

CSE 490

Assignment 001

Name : Nafid Faham

ID : 18101107

## Answer to the Question-1

Given ciphertext :

VSRQJHEREVTXDUHSDQWU — ①

If we shift the plain text by 3, we get the corresponding ciphertext :

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

So for the given ciphertext ①, the plain text will be :

spongebobsquarepants

x

## Answer to the Question-2

Given message is,

we are all together.

By creating  $4 \times 4$  matrix we get,

|   | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | w | e | a | r |
| 2 | e | a | l | l |
| 3 | t | o | g | e |
| 4 | t | h | e | r |

We are now gonna do row ~~permutation~~ permutation

$$(1, 2, 3, 4) \Rightarrow (2, 4, 1, 3)$$

|   | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 2 | e | a | l | l |
| 4 | t | h | e | r |
| 1 | w | e | a | r |
| 3 | t | o | g | e |

After doing column permutation we get,

$(1, 2, 3, 4) \rightarrow (3, 1, 2, 4)$

|   | 3 | 1 | 2 | 4 |
|---|---|---|---|---|
| 2 | l | e | a | h |
| 4 | e | t | h | r |
| 1 | a | w | e | r |
| 3 | g | t | o | a |

The required ciphertext: LEALETHRAWERGTOE  
(Ans)



## Answer to the question-3

Given table -  $2 \times 1 \Rightarrow$

|        |     |     |     |     |     |     |     |     |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|
| letter | e   | h   | i   | k   | L   | p   | s   | t   |
| binary | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

Ciphertext (KITLKE) = 011 010 111 100 011 000

a) In case of "thrill" :

Plaintext : 111 001 101 010 100 100

⊕ Ciphertext : 011 010 111 100 011 000

key : 100 011 010 110 111 100  
L K i s t L

b) In case of "tiller" :

Plaintext : 111 010 100 100 000 101

⊕ Ciphertext : 011 010 111 100 011 000

key : 100 000 011 000 011 101  
L e k e k p