HILL CIPHER

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | ….. |  |  |  | Z |
| 0 | 1 | 2 | 3 | 4 |  |  |  |  | 25 |

Encryption:

CT = (PT\*KEY) mod 26

Matrix multiplication

PT=abcd = 0,1,2,3

Key= pqrs = 15,16,17,18

|  |  |
| --- | --- |
| A (0) | B (1) |
| C (2) | D (3) |

2\*2 matrix

|  |  |
| --- | --- |
| P(15) | Q(16) |
| R(17) | S(18) |

2\*2 matrix

(2\*2) (2\*2)

2\*2 is resultant matrix

(3\*2) (2\*4)

3\*4 is resultant matrix

CT=(PT\*KEY) mod 26

\* = mod 26 = =

Note:

* When you framing the matrix, make sure that it will satisfy the basic matrix multiplication rule
* If you start assigning numbers from 0, then mod 26
* If u start from 1, then mod 27

Decryption

PT=(CT\*K-1) mod 26

Where K-1 is the inverse of key matrix

6 mod 2 = 0

2 mod 6 = 2

-5 mod 2 = 1

5 mod -3 invalid

5-1mod3 -🡪 Euclidean Algorithm

Assignment

PT=CHAIRS

Key=SCREEN

CT = ?

PT = ----- -----

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C | H | A | I | R | S |

Key

|  |
| --- |
| S |
| C |
| R |
| E |
| E |
| N |

Key = --------------

CT = ( PT \* Key ) mod 26

Case 1 : (2\*3) (3\*2) ---- Not valid – number of characters mismatch

Case 2: (3\*2) (2\*3) --- Not valid

Case 3: (1\*6) ----- Not

Suggestion:

If resultant matrix size is not same as Plain Text matrix size, then preferably try to make it as square matrix by adding extra characters (X)

Transposition Ciphers

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | R | E | S | I | D | E | N | C | Y | C | S | E | I | T |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P |  | E |  | I |  | E |  | C |  | C |  | E |  | T |
|  | R |  | S |  | D |  | N |  | Y |  | S |  | I |  |

CT : PEIECCETRSDNYSI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | 1 | 4 | 2 | 3 |
| P | R | E | S | I |
| D | E | N | C | Y |
| C | S | E | I | T |

CT : PDCRESENESCIIYT --- without assigning any numbering

CT = RESSCIIYTENEPDC --- With some numbering (32 different combinations)