Name :- KRISHANT CHAUHAN
Course :- BCA 6A
Roll no :- 29
Uni Roll no :- 1921085

① Importance of Cryptography

It ensure the integrity of data using having algo. & manage digits. Cryptography is the study of tech. for seach info. & data.

② Role of crypto.

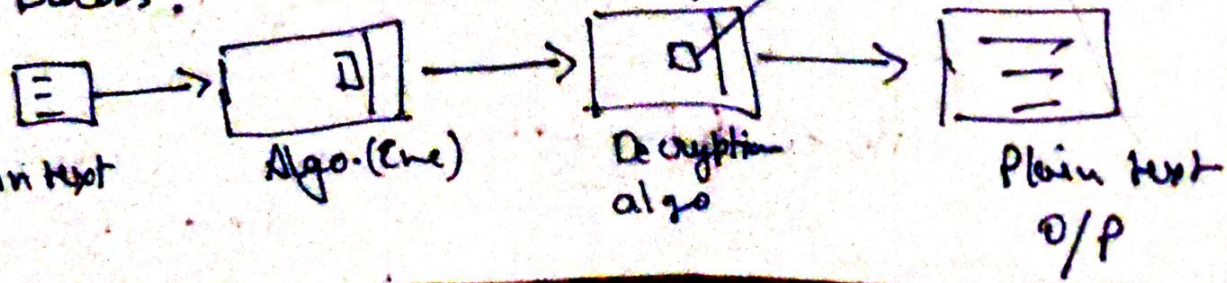
It is the study of secure comm. tch. that allow only the sender email & intended of msg to view its content

③ It is use to Protect Confidentiality as it stored on Computer Sys. & transmitted using the internet or other Network.

④ mainly 2 type
- Active & Passive

| Passive | Active |
|---|---|
| • It is very dang. | • Modifying your data/info |
| • No modification | → Bruteforce<br>→ Man In Middle |

⑤ In this Both use same key to Send & Recive Msg.
→ Fast Process.



6.

| Block cipher | Stream Cipher |
|---|---|
| • It converts the plain text into cipher text by taking plain text block at a time | • It converts the plain text into cipher text by taking 1 byte of plain text at a time. |
| • Complexity is simple | • Complexity is Complex. |
| • Reverse Eng. text is hard. | • Rev. Engg is easy |
| • Is Slow | • Fast. |

(a) $-5 \bmod 26$

$= 26 - (5 \% 26)$

$= 26 - 5$

$= 21$

(b) $12 + 18 \pmod 8$

$= 12 + 18$

(c) Subtract 11 from 7 in $Z_{13}$

$(7 - 11) \bmod 13 \rightarrow -4 \bmod 13$

$= 13 - (4 \bmod 13)$

$= 13 - 4$

$= 9$

(d) Multiply 11 by 7 in $Z_{20}$

$(7 \times 11) \bmod 20 \rightarrow 77 \bmod 20$

$= 17$

(e) $3 * 7 \pmod{11}$

$3 * 7$

$= 21$

$\cong$ or not

(i) $(200 + 301) \bmod 11 \cong (2+4) \bmod 11$

$(501) \bmod 11 \cong 6 \bmod 11$

$6 \cong 6$

Hence it is Cong.

iii) $-13 \cong 13 \pmod{26}$

LHS $-13 \bmod 26$

$26 - (13 \% 26)$

$13$

RHS $13 \bmod 26$

$13$

L.H.S = R.H.S

Hence it is Cong.

ii) $172 \equiv 17 \pmod{25}$

| LHS | RHS |
|---|---|
| 2 | 2 |

LHS = RHS

Hence it is log.

(7)

C O V I D
3 15 22 9 4

∴ taken as the operation of next multiplication by a sq. matrix order the msg out in log 3

$[3 \quad 15 \quad 22] \quad [9 \quad 4 \quad 0]$

$$[3 \quad 15 \quad 22] \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 6 \end{bmatrix} = [55 \quad -18 \quad 3]$$

$$[9 \quad 4 \quad 0] \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = [17 \quad -13 \quad 9]$$

$$A^{-1} = \frac{1}{|A|} \text{adj } A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$

Now Reciver decode the coded.

Coded matrix $[55 \quad -18 \quad 3]$ Decoding matrix $\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$ Decoded row matrix $= [3 \quad 15 \quad 22]$

$$[17 \quad -13 \quad 9] \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix} = [9 \quad 4 \quad 0]$$

So, the sequence of decoded row matrix is

$[3\ 15\ 22], [9\ 4\ 0]$

Thus the reciever read the msg. "COVID".