शक् 11 पौष 1938
विक्रमी 18 पौष 2073

("Unit-1")

JANUARY 2017
जनवरी रविवार

SUNDAY 01

Cryptography :— is the technique through which plain text is converted into cipher text.

- Cipher text is converted into plain text is known as 'cryptanalysis'.

(OR).

It is the technique to convert the readable plain text into non-readable format or vice-versa.

- Cryptography is mainly used to acheive confidentiality.

Engagements

Plain Text → Encryption → Cipher Text → Decry? → Plain text

शक् 12 पौष 1938
विक्रमी 19 पौष 2073

JANUARY 2017
जनवरी सोमवार

MONDAY 02

- Plain Text :— is the text which is in human readable format.
  eg:- Hello.

- Cipher Text :—
  CT is the text which is in non-readable format.
  eg:- KHOOR

- Encryption :— It is the process of converting original text into non-readable format by using some encryption algorithm.

- Decryption :— is a process of converting encrypted data in a readable format.

Engagements

बुद्धि द्वारा सधा हुआ उत्साह ही लगन है — पास्कल

03 TUESDAY

Private Key :- It is also known as secret key. The same key is used for encryption and decryption of data.

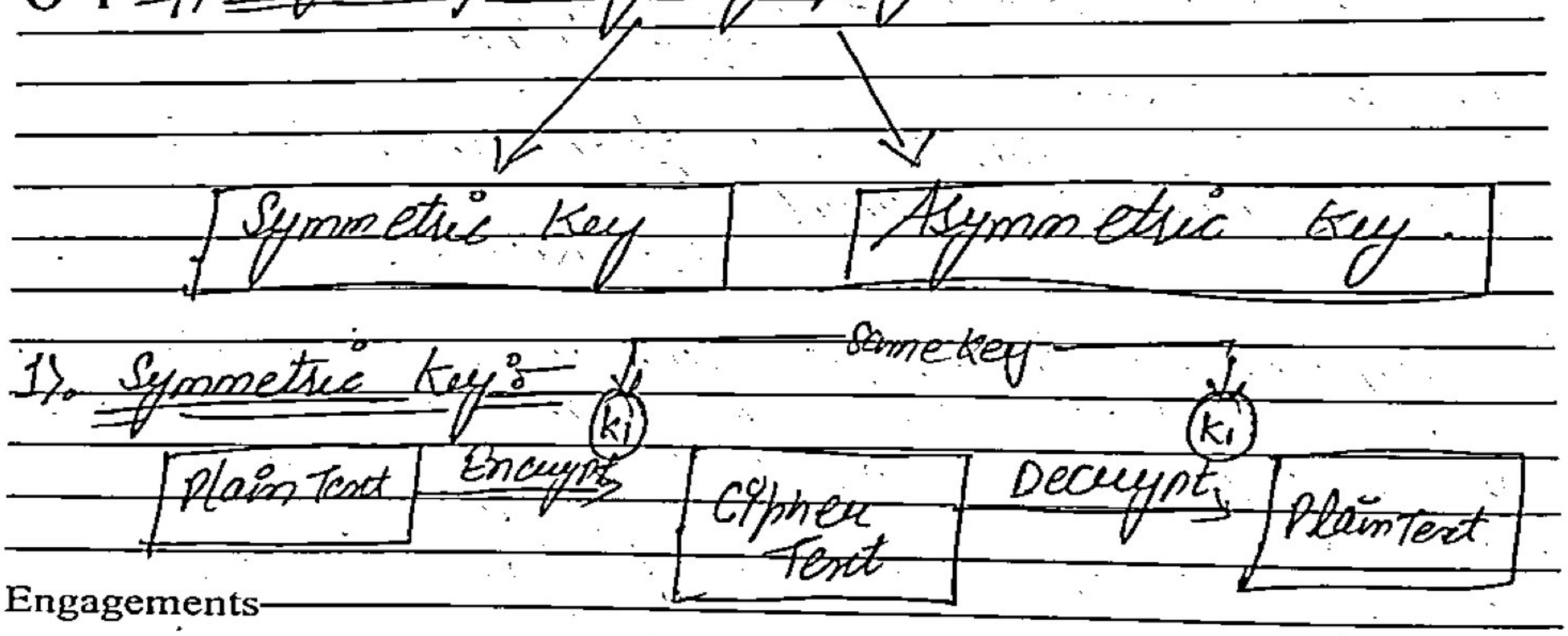
- Private key is symmetric because same key is used.

Public Key :- In public key, two keys are used. one is for encryption and other is for decryption.

Public key is asymmetric because two different keys are used.

04 WEDNESDAY

Types of cryptography :-



काम सरल है, विचार कठिन — गेट

शक् 15 पौष 1938
विक्रमी 22 पौष 2073

JANUARY 2017
जनवरी वीरवार

THURSDAY 05

- It is the simplest kind of encryption technique that involves only 1 Key to encrypt and decrypt.
- It is also called Secret Key cryptography / private key cryptography.
- Examples of symmetric key cryptography are:- DES (56bit), 3DES (192bits), AES (128, 192, 256 bits).
- Problem → Key Exchange. (Which can be solved by Deffi helman Algorithm.

Engagements
- Sharing of Keys b/w A & B is not safe.

2). Asymmetric Key:-

शक् 16 पौष 1938
विक्रमी 23 पौष 2073

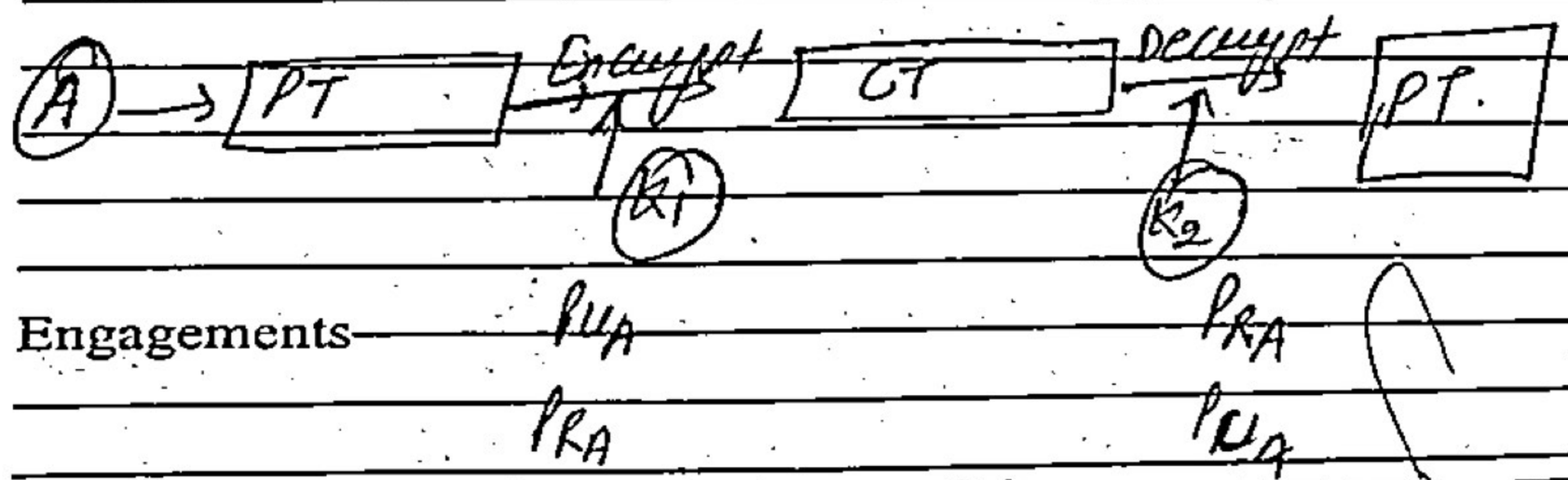
JANUARY 2017
जनवरी शुक्रवार

It is also called Public Key Cryptography.

FRIDAY 06

- It uses 2 keys, a pair of keys for encryption and decryption

2 keys
- Public Key (Known to everyone)
- Private Key (Known only to that particular person)



जिस आदत से आनन्द मिले, वह आदत मत डालो – इमर्सन

Examples of Asymm :- RSA, Deffie helman, DSA.

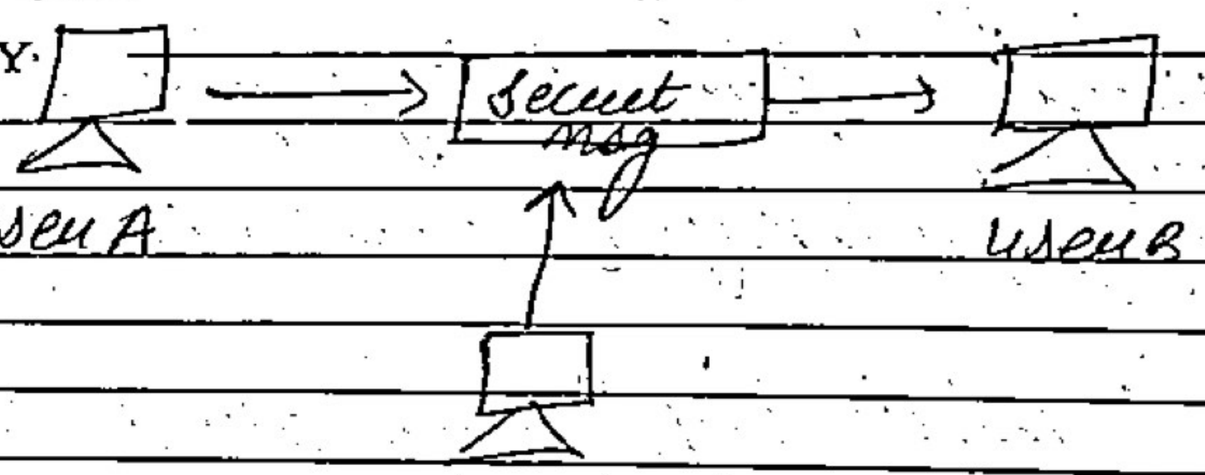
07 SATURDAY

Important Note:- A msg that is encrypted using a public key can only be decrypted using a private key. While also a message encrypted using private key can be decrypted using public key.

Security Goals:- (CIA triad in cryptography)

1) Confidentiality:-
- It allows authorized users to access sensitive and protected data.
- The data should not accessed by unauthorized users.

08 SUNDAY



: (Loss of Confidentiality.)

- Attacker will try to capture data. To avoid this various encryption technique are used to safeguard our data, so that even if attacker gains access, he/she will

not be able to decrypt it.

2) Integrity :- Means maintaining consistency, accuracy and completeness of data.

• It is about protecting data from being modified or misused by an unauthorized user.

eg:- In a bank, when we deposit / withdraw money, the balance needs to be maintained.

3) Availability :- Data must be available to the authorized user. Information is useless if we cannot access it.

eg:- What would happen if we cannot access our bank accounts for transactions.

Security Services :-

1) data confidentiality 2) Data Integrity.

3) Authentication 4) Non-repudation

5) Access Control

3). Authentication :- is the process of verifying the identity of a person or device. A common example is entering a username and password when you log into a website.

11 WEDNESDAY

4) Non-Repudiation:- is a service which provides proof of the origin of data and the integrity of the data.

(or)

It is the assurance that someone cannot deny the validity of something.

eg:- A gives 1000 Rs check to B, and later B denyl it. It cannot happen because A will have its proof.

5) Access Control :- to whom the access should be given can be availed.

Engagements

(or) The prevention of unauthorized use of a resource

12 THURSDAY

(i.e, this service controls who can have access to our information under what condition.

Security Attacks in cryptography :-

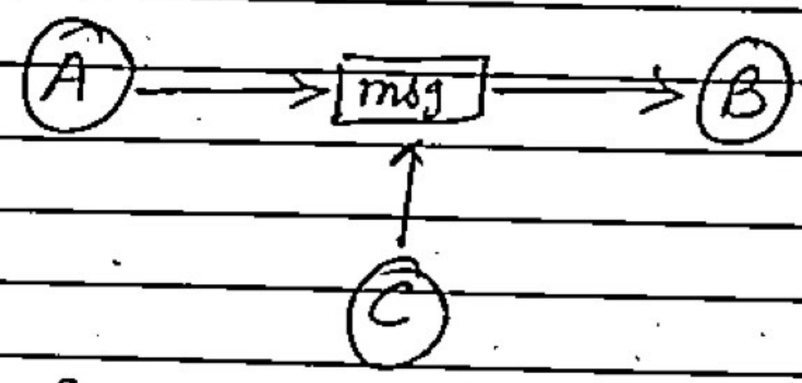
- Passive Attack
- Active Attack

Engagements
- → Release of msg content
- → Traffic analysis

तुम्हारी बुद्धि ही तुम्हारा गुरू है – शेक्सपियर

1) Passive Attacks — attempts to learn or make use of information from the system but does not affect system resources.

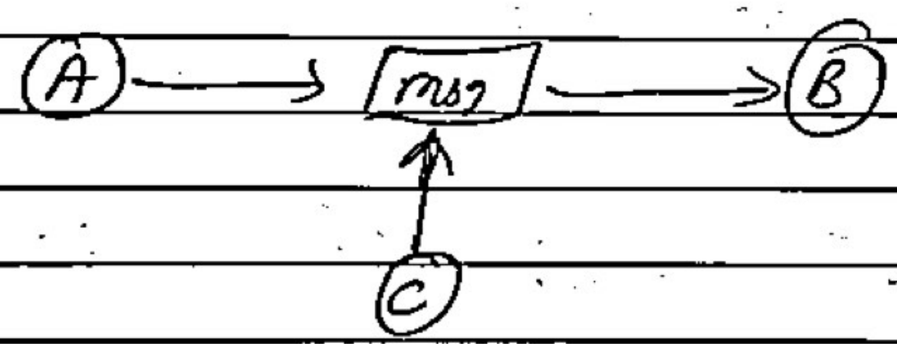
- Data does not modified by the third party.



eg:- Monitoring unencrypted communications such as email or telephone calls.

Engagements

ii) Release of msg content :- Telephonic conversation on electronic mail message or a transferred file may contain sensitive or confidential information.



Here, A is sending msg to B and C simply observes the conversation. So here confidentiality loses, as confidentiality means only (B) or receiver reads/receives the msg which is sent by sender (A).

Engagements

15 SUNDAY

(1) Traffic analysis :- Suppose that we had a way of encryption of message information, so that the attacker even if captured the message could not extract any information from the message.

- The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.

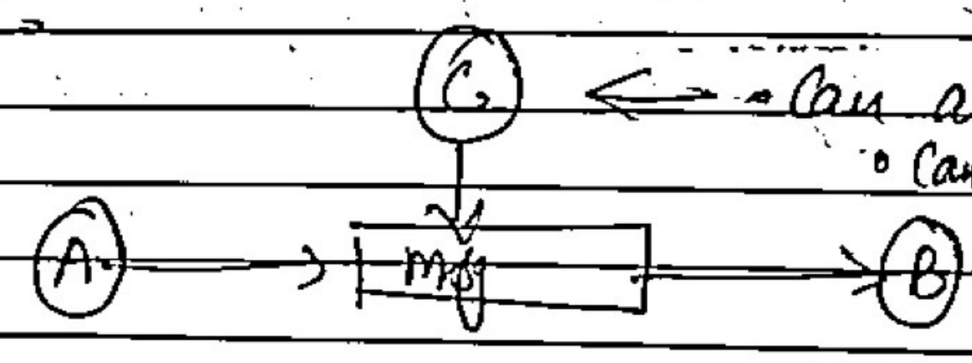
Engagements

- This information might be useful in guessing the nature of the communication that was taking place.

16 MONDAY

Or identify the origin, to whom the msg is going, from where it is going, size (traffic analysis).

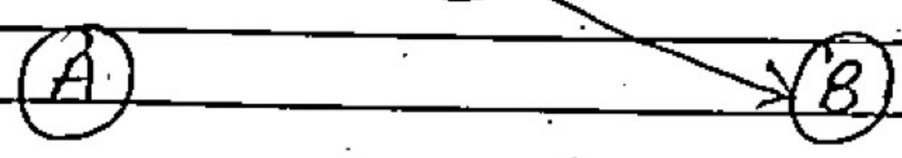
(2) Active attacks :- attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement.



- Can alter (delete, modify data)
- Can induced error bits.

Engagements

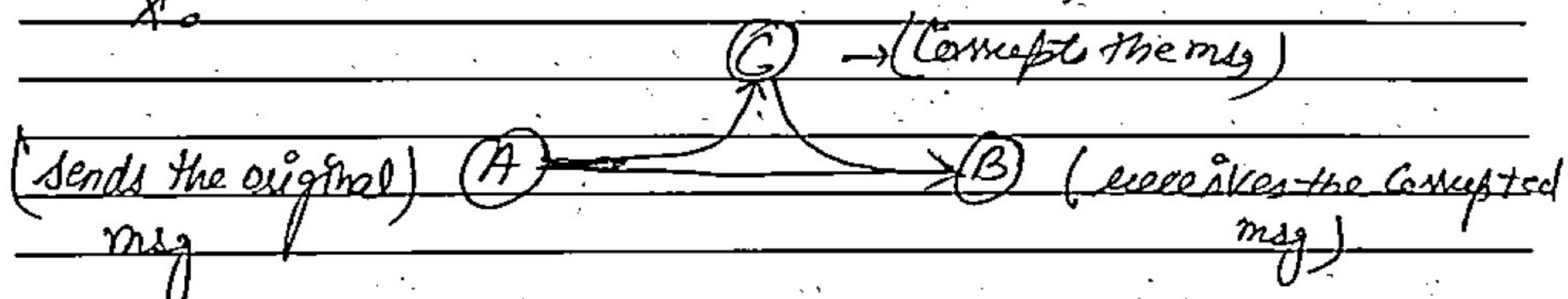
(i) Masquerade :- Masquerade attack takes place when one entity pretends to be different entity.



Here, C is sending msg to B and B thinks that A is sending msg to him, but C is sending msg pretending to be someone else.

(ii) Modification of message / Relay :- It means that some portion of a message is altered or that message is delayed or rendered to produce an unauthorized effect.

eg:- "Allow Rohan to read Confidential file X" is modified as "Allow Sohan to read confidential file X.



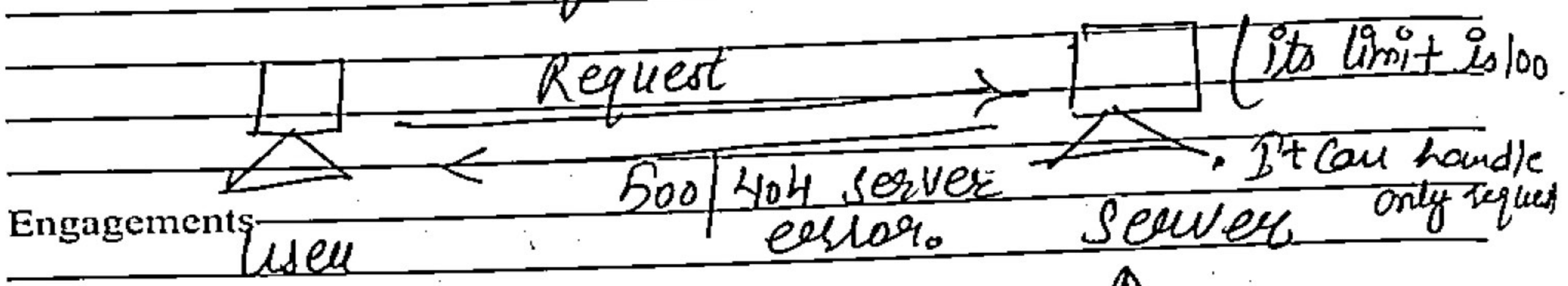
Here, Integrity loses.

(iii) Denial of service :- It prevents normal use of communication facilities. This attack may have a specific target.

19 THURSDAY

For example :- an entity may suppress all messages directed to a particular destination.

• Another form of service denial is the disruption of an entire network by disabling the network or by overloading it by messages so as to degrade its performance.



Overloads the server by fake request.

Attacker

20 FRIDAY

• problem :- availability

(iv) Repudiation :- This attack is done by either sender or receiver. The sender or receiver can deny later that he/she send or receive a message.

For example :- Customer ask his bank "To transfer an amount to someone" and later on the sender (customer) deny that he had not made such a request this repudiation.

27 FRIDAY

Encryption Techniques

Substitution
- → Caesar cipher
- → monoalphabetic
- → polyalphabetic → vigenere, → vernam

Transposition
- → Rail fence
- → Columnar.

Engagements
- → Play fair cipher
- → Hill cipher

→ One Time Pad (Vernam)

28 SATURDAY

(I) Substitution Technique :- It replaces the character. It is simpler and easy to break.

1) Caesar cipher :- is also known as 'shift cipher' or additive cipher'.

- It is the earliest and simplest method of Enc. technique.

- In Caesar cipher each character is shifted three places up or according to the key given.

Engagements

प्रेम की सम्पूर्ण पेय मात्राओं में यौवन सर्वाधिक शक्तिशाली है – ऐलेन

$C = (P+K) \bmod 26$ → for encryption.

① Eg:-

PT = A B C (1 2 3)

Key = 3

CT = ? D E F (By adding 3 in each alphabets).

1 2 0 2 0 1 3 11 1 20 15 14 13 5

② eg:- ATTACK AT ONCE

key = 4. , CT = ? EXXEGOEXSRGI

For decryption:-

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

③ eg:- PT = C A T (3 1 20)

key = 1 2 3 , CT = ?

4 3 23

D C W

Q) Monoalphabetic:- A single cipher alphabet for each plain text alphabet is used throughout the process.

i.e. fixed substitution will be done always (one to one).

- If 'N' → I use 'X' then always, I will use 'X' only in place of 'N'.

eg:- MY NAME → Xp XBNZ

3) Polyalphabetic :- There is no fixed substitution

- Each occurence of a character may have a different substitute, i.e we can use more than 1 substitution for the same letter.

- The relationship b/w a character in the PT is a character in the CT is one to many.

eg:- MY NAME → NP OBXP

a) Vigenere cipher :- It is a polyalphabetic substitution cipher.

eg:-
Plain Text :- GIVE MONEY
Key :- LOCK

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

eg:- Try this key=key

Repeat the letters of the key so that the no. of letters in PT and K that is plain Text and key becomes equal.

7430

NOTES/टिप्पणी

Colums → PT
Rows → Keys.

Note :- The encryption is done using a (26 X 26) matrix or a Table.

CT → | R W X O X C P O J |

For decryption :

CT →	R	W	X	O	X	C	P	O	J
key	L	O	C	K	L	O	C	K	L
PT →	G	I	V	E	M	O	N	E	Y

b) Vernam cipher :- Length of key = Length of PT.

eg :- ~~PT = RAMSWARUPK~~

PT =	R	A	M	S	W	A	R	U	P	K
	17	0	12	18	22	0	17	20	15	10
Key =	17	0	13	2	7	14	1	0	1	0
	R	A	N	C	H	O	B	A	B	A
(PT+K) =	34	0	25	20	29	14	18	20	16	10
	−26				−26					
if No. 26 ≤										
Sub from 26.	8				3					

CT = I A Z W

CT = QCPW COFSRXHS.

b) Vernam Cipher :- [Length of Key = Length of PT]

Eg:- PT = H E L L O

Key = D G H B C

PT = H E L L O
7 4 11 11 14

(PT+K) +
D G H B C
3 6 7 1 2
10 10 18 12 16

Engagements

CT = K K S M Q

Note :- if no is greater than 26 than Subtract 26 from that No.

For Decryption :-

CT = K K S M Q
10 10 18 12 16

(CT-K)
− D G H B C
3 6 7 1 2
7 4 11 11 14

PT = H E L L O

Eg:- PT = This is secret

Engagements Key = XVHG UW NOPGDZ

CT = ?

दूसरों का सम्मान करो, लोग तुम्हारा भी सम्मान करेंगे – रविन्द्रनाथ ठाकुर

03 FRIDAY

4). Playfair Cipher :-

- Create 5x5 matrix.
- If will be combined together.
- Insert key first into matrix, fill rest of the cells by alphabets.
- pairing of 2 alphabets.
- No repitation is allowed.
- pair cannot be made with same letter, break the letter into single and add 'x' to the previous letter.

Eg:- PT HELLO → HE LX LO

Engagements

Rules: (i) Same row, replace with immediate right.

04 SATURDAY

(iii) Digonal → corresponding elements.

Eg:- (1)

PT: Instruments

Key: Monarchy

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

Engagements

बुद्धि द्वारा सधा हुआ उत्साह ही लगन है → पास्कल

PT:- INSTRUMENTS.

IN ST RU ME NT SZ

CT:- GA TL MZ CL RQ TX

eg:- (2) PT:- Why don't you (3) PT:- Come to the window.

Key:- keyword.

PT:- (4) Play fair
Keywords Example

PT:- (5) hide the gold.
Keyword:- play fair.

Engagements

(5) Hill cipher:- Polyalphabetic cipher.

To Encrypt:- $\boxed{C = KP \bmod 26}$

eg:- PT= ATTACK.

Let key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}_{2\times 2}$. $n \times n$

vector length $\leftarrow (n\times 1) = 2\times 1$

Since the key is a 2X2 matrix, plain Text should be converted into vectors of length 2.

So,

$$\begin{bmatrix} A \\ T \end{bmatrix}_{2\times 1} \begin{bmatrix} T \\ A \end{bmatrix}_{2\times 1} \begin{bmatrix} C \\ K \end{bmatrix}_{2\times 1}$$

Engagements

07 TUESDAY

(I) Encryption :-

1st Vector $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$; Key $= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$$\boxed{C = KP \bmod 26}$$

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

Engagements $= \begin{bmatrix} 2\times 0 + 3\times 19 \\ 3\times 0 + 6\times 19 \end{bmatrix} \bmod 26$

$C = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$

08 WEDNESDAY

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

∴ Plain Text $\begin{bmatrix} A \\ T \end{bmatrix}$ becomes $\begin{bmatrix} F \\ K \end{bmatrix}$ is $\boxed{AT \rightarrow FK}$

(2) 2nd Vector :-

$\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$, Key $= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$$\boxed{C = KP \bmod 26}$$

Engagements

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

$$= \begin{bmatrix} 2\times19+3\times0 \\ 3\times19+6\times0 \end{bmatrix} \bmod 26.$$

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

Engagements

$$\therefore \boxed{TA \rightarrow MF}$$

(B) 3rd Vector -

$$\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$$

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

$$= \begin{bmatrix} 2\times2+3\times10 \\ 3\times2+6\times10 \end{bmatrix} \bmod 26$$

Engagements

$$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26$$

Transposition Technique :- is a cryptographic technique that converts the plain text to cipher text by performing permutations on the plain text i.e. change the position of each character of plain text for each round.

• It includes the various techniques like :

1) Rail fence 2) Simple Columnar transposition technique.

Engagements

सभी प्राणियों के लिए सद्भावना ही सच्चा धर्म है – बुद्ध

FEBRUARY 2017 (Keyless cipher) शक 30 माघ 1938
फरवरी रविवार विक्रमी 8 फाल्गुन 2073

19 SUNDAY (II) 1) Rail fence Transposition Technique :-

- Plain Text is written down as a sequence of diagonals and then read as sequence of rows.

eg:- PT:- all the best for exams.

a l l t h e b e s t f o r e x a m s

Engagements CT: a l h b s f r x m l t e e t o e a s.

Notes
- used for short msgs, not much safe
- Easy to break by the attacker

FEBRUARY 2017 शक 1 फाल्गुन 1938
फरवरी सोमवार विक्रमी 9 फाल्गुन 2073

20 MONDAY Row/Column Transposition cipher :-

In this cipher, we write message row by row and read message column by column.

eg:- PT = Attack Postponed until two Am.

Key :- 4 3 1 2 5 6 7

Acc to rule :-

4	3	1	2	5	6	7
A	t	t	a	c	k	P
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	A	m	X	Y	Z

PT:- Attack Postponed until two Am XYZ

Engagements

मां का हृदय बच्चों की पाठशाला है।- एच. डब्ल्यू. चेस

CI:- ttnA aPtm tSuo AodW GOY
Knly Petr.

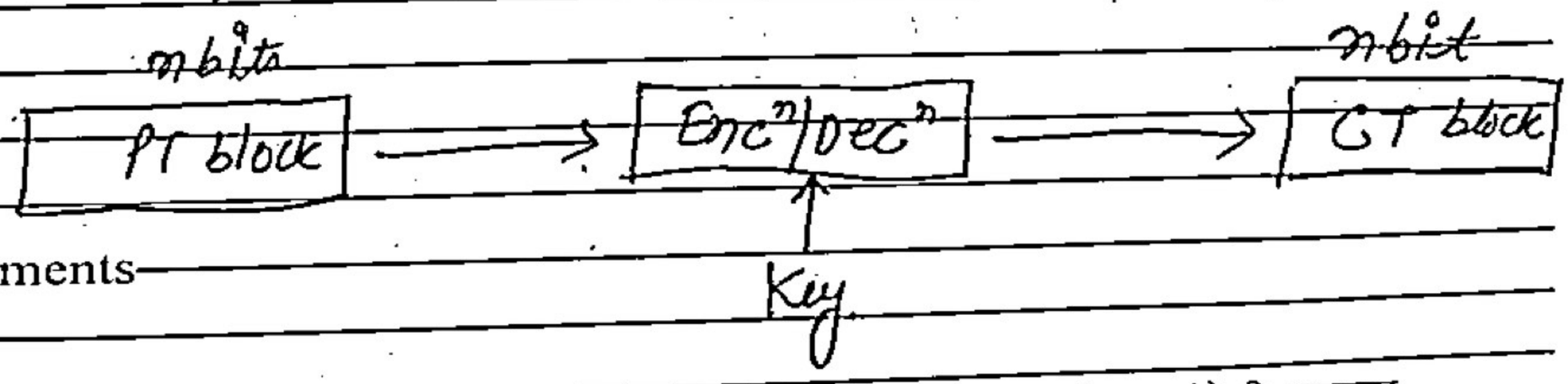
2. eg: Five minutes Engineering.
Key- 43512

Block cipher :- is a encryption and decryption method which operates on the blocks of plain Text, instead of operating on each bit of plain Text separately.

Engagements—
- Each block is of equal size and has fixed no. of bits.

- At a time block cipher operates only one block of plain Text and applies key on it to produce the corresponding block of cipher text.

- While Decryption also only one block of cipher text is operated to produce its corresponding plain Text.



Engagements—

मूर्ख और उसकी सम्पत्ति दोनों को शीघ्र ही विलग होना पड़ता है — अंग्रेजी कहावत

23 THURSDAY

Examples of Block ciphers:-

- DES is the Best example of it. DES divides the plain text into the number of blocks, each of 64 bits.
- DES operates on one block of PT at a Time. Key of 56 bit is applied to each block of plain text to produce its corresponding CT of 64 bit.

Block cipher Modes of operation :-

Engagements

For different type of messages, we need different modes of operations.

24 FRIDAY

5 modes of operation are:

1) ECB (Electronic code book) mode
2) CBC (cipher block chaining) Mode
3) CFB (cipher feedback mode)
4) OFB (output feedback mode)
5) CTR (Counter Mode).

Engagements