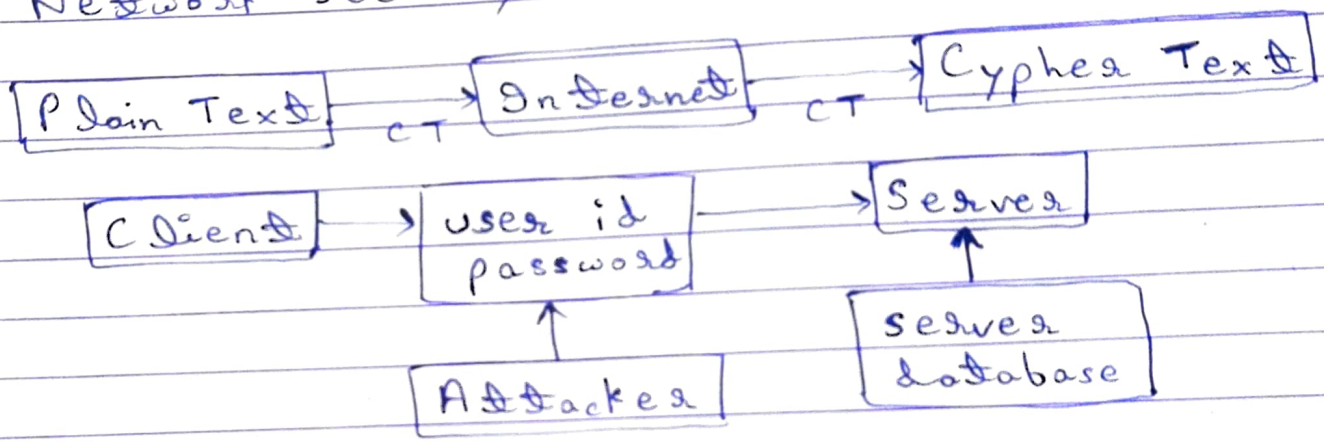
*) Cryptography

Sending the data from one end to another end securely is termed as cryptography.

- Security Model

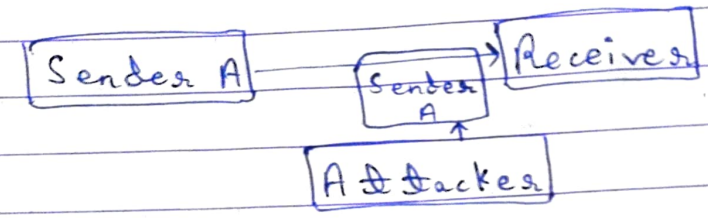
- No security
- Security through obsecurity
- Host security
- Network security



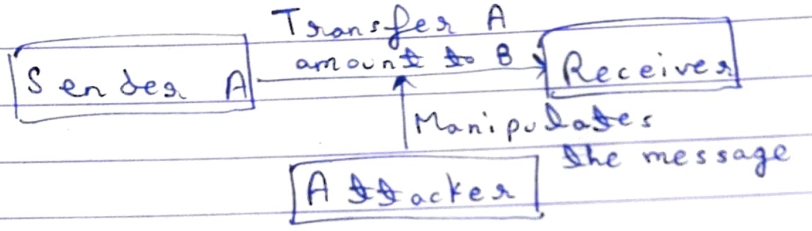
*) Principle of Security

1) Confidentiality
2) Authentication
3) Integrity
4) Non-repudiation
5) Access Control
6) Accessibility

- Interception causes loss of confidentiality



Authenticity



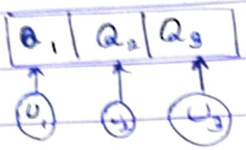
Integrity

- Non-repudiation

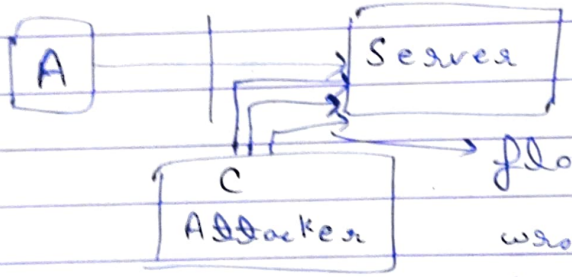
[Sender A] never send the message which B claims to receive → message content ← [Receiver B]

- Access - Control

↳ Who shall be allowed and what ?



- Availability



floods the server with wrong Id & password & keeps the server busy

Type of Attacks

- General View
  - Criminal Attack
  - Publicity Attack
  - Legal Attack
- Technical View
  - Theoretical side of attacks
    - Passive Attack
      - Release of message content
      - Traffic Analysis Attack
    - Active Attack
      - Interruption (Masquerade)
      - Modification
        - Replay Attack
        - Fabrication
          - Alteration Attack
  - Practical side of attacks
    - Application Level Attack
    - N/w Level Attack

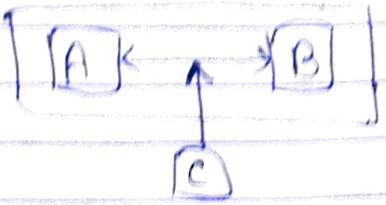
⇒ Criminal Attack

- Fraud
- Scams
- Identity theft
- Destruction
- IP theft
- Brand theft

→ Passive Attack

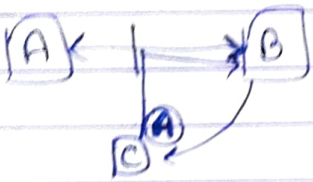
↳ Hard to detect

An individual is intercepting between two other invidual.

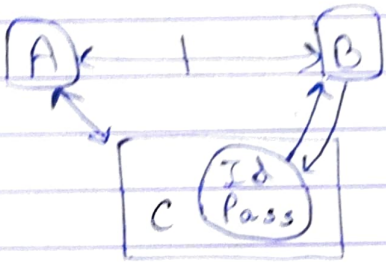


For security, individuals talk in code language.

→ Active Attack

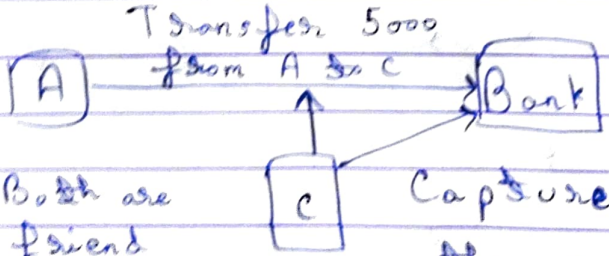


Interruption



Masquerade

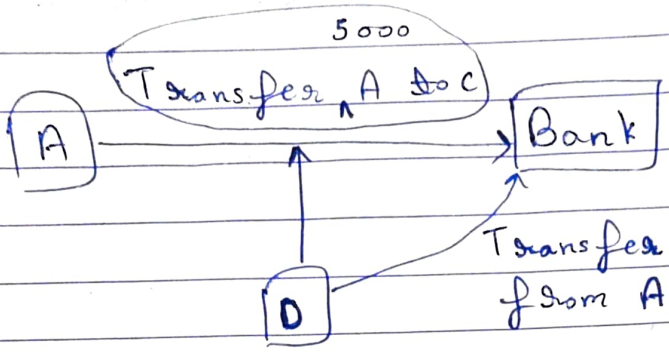
→ Replay Attack



Both are friend

Captures & resend the message to the server

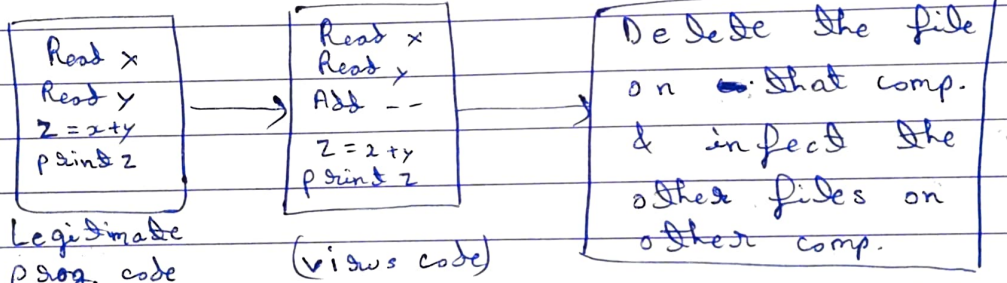
⇒ Alteration Attack



In this attack, attacker captures and modifies the message & send to the server

⇒ Practical side of attack

- Virus
- Worms
- Trojan Horse

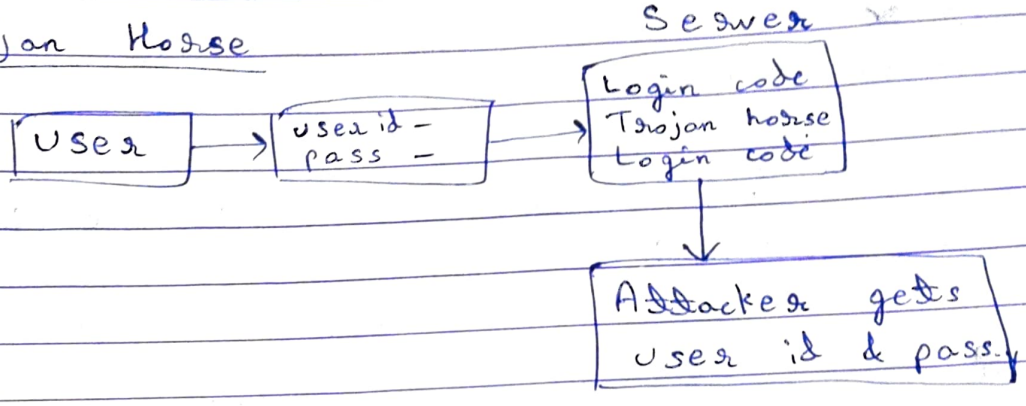


Worms

↳ A ~~malicious~~ worm is a type of malware or malicious software that can replicate rapidly and spread across devices within a network. Worms can also change and delete files or introduce other malware.

⇒ does not perform any destruction
⇒ only consumes resources

Trojan Horse



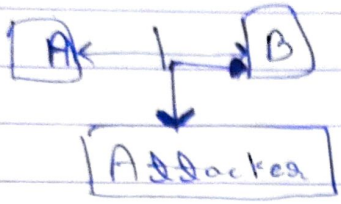
Specific Attacks

- Sniffing or Packet Sniffing or IP Sniffing
- Spoofing or Packet Spoofing or IP Spoofing
- Phishing
- DNS Spoofing → DNS poisoning

⇒ Sniffing

It is like a passive attack, where attacker silently listening the conversation & do not perform destruction. Conversation is in packet form that's why known as packet sniffing.

- Spoofing



Attacker changes the source add. of A and then starts communicating with B.

- Phising

Set up website which is a replica of the original website & gets the sensitive information from the host.

- DNS Spoofing

Attacker changes the IP of the server & try to enter into the ISP of the server or into the network.

Cryptography

*) Conventional & classical encryption techniques

Plain Text (PT) —Encryption→ Cipher Text (CT)

⇒ Substitution Cipher Techniques

- Caeser Cipher → Julius cipher

HELLO → KHOOR
PT CT

- Modified Caeser Cipher

CT ⇒ KWUM PMZM
⇓
PT ⇒ COME HERE

- Mono-alphabetic

A → B to Z
B → A to Z except B

- Homophonic Substitution Cipher

B → (C . D . E . ...)
D → (B ...)
↑ ↑
Similar sound

- Polyalphabetic Substitution Cipher

HELLO ⟶ YUVVW
PT CT

HELL → ZVWW ✓ ✗ YUVV ✗
PT CT

⇒ Transposition Cipher Techniques

- Rail Fence Technique

PT ⇒ COME HOME TOMORROW

O E O E O O R W
C M H M T M R O

CT ⇒ OEOEOORWCMHMTMRO

- Simple Columner Technique (Simple Round)

PT ⇒ COME HOME TOMORROW

5×5

C	O	M	W	
O	M	O		
M	E	R		
E	T	R		
H	O	O		

CT ⇒ COMWOMOMERETRHOO

- Simple Columner Technique (Multiple Round)

PT ⇒ COME HOME TOMORROW

5×5

C	M	E	O	
O	O	T		
M	M	R		
W	E	H		
O	R	O		

CT ⇒ CMEOOOTMMRWEHORO

- Vernan Cipher (One time pad)

PT ⇒ HOW ARE YOU

Converted value in no. ⇒ 7 14 22 0 17 4 24 14 20

One time pad (given) ⇒ NCB TZQ ARX

13 2 1 19 25 16 0 17 23

20 16 23 19 42 20 24 31 43

sum > 25

subtract 26

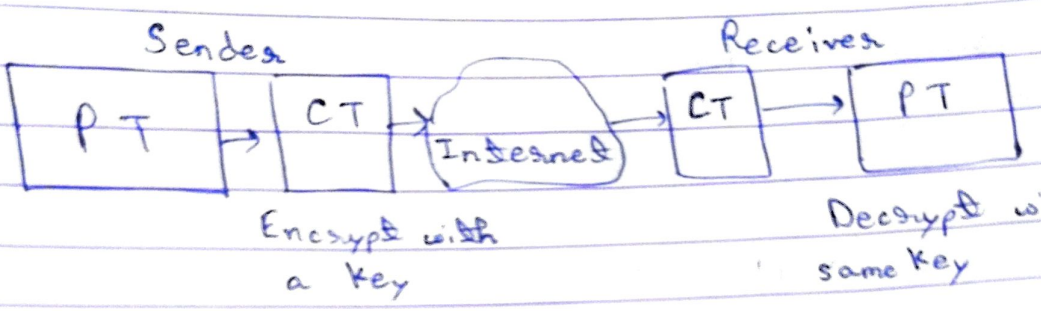
20 16 23 19 16 20 24 5 17

CT ⇒ U Q X T Q U Y F R

- Book Cipher

Take one meaningful sentence & use that same length sentence as one time pad for converting PT to CT.

*) Encryption - Decryption



Cryptography

- Symmetric key Cryptography (Same key)
- Assymmetric key Cryptography (diff key) [public key & private key]

- Diffie - Hellman key Exchange / Agreement Algorithm

  - Select two large prime no. [Sender & Receiver → n & g]
    (A) (B)

  - Sender selects a random no. x
  - Sender calculate $A = g^x \bmod n$
  - Sender sends this value A to receiver
  - Receiver selects a random no. y
  - Receiver calculates $B = g^y \bmod n$
  - Receiver sends B to sender A
  - Sender calculates $k_1 = B^x \bmod n$
  - Receiver calculates $k_2 = A^y \bmod n$

Sender (A)

$n = 11$, $g = 7$

$x = 3$

$A = g^x \bmod n$

$= 7^3 \bmod 11$

$\boxed{A = 2}$

$B = 4$

$k_1 = 4^3 \bmod 11$

$k_1 = 9$

Receiver (B)

$n = 11$, $g = 7$

$y = 6$

$B = g^y \bmod n$

$= 7^6 \bmod 11$

$\boxed{B = 4}$

$A = 2$

$k_2 = 2^6 \bmod 11$

$k_2 = 9$

$\boxed{k_1 = k_2 = 9}$

No need to transfer the key.

Sender (A)

$n = 11$, $g = 7$

$x = 3$

$A = 7^3 \bmod 11 = 2$

$\boxed{A = 2}$ → $B^* = 4$

$k_1 = 4^3 \bmod 11 = 9$

$\boxed{k_1 = 9}$

Attacker

$n = 11$, $g = 7$

$x = 8$, $y = 6$

$A^* = 7^8 \bmod 11 = 9$

$B^* = 7^6 \bmod 11 = 4$

$k_1^* = 8^8 \bmod 11 = 5$

$k_2^* = 2^6 \bmod 11 = 9$

$\boxed{k_1^* = 5}$ $\boxed{k_2^* = 9}$

Receiver (B)

$n = 11$, $g = 7$

$y = 9$

$B = 7^9 \bmod 11$

$\boxed{B = 8}$ → $A^* = 9$

$k_2 = 9^9 \bmod 11 = 5$

$\boxed{k_2 = 5}$

This type of attack is known as man-in the middle attack or bucket bridge attack.

*) Symmetric key Cryptography

Algorithm Types

Stream Cipher	Block Cipher

- Stream Cipher

- Perform the encryption one byte at a time

- XOR
  - Reversible
  - A = 101 PT
  - k = 110
  - C → A ⊕ k → 011 CT
  - C ⊕ k → 101 → A → PT

HOW ARE YOU → PT

CT

- Block Cipher

- Perform the encryption one block at a time
- faster
- Converts same PT to same CT → Drawback

HOW ARE YOU → PT

CT

Algorithm Mode

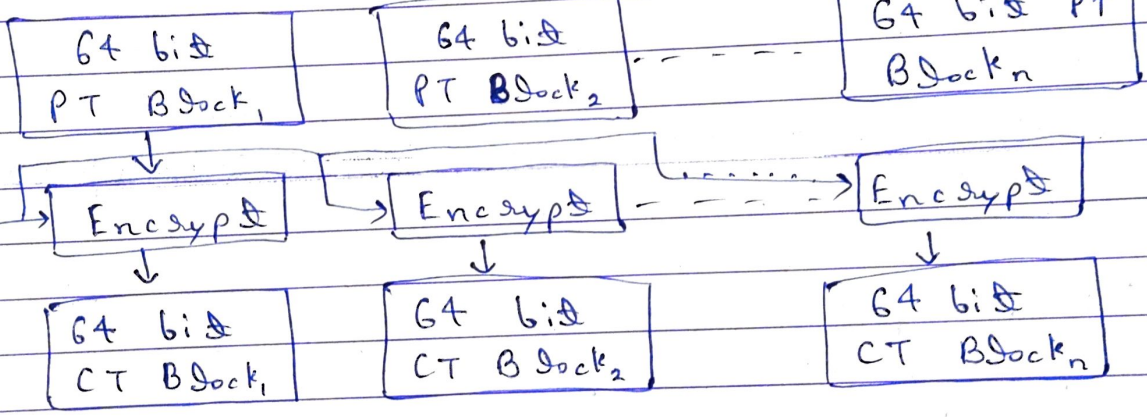
- Electronic Code Block (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feed Back (CFB)
- Output Feed Back (OFB)

⇓ Stream Cipher

⇓ Block Cipher but act as a stream cipher

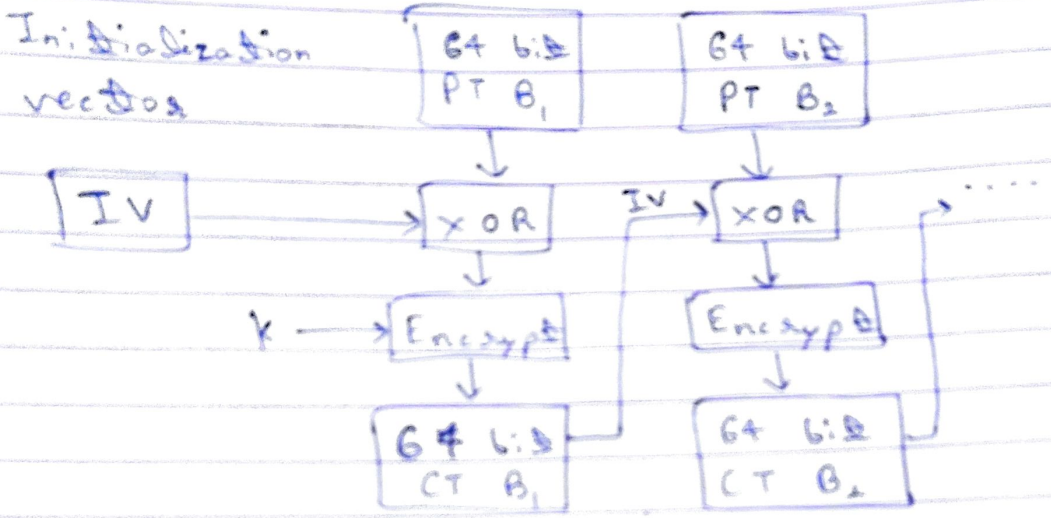
- Electronic Code Block (ECB)

Ex ⇒ 1024 bits



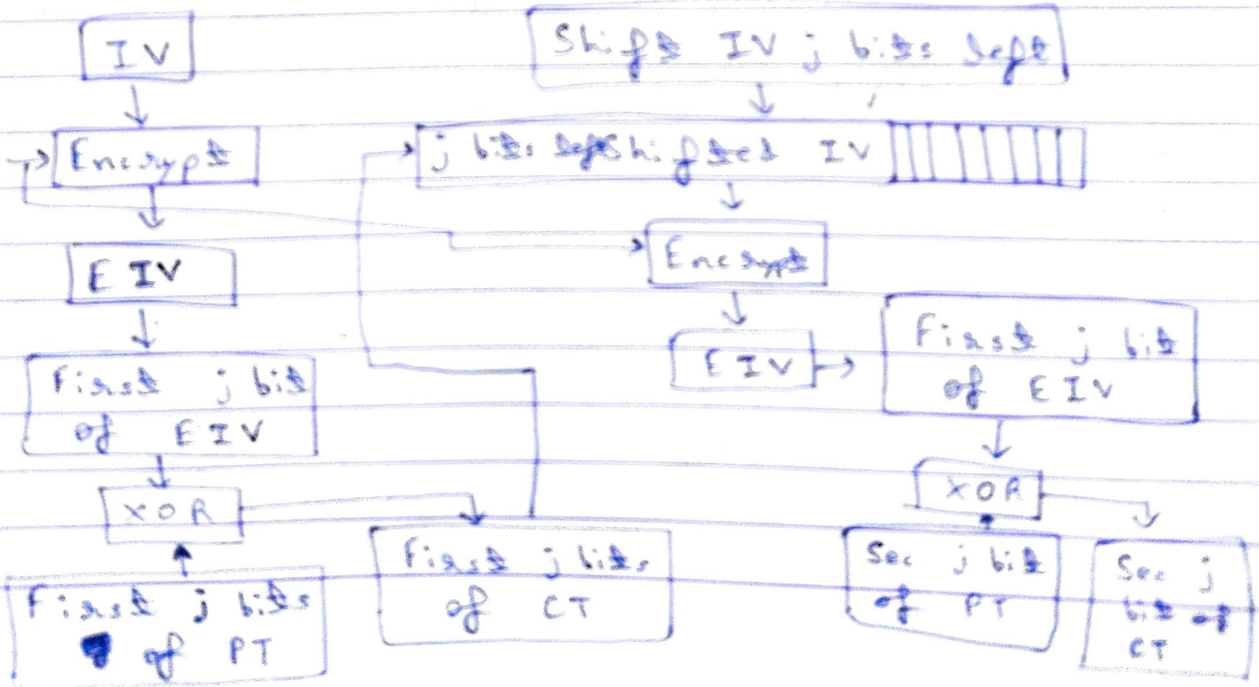
⇒ Slow Method
⇒ Same CT for same PT } Drawbacks
⇒ Always divide into 64 bits
⇒ Add padding if PT is smaller than 64 bit.

- CBC (Cipher Block Chaining)

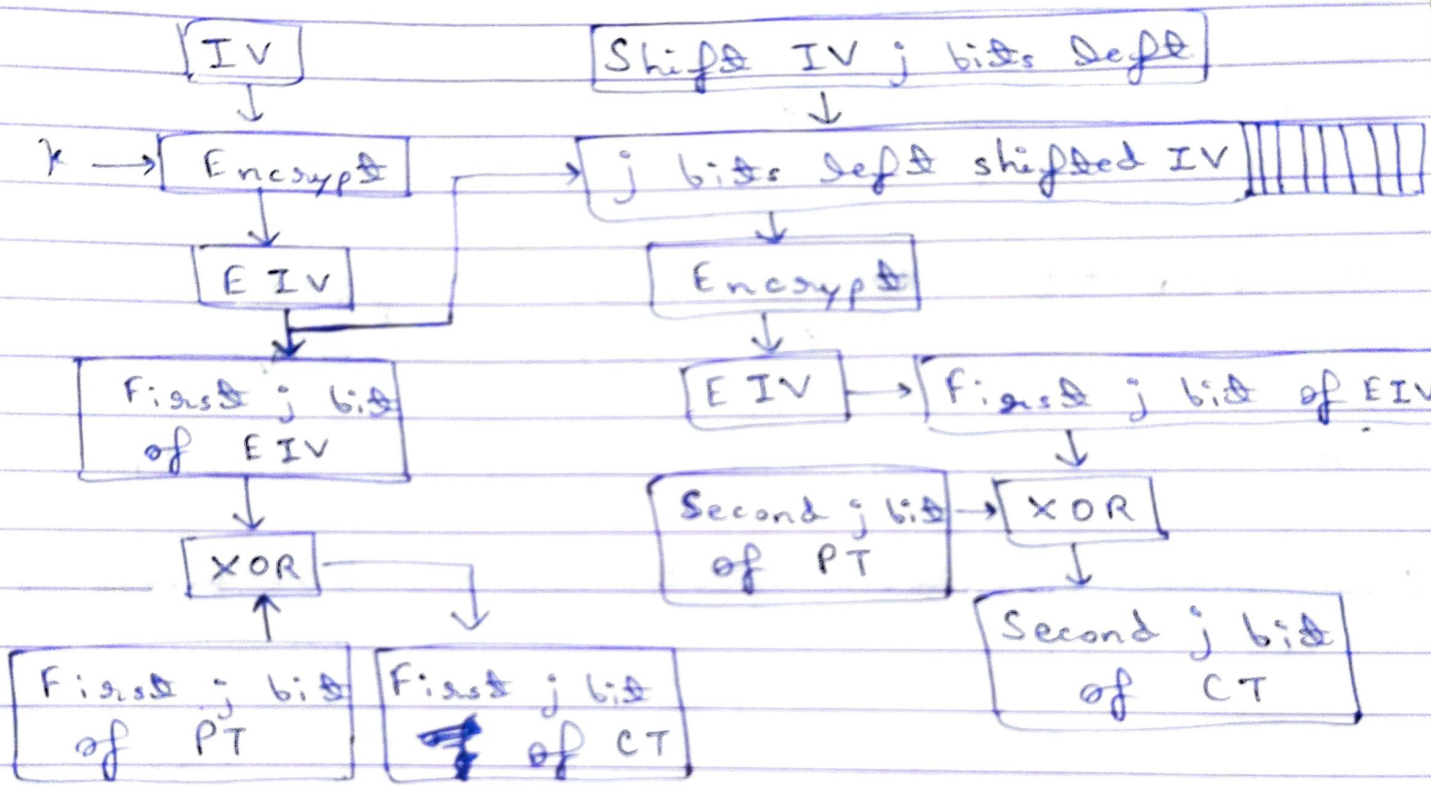


- It solved the problem of same CT for same PT
- But there is a problem of ~~error~~ errors in this case which is propagated if it occured in anyone block

- CFB (Cipher Feed Back)



- Same problem exists in CFB of error propagation.
- OFB (Output Feed Back)
- It solves the problem of error propagation.



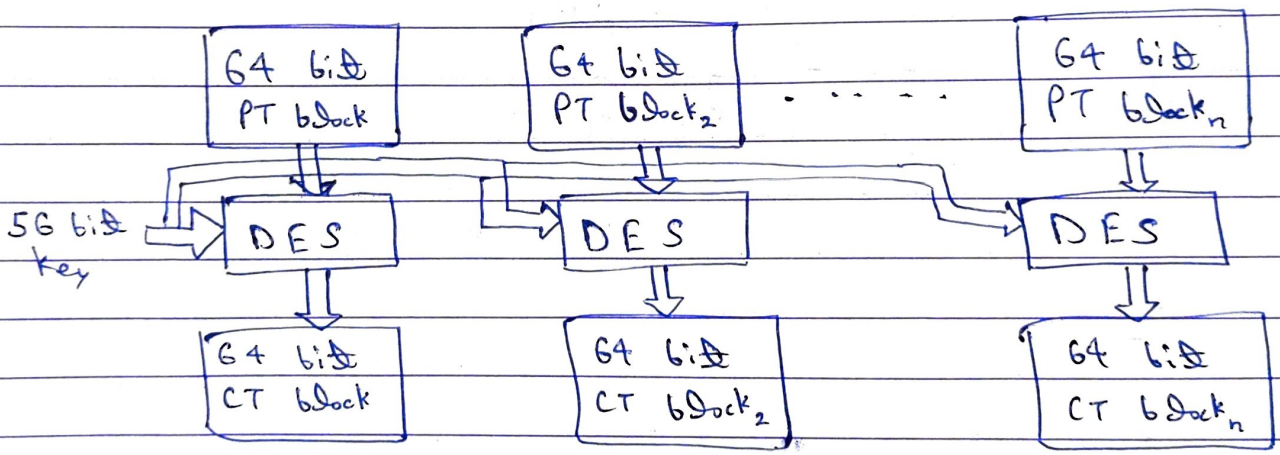
Differences between Symmetric key & Asymmetric key encryption

1) There are only two keys in Asymmetric key technique while there are various keys in symmetric key techniques when more than two persons are present.
2) Man in the middle problem in symmetric key technique
3) Symmetric key technique is faster than asymetric key encryption technique

Symmetric key Encryption	Asymmetric key Encryption
• It only requires a single key.	• It requires two keys
• Size of CT is same or smaller than PT	• Size of CT is same or larger than PT
• It is used when a large amount of data is req. to transfer.	• It is used to transfer small amount of data.
• It only provides confidenti-ality.	• It provides confidentiality, authenticity, & non-repudiation.
• More efficient	• Less efficient.
• Less security	• More security.

*) Data Encryption Standard (DES)

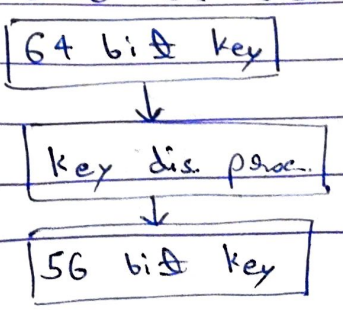
- Symmetric key
- Works on the principle of Block Cipher
- Uses substitution and transposition techniques
  - substitution ⇓ Confusion
  - transposition ⇓ Diffusion
- 64 bit PT block
- Same key is used for E & D
- 56 bit key (initially 64 bit)



- Key discarding process

Discard every 8th bit from the 64 bit key & make 56 bit key

1, 2, 3, 4, 5 .. 7
9 15
. . . .



Step-1) 64 bit PT block

Step-2) Initial Permutation

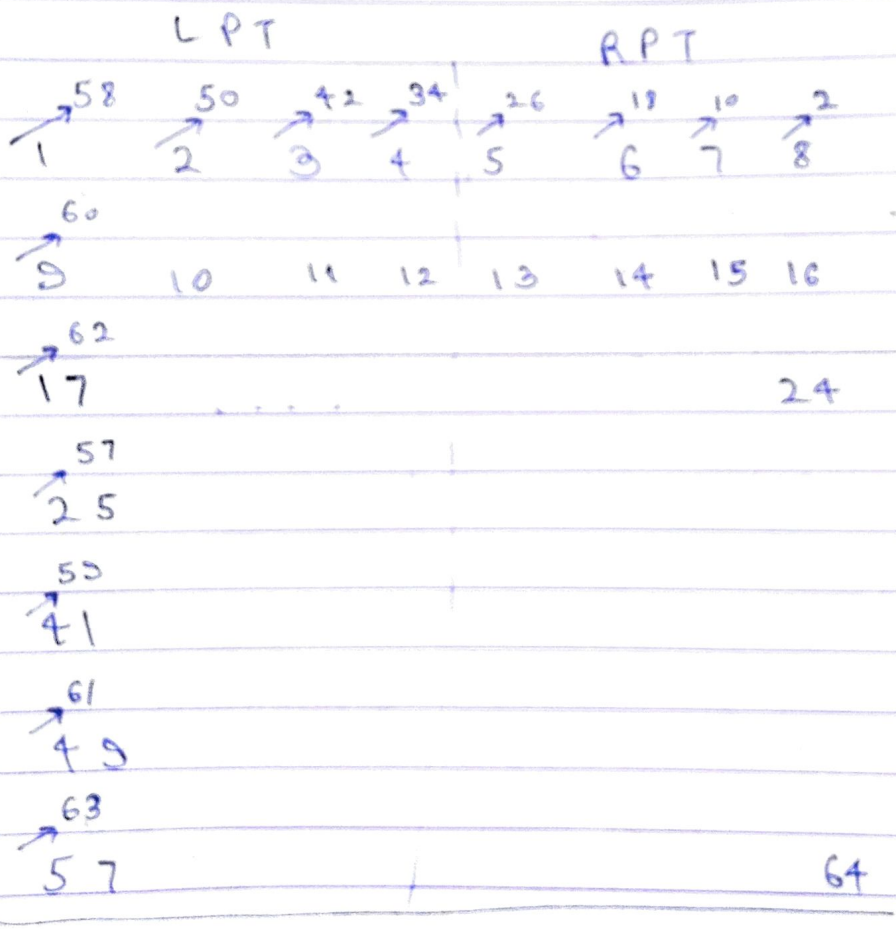
Step-3) LPT (32 bit) | RPT (32 bit)

LPT ⇒ Left PT
RPT ⇒ Right PT

Step-4) 16 Rounds | 16 Rounds

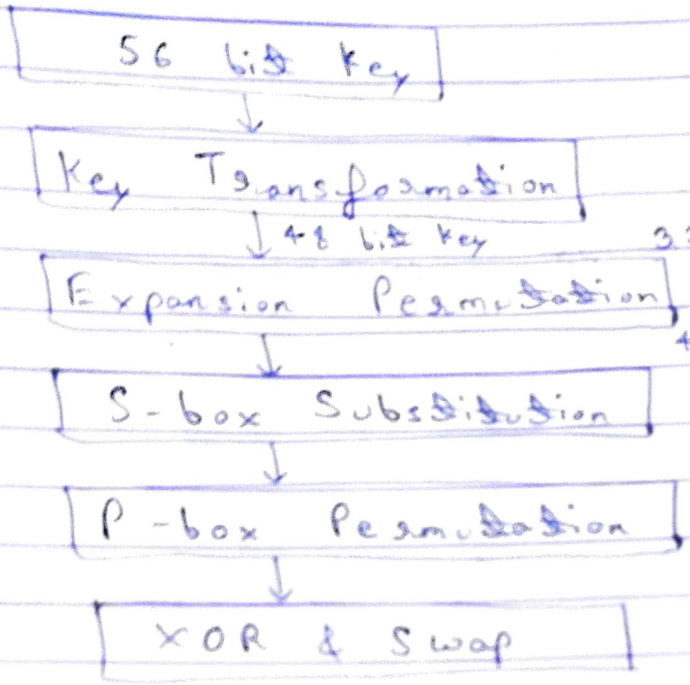
Step-5) Final Permutation

Step-6) 64 bit CT block

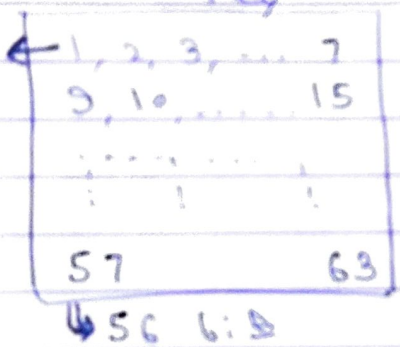


- Every bit is replaced

- One Round



Key

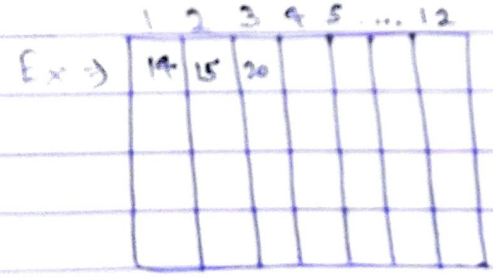


56 bit

Round No.
1, 2, 9, 16
⇓
Shift 1 bit left

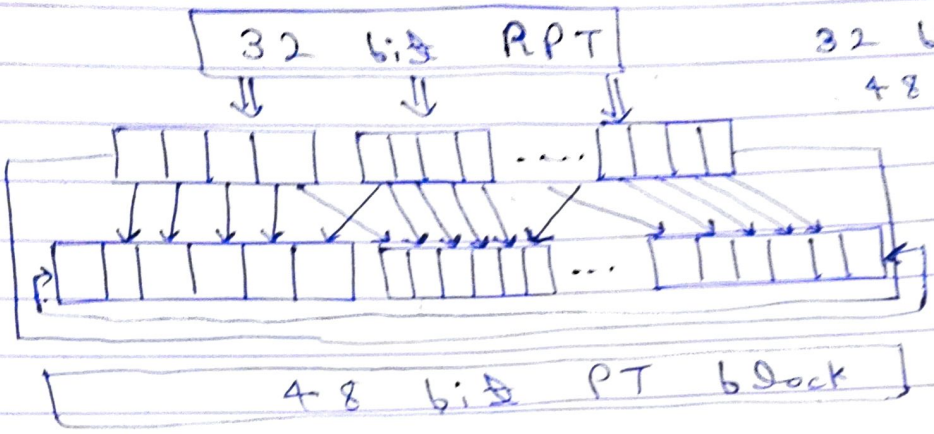
For rest of the rounds shift 2 bits

Compression Permutation Table of 48 bit



Put the content of 14th bit into 1st bit & 15th bit into 2nd bit

- Expansion Permutation

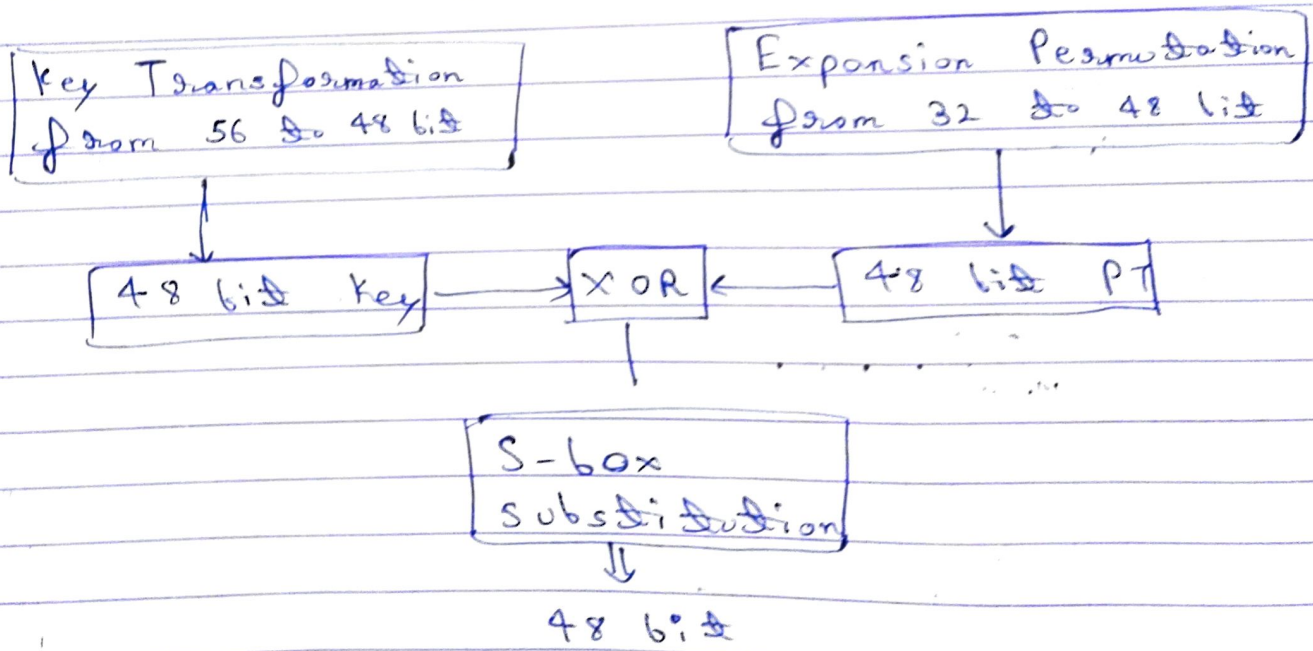


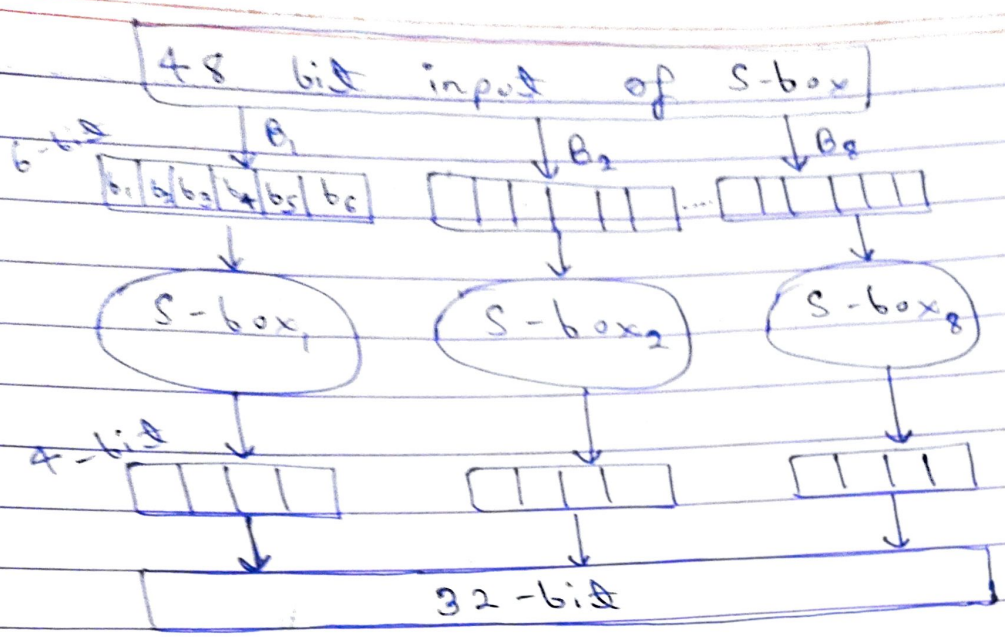
Conversion of 32 bit RPT to 48 bit RPT

- We will again change the position of bits & that will be the output of expansion permutation

- S-box substitution

Now the size of key & RPT both are 48 bit





b_1 & b_6 ⇓ Row no. 0 - 3

b_2 b_3 b_4 b_5 ⇓ Column no. 0 - 15

b_1 B_2 b_3 b_4 b_5 b_6

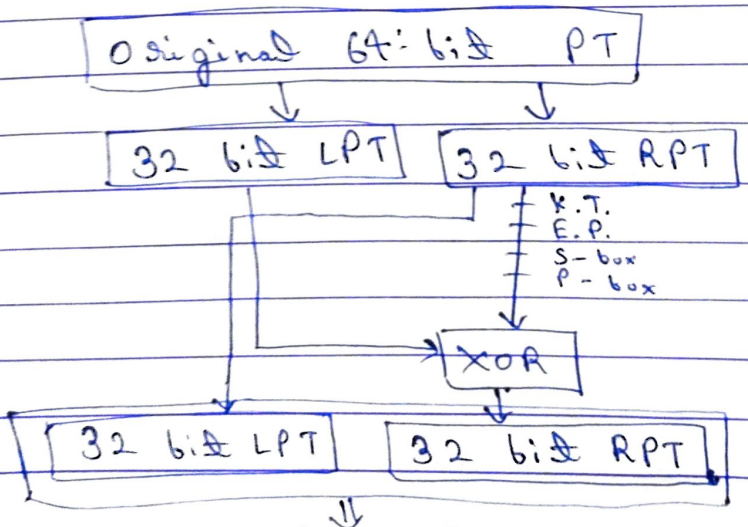
1 | 0 | 0 | 1 | Ex

S-box Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0																
1																
2																
3						x										

AES DIY
IDEA
encryption
operation

⇒ For next Round



~~All~~ ~~Books~~

$2^{56} = 7.2 \times 10^{10}$ years

strength of algorithm

*) DES Decryption

E → $k_1, k_2 \ldots k_{16}$ {16 Rounds → 16 keys}

D → $k_{16}, k_{15} \ldots k_1$

Strength of DES → key

k = 56

$2^{56} \Rightarrow 7.2 \times 10^{16}$ ⇒ Brute Force Attack

⇒ One computer capable to perform 1 DES per microsecond

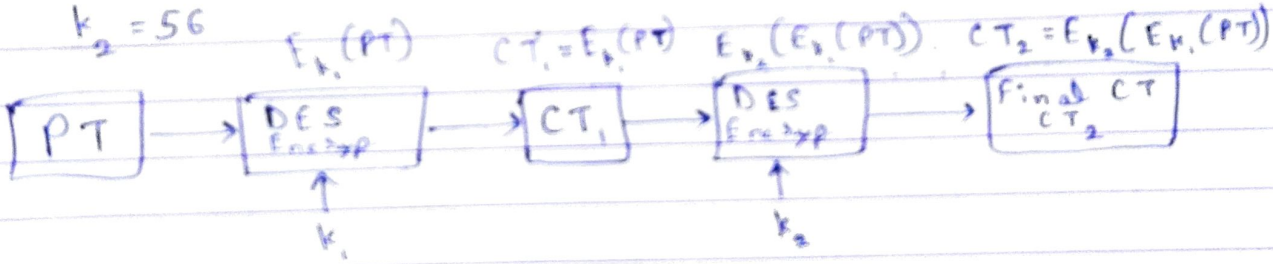
⇒ still it takes 1000 years

*) Double DES

- Perform DES twice

$k_1 = 56 \Rightarrow 2^{112} \Rightarrow 5.5 \times 10^{33}$

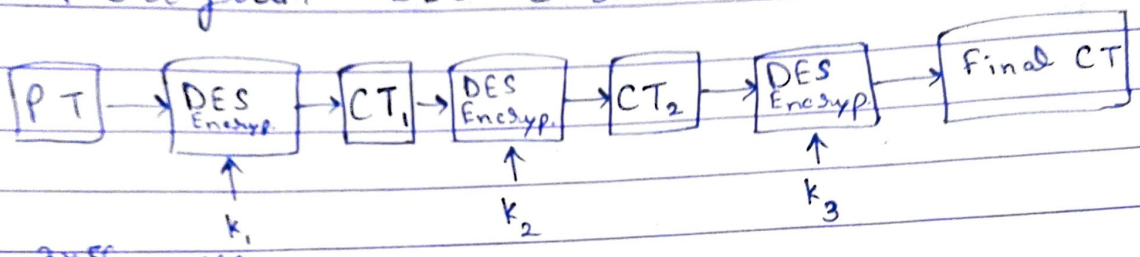
$k_2 = 56$



∴ The attacker performs encryp. from one side & decryp from another side & get the PT & this attack is termed as Man in the middle attack.

*) Triple DES

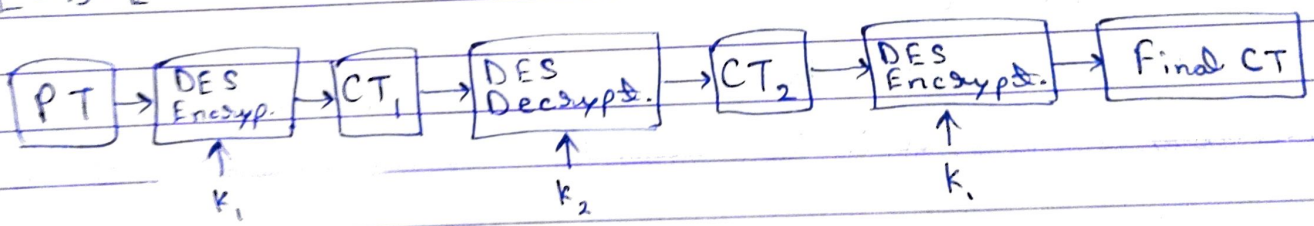
- Perform DES thrice



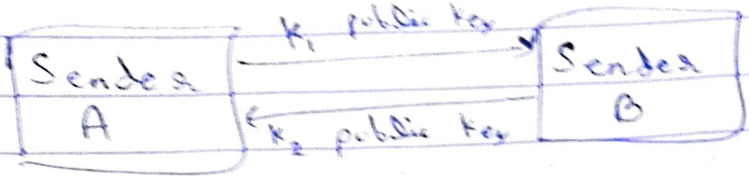
$2^{3\times56} \Rightarrow 2^{168}$

- It uses very high storage & computing power that's why we use two key sets for solving the issue.

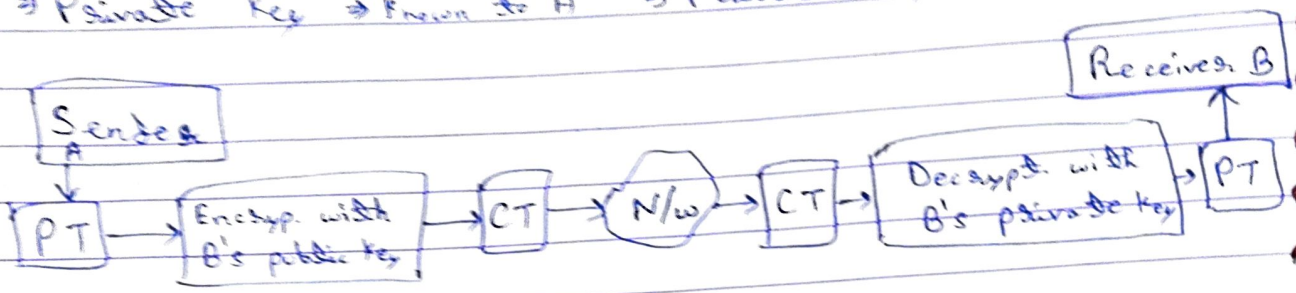
E-D-E



*) Asymmetric key Cryptography



⇒ Public key ⇒ known to A & others
⇒ Private key ⇒ known to A
⇒ Public key ⇒ known to B & others
⇒ Private key ⇒ known to B



*) RSA Algorithm

- Name on three scientist names
  - Ron Rivest
  - Adi Shamir
  - Leonard Adleman

Algorithm

-
- Select two large prime no. P & Q
- $N = P \times Q$
- Select then encryption key (E) (public key of B) such that E is not a factor of (P-1) & (Q-1)

- Select the private key or decrypted such that $D \times E \bmod (P-1) \times (Q-1) = 1$
- $CT = PT^E \bmod N$
- $PT = CT^D \bmod N$

Ex ⇒ P = 7 Q = 17

Calculate E, D & encrypt the PT = F

Verify your result by decrypting the CT

$N = 7 \times 17 = 119$

$6 \times 16 = 96$

$2 \times 2 \times 2 \times 2 \times 2 \times 3$

$2^x \; 3^x \; 4^x \; 5^{\checkmark}$

$E = 5$

$D \times E \bmod 96 = 1$

$D \times 5 \bmod 96 = 1$

$D = 77$

$CT = 6^5 \bmod 119$

$= 41$

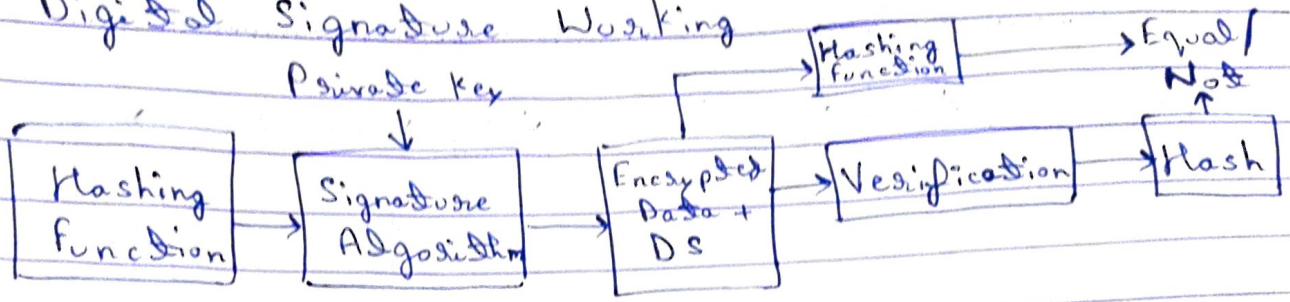
$PT = (41)^{77} \bmod 119$

$= 6$

Parameters	SKC	ASKC
- Key used for En & De.	- Same key	- Different key (public & private)
- Speed of E & D	- Faster	- Slower
- Resulting size of CT	- Same or less than the size of PT	- Larger
- No. of keys required	- Close to square of no. of communicating parties	- Only two keys
- Key agreement/ exchange	- Big problem	- No problem
- Usage	- E & D	- E & D, Digital signature & non-repudiation

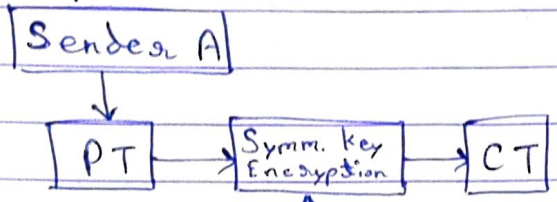
Digital Signature
- It is used for authentication
Ex. - You cannot deny to the transaction if there is a digital signature. → Non-repudiation
- Once commited then you cannot deny

Digital Signature Working

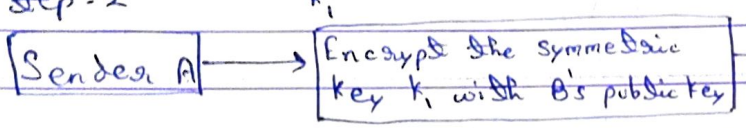


*) Best of both symmetric & asymmetric key cryptography

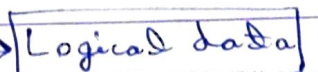
Step-1



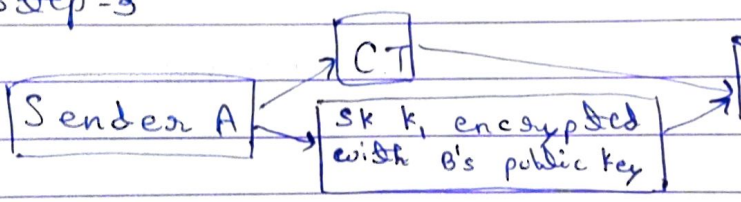
Step-2



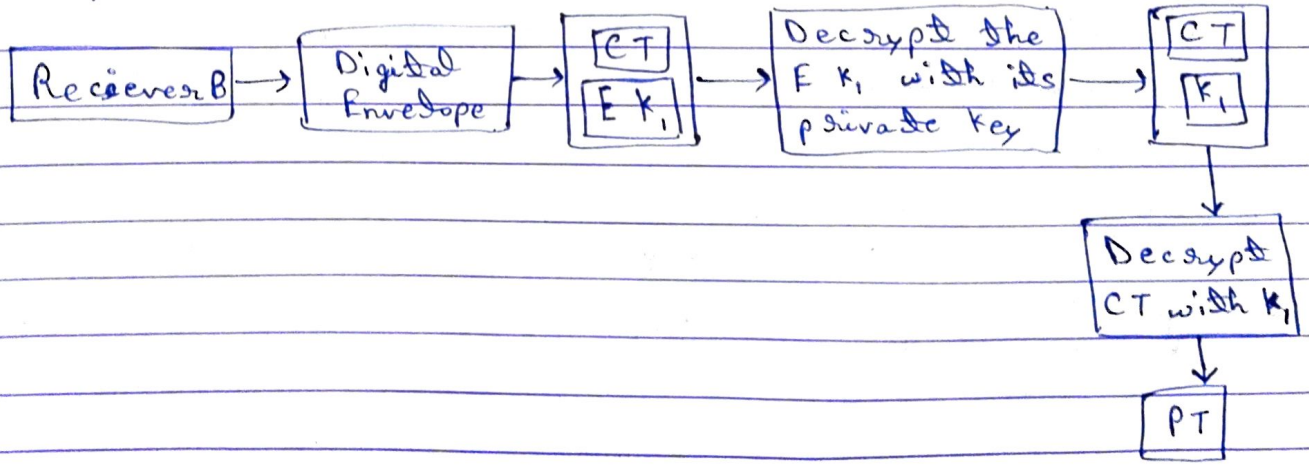
Key wrapping



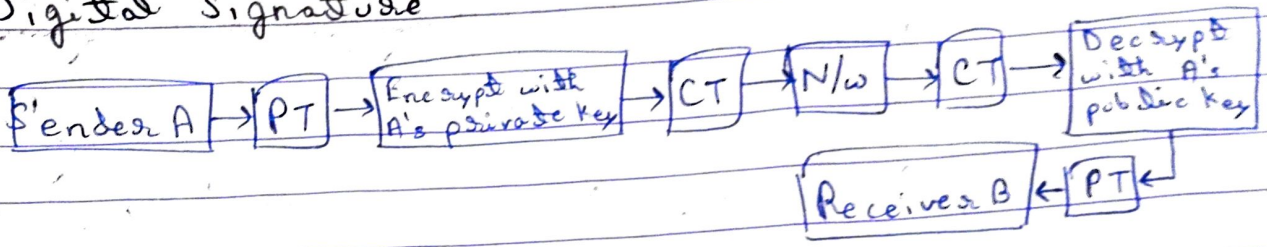
Step-3



Step-4



*) Digital Signature



- Authentication & Non-repudiation
  - ↳ Receiver knows the message is coming from authentic sender.
- In digital envelope, confidentiality is also maintained with authentication and non-repudiation

*) Message Digest (MD)

- Not an encryption method.
- Fingerprint or summary of message.
- Works on the principle of LRC & CRC.
- Select message digest too long so that it could not be same.
- Length - 128 or 160
  - ↳ 2^{128} ⇒ Repetition is rarely possible.
- If it repeats then we called it collision.

*) MD Algorithm

MD_1 → Ron Rivest, Prof., MIT

PT ⇒ 7392439

$7 \times 3 = \not{2}1$
$1 \times 9 = 9$
$9 \times 2 = \not{1}8$
$8 \times 3 = \not{2}4$
$4 \times 4 = \not{1}6$
$6 \times 3 = \not{1}8$
$8 \times 9 = \not{7}2$

MD = 2

⇒ It was attacked

MD_2 → Again cracked

MD_3 → During implementation → attacked

MD_4 → Attacked

MD_5 → Final Algorithm. (still used)

*) MD_5 Algorithm & SHA-1

Works on 128 — 160 — 20

④ 16 iterations ⑤ chaining algo.

⇒ For DS we use SHA-1

⇒ SHA-1 is not attacked till now

(Secured Hashing Algorithm)

MD_5

⇒ Padding

⇓

⇒ Convert original message (PT) into 64 bit less than the exact multiple of 512.

PT ⇒ 1000 bit ⇒ 1472 (1536-64)

472 padding bit

⇒ [original message] ⊕ [Padding]

⇓

[original message | Padding] ⊕ [Append]

⇓

[O | P | A]

⇓ Multiple of 512

⇒ Divide the message which is to be hashed into a no of blocks of size 512 bit.

original message (hashed)			
512 bit block	512 bit block	.....	512 bit block