciphertext and plain text.

2) confusion -
It hides relation b/w ciphertext and key.
If a single bit in key is changed then most/all bit of cipher text will also change.

Feistel cipher structure -
- most block cipher follow this technique.
- plain text divided into two parts.
- the 2 halves data pass through n rounds of processing and then combine to produce ciphertext block.
- on right we apply f(n) we will use subkey generated from master key.
The op of this is XOR with left half and their o/p will be swapped. this is single round



Block size - large block size more secure

key size - large means more secure but decrease the speed of encryption/decryption.

No. of round → more, more secure.

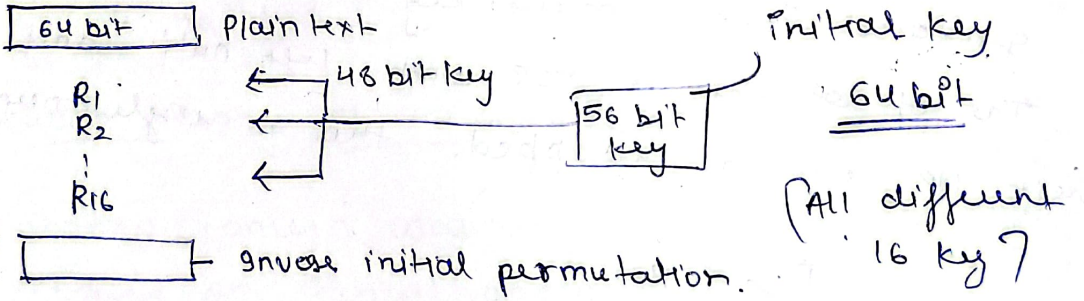
Subkey algo - more complex, more secure

Function - ↑↑

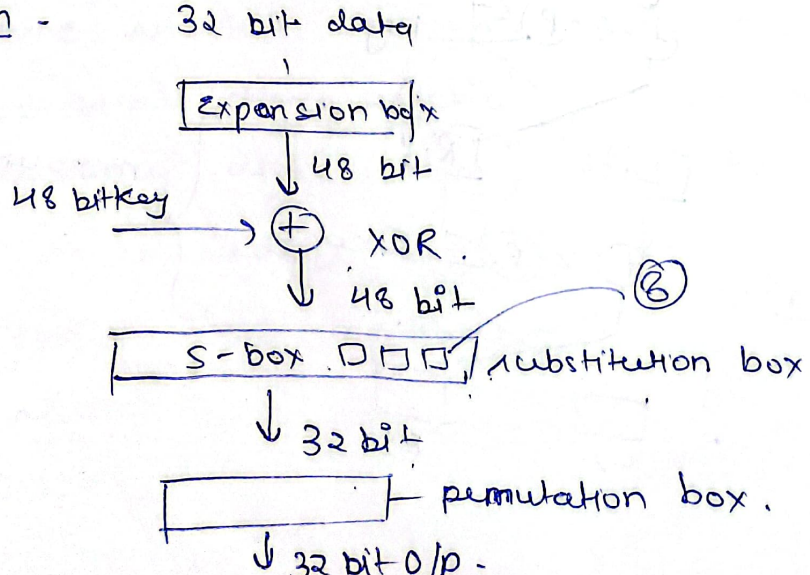
DES - Data encryption standard.

i) block cipher
ii) symmetric cipher
iii) 64 bit - plain text block
iv) ~~***~~ * 16 rounds each round is feistel round.

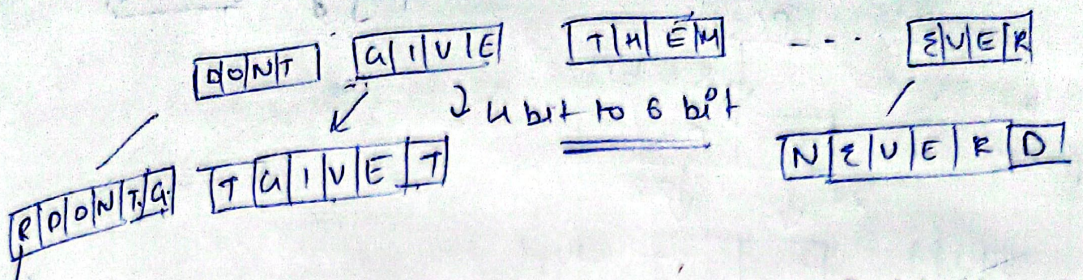
steps -
i) Initial permutation.
ii) 16 feistel round
iii) swapping
iv) final permutation (inverse initial permutation)



function -

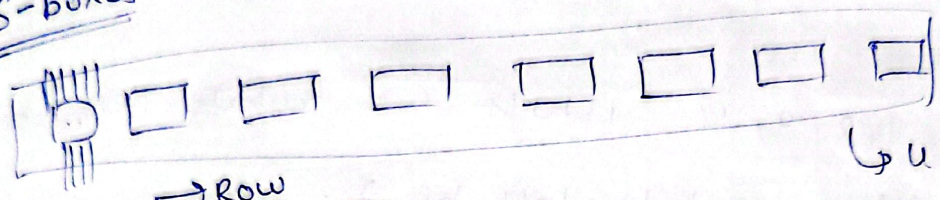


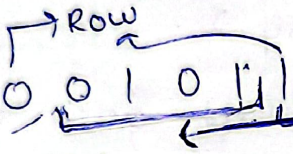
Expansion box



from last
└ 8 block of 4 bit converted to 8 block of 6 bit.

S-boxes





eg - 0 0 1 0 1 1

01 = 1
0101 = 5

S-box row table.

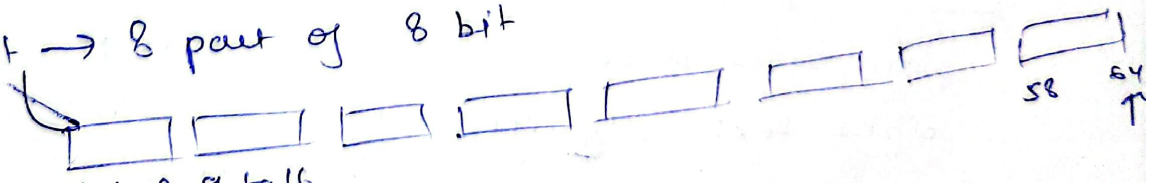
	0	1	2	3	4	5	6	7	----	15
0	3	5	7	0	1					
1	-	-	-	-			-	-	-	
2										
3										

convert to binary = 7
= 0111

Key generation

We have 64 bit key which is go as i/p to PC-1 (permuted choice 1) and will get o/p · 56 bit key.

64 bit → 8 part of 8 bit

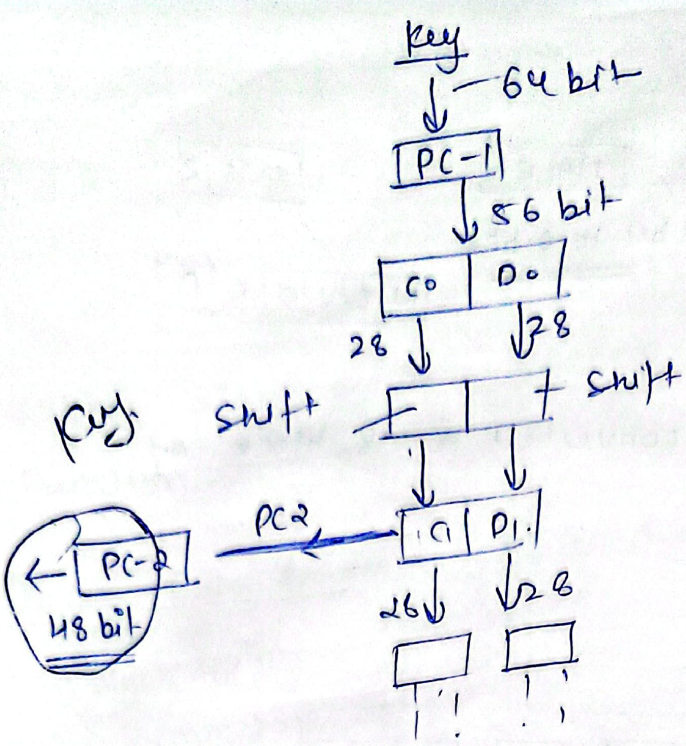


discard last bit of each block

8, 16, ---- 64 discarded.

Hence 8 × 7 = 56 bits.

Key generation



Round i = 1, 2, 9, 16 shift 1-c rotate left 1 bit

all other rotate left by 2.

shifting we get $C_1 D_1$ which goes to PC-2

PC-2 has predefined table then we get our first key.

$C_1 = 1-28$

$D_1 = 29-56$

left half C_1 = 9, 18, 22, 25 — position bit are missing

Right D_1 = 35, 38, 43, 54 — position are removed

= 48 bit key

DES Analysis

Avalanche effect - It means small change in plain text then it should change cipher text significantly.

DES is very strong due to this.

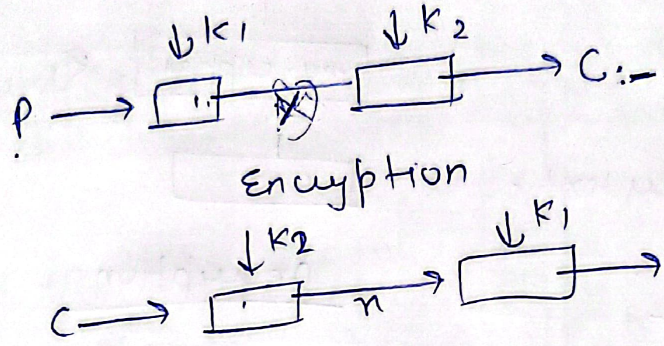
completeness effect - It means that each bit of cipher text needs to depend on plain text.

confusion & diffusion by S, D box in DES have strong completeness effect.

~~DES weakness~~

Double DES - since DES attack was vulnerable to brute force attack. so multiple DES was introduced.

1) Two different keys are used.



Drawback -

meet in the middle attack →

Require some plain text and ciphe text.

i) encrypt P for all 2^{56} possible key (K_1) and store in result table.

ii) decrypt C using all 2^{56} possible (K_2) key on result, check against table for match

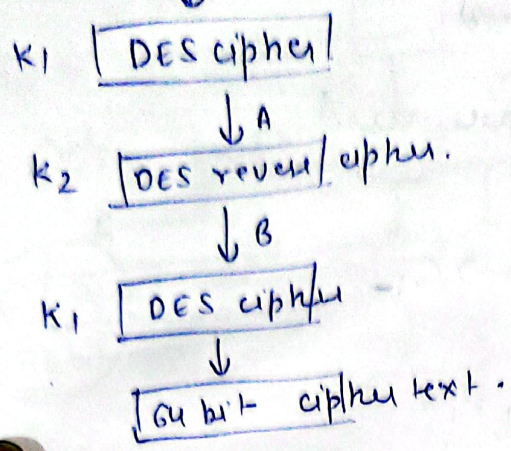
iii) when match we possibly found correct pair of keys.

(It is twice powerful then DES

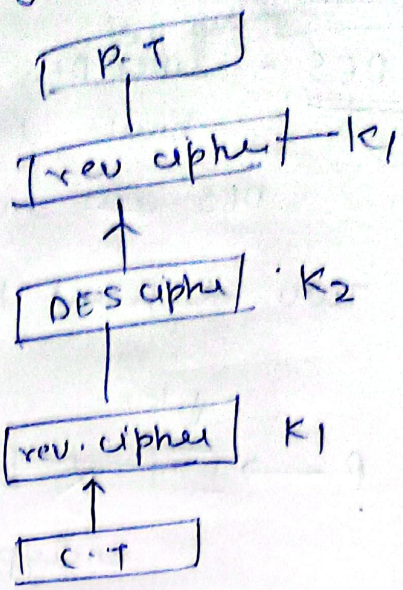
$2 \times 2^{56} = 2^{57}$

Triple DES - here 3 or 2 key can be used.

Encryption / decryption using 2-keys.

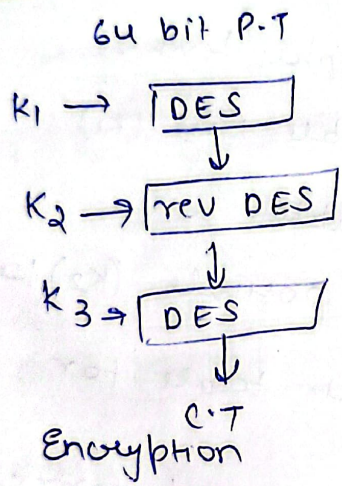


Encryption

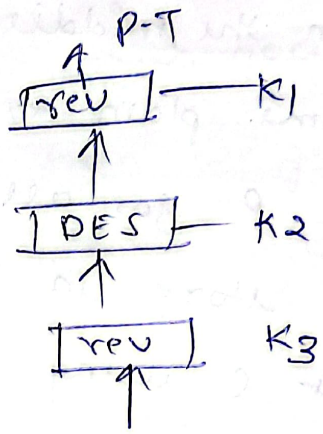


Decryption

Using 3 keys



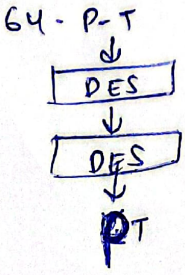
Encryption



DES weakness-

→ DES it can be cracked by 2^{56} permutation of key.

→ weak keys- if we encrypt block twice with weak key we get original block.



four out of 2^{56} are weak key.

It contain all 0' or all 1 or half key 0 or half key 1

Semi weak Keys

A semiweak key creates only two different round keys and thus repeated 8 times.

Possible weak keys - 48 keys are possible weak keys.

Keys clustering - Means 2 or more different key can create same cipher text from plain text

weakness in cipher design -

Two specifically chosen i/p to S-box array can create the same o/p.

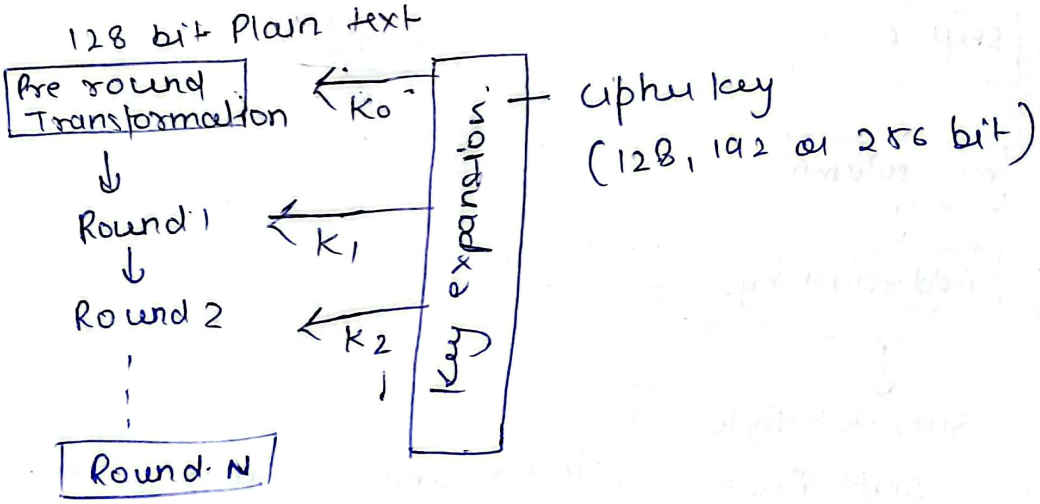
AES - Advanced encryption standard

Symmetric key block cipher.
more secure and powerful encryption.

Block size = 128 bits. 16 bytes = 4 words

1 word = 32 bit.

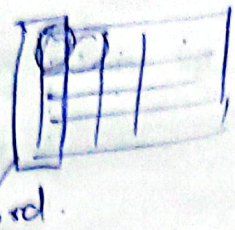
Rounds	no. of bit in key	
10	128.	AES-128 version.
12	192	
14	256	



n round have (n+1) keys.

State - 16 bytes (4×4) matrix
store intermediate result.

Input array -



State array - 16 byte 4×4

1st byte of 0th word.

2nd byte of word.

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

Key - 128 bit i.e 4 ~~word~~ words.
w_0 w_1 w_2 w_3

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

Expand key algo →

w_0	w_1	- -	w_{43}

44 words

Plain text

Key (128 bit) 4 word

w_{0-3}

Substitute byte

Shift Rows

mix column

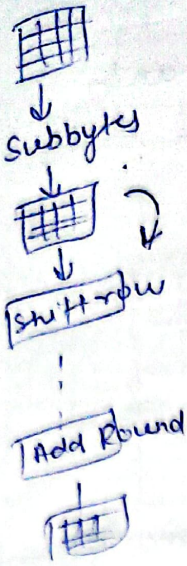
Add round keys w_{4-7}

Round-1

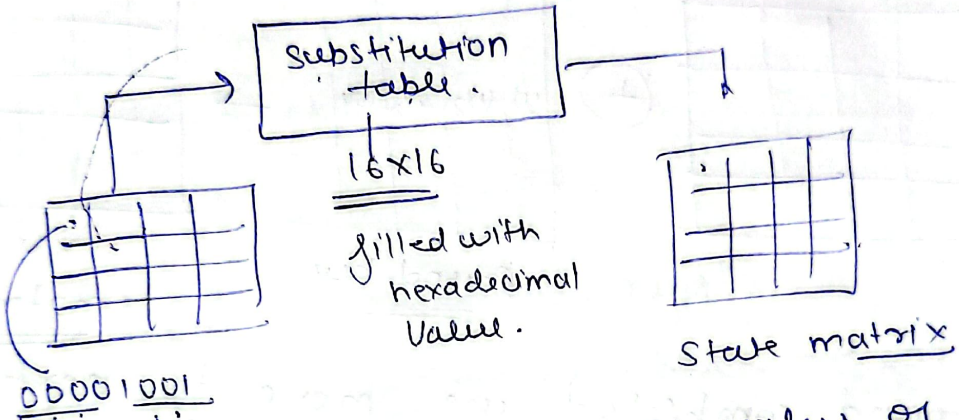
Substitute Byte
Shift Rows
Add Round keys

last round

mix column not in last round.



Subbytes - one table is used at a time for transformation.



→ Do for all values of matrix.

if two byte are same they have same transformation.

Shift Rows - Shifting is done to left. it uses previous state matrix.

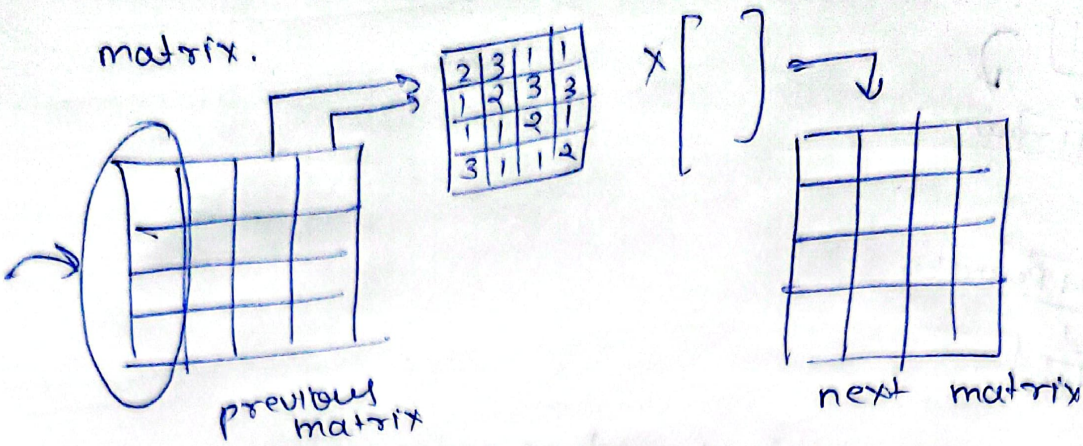
Row				
0	63	C9	FE	30
1	F2	F2	63	26
2	C9	C3	7D	D4
3	BA	63	42	D4

Shift →

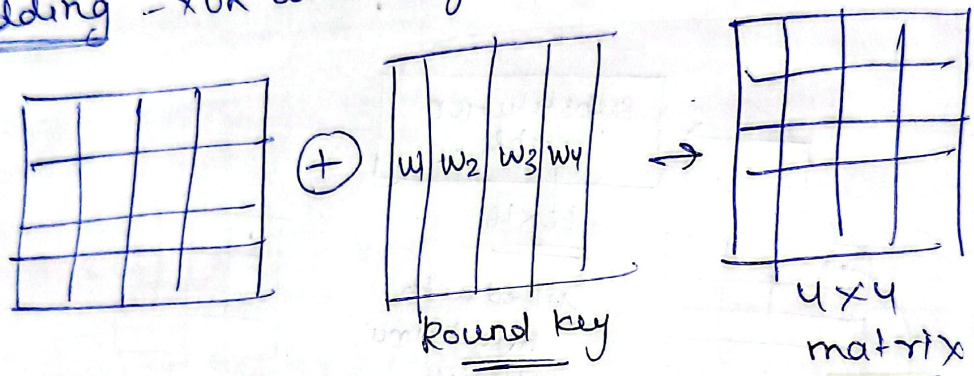
63	C9	FE	30
F2	C3	26	F2
7D	D4	C9	C3
D4	BA	63	B2.

mixing -

Take each word and multiply with constant matrix.



Key adding - XOR with keys.



Now round completed we move to next round.

AES	DES
Advanced encryption Standard	Data encryption standard
Key length can be 128, 192, 256 bit	Key length is 64 bit (56 in each round)
No of round can be 10, 12, 14	No of round - 16.
Structure is based on substitution & Permutation	Structure based on fiestel structure.
Round - Byte substitution Shift Row mixing Key addition	Round - Expansion XOR operation substitution & Permutation.

Encrypt 128 bit plain text.

Derived from square cipher.

No known attack

faster.

Encrypt 64 bit P-T

derived from Lucifer cipher.

Brute force, linear cryptanalysis.

slower.

~~Blowfish Algorithm~~

IDEA Algorithm - International data encryption Algorithm.

also called IPES (Improved proposed encryption standard).

Symmetric key block cipher.

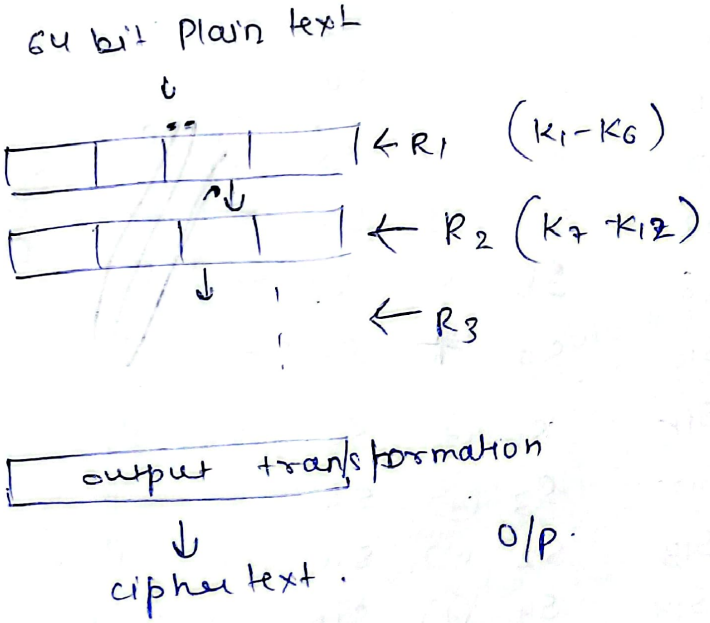
It replaced DES.

Key size = 128 bits. ⟶ 52 keys.

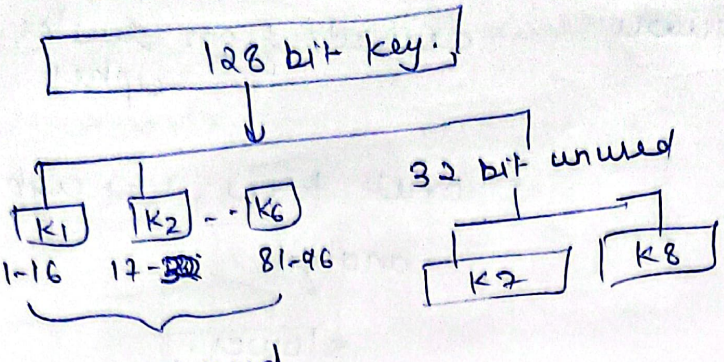
Block size = 64 bits ⟶ each block - 4 part

8 identical Transformation round. ⟶ 6 subkey are used. (16 bit key)

One hay round transformation ⟶ Use 4 subkeys (16 bit) key

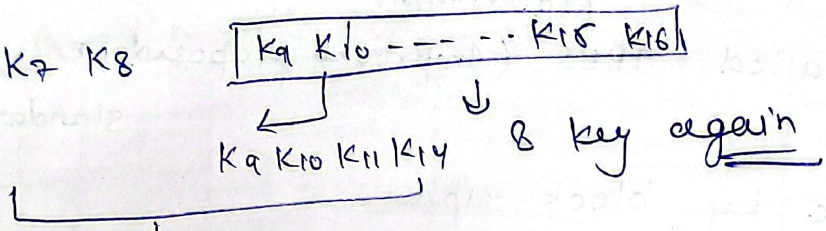


Sub key generation



Round-1

circular left shift by 25 bit



used in Round-2.

do this process again.

Round details

$S_1 = P_1 \times K_1$

$S_2 = P_2 + K_2$

$S_3 = P_3 + K_3$

$S_4 = P_4 \times K_4$

$S_5 = S_1 \oplus S_3$

$S_6 = S_2 \oplus S_4$

$S_7 = S_5 \times K_5$

$S_8 = S_6 + S_7$

$S_9 = S_8 \times K_6$

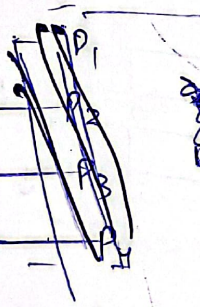
$S_{10} = S_7 + S_9$

$S_{11} = S_1 \oplus S_9$ — P_1

$S_{12} = S_3 \oplus S_9$ — P_2 } Swap

$S_{13} = S_2 \oplus S_{10}$ — P_3 }

$S_{14} = S_4 \oplus S_{10}$ — P_4



P_1
P_3
P_2
P_4

No swapping

One half round

$R_1 \times k_{44} \rightarrow c_1$
$R_2 + k_{50} \rightarrow c_2$
$R_3 + k_{51} \rightarrow c_3$
$R_4 \times k_{52} \rightarrow c_4$

} ciphertext

Block cipher modes of operation

Four modes of operation are-

i) ECB - Electronic codebook mode
ii) CBC - cipher block chaining mode
iii) CFB - cipher feedback mode.
iv) OFB - output feedback mode.
v) CTR - counter mode.

ECB → Divide into fix block add padding if required.

Hello everyone.

112=5

| Hello | every | onexx |

↓ block-1 | Algo | — cipher block1

but for short data, Not secure for lengthy algo.

CBC → 8. to overcome challenge of ECB.

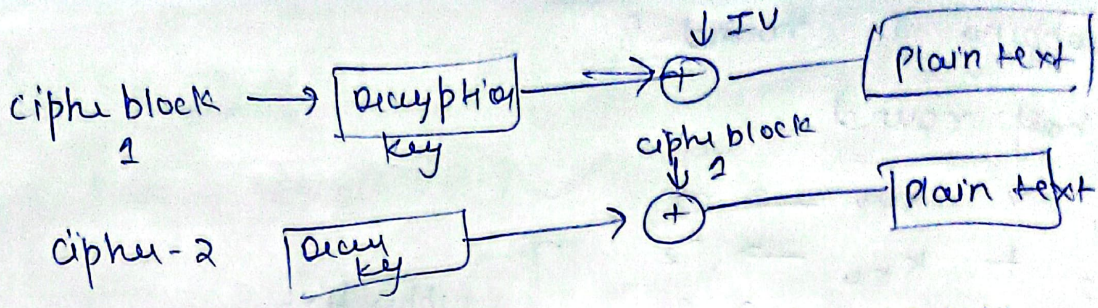
IV → Initialization vector

Block 1 — ⊕ — encryption algo — cipher block 1

cipher-1 ↓

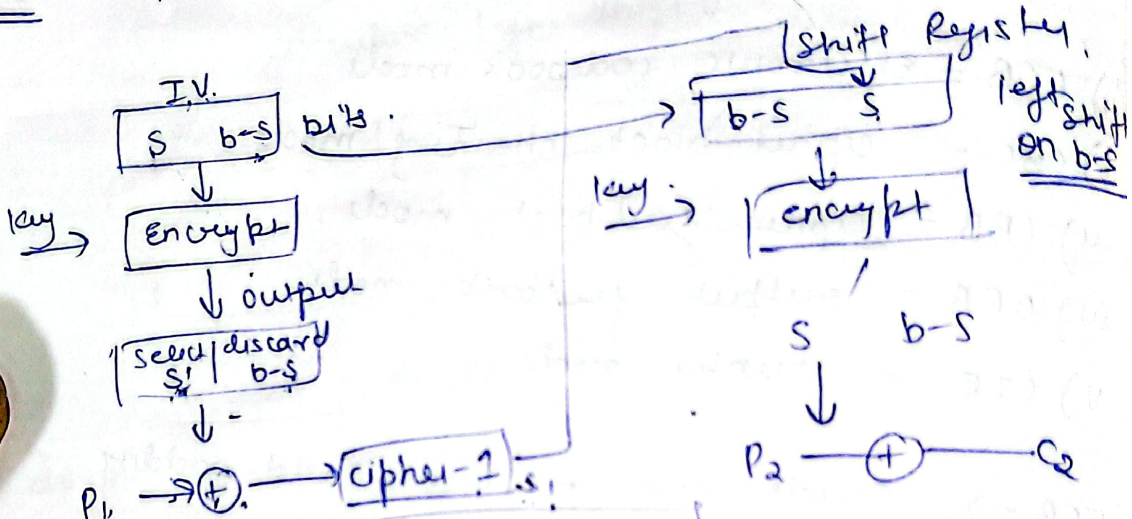
Block-2 — ⊕ — Algo — cipher-2.

It creates different cipher for same Block.



limitation - 2 identical msg & if we use same IV, cipher will be same.

CFB - Plain text divided into segment of 1 bit.



Same decryption P1 change with C1

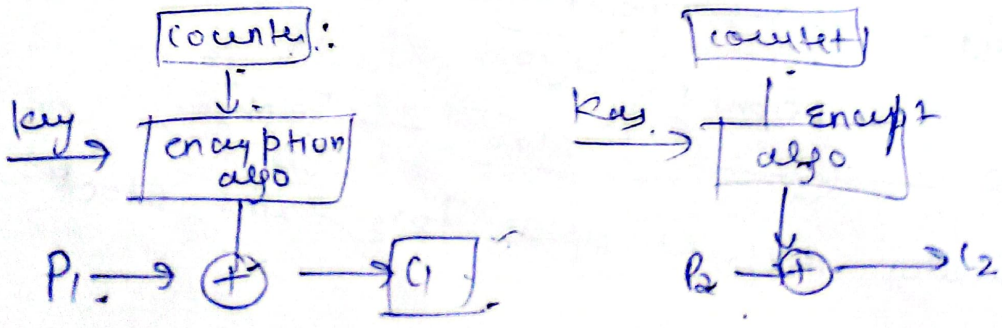
OFB - take 1 bit in next operation from previous before taking XOR all other same as CFB.

Counter mode

Simple and fast-

a counter equal to plain text block size is used.

counter is incremented by 1.



Modulus

$15 \bmod 7 = 1$

$-15 \bmod 7 = \pm 6$

$-23 \bmod 7 = 5$

$a \equiv b \pmod n$

means = n divides $(a-b)$

modular arithmetic

mod is just remainder.

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

$(a-b \bmod n)$ — —

$(a \times b \bmod n)$ × ×

Exponentiation

$11^7 \bmod 13.$

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

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

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

$= 3 \times 4 \times 11$

$= 132 \bmod 13 = 2$ Ans

Euler's totient function -

represented by (ϕ)

It is defined as +ve integer less than n that are coprime to n.

$\phi(5) = \{1, 2, 3, 4.\}.$

$\phi(6) = \{1, 5\}$

$\gcd(a,b) = 1$ then a, b are co-prime.

when $n \rightarrow$ prime

$\phi(n) = n-1$

$\phi(5) = 4$

$\phi(a*b) = \phi(a) * \phi(b)$ a & b should be co-prime

$= \phi(7) * \phi(5)$

$= 6 \times 4$

$= 24$

Euler theorem

also called fermat - Euler theorem or Euler's totient theorem.

It states that n and n are coprime integer then

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

$\phi(n)$ = Euler totient function.

Ex $n = 11$, $n = 10$ both co-prime.

$$11^{\phi(10)} \equiv 1 \bmod 10$$

$$11^4 \equiv 1 \bmod 10$$

$$14641 \equiv 1 \bmod 10$$ true

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

find - $4^{99} \bmod 35$

$$4^{\phi(35)} = 1 \bmod 35$$

$$4^{24} \equiv 1 \bmod 35$$

7×5

$6 \times 4 = 24$

$4^{99} = 4^{24\times4} \cdot 4^3$

$= (4^{24})^4 \bmod 35 \cdot 4^3 \bmod 35$

$= 1 \times 4^3 \bmod 35$

$= 29$

Fermat's theorem - also called fermat's last theorem.

- special case of euler's theorem.

If n is prime and x is +ve integer not divisible by n.

$$x^{n-1} \equiv 1 \bmod n$$

$x = 3 \quad n = 5$

$3^4 \equiv 1 \bmod 5$

$81 \equiv 1 \bmod 5$ true

RSA Algorithm

Rivest, Shamir, Adlemen algorithm.

It is a asymmetric cryptographic algo having 2 keys.

Public key - known to all

Private key - kept secret, not shareable.

If public key of A is used for encryption then only private key of A can decrypt it

RSA is a block cipher in which plain text and ciphertext are integer b/w 0 & n-1

Key generation

i) select 2 large prime number p and q

ii) calculate $n = p * q$

iii) calculate $\phi(n) = (p-1)*(q-1)$

iv) choose value of e

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

v) calculate

$d \equiv e^{-1} \bmod \phi(n)$

$ed \equiv 1 \bmod \phi(n)$

Public key $= \{e, n\}$

Private key $= \{d, n\}$.

Let $p = 3$ $q = 11$

$n = p * q = 3 * 11 = 33$

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

$= 2 \times 10$

$= 20$

$1 < e < \phi(n)$ such that $\gcd(\phi(n), e) = 1$

$\boxed{e = 7}$

$de \equiv 1 \bmod (\phi(n))$

$7 * d \equiv 1 \bmod \phi(n)$

$(7 * d) \bmod 20 = 1$

d = 3

public key = $\{7, 33\}$

private key = $\{3, 33\}$.

↓ Plaintext.
$M < n$

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

Decryption - $M = C^d \bmod n$.

chinese remainder theorem

if $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

find (x) if can find x if $m_1 m_2 m_3$ are co-prime.

$\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3 m_1) = 1$

4) $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M \text{ ---- } M_n x_n a_n) \bmod M.$

$M = m_1 * m_2 * m_3 \text{ ---- } m_n$

$M_i = \frac{M}{m_i}$

to calculate x_i $M_i x_i \equiv 1 \bmod m_i$

Q = $x \equiv 1 \bmod 5$

$x \equiv 1 \bmod 7$

$x \equiv 3 \bmod 11$

$a_1 = 1$

$a_2 = 1$

$a_3 = 3$

$m_1 = 5$

$m_2 = 7$

$m_3 = 11$

$M = 5 \times 7 \times 11$

$= 385$

$M_1 = 77$

$M_2 = 55$

$M_3 = 35$

$x_1 =$ $M_1 X_1 \equiv 1 \bmod m_1$

$77 x_1 \equiv 1 \bmod 5$

$77 x_1 \pmod 5 = 1$

$2 x_1 \pmod 5 = 1$

$\boxed{x_1 = 3}$

Similarly $x_2 =$ $55 x_2 \bmod 7 = 1$

$6 x_2 \bmod 7 = 1$

$x_2 = 6$

Similarly $x_3 = 6$

put in formula:

Diffie Hellman key exchange -

It is not an encryption algorithm, it is used to exchange keys between 2 user.

we will use asymmetric encryption to exchange the secret key.

i) consider a prime number q q = 7

ii) select α such that it must be primitive root of q.

'α' is primitive root of q if

α mod q.
α^2 mod q
!
!
α^{q-1} mod q

give result = {1, 2, 3 --- q-1}.

$3^1 \bmod 7 = 3$
$3^2 = 4$ — 2
$3^3 = 6$ — 3
$3^4 = 4$
$3^5 = 5$
$3^6 = 1$.

α = 3

α < q

we can take any value of α.

α = 5

α and q are global.

X_A (private key). $X_A = 3$

$Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7$

$Y_A = 6$

assume X_B $X_B = 4$

$Y_B = \alpha^{X_B} \bmod q = 5^4 \bmod 7$

$Y_B = 2$

Secret key

$K_1 = (Y_B)^{X_A} \bmod q$

$= (2)^3 \bmod 7 = 1$

$K_2 = (Y_A)^{X_B} \bmod q$.

$K_2 = 6^4 \bmod 7 = 1$

$\therefore K_1 = K_2 = 1$

Elliptive curve cryptography

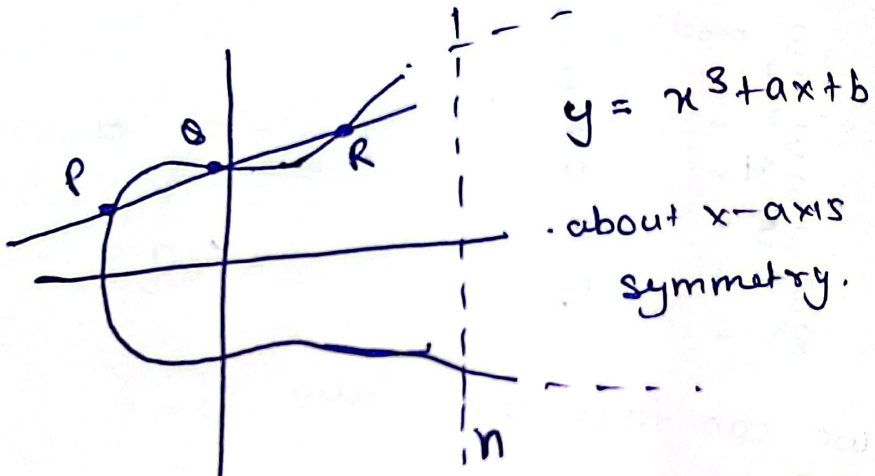
It is asymmetric / public key crypto system.

It provide equal security with smaller key size as compared to RSA.

small key high security.

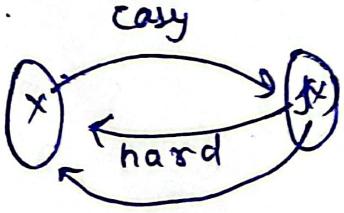
It make use of elliptic curves.

Elliptic curve are defined by some mathematical function $y = x^3 + ax + b$



If we draw line it can cut max 3 point or less.

Trapdoor function - is a function that is easy to compute in one direction yet difficult to compute in opposite direction.



let $E_p(a,b)$ be elliptic curve.

consider $Q = kP$

if Q, P are point on curve

If k and P given it should be easy to find Q but if we know Q & P it should be extremely difficult to find k. This is called discrete logarithmic problem for e. curve.

$A \rightarrow B$ easy

$B \rightarrow A$ hard.

ECC Key Exchange

Global Public element

$E_q(a,b)$: elliptic curve with parameter a, b and q prime no. or integer of form 2^m

G : Point on curve whose order is large value of n.

User A key

Select private key (n_A) $n_A < n$

public key P_A = $P_A = n_A \times G$.

User B

Select Private key n_B

public key = $n_B \times G$.

Calculation of secret key by user A

$K = n_A \times P_A$

Calculation of secret key by user B

$K = n_B \times P_A$

ECC Encryption

Let message be M.

first encode M into point on curve.

Let point be P_M.

For encryption choose random positive integer k.

cipher point will be

$$C_m = \{kG, P_m + kP_B\}$$

P_B ← Public key of B.

↳ sent to receiver.

Decryption –

multiply first point with private key.

i.e $kG * n_B$

then subtract it from 2nd point (co-ordinate in the pair)

i.e $P_m + kP_B - kG * n_B$

$$P_B = n_B \times G$$

so, $= P_m + kP_B - kP_B$

$= P_m$ original point

so receiver gets message.

Euclid algo

$gcd(a,b) = gcd(b, a \bmod b)$

$gcd(a,0) = a.$

Ex- gcd (1025, 35)

= gcd (35, 10)

= gcd (10, 5)

= gcd (5, 0)

gcd = 5

gcd (11, 7)

gcd (7, 4)

gcd (4, 3)

gcd (3, 1)

gcd (1, 0)

gcd = 1

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
6	180	20	0
		[20]	0

gcd = 20

Extended Euclid

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

$s = s_1 - q s_2$

$t = t_1 - q t_2$

Given a, b 161, 28

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	161	28	121	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
	[7]	0		[-1]	4		[6]	-23	

gcd.

$S_1 = -1$ $T_1 = 6$

multiplicative inverse

Z_n = set of residues $\{0, 1, 2, \ldots, (n-1)\}$

11 in 226

gcd(11, 26) = 1 true

$T = t_1 - q t_2$

q	r_1	r_2	r	t_1	t_2	t
	26	11		0	1	-2
2	11	4	3	1	-2	5
2	4	3	1	-2	5	-7
1	3	1	0	5	-7	26
3	1	0		-7	26	

gcd = 1

$t_1 = -7$

$-7 + 26 = 19$ Ans

Elagmal encryption

Assymmetric key cryptography

1) key generation
2) encryption
3) decryption

select large prime number p = 11

select a decryption key private key

d = 3

second part of encryption key

$e_1 = 2$.

third part = e_2 =

$e_2 = e_1^d \bmod p$

$= 2^3 \bmod 11$

$e=2=6$

Public key = $(\varepsilon_1, \varepsilon_2, P)$

Private key = d.

Pub key = $(2, 8, 11)$

Encryption - select random integer R;

$R=4$

$c_1 = \varepsilon_1^R \bmod P$

$= 2^4 \bmod 11$

$c_1 = 5$

calculate $c_2 = (P_T \times e^{2R}) \bmod P$ $\quad P_T = 7$

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

$c_2 = 6$

Cipher text $= (c_1, c_2)$ $\quad (5, 6)$

Decryption $= [c_2 \times ((c_1)^0)^{-1}) \bmod p$

$= 6 \times ((5)^3)^{-1} \bmod 11$

$= 6 \times 125^{-1} \bmod 11$

$= 125 x \bmod 11$ ← solve x $\quad x=3$

$= 6 \times 3 \bmod 11$

$= 18 \bmod 11$

$= 7$

Groups - A group is set of with a binary operation * that must satisfy four property.

closure property - If a & b are element of G then $c = a * b$ belong to G

Associative - If a, b, and c are element of G
$(a * b) * c = a * (b * c)$

Existence of identity - for all a in G there exist e thus that
$a * e = a$

Existence of inverse - for each a in G there exist a^{-1}
$a * a^{-1} = e$ or $a^{-1} * a = e$

Abelian group
└ Extra property commutative.
for all a, b in G.
$a * b = b * a$

Ring - Ring is denoted as $R = \langle \{\cdots\}, *, \square \rangle$ is algebric structure with two binary operation $*, \square$.

first operation satisfy - closure
Associative
commutative
{ identity
inverse

Second satisfy - closure
Associative

second operation should be distributive over

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

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

ring having commutative property called commutative ring.

Field - A field F is denoted by

$F = \langle \{\cdots\}, *, \square \rangle$ is commutative ring in which second operation satisfy all five property defined for first operation - except identity and has no inverse w.r.t to second.

A finite field has finite element.

For field to be finite no. of element should be p^n where p is prime n is +ve integer.

finite field are called Galois field.

a $F(p^n)$