① Hill cipher:

Encryption: $C = (P \times K) \bmod 26$.

$$\text{key} = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

Message = ATTACK IS TONIGHT.

$$PT = \begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 551 & 247 & 646 \\ 130 & 58 & 204 \\ 555 & 318 & 789 \\ 374 & 289 & 637 \\ 329 & 199 & 562 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} F & N & W \\ A & G & W \\ J & G & J \\ K & D & N \\ R & R & Q \end{bmatrix}$$

Cipher Text = FNWAG GJ KDNRRQ

Decryption: $P = C \times K^{-1} \bmod 26$

finding K^{-1}.

$$K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

$$K^{-1} = \frac{1}{|K|} \text{adj } K.$$

$$|K| = 3(85) - 10(187) + 20(-1).$$

$$= -1635 \bmod 26.$$

$$= 3 \bmod 26.$$

$$|K| = 3.$$

finding adj K :

$$
\begin{array}{c} \\ 20 \\ 9 \\ 3 \\ 20 \end{array}
\begin{array}{c}
\begin{array}{cccc} 3 & 10 & 20 & 3 \end{array} \\
\begin{bmatrix} 9 & 17 & 20 & 9 \\ 4 & 17 & 9 & 4 \\ 10 & 20 & 8 & 10 \\ 9 & 17 & 20 & 9 \end{bmatrix}
\end{array}
\begin{array}{c} \\ 10 \\ 4 \\ 10 \\ 9 \end{array}
$$

$$
\text{adj } k = \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix}
$$

$$
k^{-1} = \frac{1}{3} \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} \mod 26.
$$

$$
k^{-1} = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}.
$$

$$
P = \begin{bmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 4 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix} \mod 26.
$$

$$= \begin{bmatrix} 520 & 227 & 409 \\ 416 & 154 & 192 \\ 294 & 252 & 279 \\ 352 & 247 & 242 \\ 578 & 527 & 643 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 4 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \Rightarrow \begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix}$$

② Vigenere cipher:

Alternate method:

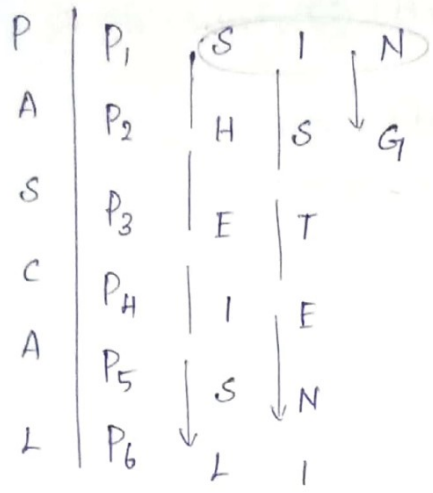
key: PASCAL.

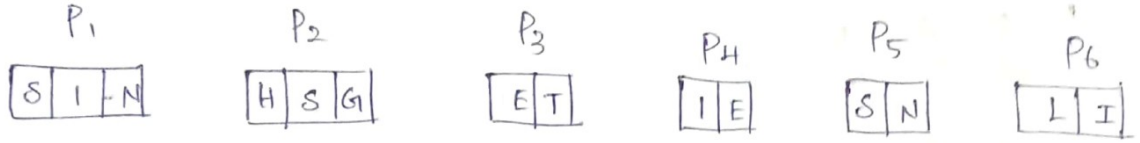
plaintext: SHE IS LISTENING.

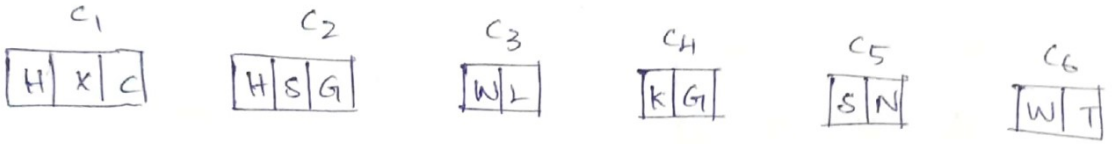
S	H	E	I	S	L	I	S	T	E	N	I	N	G
↓	↓	↓	↓	↓	↓							↓	↓
P	A	S	C	A	L							P	A
						P	A	S	C	A	L		

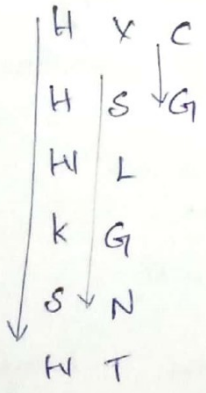
ciphertext: HHWKSWXSLGNTCG.

Method ②:









cipher Text = HHWKSWXSLGNTCG.

③ Permutation:

Method 1:

PT = ENEMY ATTACKS TONIGHT.

key = 31452

1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
E N E M Y	A T T A C	K S T O N	I G H T (Z)

E E M Y N	T A A C T	T K O N S	H I T Z G
3 1 4 5 2	3 1 4 5 2	3 1 4 5 2	3 1 4 5 2

cipher text ↓

Method 2:

key size is 5, so choose 5 column.

1	2	3	4	5
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	(Z)

:

3	1	4	5	2
E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	(Z)	G

writing row-wise ⇒

EEMYN TAACT TKONS HIT(Z)G.

④ Railfence Technique: (Zig Zag)

Method 1:

PT: COMPUTER TECHNOLOGY.

C M U E T C N L G
O P T R E H O O Y

CT: CMUETCNLG OPTREHOOY.

Method 2:

(4 × 4 matrix)

$$\begin{bmatrix} C & O & M & P \\ U & T & E & R \\ T & E & C & H \\ N & O & L & O \\ G & Y & \square & \square \end{bmatrix}$$

filling row-wise.

But

writing column-wise.

No Bogus

CT: CUTNG OTEOY MECL PRHO.

⑤ Elliptic curve:

Equation $y^2 = x^3 + x + 1$, prime = 13.

$x = 0$ to $k = \frac{P-1}{2}$.

$x = 0, 1, 2, 3, 4, 5, 6, \ldots 12.$

y^2 form: $0^2 \bmod 13 = 0$

$1^2 \bmod 13 = 1$

$2^2 \bmod 13 = 4$

$3^2 \bmod 13 = 9$

$4^2 \bmod 13 = 3$

$5^2 \bmod 13 = 12$

$6^2 \bmod 13 = 10$

$x=1$, $y^2=3$.

$x=2$, $y^2=11$.

$x=3$, $y^2=31 \Rightarrow 5$

$x=4$, $y^2=69 \Rightarrow (4,2)$

$x=5$, $y^2=131 \Rightarrow (1,1)$

$x=6$, $y^2=223 \Rightarrow 2$

$x=7$, $y^2=351 \Rightarrow (0,0)$

$x=8$, $y^2=521 \Rightarrow (1,1)$

$x=9$, $y^2=739 \Rightarrow 11$

$x=10$, $y^2=1011 \Rightarrow 10$

$x=11$, $y^2=1343 \Rightarrow (4,2)$

$x=12$, $y^2=1741 \Rightarrow 12$.

$x=0$, $y^2=x^2+x+1=1$.

$(0,1)$ $(0,-1) \Rightarrow (0,1)$ $(0,12)$

$x=1$, $y^2=(1+1+1) \bmod 13 = 3$.

$y=\pm 4 \Rightarrow (1,4)$ $(1,-4)$

$x=2$, $y^2=11 \Rightarrow 11$ is not perfect square.

$x=3$, $y^2=31 \Rightarrow 5$ is not perfect square.

$x=4$, $(4,2)$ $(4,11)$.

$x=5$, $(5,1)$ $(5,12)$.

$x=6$, No points.

$x=7$, $(7,0)$

$x=8$, $(8,1)$ $(8,12)$

$x=9$, No points

$x=10$, $(10,1)$ $(10,7)$

$x=11$, $(11,2)$ $(11,11)$

$x=12$, $(12,5)$ $(12,8)$

(6) Elliptic Curve with point Addition:

$P1(11, 2)$ $P_2(10, 6)$

The above 2 points are not equal, so go for point addition $(P_1 \neq P_2)$.

$y^2 = x^3 + x + 1$, prime $= 13$.

$x = 0$ to $\frac{p-1}{2}$.

Formula for point addition.

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

$$x_3 = m^2 - x_1 - x_2.$$

$$y_3 = m(x_1 - x_3) - y_1.$$

Soln:

x_1	x_2	y_1	y_2
(11,	2)	(10,	6)

$$m = \frac{6-2}{10-11} \Rightarrow \frac{11}{6}.$$

$$= 11 \cdot 6^{-1} \bmod 13.$$

$6^{-1} \Rightarrow \text{Gcd}(13, 6)$

$= (11 \times 11) \bmod 13.$

$= 121 \bmod 13.$

q	r_1	r_2	r	t_1	t_2
2	13	6	1	0	1
6	6	1	0	1	1-2

$13 - 2 \Rightarrow 11$

$x_3 = 25 - 4 - 10 = 11.$

$y_3 = 5(4-11) - 2.$

$= 5(-7) - 2.$

$= -35 - 2 \Rightarrow -37 + 13.$

$= -24 + 13.$

$= -11 + 3 \Rightarrow 2.$

$P_3 (11, 2).$

(7) Elliptic curve with point Doubling:

$$m = \left(\frac{3x_1^2 + a}{2y_1}\right) \bmod p., \quad p = 13.$$

$x_3 = m^2 - x_1 - x_2.$

$y_3 = m(x_1 - x_3) - y_1.$

Here, $y^2 = x^3 + x + 1$ is of form.

$y^2 = x^3 + ax + b.$

Here, $a = 1, b = 1.$

Soln:

$P_1(4,2), \quad P_2(4,2)$

$$m = \frac{3(16)+1}{2(2)}$$

$$= \frac{48+1}{4} = \frac{49}{4} = 49 \cdot 4^{-1}.$$

$4^{-1} \Rightarrow \gcd(13, 4)$

q	r_1	r_2	r	t_1	t_2
3	13	4	1	0	1
4	4	1	0	1	$\boxed{-3}$

$= 13 - 3 = 10$

$w = 49 \times 10$

$= 490 \bmod 13.$

$\boxed{w = 9}$

$x_3 = 81 - 4 - 4 = 73 \bmod 13 = 8.$

$y_3 = 9(4-8) - 2 = 38 \bmod 13.$

$= -12 + 13 \Rightarrow 1.$

$\therefore P_3(8, 1).$

(8) RSA:

$P = 13, \; q = 17, \; m = 127.$

$n = 13 \times 17 \Rightarrow 221.$

$\varphi(221) = 12(16) = 192.$

public key: $1 < e < 192.$

Let us take $e = 5.$

finding gcd (192, 5),

q	r_1	r_2	r	t_1	t_2	
38	192	5	2	0	1	
2	5	2	1	1	-38	
2	2	1	0	-38	77	

$d = 77$ // private key.

$\therefore c = p^e \bmod n$.

$= 127^5 \bmod 221$.

$= 33038369407 \bmod 221$.

$\boxed{c = 43}$

$\therefore p = c^d \bmod n$.

$= 43^{77} \bmod 221$.

$\boxed{P = 127}$

(9) Diffie Hellman - key:

Formula for public key: $Y_A = \alpha^{X_A} \bmod p$.

$Y_B = \alpha^{X_B} \bmod p$.

Formula for private key: $Z_A = Y_B^{X_A} \bmod p$.

$Z_B = Y_A^{X_B} \bmod p$.

$p = 71, \quad \alpha = 7$

Private key of A, $X_A = 5$

Private key of B, $X_B = 12$

$X_A = 5$

$Y_A = \alpha^{X_A} \bmod p$

$= 7^5 \bmod 71$

$= 51 \bmod 71.$

sending public key Y_A to B

$Z_A = Y_B^{X_A} \bmod p$

$= 44^5 \bmod 71$

$= 30 \bmod 71.$

$X_B = 12$

$Y_B = \alpha^{X_B} \bmod p$

$= 7^{12} \bmod 71$

$= 51 \times 51 \times 49 \bmod 71$

$= 4 \bmod 71$

sending public key Y_B to A

$Z_B = Y_A^{X_B} \bmod p$

$= 51^{12} \bmod p$

$= 45 \times 37 \times 32 \bmod p$

public key, $Y_A = 51.$

shared key

$(Z_A = Z_B = k) = 30.$

(10.) DES:

Given.,

PT: 0 1 2 3 4 5 6 7 8 9 A B C D E F

k: 1 3 3 4 5 7 7 9 9 B B C D F F 1

Ip: CC00CCFF F0AAF0AA.

⇒ 0000 0011 0011 0100 0101 0111 0111 1001
1001 1011 1011 1100 1101 1111 1111 0001

⇒ From parity bit table.,

1111	0000
1100	1100
1010	1010
0000	1010
1010	1100
1100	1111
0000	0000

Lo: 1111 0000 1100 1100 1010 1010 0000

Do: 1010 1010 1100 1100 1111 0000 0000

⇒ Round 1 2 9 16 Round 3 4 5

shift 1 shift 2

⇒ Round 1:

L1: 1110 0001 1001 1001 0101 0100 0001

D1: ~~1010~~ 0101 1001 1001 1110 0000 0001

→ from key compression table,

0000 1011
0000 0010
0110 0111
1001 1011
0100 1000
1010 0101

Round 1 key:

L_1 : 0000 1011 0000 0010 0110 0111
D_1 : 1001 1011 0100 1001 1010 0101.

Encryption:

L_I : 1100 1100 0000 0000 1100 1100 1111 1111
R_I : 1111 0000 1010 1010 1111 0000 1010 1010

→ Expansion & DBox (R_I) :

0 1 1 1 1 0
1 0 0 0 0 1
0 1 0 1 0 1
0 1 0 1 0 1
0 1 1 1 1 0
1 0 0 0 0 1
0 1 0 1 0 1
0 1 0 1 0 1

⇒ Expansion ϕ SBox Exor key.

0111 0001 0001 0111 0011 0010

0110 0001 0101 1100 1111 0000

After the result ϕ SBox.,

output : Next round's R_I.

Previous R_I : Next round's L_I.