0801CS171077
Shikhar Mahajan Shikhar



17/03/21

# INS Assignment - 01

Q1

(a) 1) No. of students = 105
Therefore, No. of keys = $\frac{105 \times 104}{2}$

$= 5460 \equiv {}^{105}C_2$

2) If every student trust instructor, then the no. of keys must be between instructor and students
and
No. of keys = No. of students = 105
i.e., 105 keys are between every student and instructor

3) If 2 students wants to communicate by exchanging data with each other then they should contact the instructor first followed, there will be 105 keys.
i.e; 1 key between instructor & student.

0801CS171077
Shikhar Mahajan Shikhar

(2)

17/03/21

Q1(b)

Plain text Given

⇒ WE LIVE IN AN INSECURE WORLD.

$$\text{Key} = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

Converted Numeric Index text

⇒ 22 4 11 8 21 4 8 13 0 13 18 4 2 20 17 4
22 14 17 11 3

Cipher text performing **P x key**

- $[22\ 4] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [86\ 72] \% 26 = [08\ 20]$
- $[11\ 8] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [73\ 78] \% 26 = [21\ 0]$
- $[21\ 4] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [83\ 70] \% 26 = [5\ 18]$
- $[8\ 13] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [89\ 107] \% 26 = [11\ 3]$
- $[0\ 13] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [65\ 91] \% 26 = [13\ 13]$
- $[18\ 4] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [74\ 64] \% 26 = [12\ 22]$

0801CS171077
Shikhar Mahajan

(3)

17/3/21

- $[2 \quad 20] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [106 \quad 144] \% 26 = [2 \quad 14]$
- $[17 \quad 4] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [71 \quad 62] \% 26 = [13 \quad 10]$
- $[22 \quad 14] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [136 \quad 142] \% 26 = [6 \quad 12]$
- $[17 \quad 11] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [106 \quad 111] \% 26 = [2 \quad 7]$
- $[3 \quad 23] \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \% 26 = [124 \quad 167] \% 26 = [20 \quad 11]$

So, the cipher text

=> 8,20 21,0 5,18 11,03 13,13 12,22 2,14 13,10
6,12 2,7 20 11

Ans => IU UA FS LD ANN MW CD TK GM CH OL

0801CS171077
Shikhar Mahajan

(4)

(7|3|2)

(c) Given Key = HEALTH

= [7 4 0 11 19 7]

Plain text

⇒ LIFE IS FULL OF SURPRISES.

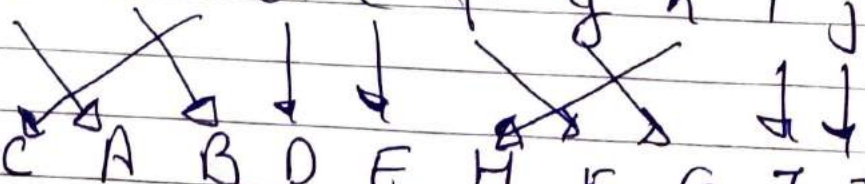
| LIFE | IS | FULL | OF | SURP | RI | SES |
|---|---|---|---|---|---|---|
| 11 18 5 4 | 8 19 | 5 20 11 11 | 14 5 | 18 20 7 15 | 17 8 | 18 4 18 |
| 7 4 0 11 | 19 7 | 7 4 0 11 | 19 7 | 7 4 0 11 | 19 7 | 7 4 0 |
| 18 12 5 | 15 25 | 12 24 11 22 7 | 12 | 25 24 17 0 10 | 15 | 25 8 18 |

Cipher text = SMFPBZMYLWHMZYRA KPZIS.

Ans

(d) Plain text attack as Eve select his own plain text & get cipher text of that given plain text. Eve has a plain-text cipher text combination.
Therefore, plain text attack is chosen.

(ii) plain text a b c d e f g h i j




Since, pattern repeats after 5

Ans: Therefore permutation key is = 5

(e) Cipher text

NCJAEZRCLASJLYODEPRLY
ZRCLASJLCPEHZOTOPDZQL
NZTY

Key = 13

Plain text

APWNRMEPYNFWYLBQRCEYLMB
PYNFWYPCRUMQGBCQMDYAMGL

Key = 12

Plain text

BQXOSNFQZOGXZMCRSDEZMNE
QZOGXZQDSUNRHCDRNEZBNHM

Key = 11

Plain text

CRYPTOGRAPHYANDSTEGANDGRAPHY
ARE TWO SIDES OF A COIN.

∴ Key = 11

0801CS171077
Shikhar Mahajan Shikhar. (6)
17/3/21

and the plain text is

⇒ CRYPTOGRAPHY and STEGANOGRAPHY are two sides of a coin.

(f)

Encryption key = [3, 2, 6, 1, 5, 4]

Decryption key = [4, 2, 1, 6, 5, 3]

Q2

(a) According to Sherlock holmes chapter the message refers to the pages of the book.

- The 534 refers to 534th page.
- C2 means column No. 2nd
- and, the following numbers are the words in the column
- The names did not appear on the page.

———— X ———— X ———— X ————