**Maida Shahid**

**Assignment 1**

**Information Security**

**Plain Text**

**20L1377-Shahid Aslam-35202-7166376-8**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A=0 | B=1 | C=2 | D=3 | E=4 | F=5 |
| G=6 | H=7 | I=8 | J=9 | K=10 | L=11 |
| M=12 | N=13 | O=14 | P=15 | Q=16 | R=17 |
| S=18 | T=19 | U=20 | V=21 | W=22 | X=23 |
| Y=24 | Z=25 | 0=26 | 1=27 | 2=28 | 3=29 |
| 4=30 | 5=31 | 6=32 | 7=33 | 8=34 | 9=35 |

**Caesar Cipher:**

**Encryption:**

**key**=2 shift left

**Cipher Tex**t=

42N3599-UJCJKFCUNCO-57424-9388598-0

**Decryption:**

  If we get 2 shifts of letters to the right side, we can easily decrypt.

**key**=2 shift right

**Plain Text**=

20L1377-Shahid Aslam-35202-7166376-8

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A=S | B=L | C=M | D=J | E=D | F=E |
| G=Y | H=P | I=Q | J=R | K=Z | L=A |
| M=W | N=B | O=I | P=C | Q=U | R=F |
| S=H | T=V | U=K | V=N | W=G | X=O |
| Y=X | Z=T | 0=7 | 1=9 | 2=0 | 3=1 |
| 4=5 | 5=3 | 6=2 | 7=4 | 8=6 | 9=8 |

**Monoalphabetic Cipher:**

**Encryption:**

**key**=SLMJDEYPQRZAWBICUFHVKNGOXT7901532468

**Cipher Tex**t=

07A9144-HPSPQJ SHASW-13070-4922142-6

**Decryption:**

  From table we can easily decrypt it by using the key and replace the alphabet to its original alphabet

**key**=SLMJDEYPQRZAWBICUFHVKNGOXT7901532468

**Plain Text**=

20L1377-Shahid Aslam-35202-7166376-8

**Hill Cipher:**

**Encryption:**

**key**=dbgf

|  |  |  |
| --- | --- | --- |
| SH=SB | AH=QJ | ID=QX |
| AS=EM | LA=HL | MX=SX |

**Cipher Tex**t=

20L1377-SBQJQXEMHLSX-35202-7166376-8

**Decryption:**

 From the key matrix we can easily decrypt the text by formula

P= CK^-1 mode 26

**key**=dbgf

Taking inverse K^-1:

Key=

**Plain Text**=

Which is equal to SH

Which is equal to HA

Hence the decrypt text is:

20L1377-Shahid Aslam-35202-7166376-8

**Playfair Cipher:**

**Encryption:**

To tackle the numbers, we are making a 6 by 6 matrix.

**key**=Maida Shahid

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M | A | I | D | S | H |
| B | C | E | F | G | J |
| K | L | N | O | P | Q |
| R | T | U | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**Cipher Tex**t=

31OZ198DMIMDSIAPIAZ931180790879W

**Decryption:**

  From table we can easily decrypt it by using the key and replace the alphabet to its original alphabet.

We just have to reverse the rules:

a. If both letters of the digram are in the same row, replace each letter with the letter to its left

b. If both letters are in the same column, replace each letter with the letter above it.

c. If neither of the above cases applies, form a rectangle with the two letters and replace each letter with the letter in the same row but in the opposite corner of the rectangle.

**key**=Maida shahid

**Plain Text**=

20L1377Shahid Aslam3520271663768

**Vigenère Cipher:**

**Encryption:**

C=(P+K) mod 26

**key**=SHAHID

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | H | A | H | I | D | A | S | L | A | M |
| S | H | A | H | I | D | S | H | A | H | I |
| 10 | 14 | 0 | 14 | 16 | 6 | 18 | 25 | 11 | 7 | 20 |

**Cipher Tex**t=

20L1377-KOAOQGSZLHU-35202-7166376-8

**Decryption:**

P=(C-K) mod 26

**key**=SHAHID

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| K | O | A | O | Q | G | S | Z | L | H | U |
| S | H | A | H | I | D | S | H | A | H | I |
| 18 | 7 | 0 | 7 | 8 | 3 | 0 | 18 | 11 | 7 | 12 |

**Plain Tex**t=

20L1377-Shahid Aslam-35202-7166376-8

**Vernam Cipher:**

**Encryption:**

C=(P XOR K)

First, we convert it into bits then take XOR and then convert it into decimal.

S=18 =10010

B=1=00001

XOR= 10011=19=T

Thus:

**key**=BEDANDBREAK

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | H | A | H | I | D | A | S | L | A | M |
| B | E | D | A | N | D | B | R | E | A | K |
| 19 | 3 | 3 | 7 | 5 | 0 | 1 | 13 | 15 | 0 | 6 |

**Cipher Tex**t=

20L1377-TDDHFABDPAG-35202-7166376-8

**Decryption:**

P= (C XOR K)

First, we convert it into bits then take XOR and then convert it into decimal.

T=19 =10011

B=1=00001

XOR= 10010=18=S

Thus:

**key**=BEDANDBREAK

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | D | D | H | F | A | B | D | P | A | G |
| B | E | D | A | N | D | B | R | E | A | K |
| 18 | 7 | 0 | 7 | 8 | 3 | 0 | 18 | 11 | 7 | 12 |

**Plain Tex**t=

20L1377-Shahid Aslam-35202-7166376-8

**One Time Pad Cipher:**

**Encryption:**

C=(P XOR K)

First, we convert it into bits then take XOR and then convert it into decimal.

S=18 =10010

B=1=00001

XOR= 10011=19=T

Thus:

**key**=BURGERFRIES

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | H | A | H | I | D | A | S | L | A | M |
| B | U | R | G | E | R | F | R | I | E | S |
| 19 | 19 | 17 | 1 | 12 | 18 | 5 | 3 | 3 | 4 | 4 |

**Cipher Tex**t=

20L1377-TTRBMS FDDEE-35202-7166376-8

**Decryption:**

P=(C XOR K)

First, we convert it into bits then take XOR and then convert it into decimal.

T=19 =10011

B=1=00001

XOR= 10010=18=S

Thus:

**key**=BURGERFRIES

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | T | R | B | M | S | F | D | D | E | E |
| B | U | R | G | E | R | F | R | I | E | S |
| 18 | 7 | 0 | 7 | 8 | 3 | 0 | 18 | 11 | 7 | 12 |

**Plain Tex**t=

20L1377-Shahid Aslam-35202-7166376-8

**Problems:**

In Caesar cipher, the key is small, and anybody can guess the cipher text.

In monoalphabetic the cipher is jumbled up but with frequency distribution, one can easily get the plain text.

In hill cipher, it is difficult to find the key, which is not close to the text, yet the matrix is an identity matrix. But it is a strong cipher.

In one time pad cipher, the key generation of truly random words of length of text is challenging. High GPUs should be used.