HILL CIPHER:

Given is plaintext and key matrix

PT:HEL

key matrix:

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

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

Matrix multiplication rule first- mxn second nxp

Step1 : Convert the alphabets of plaintext into their corresponding numerical equivalents-

H->7 E-> 4 L->11

Step 2: Multiply key matrix with Plaintext matrix

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Multiply

|  |  |  |
| --- | --- | --- |
| 7 | 4 | 11 |

=

|  |  |  |
| --- | --- | --- |
| 48 | 114 | 180 |

Step 3: Apply mod 26 to each element of the resultant matrix

48 mod 26 = 22

114 mod 26=10

180 mod 26= 24

Step 4: Convert the output of the step3 into their corresponding alphabets.

22-> W 10->K 24-> Y

WKY

Given PT : COLD

Key matrix:

|  |  |
| --- | --- |
| 3 | 2 |
| 5 | 7 |

C->2 O->14

|  |  |
| --- | --- |
| 2 | 14 |

Key matrix:

|  |  |
| --- | --- |
| 3 | 2 |
| 5 | 7 |

Multiply

L->11 D->3

|  |  |
| --- | --- |
| 11 | 3 |

Decryption of HILL CIPHER-

Given CT and Inverse of key matrix:

CT: HL

Inverse of key matrix:

|  |  |
| --- | --- |
| 3 | 14 |
| 9 | 5 |

H-> 7 L-> 11

Step 1: Multiply inverse of key matrix with ciphertext matrix.

|  |  |
| --- | --- |
| 3 | 14 |
| 9 | 5 |

Multiply

|  |  |
| --- | --- |
| 7 | 11 |

=

|  |  |
| --- | --- |
| 175 | 180 |

Step2: Apply mod 26 to resultant matrix

175 mod 26=19

118 mod 26=14

Step 3: convert these numerical equivalents to alphabets.

19-> T 14-> O

B. TRANSPOSITION –

Changing the positions of the alphabets of the plaintext.

RAIL FENCE TECHNIQUE

SIMPLE COLUMNAR TECHNIQUE

ONE-TIME PAD or VERNAM CIPHER

1. RAIL FENCE – It is the technique in which the alphabets of the given plaintext is organized in diagonals.

Given PT depth by default is 2.

Depth is actually how many rows it has to be defined.

PT: COME HOME TOMORROW depth=2

Step 1: Arrange the alphabets of the plaintext in diagonals

C M H M T M R O

O E O E O O R W

Step 2: Write all the alphabets of first row then second row.

CMHMTMROOEOEOORW

1. SIMPLE COLUMNAR TECHNIQUE:

Given PT And random order of column

PT : COME HOME TOMORROW

Random order of the columns: Suppose 6 columns :

Random order : 6,4,3,5,1,2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| C | O | M | E | H | O |
| M | E | T | O | M | O |
| R | R | O | W |  |  |
|  |  |  |  |  |  |

Step 1: Arrange the alphabets of the plaintext horizontally .

Step 2: According to the random order

Write the alphabets –

OOEOWMTOHMCMROER -> Ciphertext.

1. ONE TIME PAD or VERNAM Cipher:

Encryption:

Given PT and the ONE TIME PAD is given

PT: HOW ARE YOU? ONE TIME PAD: NCBTZQARX

Step 1: Convert the alphabets of the plaintext and the one –time pad into their corresponding numerical equivalents .

Step2: Add their corresponding numerical equivalents.

H O W A R E Y O U

7 14 22 0 17 4 24 14 20

N C B T Z Q A R X

13 2 1 19 25 16 0 17 23

20 16 23 19 **42** 20 24 **31** **43**

Step 3: Subtract 26 if sum > 25 otherwise it will be same.

42-26=16

31-26=5

43-26=17

20 16 23 19 16 20 24 5 17

Step 4: convert it into corresponding alphabets.

U Q X T Q U Y F R

Decryption:

Given the CT: UQXTQUYFR and One Time PAD:NCBTZQARX

Step 1: Convert the alphabets of the ciphertext and the one –time pad into their corresponding numerical equivalents.

Step 2: subtract the corresponding numerical equivalents.

20 16 23 19 16 20 24 5 17

U Q X T Q U Y F R

N C B T Z Q A R X

13 2 1 19 25 16 0 17 23

7 14 22 0 **-9** 4 24 **-12** **-6**

Step3: Add 26 wherever negative values are there.

-9+26=17

-12+26=14

-6+26=20

HOW ARE YOU