**Hill cipher**

Message : Attack Is Tonight

Key = 3 10 20

20 9 17

9 4 17

Cipher text = (plain text \* key ) Mod 26

Plain text = (Cipher text \* Key(inverse) ) Mod 26

Cipher text = A T T \* 3 10 20

A C K 20 9 17

I S T 9 4 17 Mod 26

O N I

G H T

Cipher text = 0 19 19

0 2 10

8 18 19

14 13 8

6 7 19

Decryption :

Step 1 : determinant of key

Step 2 : transpose of key

Step 3 : find minor

Step 4 : find cofactor

Step 5 : key ( inverse) = (det(key)) (inverse) \* adj(key)

STEP 1 ANS : 3

(DET(KEY))(INVERSE) : (inverse of 3) = 9

STEP 2: 3 20 9

10 9 4

20 17 17

STEP 3 : (17\*9 - 17\*4)

(10\*17-20\*4)

ANS : 85 90 -10

187 -129 -349

-1 -78 -173

STEP 4 : FIND COFACTOR

+ - +

- + +

+ - +

STEP 5 : KEY(INVERSE) : (DET(KEY))(INVERSE) \* ADJ (KEY)

**AFFINE CIPHER :**

C = (P \* K1+K2) MOD 26

P = (C-K2)\*K1(INVERSE)) MOD 26

PLAIN TEXT : HELLO

KEY : ( 7 ,2)

PLAIN TEXXT : ( 7 4 11 11 14)

C = (7\*7)+2 ) MOD 26

C = 25 = Z

C = ( 4\*7)+2 )MOD 26

C= 4 = E

C= (11\*7)+2 MOD 26

C= 1 = B

C= (11\*7)+2 MOD 26

C= 1 = B

C= (14\*7)+2 MOD 26

C= 22 = W

C= ZEBBW kwy = (7,2)

PLAIN TEXT = (C-K2)\*K(INVERSE)MOD26

P(Z) = (25-2) (7 INVERSE ) MOD 26

P(Z) = 345 MOD 26 = 7 = H

PLAIN TEXT = HELLO

Plain text : charusat

Key : (5,2) perform encryption and decryption using affine cipher

**VIGENERE CIPHER :**

PLAIN TEXT : SHE IS LISTENING = ( 18 7 4 8 18 11 8 18 19 4 13 8 13 6)

KEY : PASCAL = (15 0 18 2 0 11 15 0 18 2 0 11)

C = (P+K) MOD 26

C = 7 = H

C = HHWKSWXSLGNTCG

P = ( C - K ) MOD 26

P = 18 = S

P = SHE IS LISTENING

GCD ( 123456,234)

Q R1 R2 R

527 123456 234 138

234 138

Plain text : Shiven Patel

Key : maher

**CHINESE REMAINDER THEREORM**

**X MOD Z = Y OR X EQUIVALENT Y MOD Z**

1. **X EQUIVALENT 3 MOD 5**

**X EQUIVALENT 1 MOD 5**

**3 = A1 1 = A2**

**5 = M1 5 = M2**

**STEP 1 : M = ? M= 3\*5=15**

**M1 = M/m1=15/5=3**

**M2 = M/m2 = 15/3=5**

**MULTIPLICATIVE CIPHER :**

C= (P\*K)MOD26

P=(C\*K(INVERSE))MOD 26

PLAIN TEXT : HELLO = [ 7 4 11 11 14 ]

KEY = 5

**VERNAM CIPHER**

**LENGHT KEY = LENGTH OF PLAIN TEXT**

**C = P+KEY**

**P =C-K**

**17+17=34 -26**

**PLAIN TEXT = vishva = [ 21 8 18 7 21 0]**

**KEY : charmi [ 2 7 0 17 12 8 ]**

**C = p + k**

**C= 23 mod 26 = 23 = x**

**C= 17 mod 26 = 17 = r**

**C= 18 = s**

**C= 24 = y**

**C= 7 =h**

**C= 8 = I**

**C = XRSYHI**