IS Section CSA1 online Class (24-03-2023)

Plain Text: t h i s c r y p t o s y s t e m i s n o t s e c u r e

keyword: R A M Z A N m = 6

you need to define any permutation of m i.e. 6

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| t | h | i | s | c | r |
| I | C | T | R | H | S |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| y | p | t | o | s | y |
| T | S | Y | Y | P | O |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| s | t | e | m | i | s |
| E | I | S | S | T | M |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| n | o | t | s | e | c |
| T | E | N | C | O | S |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| u | r | e | q | q | q |
| E | Q | U | Q | R | Q |

How many different ways to permute 6 digits??

6! = 720

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 2 | 4 |

For decryption, you have to computer k-1 ?? (sort the key based on Row#2)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| E | Q | U | Q | R | Q |
| u | r | e | q | q | q |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| T | E | N | C | O | S |
| n | o | t | s | e | c |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| E | I | S | S | T | M |
|  |  |  |  |  |  |

RAIL FENCE CIPHER

It is based on 2-dimensional structure (ROWs and COLUMNs)

Keyword = TEN m = 3 (it denotes number of ROWS)

Plain Text = t o d a y i s t h e f i r s t F r i d a y o f R a m z a n

Length of Plain/Cipher Text = 29 (number of Columns in a ROW = ROWSIZE)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 | 26 | 27 | 28 | 29 |
| 1 | T |  |  |  | Y |  |  |  | H |  |  |  | R |  |  |  | R |  |  |  | Y |  |  |  | A |  |  |  | N |
| 2 |  | O |  | A |  | I |  | T |  | E |  | I |  | S |  | F |  | I |  | A |  | O |  | R |  | M |  | A |  |
| 3 |  |  | D |  |  |  | S |  |  |  | F |  |  |  | T |  |  |  | D |  |  |  | F |  |  |  | Z |  |  |

IS Section CSA1 Online Class (30-03-2023)

For Encryption

Step#3

You have to write Plain text diagonally

Step#4 (how to get Cipher text)

Read text Horizontally (Row-wise)

Cipher text: TYHRRYAN CAITEISFIAORMA DSFTDFZ

For Decryption

Keyword = TEN m = 3 (it denotes number of ROWS) GIVEN

Length of Plain/Cipher Text = 29 (number of Columns in a ROW = ROWSIZE)

You have to infer this info yourself

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 | 26 | 27 | 28 | 29 |
| 1 | T |  |  |  | Y |  |  |  | H |  |  |  | R |  |  |  | R |  |  |  | Y |  |  |  | A |  |  |  | N |
| 2 |  | C |  | A |  | I |  | T |  | E |  | I |  | S |  | F |  | I |  | A |  | O |  | R |  | M |  | A |  |
| 3 |  |  | D |  |  |  | S |  |  |  | F |  |  |  | T |  |  |  | D |  |  |  | F |  |  |  | Z |  |  |

Step#3

You have to write the Cipher Text horizontally (Row-wise)

Step#4

You have to read the Plain text diagonally

Row Transposition Cipher

It is also based on 2D Structure (Rows & Columns)

Let’s assume keyword is R A M Z A N

17 0 12 25 0 13

m denotes length of the keyword. m = 6 (# of COLUMNS)

Plain text is = “write text of message out in rows” 27 Letters

How you will determine # of Rows??????????

Ceil [length of the Plain/Cipher Text/m]

Ceil [27/6] = 5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R  17 | A  0 | M  12 | Z  25 | A  0 | N  13 |
| w | r | i | t | e | t |
| e | x | t | o | f | m |
| e | s | s | a | g | e |
| o | u | t | i | n | r |
| o | w | s | q | q | q |

Step#3

Write Plain Text Horizontally (Row-wise)

Step#4 (how to generate Cipher text)

Read Column-wise (as per ascending Order of the Keyword)

Cipher Text: RXSUW EFGNQ ITSTS TMERQ WEEOO TOAIQ = 30 letters

For Decryption

Step#1 m = 6 (RAMZAN) # of COLUMNS

Step#2 # of ROWS 30/6 = 5 (COLUMN SIZE🡺 # of Rows in a Column)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R  17 | A  0 | M  12 | Z  25 | A  0 | N  13 |
| W | R | I | T | E | T |
| E | X | T | O | F | M |
| E | S | S | A | G | E |
| O | U | T | I | N | R |
| O | W | S | Q | Q | Q |

Cipher Text: RXSUW EFGNQ ITSTS TMERQ WEEOO TOAIQ

Step#3

Write Cipher text vertically (according to ascending Order of index of the Keyword)

Step#4

Read Plain Text Horizontally

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C | I | P | H | E | R |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 4 | 2 |
| P | E | C | R | H | I |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | E | C | R | H | I |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 6 | 1 | 5 | 2 | 4 |
| C | I | P | H | E | R |

IS Section CSA1 online Class (31-03-2023)

HILL CIPHER

Matrix =

Order of Matrix (m,n) m×n m by n

Where ‘m’ is the number of Rows and ‘n’ is the number of Columns

Square Matrix (if m == n)

Rectangular Matrix (if m != n)

What is an invertible Matrix??

A Matrix ‘A’ is said to be invertible if (pre-condition🡺 A is non-singular) and it’s inverse exists

Singular Matrix = = 0

Non-Singular Matrix = != 0

A**-1** =

ad – bc

By expanding Matrix from R1, we get

a11(b22c33 b21c33-b23c31) + a13(b21c32-b22c31)

A**-1** = () **-1** ×a

GCD(

In modulo Arithmetic

Pre-condition of Matrix Multiplication

A**(p,q)**B**(q,k)** = C**(p,k)**

A**(3,4)**B**(4,1)** = C**(3,1)**

= y()

IS Section CSA1 online Class (06-04-2023)

HILL CIPHER

EK(x) = X1mKmm = Y1m

Plain Text (I N) (V E) (R T) (I B) (L E)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Letter | I | N | V | E | R | T | I | B | L | E |
| Index | 8 | 13 | 21 | 4 | 17 | 19 | 8 | 1 | 11 | 4 |

22

A**-1** =

**You have to validate KEY first. For this what are the Pre-Conditions??**

1. Whether K is an invertible Matrix or Not?? (Non-Singular0 )
2. GCD (🡺

= 7724 = 53 mod 26 = 10

EK(x) = X1mKmm = (8 13)

=(8= (88+39 64+91)

=(127 155) = (23 25) = (X Z)

(I B) = (8 1) = (88+3 64+7) = (91 71) = (13 19) = (N T)

**For Decryption**

DK(y) = X1mK**-1**mm = X1m

K**-1 =** = **-1** (adj K)

For a 2how you will compute Adjoint

then adjoint (K) =

=

K-1 = (1)-1 =

(13 19) = (91+437 234+209) = (528 443) = (8 1) = (I B)