Date .....

Computer Security

Computer Security is the Protection offorded to an automated Information System in order to attain the integrity, availability & confidentiality of information system resources.

(i) Confidentiality:

It Assures that data sent by sender is not disclosed to unauthorized user and also it must assure that the data should only collected or stored to the authorized user.

(ii) Integrity:

It assures that the information should not be changed by an ~~one~~ unauthorized individual during keeping of data.

(iii) Availability:

It assures that systems work promptly and service are not denied to authorized users.

Spiral

Date .....

Computer Security

Computer Security is @ the Protection afforded to an automated information system in order to attain the integrity, availability & confidentiality of information system resources.

(i) Confidentiality:

It Assures that data sent by sender is not disclosed to unauthorize user and also it must assure that the data should only collected or stored to the authorized user.

(ii) Integrity:

It assures that the information should not be changed by an ~~user~~ unauthorized individual during transfer of data.

(iii) Availability:

It assures that systems work promptly and service are not denied to authorized users.

Date .....

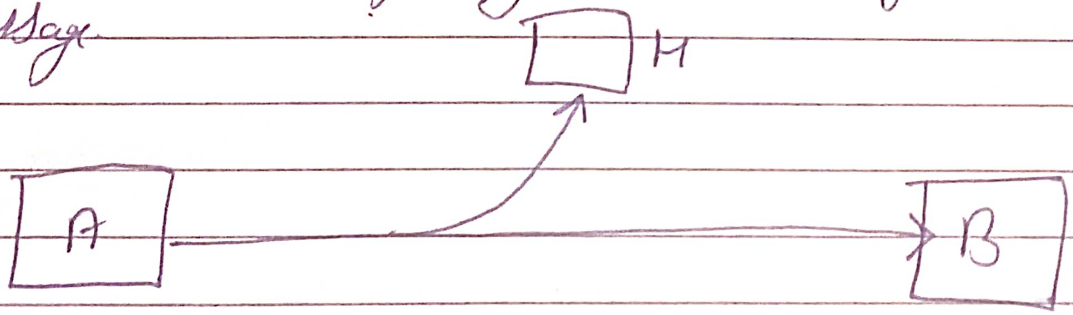
OSI Security Architecture

- Security attack
- " mechanism
- Security service

Security Attack

Passive Attacks Active attacks

Passive attack : In this attack the attacker observes the messages but does not try to change the information of content.
Although Passive attack don't harm the system they can be danger for the confidentiality of the message.



Date .....

Active Attack -

In active attack the hacker attempts to change or transform the content of message.

The attacker is inserting his data into original data stream.

Type of Passive attack

- ~~Telephonic~~.
  Release of message content.

Telephonic conversation, an electronic mail or a transferred file may contain sensitive or confidential information. Seen by attackers.

- Traffic Analysis

In this attack, the sender sends a message in encrypted form to the receiver.
The hacker analyse the traffic & observes the pattern to decrypt the message.

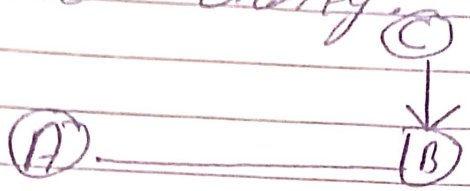
Spiral

Date .....

Type of Active attack

- Masquerade

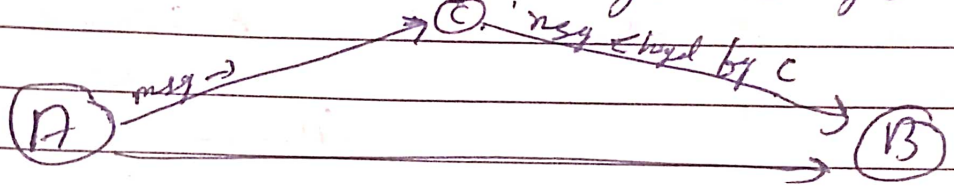
It Take Place when one entity Pretends to be different entity.



C → Stole A login / Pass & Send data to B as identity of A

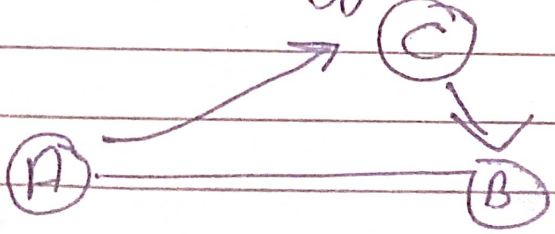
- Modification of message :

In this attack, Some portion of a message is changed or message is altered ; or messages are delayed or reor



Replay

It involves the passive capture of a msg & its subsequent retransmission to produce an unauthorized effect



Error Detecting / Correcting

Date .....

Intro to Linear Block Codes

A block code is said to be linear if the sum of any two code word gives an another codeword.

Example: {0000, 0101, 1010, 1111}

0000	0101
0101	1010
0101	1111

In linear block code each block containing k messages bits is encoded into a block of n-bits by adding (n-k) parity check bits.

msg bits → Parity bits

k bits	(n-k) bits

n bits

Codeword

n → length of codeword
n-k → Parity check bits
k → msg bits

★ Weight = no. of 1's

distance = no. of different value at diff pos

{0000 (w=0) 0101 (w=2) 1010 (w=2) 1111 (w=4)}

d=2 d=4 d=2

$d_{min} = 2$

$w_{min} = 2$

Spiral

Date .....

- if $C_K = C_i + C_j$ then

$$d(C_i, C_j) = W(C_K)$$

eg $C_i = 0101$

$C_j = 1010$

$C_K = 1111$

$$d(C_i, C_j) = 4$$

$$W(C_K) = 4$$

* $d_{min} = min\, W(C)$. { except all zero code }

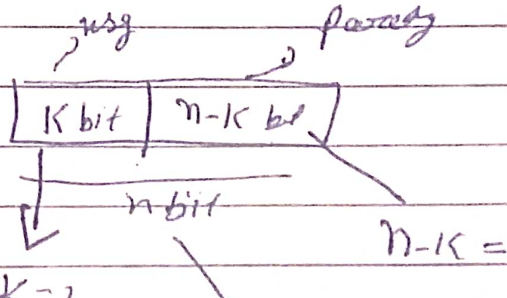
Q. A generator matrix of (6, 3) linear block code

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

→ find codeword for msg = 011

→ Decode the received sequence 101101

⇒ [Codeword] = [msg] [Parity]



$[C] = [m] [P]$

$$[C_1\ C_2\ C_3] = [m_1\ m_2\ m_3] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

We find C_1, C_2, C_3 for $m_3 = 011$

Spiral

Date .....

$$c_1 = \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

$c_1 = 0 \oplus 0 \oplus 1 \oplus 0 = 1$

$$c_2 = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$= 0 \oplus 1 \oplus 1 = 0$

$$c_3 = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$= 0 \oplus 0 \oplus 1 = 1$

Codeword = $m_1 m_2 m_3 c_1 c_2 c_3$

$= 0 1 1 1 0 1$

Date .....

Q. The (7,4) Linear code has generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

If $U = 1101$ is the msg, find out corresponding codeword

msg (K) = 4, codeword = 7, parity bit = 3

$$[1101] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$C_1 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$C_2 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$

$C_3 = 0 \oplus 1 \oplus 0 \oplus 1 = 0$

Codeword = 0001101

Q. The Received code vector is [1100010]. Check whether this is a correct codeword

Spiral

Date .....

H → Parity Check Matrix

$$H = \begin{bmatrix} I_{n-k} & P^T \end{bmatrix} \qquad P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

$$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \rightarrow 001 - 3^{rd}$$

Now we find Syndrom

if Syndrom is 000

Return Corrected Codeword

Else

Incorrect

Date .....

$S = [\text{received codevect}] [H^T]$

$= [1\,1\,0\,0\,0\,0\,1\,0] \cdot H^T$

$1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 1$

Syndrome = 001

* Check posⁿ of 001

⇒ ie → 3rd row

$e = 0\,0\,1\,0\,0\,0\,0$

Corrected codeword = (received codevect) ⊕ e

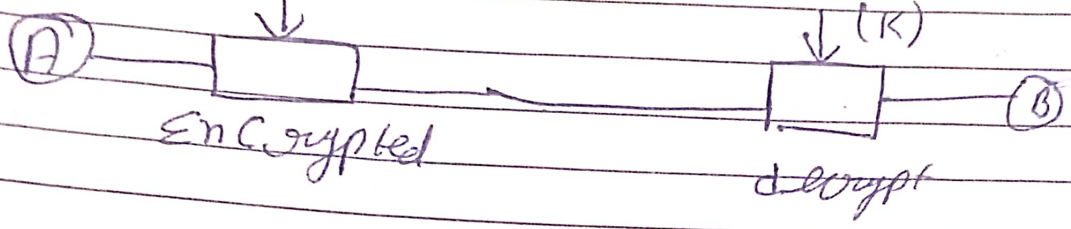
$[1\,1\,0\,0\,0\,1\,0] \oplus [0\,0\,1\,0\,0\,0\,0]$

$= 1\,1\,1\,0\,0\,1\,0$

Date .....

Encryption: It is a method by which information is converted into secret code that hides the information's true meaning

Decryption - The conversion of encrypted data into its original form is called Decryption



Cryptanalysis

Cryptanalysis is the art of trying to decrypt the encrypted messages without using the key that was used to encrypt the message.

Hackers use the mathematical analysis and algo to decrypt the ~~mes~~ code

Type of cryptanalysis:

(i) Known plain text analysis (KPA)

(ii) Chosen " " (CPA)

(iii) Cipher text - only analys (COA)

Spiral

Date .....

(i) Known Plaintext analysis (KPA)

In this type of attack, some plaintext, ciphertext pairs are already known. Attacker maps them in order to find the encryption key.

(ii) Chosen - Plaintext Analysis (CPA)

: In this type of attack the attacker chooses random plaintext and obtain the corresponding ciphertext and tried to find the encryption key.

(iii). Ciphertext-only Analysis (CoA)

: In this type of attack, only some ciphertext is known. An attacker tries to find the corresponding encryption key and plaintext.

Steganography

It is a method in which secret message is hidden in a cover media.

Form → audios, videos, images

Brute force attack

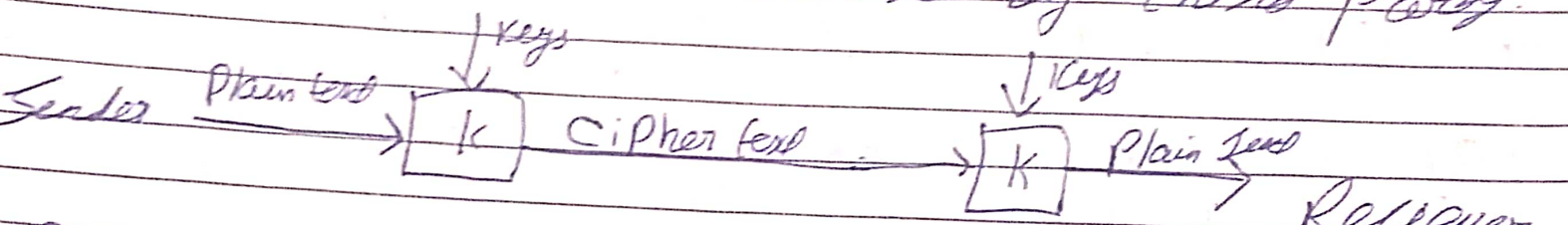
In this attack, the attackers tries every possible key on a ciphertext to decrypt the plaintext.

Spiral

Date .....

Cryptography

Cryptography is the study and practice of techniques for secure communication in the presence of third parties. So that the message or data shared between two parties can't be accessed by third party.



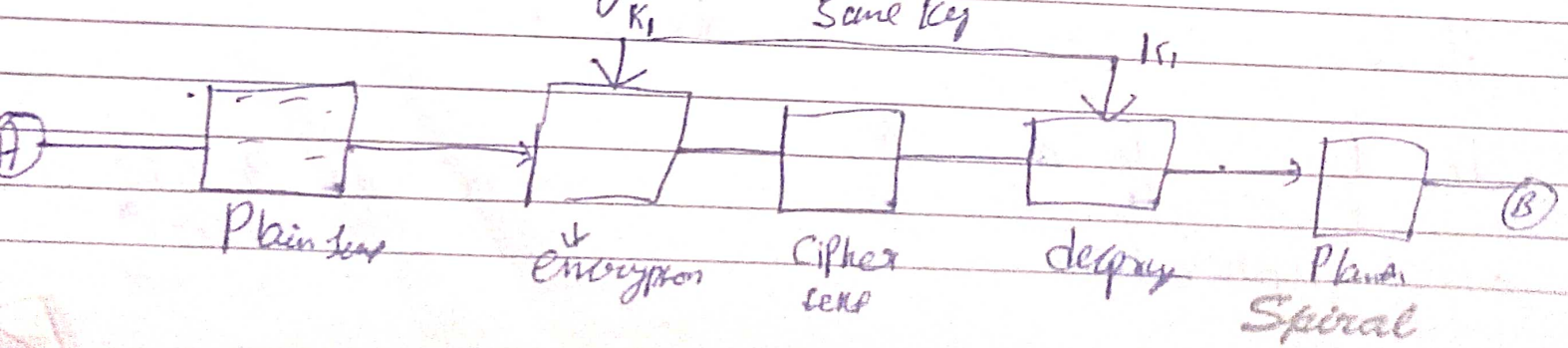
Plain text : Information that can be directly red by anyone.

Cipher text : An encrypted text transformed from plain text using an encryption algo.

Type

(i) Symmetric key cryptography (Secret key)

- It uses single key to encrypt data
- Both encryption & decryption in symmetric key cryptography uses the same key.



Spiral

Date .....

(ii) Asymmetric key Cryptography

Under this system a pair of key is used to encrypt and decrypt information.

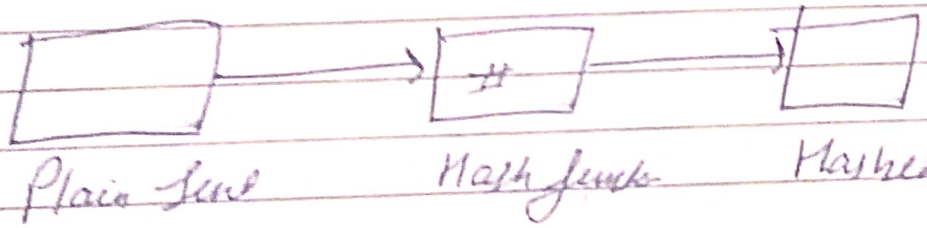
A public key is used for encryption and private key is used for decryption

Sender public key is used for encryption and sender private key is used for decryption at receiver end.

(iii) Hash function

There is no usage of any key in this algorithm.

A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.



Spiral

- Caesar
- Monoalphabatic
- Play fair
- Hill
- Polyalphabetic

- Vernam
- One time pad

Date

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or numbers or symbols.

Caesar Cipher

It is a type of substitution cipher where each letter of plaintext is replaced by another letter

Eg

PT = BOY

Key = 2

CT = DQA [shifted 2 place.]

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

Eg Hello

K = 4

$C = E(4, H) = (7 + 4) \bmod 26 = 11$

H → L

use for e.

L

L

O

Spiral

Date .....

For decryption

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

Playfair Cipher

- It is an encryption algorithm to encrypt or encode a message.
- It initially create a key-table .y :5*5 matrix
- The matrix contain alphabets that act as the key for encryption of plaintext.
- Any alphabet should not be repeated.
- There are 26 Alphabets and we have only 25 blocks to put a letter inside it.

eg PT = JAZZ Key = ATHENS

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

→ Make pair of Plaintext
→ If repeating letters take any other alphabet to overcome
eg ZZ => ZX, ZX
→ JAZZ => JA, ZX, ZX
GREET => GR, EX, ET
OFF => OF, FP

Spiral

Date .....

Key = Monarchy

PT = JA ZZ , OFF

↓

JA ZX , ZX

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

- Find JA in matrix, both are in same Column so the next bottom element of replaced with it

J → S A → B JA ⇒ SB

- For ZX both are in same row so it is element by the next "" element

Z → U X → Z

- for OFF < OS FX

→ O → H F → P → FX → both are in different col

Ciphertext

Date .....

in this case make a rectangle with f x

In this case for f, check f column row and element and for x check x-row last element and exchange it

f	g	i/j
p	q	s
v	w	x

f → i
x → v

OFF → OF FX → HP IV

JAZZ → JA ZX ZX → SB UZ UZ

~~Vernam Cipher~~
Monoalphabetic ~~Substitution~~ Cipher

: ~~A Single~~ A type of encryption technique where each character of plain text is mapped to another fixed character of cipher text

MEKRP

ABACN

Date .....

Hill cipher

It is a polygraphic substitution based on linear algebra.

Each letter is represented by a no. modulo 26

For encryption

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

Key = 2 x 2 $\Rightarrow$ plain text matrix = 2 x 1
" = 3 x 3 $\Rightarrow$ " " " = 3 x 1

eg

Key : QUICKNESS

A = 0
B = 1
C = 2
D = 3

$$\Rightarrow \begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix} = \begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}_{3\times3}$$

PT = ATTACK, & Key $\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}_{2\times2}$

Since Key = 2 x 2 then PT = 2 x 1

So $\begin{bmatrix} A \\ T \end{bmatrix}, \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$ } $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

Solved

Date .....

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

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

$$\begin{bmatrix} 2\times0 + 3\times19 \\ 3\times0 + 6\times19 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$$

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

Now

$$\begin{bmatrix} A \\ T \end{bmatrix} \Rightarrow \begin{bmatrix} F \\ K \end{bmatrix}$$

Same as

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

$$\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

Plain text = ATTACK

Cipher text = FKMFIO

For decryption

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

Date .....

Polyalphabetic Cipher

- A polyalphabetic cipher is any cipher where a given letter of alphabet is not always encrypted by same alph. cipher text letter.

In simple word, a polyalphabetic cipher is a combination of different monoalphabetic ciphers

Vigenere Cipher

- It is a method of encrypting alphabetic text where each letter of plain text is encoded with a different caesar cipher
- It is a simple form of poly alphabetic substitution

PT : GIVE MONEY

Key = LOCK

G I V E M O N E Y
L O C K L O C K L

6
11
17
R

Date .....

VERNAM CIPHER

It is a method of encrypting alphabetic text.

It is a one of the substitution technique for converting plain text into cipher text

→ Here we assign a no to each character of the plain text and key i.e to alphabetical order

eg a=0, b=1, c=2

Here

Length of Plain text = Pt length of key

PT = O A K

Key = S O N

O = 14 — 0 1 1 1 0

S = 18 — 1 0 0 1 0

XOR

1 1 1 0 0 = 28

→ Perform XOR with plain text no. & key

→ If new no. > 26

Sub from 26

Else new no.

So 28 − 26 = 2 = C

Spiral

Date .....

One Time Pad

It is a improvement of the Vernam Cipher

- The Key should be randomly generated as long as size of message.
- The key is to be used to encrypt & decrypt a single msg and is discarded.

So encrypty every new msg require new key of the same length as the new msg is One time pad.

Plain text	H	E	L	L	O
Key	b	a	x	y	e
	7	4	11	11	14
	1	0	23	24	2
	8	4	8	9	16
	i	e	i	j	q

Spiral

Rail Fence

Date .....

Transposition Techniques

It is a cryptographic algorithm where order of alphabets in the plaintext is rearranged to form a ciphertext.

HELLO - PT

OLHEL - CT

Rail fence Cipher

In this technique a plain text is written downwards and diagonally on successive

. After we reach bottom rail, we traverse upwards

Every thing is fine

E E Y H N I F R
V R T I G S I E

EEYHNIFRVRTIGSIE

Date .....

Row Transposition Cipher

Plain text is written row by row in ☐

- To encrypt write out the column in any order by key

1	2	3	4	5
G	V	E	R	Y
T	H	I	N	G
I	S	F	I	N
G				

Key = 2 4 1 5 3

2 4 1 5 3

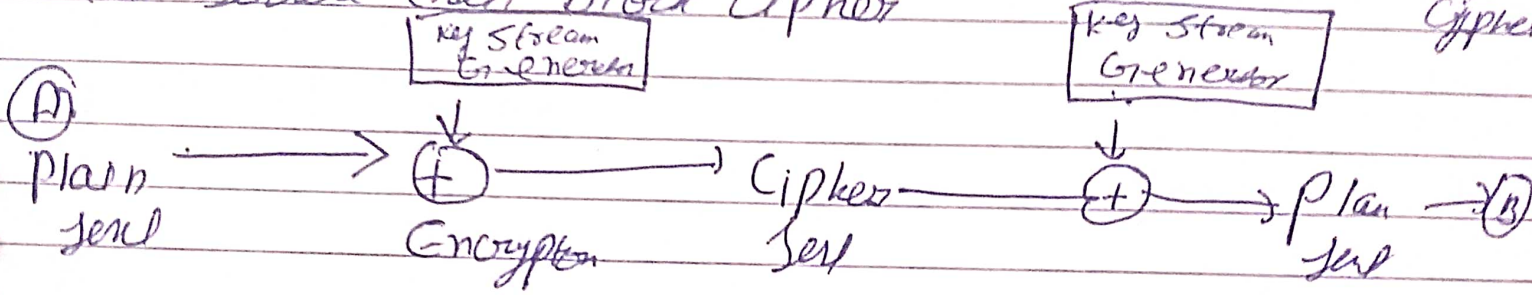
CT = EIF ETI E VGN VHS ·RNI

Date .....

Stream Cipher

It converts the plain text into cipher text by taking 1 bit plain text at a time

- It is a Symmetric key cipher
- More complex
- Uses only confusion
- Works on substitution technique → Caesar, Polyg... Cipher
- Less Secure than block cipher



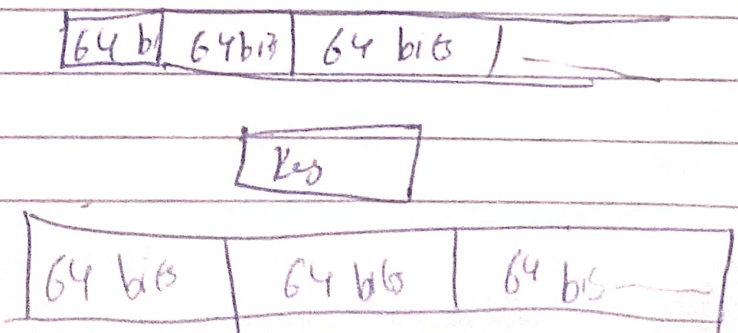
1 0 1 1 0 1 1 0 – PT
0 1 0 1 0 1 0 1 – Key

1 1 1 0 0 0 1 1

Block cipher

It converts plain text into cipher text by taking plain text's block at a time.

- Use either 64 bits or more than 64 bits



Spiral

Date .....

DES

Diffie Hellman Key Exchange

The DHKE protocol allows two parties to establish a shared secret key over an insecure channel.

- Asymmetric keys are to be used to exchange secret key.

Step 1 : Consider a prime no. P

Step 2 : Select a primitive root α of 'P'

Step 3 : Choose a private key if not given.

Step 4 : Let private key is X_A $\quad X_A < P$

X → Private
Y → Public

Step 5 : Generate public key of A

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

Step 6 : Let private key is X_B , $X_B < P$

Generate public key of B

$$Y_B = \alpha^{X_B} \bmod p$$

Date .....

Secret Key Gen^n

By Person A

$$K = (Y_B)^{X_A} \bmod p$$

$Y_B \rightarrow$ Person B Public Key
$X_A \rightarrow$ Person A Private Key

By Person B

$$K = (Y_A)^{X_B} \bmod p$$

$Y_A \rightarrow$ Pers A Public
$X_B \rightarrow$ Per B Priva

Date .....

DES

- DES is a block cipher Algorithm that takes plain text in block of 64 bits
- It is a Symmetric key algo
- There are 16 rounds of encryption in the algo. and a different key is used for each round
- The initial key consist of 64 bits, but only 48 bits used for encryption of the plain text.