→ Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

→ Cryptography is associated with scramble plaintext or ordinary text into cipher text this process is called encryption, then back again into plaintext this process is known as decryption

Cryptography Attack circumventing = दरकिनार करना

→ A cryptography attack is method of circumventing the security of cryptographic system by finding
  → weak in a code, cipher, cryptographic protocol or key management scheme

→ Attacks are typically categorized based on the action performed by the attacker.
An attack, thus, can be passive or active

Passive Attack :-

The main goal of passive attack is to obtain unauthorised access to information

for example :-

actions such as intercepting or eavesdroping on the communication channel can be regarded as passive attack

→ An passive attack often seen stealing information passive attack

Active Attacks

→ An active attacks involves changing the information in someway by conducting some process on the information

For example

→ Modifying the information in an unauthorized manner.

→ Alteration of authentication data such as originator name or timestamp associated with information.

→ Unauthorized deletion of data

Other types of attack

Dictionary Attack

→ In this attack, attacker build a dictionary of ciphertexts and corresponding plaintext that has learnt over a period of time.

→ In future, when an attacker get the ciphertext, he refer the dictionary to find the corresponding plaintext.

Brute Force Attack

→ In this method, the attacker tries to determine the key by attempting all possible keys.

→ If the key is 8 bits long, then the number of possible key is $2^8 = 256$.

→ This attack is variant of brute-force
→ It is used against the cryptographic hash function.

Man in Middle Attack

~~This target are~~

→ The target of this attack are mostly public key cryptosystem where key exchang is involved before communication takes place.

→ Host A wants to communicate to host B, hence request public key of B.

→ An attacker intercepts this requests and send his public key instead

Thus, whatever host A send to host B, the attacker is able to read.

→ In order to maintain communication the attacker re-encrypt the dater after reading with his public key sent to B

Buffer overflow Attack

→ A buffer is a temporary space for data storage.

→ Buffer overflow occurs if the data is stored by program in a buffer is greater than the maximum capacity of the buffer

→ The extra data can overflow into adjacent buffer corrupting and overwriting the valid data held in them

Ping of death attack

→ Ping of death attack takes advantage of TCP-IP protocol

→ The weakness is that many computer system cannot handle an IP packet larger than the maximum IP packet size of 65535 bytes.

Buffer overflow in Ping of Attack

DoS (Denial of service Attack)

DoS is an attack targetting the availabil

of web applications.

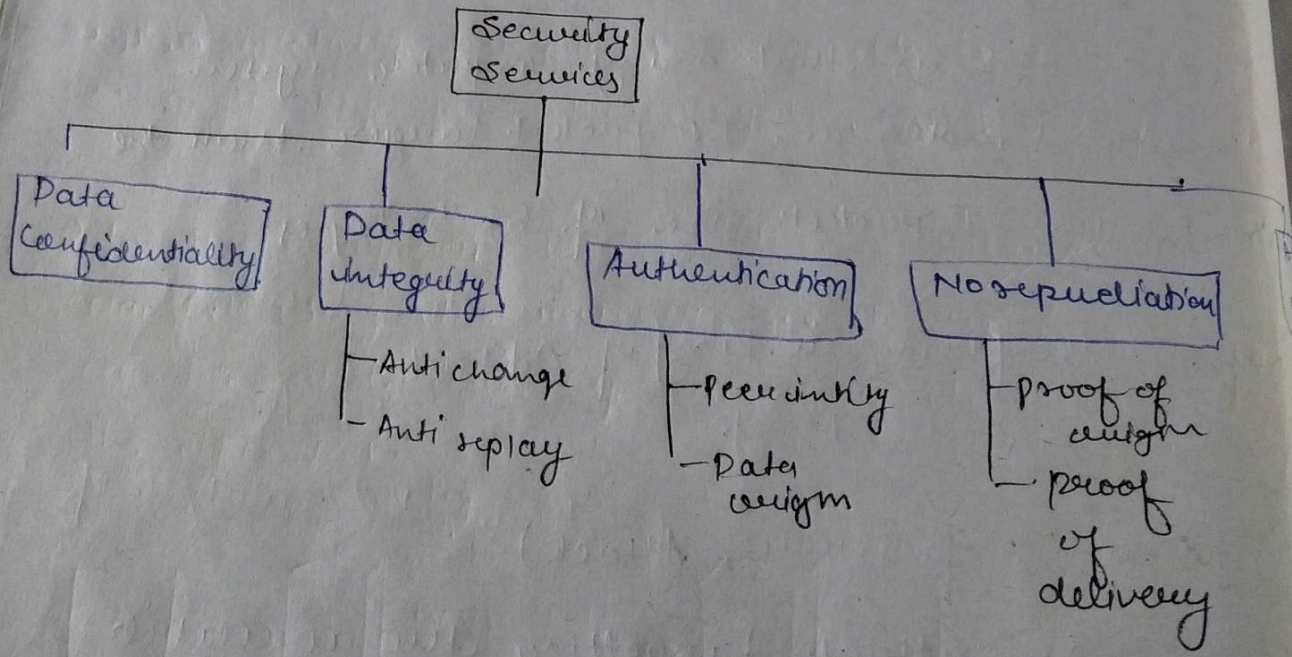
Cryptography mechanism :-

→ An element of a cryptographic application, process, module or device that provides a cryptographic service such as confidentiality, integrity, source authentication, and access control
• (e.g encryption and decryption, digital signature generation and verification)

→ Security service and Mechanism

Security services and mechanism are closely related because a mechanism or combination of mechanisms are used to provide a service

Security services



Authentication:-
assures recipient that message is from the source that it claim to be from.

Access Control:- Control who can have access to resource under what condition.

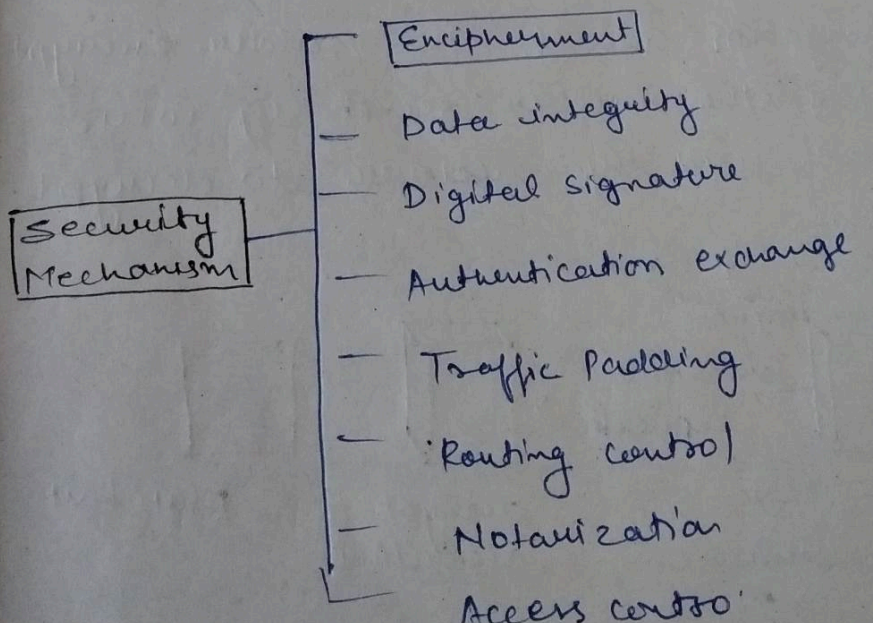
Availability:- available to authorized entities for 24/7

Confidentiality:- information is not made available to unauthorised individual.

Integrity:- assurance that the message is unaltered

Non-Repudiation:- protection against denial of sending or receiving in the communication

Security Mechanism



Relationship between security service and mechanism

Service of security	Security Mechanism
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity

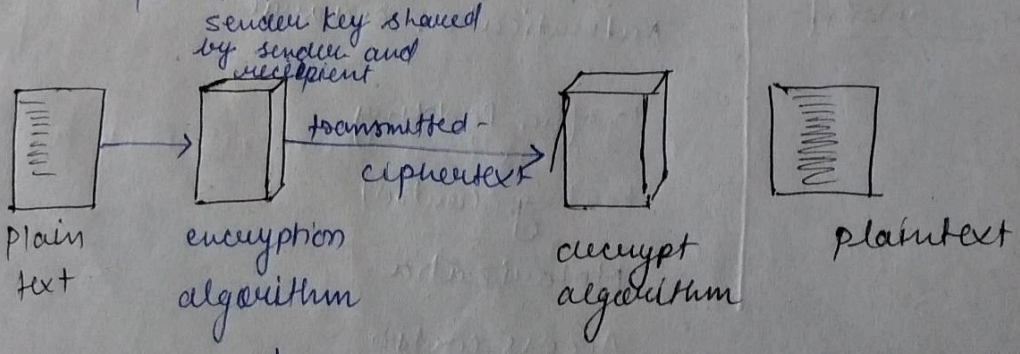
Conventional Encryption Model

Conventional Encryption

→ Conventional Encryption is a cryptographic system that uses the same key used by the sender to encrypt the message and by the reciever to decrypt the message.

→ It is relatively fast process since it is uses a single key for both encryption and decryption.

→ In this encryption model, the sender encrypts plaintext using the reciever's secret key which can be later used by reciever to decrypt the ciphertext.



thus the message is reach and security is maintained.

→ This is very old technique that is why this model is called conventional encryption.

Conventional encryption has mainly 5 ingredients

① Plain-text :- It is an original data that is given to algorithm as input.

② Encryption-Algorithm :- The

The encryption Algorithm performs various transformations on plain-text to convert into cipher text

③ Secret key -

→ The secret key is also an input to algorithm.

→ The encryption algorithm will produce different output based on the keys used at that time.

④ Ciphertext

It contain encrypted information because it contain a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it

⑤ Decryption algorithm :-

Ciphertext and secret key is input here and it produces plain text as output.

Requirements for secure use of conventional encryption

→ We need to strong encryption algorithm.

→ The sender and receiver must have obtained copies of the secret key in a secure ~~form~~ fashion and must keep the key secure

Advantage of Conventional Encryption

① simple ② Uses fewer computer resources

③ Fast

① Simple :- This type of encryption is easy to carry.

② Uses fewer computer resources :-
conventional encryption does not require a lot of resources when compared to public key encryption

③ Fast :-
Conventional encryption is much faster than asym asymmetric key encryption

Disadvantage of Conventional Encryption Model

① Origin and authenticity of the message cannot be guaranteed.

② key management and key agreement is big problem.

Substitution Cipher

Transposition Ciphers

Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending upon a key

For example

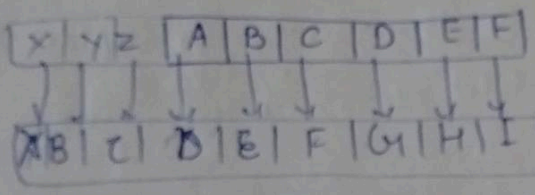
with shift of 1, A would be replaced by B, B would become C and so on.

Mathematical Representation

Encryption of letter by shift n can be described mathematically as

$E_n(x) = (x+n) \bmod 26$ (Encryption phase with shift n)

$D_n(x) = (x-n) \bmod 26$ (Decryption phase with shift n)



Substitution Technique

- Ceaser Cipher:-

∴ It is a type of substitution cipher i.e each letter of given text is replaced by a letter some fixed number of position down the alphabet.

→ This code can easily crack.

Example. Text: ATTACKATONCE

shift: 4

Cipher: EXXECGOEXSRGI

Modified Ceaser Cipher

→ In Modified Ceaser Cipher each alphabet of plain text is may not necessarily replaced by k+ key but's down the order instead the value of key is incremented and then it is replace with new key value.

→ The encryption

Modified Ceaser Cipher

1. Simple Substituted Technique
2. Key (k) range : 1-25
3. Working - Encryption
   1. Each alphabet in the message is replaced by another alphabet (k) place down the line.
4. Working - Decryption
   1. Each alphabet in the message is replace by another alphabet (k) places up the line
5. Better security compared to Simple Ceo Caesar Ciph

Ceaser Cipher Technique

1. Simple Substitution Technique
   Encryption
2. Each alphabet in the message is replaced by another alphabet 3 places down the line

Decryption

3. Each alphabet in the message is replaced by another alphabet 3 places up in the line

Monoalphabetic Cipher

⇒ Permutation

Permutation of a finite set of elements 'S' is an ordered sequence of all elements of 'S', with each element appearing exactly once

→ S = {a, b, c}

Monoalphabetic Cipher

→ The "cipher line can be any permutation of 26 alphabetic characters

→ This would seems eliminate brute-force techniques for cryptoanalysis

→ A single cipher alphabet is used per message

Example A → (B to Z)
B → (A or C to Z)

Homophonic Cipher

Hill cipher - Introduction

→ Hill cipher is a polygraphic substitution cipher based on linear algebra

→ Hill used matrices and matrix multiplication to mix up the plaintext

→ In a polygraphic substitution cipher, plaintext letters are substituted by in larger groups, instead of substituting letter individually

2) Block of plain text is replaced to get another block of cipher text

[ABCD]

[XZAB]

POLYGRAPHIC

3. BASIC POLYGRAM SUBSTITUTION CIPHER METHOD.

→ polygram alphabetic suggests this achieved by using several two, three and many key

→ In polgram cipher technique, a block of alphabet is replaced by another block of alphabet.

Example BECOME could be replaced by XAYKJIA

Problem

→ It occupies me
the encoded da

→ Secure The

→ The characte
itself in

→ It will
identify
tapping
this re

Polygraphic Su

Polygraphic substi
of letters. Then
one to of pre
and by ano

Polygraphic Su

① Playfair Cip

Problem

-> It occupies more storage for maintaining the encoded data

-> ~~Secure~~ The final result is ^

-> The character is replaced by character itself in each block differently.

-> It will make for the intruder to identify the character, thus by trapping the message in earlier way this result in security lapses.

Polygraphic Substitution Cipher

Polygraphic substitution divide the plaintext into group of letters. Then, they replace each group of letters by one of pre-defined letters, numbers, graphic symbols and by another group of characters

Polygraphic Substitution Ciphers

① Playfair Cipher ② Two-square Cipher ③ Four square cipher

Polyalphabatic cipher

It is also known as Vigenere cipher

* It consist of the 26 Caesar cipher with shifts 0 through 25.

Encryption Process:-

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

Decryption Process:-

$$P_i = (C_i - K_i \bmod m) \bmod 26$$

Key : deceptive

Plaintext: wearediscovered

Ciphertext: ZICVTWQN

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

Vigenere Cipher - Cryptanalysis

* Determine the length of keyword
* key and plaintext share the same frequency distribution of letters, a statistical technique can be applied

Vigenere proposed autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key

Vernam Ciphers

* Need of ultimate defense against cryptanalytic attack
* Length of keyword = length of the plaintext
* No statistical relationship to it
* Vernam cipher work on binary bit rather than letter
* $C_i = P_i \oplus K_i$

where

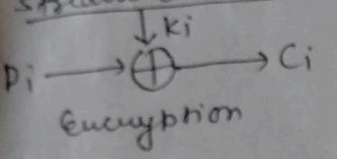
P_i = ith binary of the plaintext

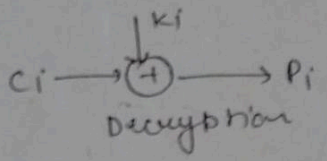
K_i = ith binary of the key

C_i = ith binary of the ciphertext

$\oplus$ = XOR operation

Cryptographic stream cipher





Vernam Cipher – Cryptoanalysis

* Construction of the key
* The use of ~~two~~ a running loop of tape that eventually repeated the key

Transposition Cipher

Rail Fence Technique

→ Here the position of letter of plaintext are going to be change

→ The plaintext is written down as a sequence of diagonal and then read off as a sequence of rows

Example

→ message → meso academy is the best

Depth: 2

m e s b a c a d e m y

m		s		a		a		e		y		s		h		b		s	
	e		o		c		d		m		i		t		e		e		t

NSAA EYSHBS EO C DM I TEET

Row column Transposition

Plaintext :

Kill Corona Virus at twelve am tomorrow

→ K 0 3 1 2 5 6 7

K	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	r	o	w	y	z

Ciphertext = ~~LATARLVTMOCIWT~~

LATARLVTMOINAER KOSVOCIWTW OREOY

RULMZ

0	3	1	2	5	6	7
L	A	T	A	R	L	V
T	M	O	I	N	A	E
R	K	O	S	V	O	C
I	W	T	W	O	R	E
O	Y	R	U	L	M	Z

More complex

Ciphertext TOOTRAISWUAMKYLTRIORNVOL LAD

RMVECEZ

Cryptanalysis :-

→ Cryptanalytic Attacks :- Based on info known to the cryptanalyst.

→ Most difficult : Ciphertext only (Not even encryption algorithm)

→ Type of cryptanalytic attacks :-

① Ciphertext Only ② Known Plaintext ③ Choosen Plaintext

④ Chosen Ciphertext ⑤ Chosen text

Type of Attack	Known to cryptanalyst
Ciphertext only	* Encryption Algorithm * Ciphertext
Known Plaintext	* Encryption Algorithm * Ciphertext * One or more PT-CT paired formed with secret key
Choosen Plaintext	* Encryption Algorithm * Ciphertext * PT message chosen by cryptanalyst, together with CT generated the secret key
Choosen Ciphertext	* Encryption Algorithm * Ciphertext CT chosen by cryptanalyst, together with its corresponding decrypted PT generated with the secret key

Steganography :-

* Conceal the existence of the message
* Hiding the message
* Not an encryption scheme
* Cryptography renders the message unintelligible to outsiders by various transformation of the text.

Example

Simply encrypt correct reading

Exactly twice secret

Steganography
* Character marking
* Invisible ink
* Pin Puncture
* Typing Typewriter color ribbon

ML
Network
Data

(AI)

Drawback
* Lot of overhead
* Once the system is discovered it become virtually worthless

Difference between Block cipher and Stream cipher

Block Cipher :- Block cipher is an encryption algorithm that takes a ~~input size~~ fixed size of input say b bits and produces a ciphertext of b bits again.

→ If the input is longer than b bits it can be divided further.

For different applications and uses, there are several modes of operation for block ciphers.

① Electronic code Book ② Cipher Block Chaining

③ Cipher Feedback Mode ④ Output Feedback Mode

⑤ Counter Mode

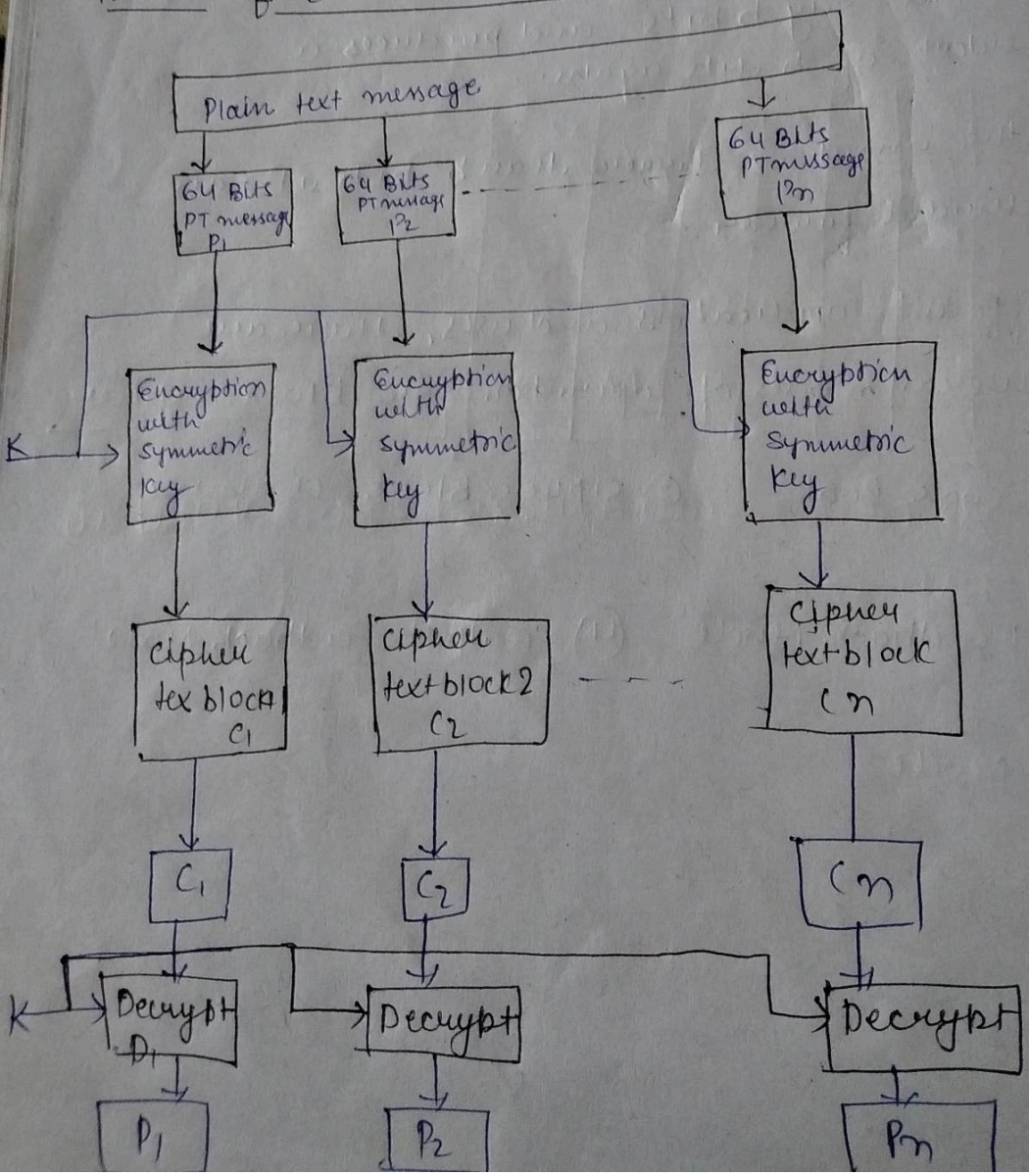
Electronic Code Book

→ Electronic Code Book is the easiest block cipher mode of functioning.

→ It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted cipher text

→ If message is longer than b bits in size, then entire message will be divided into 64 bits size then perform encryption by symmetric key

Procedure of ECB is illustrated Below



→ If Block sa
then attacke

→ The messag
so it is

Adv

→ Pa

→ Sin

→ If Block same then cipher text will be same then attacker will be getting clue

→ The message suffer from repeating message so it is suitable for short message

Advantage of FCB

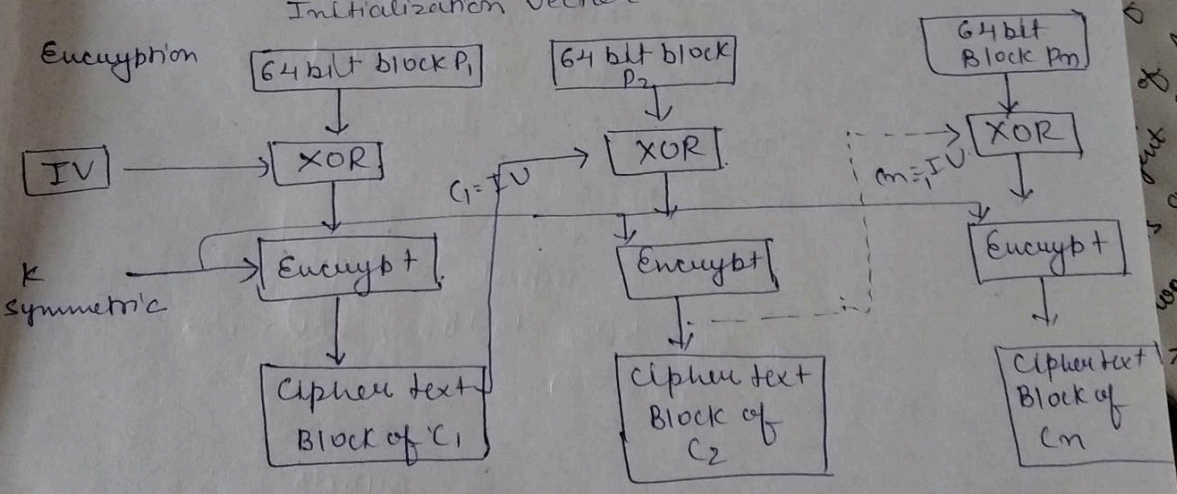
→ Parallel encryption of blocks of bits is possible thus it is faster way of encryption

→ simple way of the block cipher

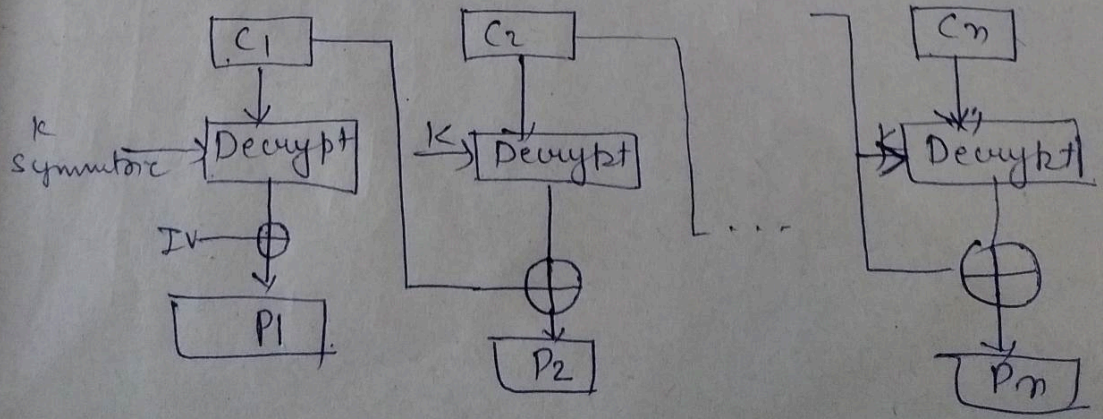
Cipher Block Chaining Encryption Process

- It works on the principal of feedback
- If same block then there will will must be different cipher block
- It is a advancement made on ECB since ECB compromises some security requirements.
- the - prem
- In CBC the previous cipher block is given as input to next encryption of algorithm after XOR with original plaintext block.
- In nutshell here, a cipher block is produced by encryption an XOR output of the cipher block and present plain text.

IV 64 bit binary number will select Initialization vector



Decryption



Advantage of CBC

- CBC works well for input greater than b bits
- CBC is good authentication mechanism
- Better resistive nature towards cryptanalysis than ECB

Disadvantage of CBC

- Parallel Encryption is not possible since every encryption requires a previous ciphes

Cipher FeedBack Mode

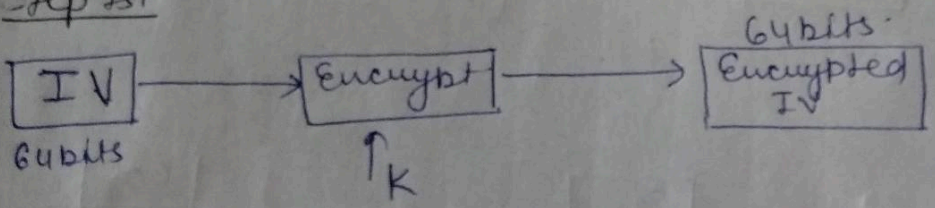
→ In this mode the ciphen is given as feedback to the next block of encryption with some new specification

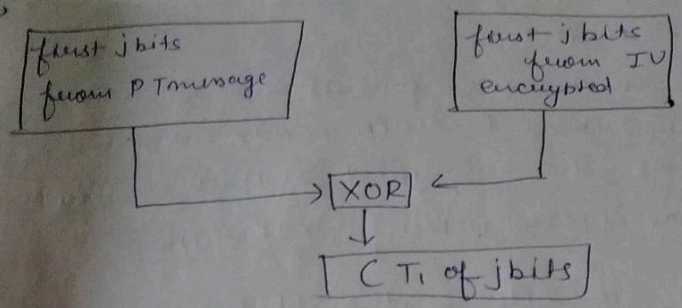
→ first, an initial vector IV is used for first encryption and output divide as a set of s and b-s bits.

→ The left-hand side s bits are selected along with plaintext bits to which an XOR operation is applied.

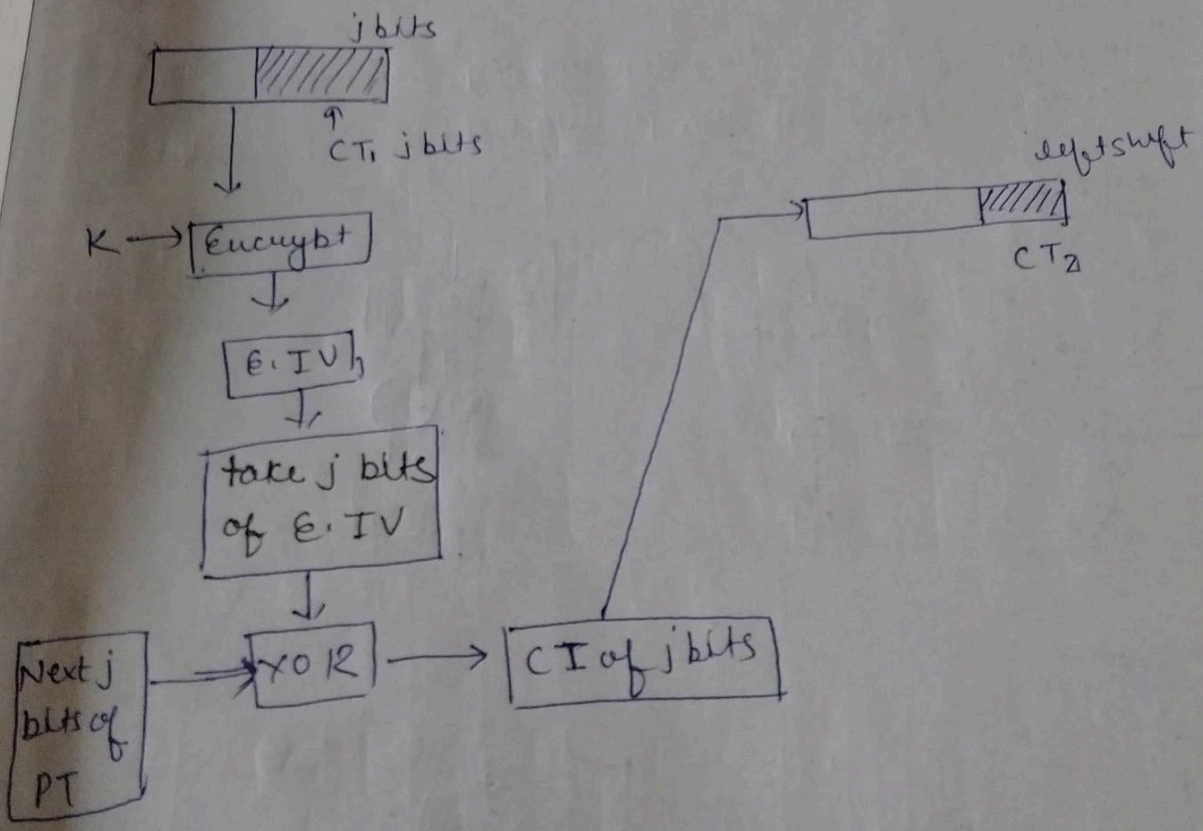
→ The result is given as input to shift register having b-s bits to lhs, s bits to lhs and process continues.

Step Ist





→ shift left j bits the IV the j bits from right will be unpredicted so put CT_1 with j bits in the j bits unpredictable



OFB

Output Feedback Mode :-

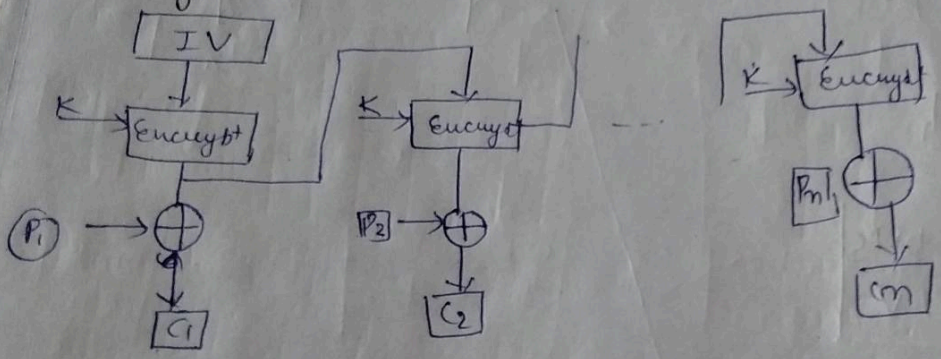
→ The output Feedback mode follows nearly same process as the cipher Feedback mode except that it sends the encrypted output instead of the actual cipher which is XOR output

→ In this mode, all bits of the block are sent instead of sending s data bits.

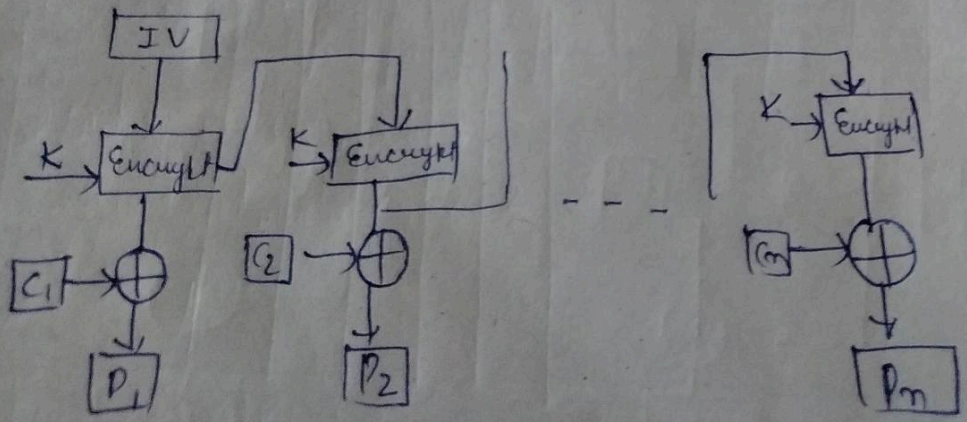
→ The output Feedback mode of block cipher hold great resistance towards bit transmission errors.

→ It also decrease the dependency or relationship of the cipher on the plaintext

Encryption



Decryption



Stream and Block Cipher

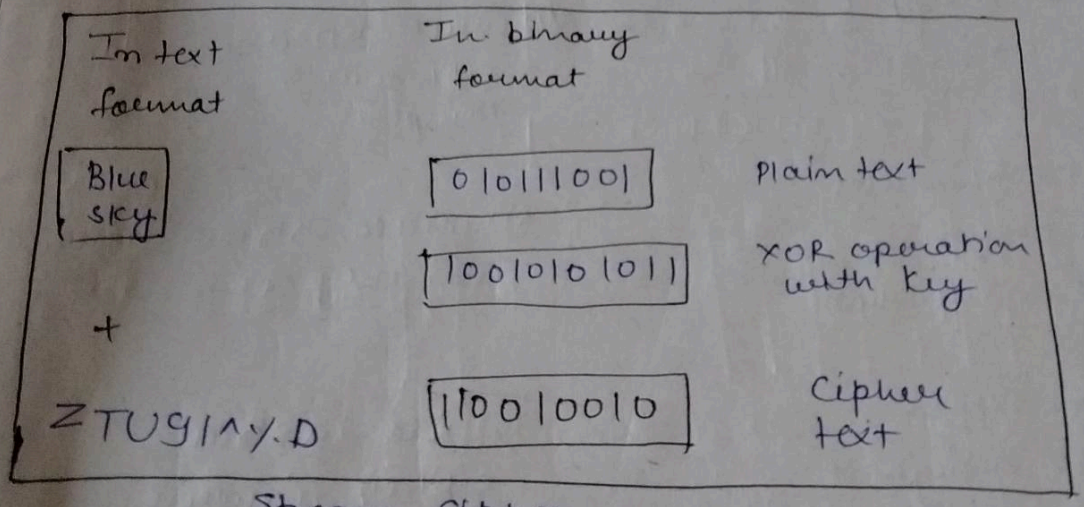
Block cipher and Stream cipher

→ belongs to symmetric key cipher

→ These two block and stream ciphers are the methods used for converting the plain text to ciphertext

→ The main difference between a Block Cipher and Stream cipher is that a block cipher convert the plain text by taking plain text's block at a time.

→ while stream cipher convert the plain text into cipher text by taking 1 byte of plain text at a time.



Stream Cipher

Difference between Block cipher and stream cipher

	Block cipher	Stream cipher
	Block ciphers convert the plain text into cipher text by taking plain text is block at a time	stream cipher convert the plain text into cipher text by taking 1 byte of plain text at a time
2	Block cipher uses either 64 bits or more than 64 bits	while stream cipher uses 8 bits
3.	The complexity of block cipher is simple	while stream cipher is more complex
4	Block cipher uses as only confusion well as diffusion	while stream cipher uses only confusion
5	In block cipher - reverse encrypted text is hard	while in stream cipher reverse encrypted text is easy
5	CBC and ECB	CFB and OFB
6	Block cipher work on transposition technique	stream cipher work on substitution technique
7	It is slower	It is faster.

① Data Encryption Standard

- from (1972 to 1976) it is open for attack
- 64 bit PT message block (work on the principle) as well as Block Cipher
- work on 56 bit symmetric key
- Using substitution and transposition technique

Problem here

64 bit PT message & 56 bit key

Basic Principle of DES is:-

① we convert the 64 bits key ~~56~~ to 56 bit symmetric key (key discarding process)

IP = 64 bits key → arbitrary 64 bit key (chosen randomly)

↓

key discarding process → discarded every 8th bit

↓

OP = 56 bit key

1	2	3	4	5	6	7	8 X
9	10	11	12	13	14	15	16 X
17	18	19	20	21	22	23	24 X
⋮							
57	58	59	60	61	62	63	64 X

Basic block diagram of DES

64 bit PT block1 → (56 bit key) → DES Encryption → 64 bit CT block1

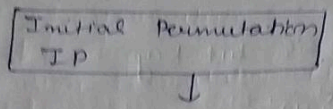
64 bit PT block2 → (56 bit key) → DES Encryption → 64 bit CT block2

64 bit PT blockn → (56 bit key) → DES Encryption → 64 bit CT blockn

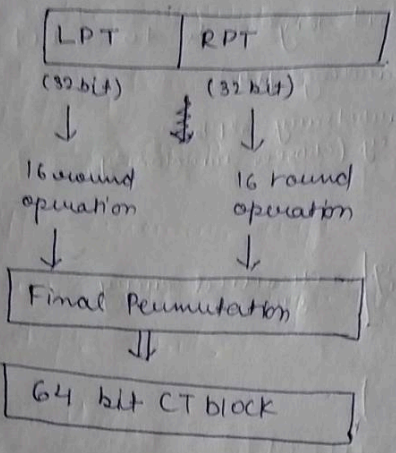
Broad step of DES Encryption

Step1: When each the size of message is large then message is divided in 64 bit block

Step2: Perform initial Permutation



Step3:



→ Ist round operation will be input for next round operation

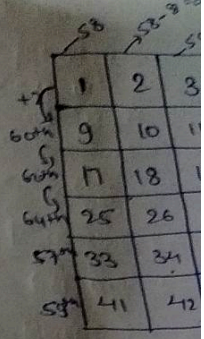
How to perform initial Permutation

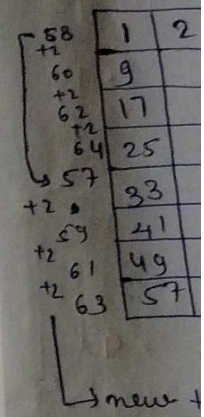
- we circularly shift . .

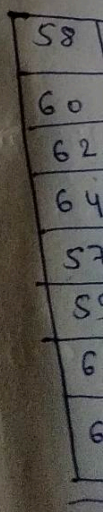
IP

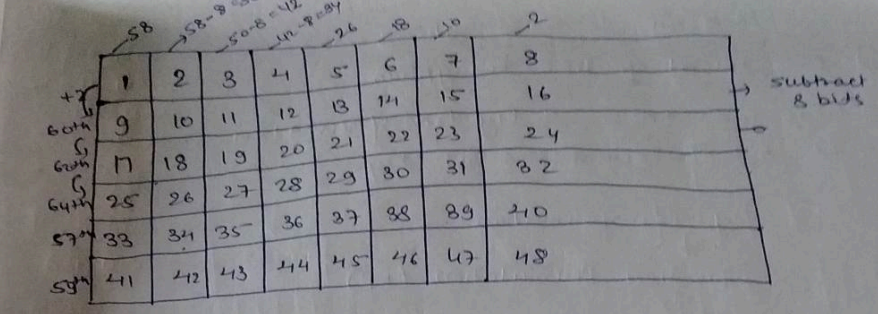
Round No	1	2	3	4	5	. . . . .	16
No of bit Shifted left	1	1	2	2	2		1

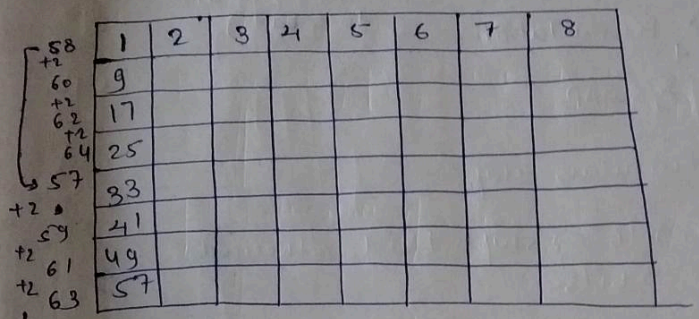
for round No: 1, 2, 9, 16 → shift 1 bit and for other shift 2 bits











↳ new table (every bit position from initial table will be changed.

58	50	42	34	26	18	10	2
60							
62							
64							
57							
59							
61							
63							

LPT RPT

Various round in DES Encryption

① One round of DES Encryption

→ Here we have 4 key transformation 32 bit RPT and 56 bit key

Key Transformation
↓
Expansion Permutation (EP)
↓
S-box substitution (convert 4 bit to 6 bit)
↓
P-box Permutation
↓
XOR & SWAP

→ we prefer circular shift

Round No – 1, 2, 9, 16 → shift 1 bit otherwise shifts 2 bits.

Key Transformation

Round No	1	2	3	4	5	6	...	16
No of bits	1	1	2	2	2	2		1

this is 16×4 matrix

56 bit key → select 48 bit key (select on the basis of P & C)

48 bit

14	17										10

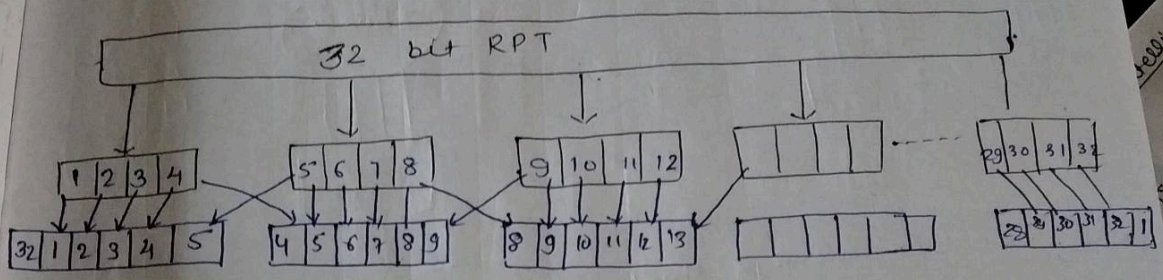
8 will bits will be discarded

(9, 18, ---)

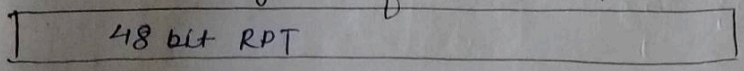
→ for every round of operation permutation & combination 48 bit table will be changed and everytime key will be different in each round

→ Now we changed 56 bits to 48 bits
Now we have →
32 bit RPT & 48 bit key

→ So, in Expansion permutation we convert 32 bit RPT into 48 bits



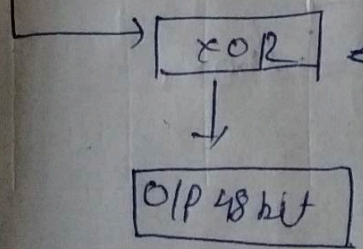
1st block (left) → filled with 32th bit
last block (right) → fill with → 1st bit



Now we have 48 bit RPT & 48 bit Key

32 bit RPT
↓
Expansion Permutation
↓
48 bit RPT

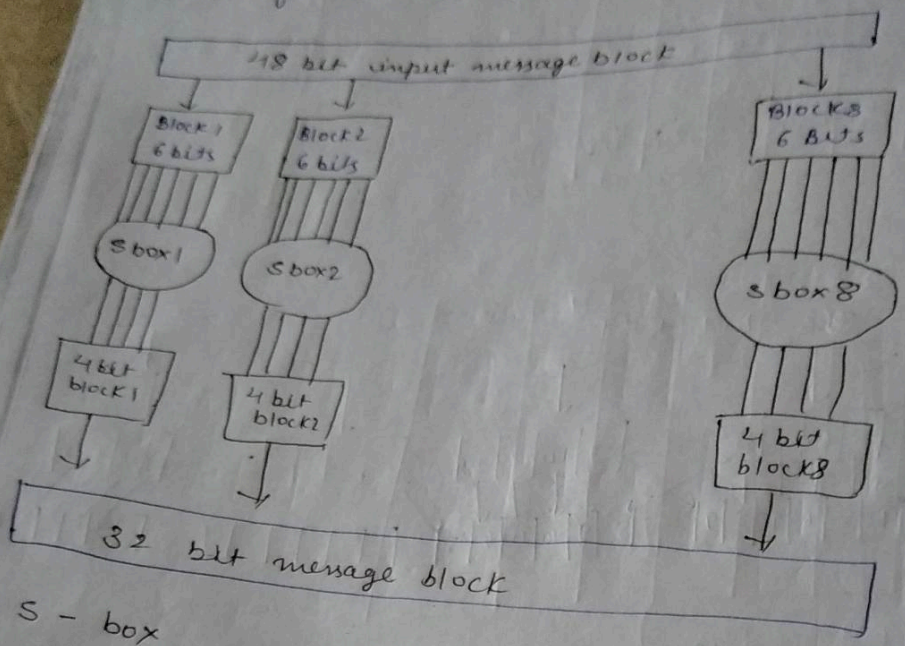
56 bit Key
↓
Key transformation
↓
48 bit Key



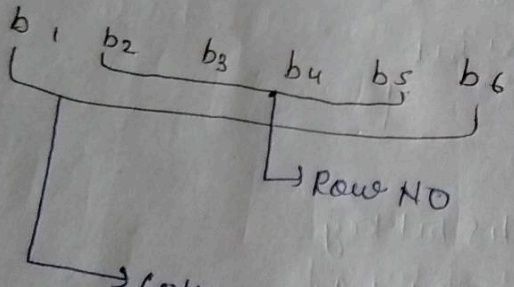
→ this will be input for s box substitution

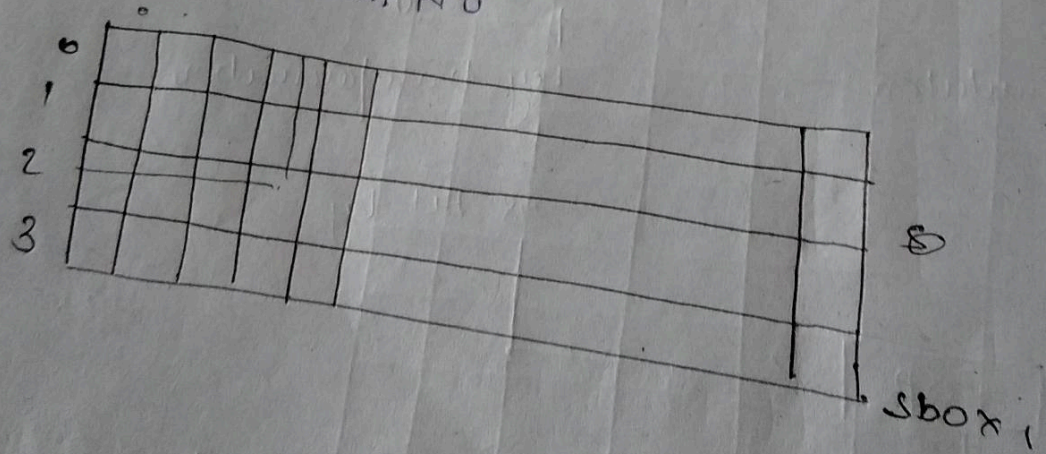
S-box substitution

Input for s box is 48 bit



S - box





1001 10
10 = 2 = Row No
11 = 3 = Column No

→ 2nd row, 3rd so column = value and convert it into binary form 15 = 0101] 4 bit Block value will contain

→ S box table will be given
0 to 15

→ S-box can have repeatedly value

Assymetric key cryptography

Asymmetric cryptography, also known as public key cryptography is a process that uses a pair of related keys - one public key and one private key - to encrypt and decrypt a message and protect it from unauthorized access or use.

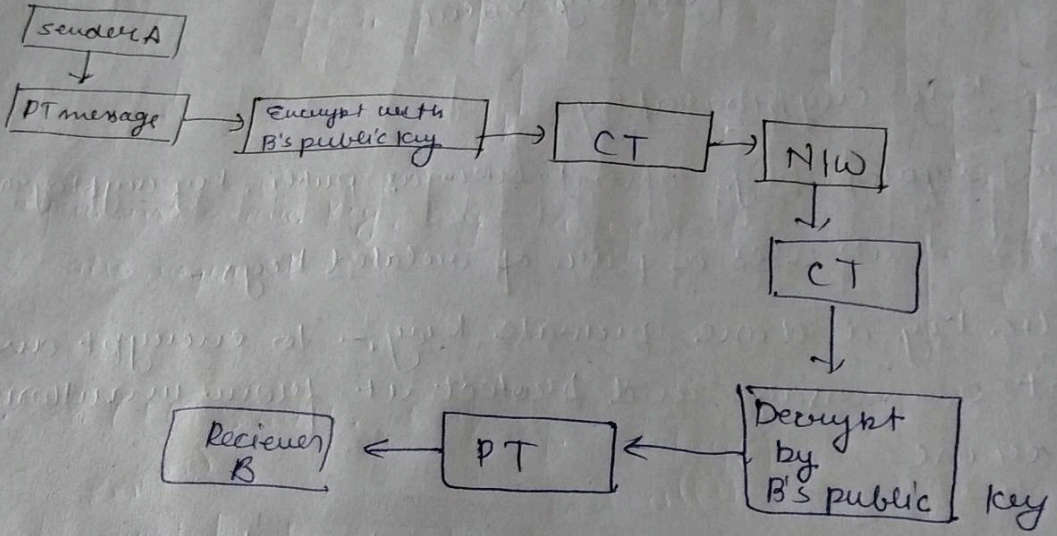
→ A public key is a cryptographic key that can be used any person to encrypt a message so that it can only be decrypt by the intended recipient with their private key A - also known as secret key - a shared only key initiates.

→ It work on the principle of 2 key

→

Key Details	Sender A A should know	Receiver B B should or NO
A's private key	yes	
B's private key	NO	yes
A's public key	yes	yes
B's public key	yes	yes

A wants to send some message to receiver B



Strength of DES

56 bit key
We are using 56 bit key
→ 2^{56} → combination possible
$2^{56} = 7.2 \times 10^{16}$

⇒ Data encryption standards is a symmetric key block cipher algorithm.

→ The algorithm is based on Feistel network.

→ The algorithm uses 56-bit key to encrypt data in 64 bit algorithm

→ $2^{56} = 7.2 \times 10^{16}$

→ Brute-force-attack will take place take 1000 years if it perform DES operation in 1 microsecond

→ So we go for DES for more security.

⇒ 2^{112} → combination possible

∴ It was cracked

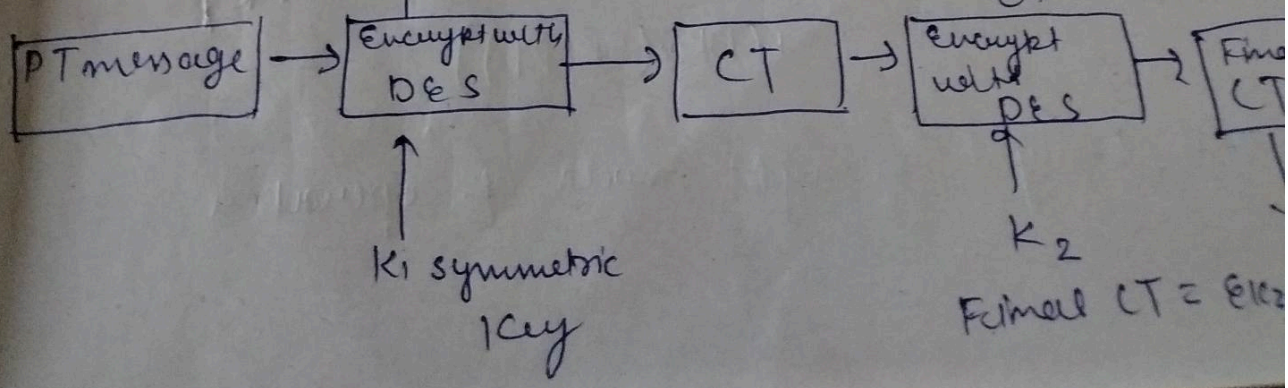
Double DES

→ we have 2 keys K_1, K_2 and each key has 56 bits

→ perform DES

$E_{K_1}(PT) = CT$

$E_{K_2}(E_{K_1}(PT))$



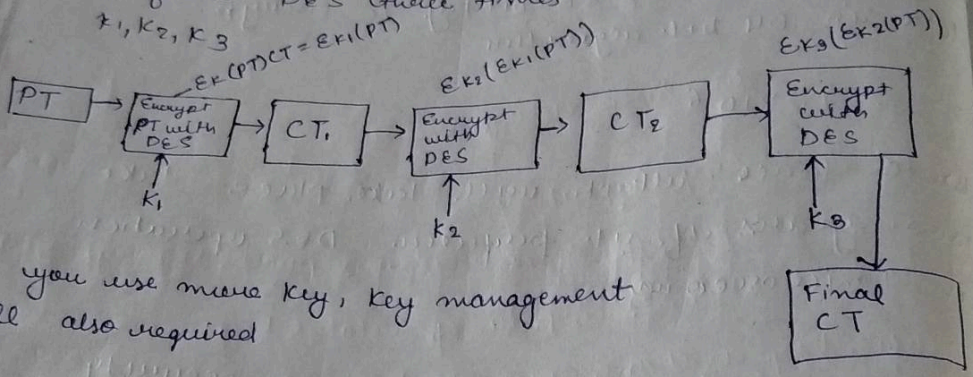
→ Perform DES three

→ ~~suffer in the middle attack~~ DDES suffer from problem of mitma meet in the middle attack

Triple DES

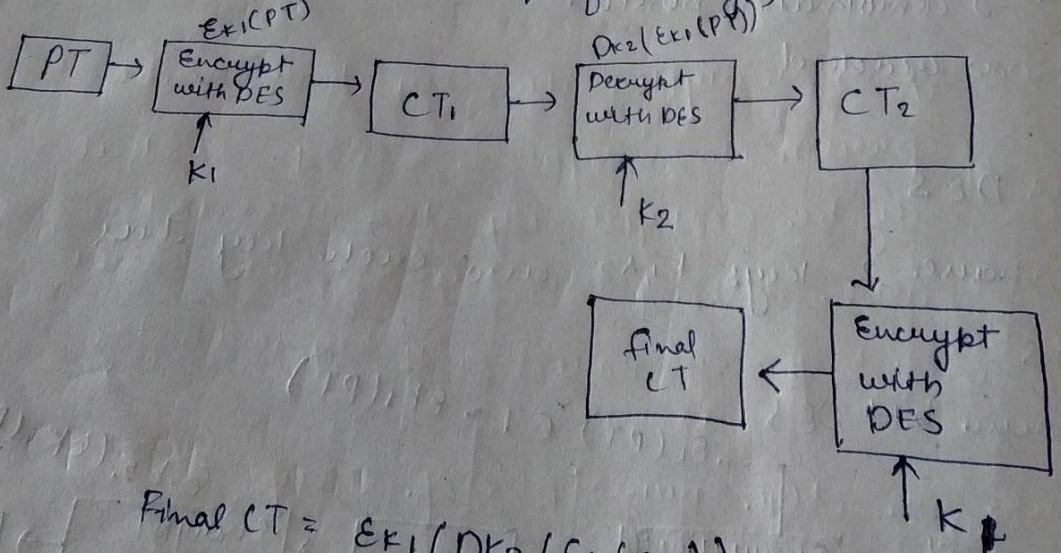
→ It use 168 bit key

→ Perform DES three times K_1, K_2, K_3



If you use more key, key management will also required

Tuchman (TDES with help of 2 keys)



Final CT = $E_{K1}(D_{K2}(E_K(PT)))$

Encrypt - Decrypt - Encrypt mode of operation

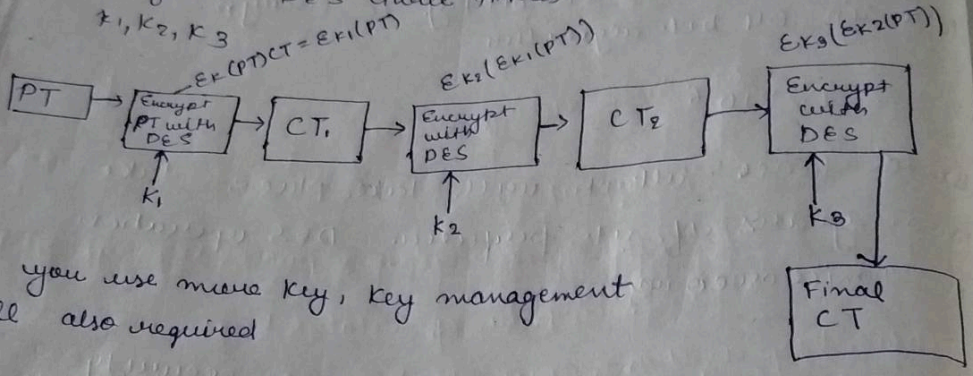
→ Perform DES three times

→ ~~will the middle attack~~ DDES suffer from problem of mitma meet in the middle attack

Triple DES

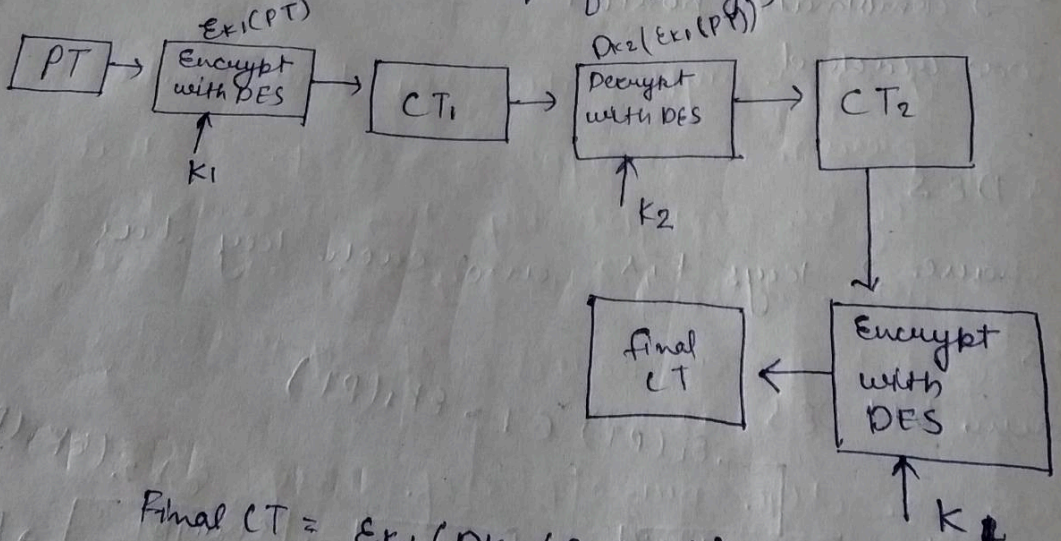
→ It use 168 bit key

→ Perform DES three times K_1, K_2, K_3



If you use more key, key management will also required

Tuchman (TDES with help of 2 keys)



Final CT = $E_{K1}(D_{K2}(E_K(PT)))$

Encrypt - Decrypt - Encrypt mode of operation

→ It does not support the non-repudiation digital signature & so it is confidential key

→ No of key required n^2

→ This will support digital signature and non-replicat both

RSA Algorithm :

(Asymmetric key cryptography)

Step 1 :-

We select two large Prime Number P and Q

Step 2 :

$N = P \times Q$

Step 3 :-

we encrypt with public key

or

select the public key (Encryption key) E such that E is not factor of $(P-1) \times (Q-1)$

Step 4 -

Convert the PT to CT

$CT = PT \bmod N$

→ Recieven will select its private key (Decryption key) D

such that

$D \times E \bmod (P-1) \times (Q-1) = 1$

→ Reverse CT convert into PT

$PT = CT^D \bmod N$

Example

$P = 7, \quad Q = 17$

find E, D and encrypt / decrypt the message [F]

→ $N = P \times Q = 7 \times 17 = 119$

→ $D \times 5 \bmod (P-1) \times (Q-1) = 1$

⇒ $D \times 5 \bmod (6)(16) = 1$ $\quad D = 77$

$96 \overline{)385}$ $\quad 384$

A → 1

B → 2

F → 6

$CT = 6^5 \bmod 119$

$CT = 41$

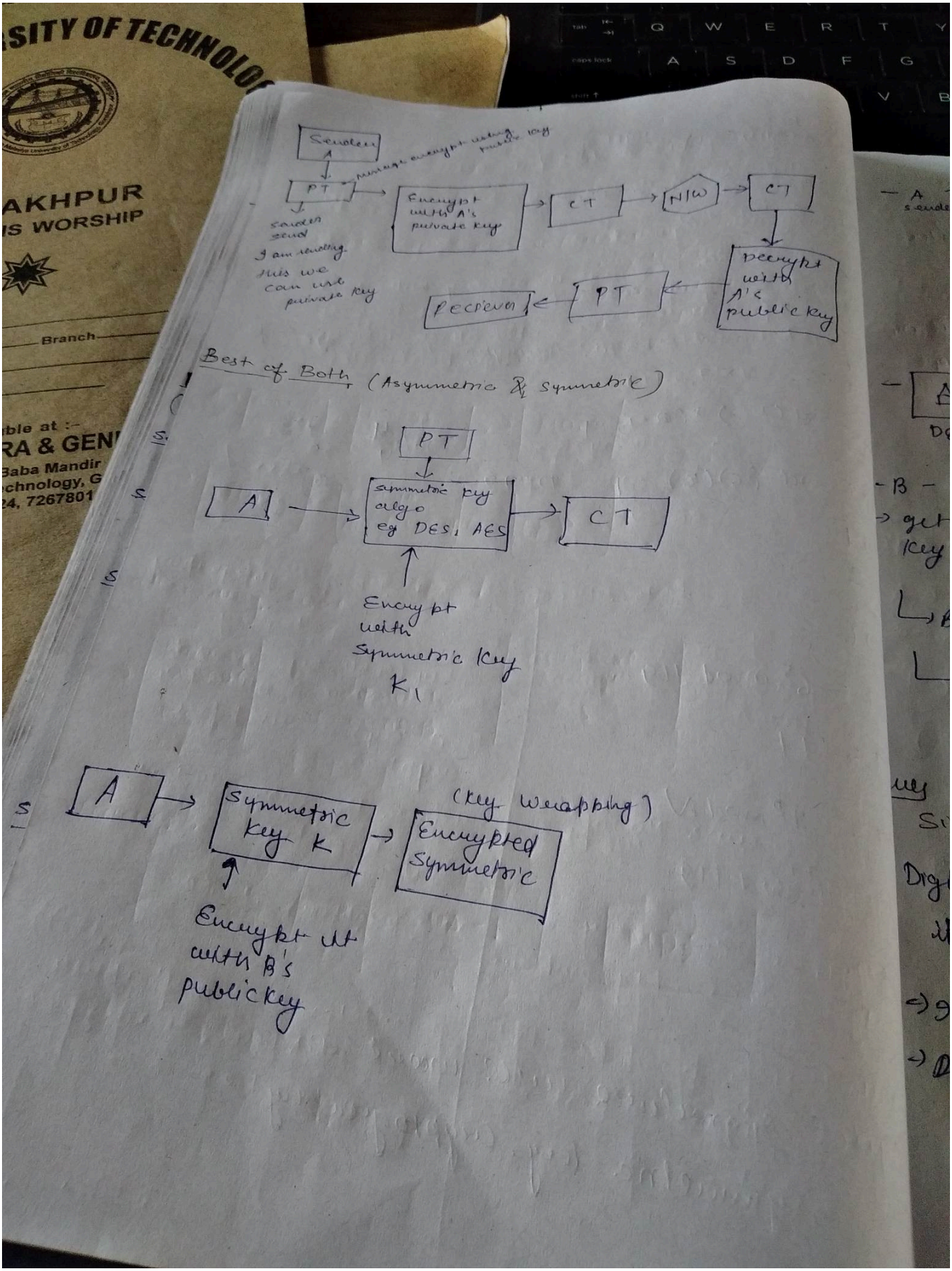
$PT = CT^D \bmod N$

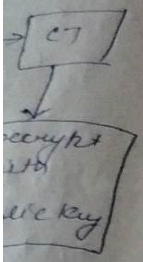
$= 41^{77} \bmod 119$

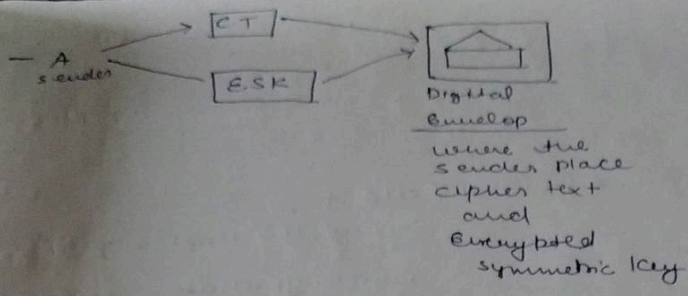
$PT = 6$

$6 = F$

Digital signature will work on the asymmetric key cryptography


Sender
PT
Encrypt with A's private key
CT
N/W
CT
I am sending this we can use private key
Decrypt with A's public key
PT
Reciever
Best of Both (Asymmetric & symmetric)
PT
A
symmetric key algo eg DES, AES
CT
Encrypt with Symmetric key K1
A
Symmetric key K
Encrypted Symmetric
(key Wrapping)
Encrypt it with B's public key





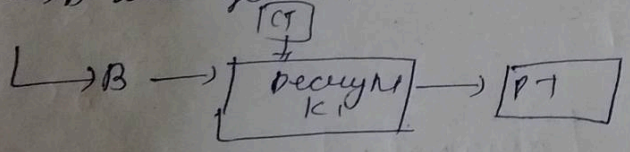
where the sender place cipher text and encrypted symmetric key

- A → Reciever.

DE

- B - Receiver open the Digited envelop
→ get the cipher text and decrypted symmetric key by using B's private key

↳ B will get K_1 CT



Why Digital envelop is better than Digital Signature

Digital signature is not secure because it it is used only for authentication and none.

→ It is used sender's private key for encryption

→ Digital Signature is working on assymmetric key.

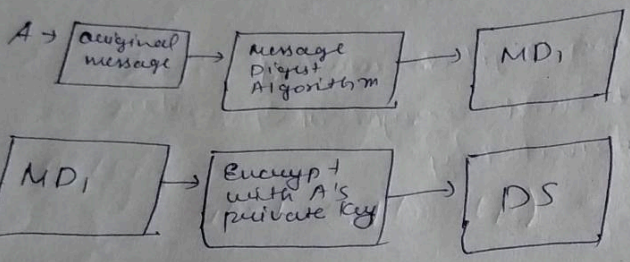
Q Principle of Digital signature and Draw the Diagram

DSA algorithm working on Digital Signature

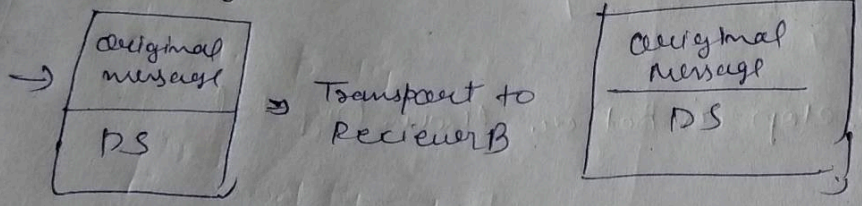
→ DS + RSA ⇒ DSA

⇒ Message digest Algorithm (SHA-1)
Secure Hash Algorithm
It
which generate message digest algorithm

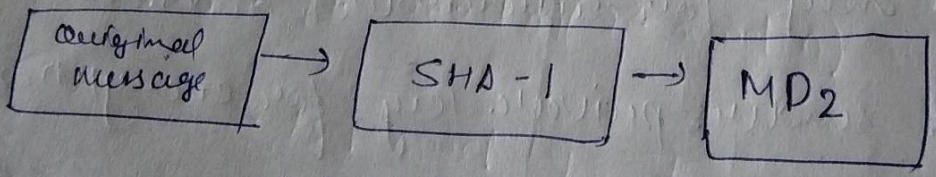
B



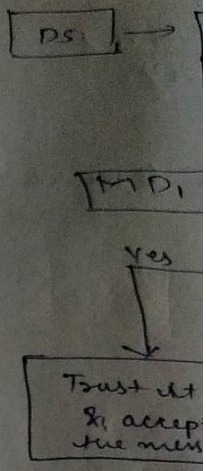
at sending time



Reciever B



Reciever MD2

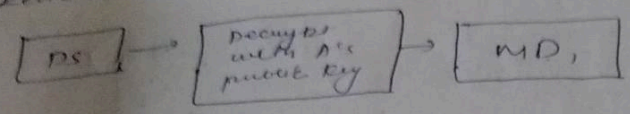


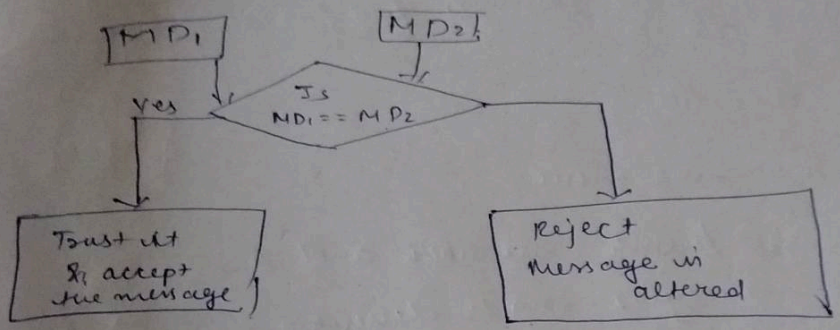
signature

algorithm

message

- Decrypt MD2





→ Prime & Relatively Prime number

Prime No :- A no which is greater than 1 which is divisible by 1 and itself.

Relatively Prime No :- No common fac factors than one

Fermat's Theorem

→ solving the mod value

→ If p is a prime number and A is positive integer not divisible by p then

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p-1} \bmod p = 1$$

Ex

$a = 7 \quad p = 19$

$7^{19-1} \bmod 19 = 1$

$7^4 \bmod 19 = (7^2 \bmod n)(7^2 \bmod n) \bmod n$

$= 121 \bmod 19 = 7$

$7^8 \bmod 19 =$

$=$

$49 \bmod 19 =$

$7^{18} \bmod 19 = 121 \bmod 19 = 7$

$\Rightarrow 7^{18} \bmod 19$

$\Rightarrow (7^{10} \bmod (19))\,(7^{8} \bmod 19) \bmod 19$

$\Rightarrow 7 \cdot 7 \bmod 19 = 7$