Hill Cipher

The Hill Cipher is a classical polygraphic substitution cipher, a type of encryption technique that uses linear algebra (matrices) to encrypt blocks of letters together rather than one at a time.

Working:

Every letter is assigned a number, A=0, B=1, C=2….Z=25.

Encryption Formula: $C=K\times P \pmod{26}$

P is plaintext vector, K is the key matrix, and C is the ciphertext vector.

Example:

Let the word be MIST.

Let the key be $\begin{bmatrix}3 & 3\\ 2 & 5\end{bmatrix}$

dividing it into pairs (since key is 2×2): MI and ST

M	12
I	8
S	18
T	19

Pair 1: M I - [12, 8]

$$\begin{bmatrix}3 & 3\\ 2 & 5\end{bmatrix}\begin{bmatrix}12\\ 8\end{bmatrix}=\begin{bmatrix}60\\ 76\end{bmatrix}$$

60 mod 26= 8, 76 mod 26=24
[8 24] is [I Y]

First ciphertext pair = **IY**

Pair 2: S T - [18, 19]

$$\begin{bmatrix}3 & 3\\ 2 & 5\end{bmatrix}\begin{bmatrix}18\\ 19\end{bmatrix}=\begin{bmatrix}111\\ 131\end{bmatrix}$$

111 mod 26=7, 131 mod 26=1

[7 1] is [H B]

Second ciphertext pair = **HB**

Final Ciphertext**: IYHB**

Rail Fence Cipher

The Rail Fence Cipher is a transposition cipher, which means letters are rearranged and not substituted.
It writes the message in a zigzag pattern across multiple "rails" (rows), and then reads it row by row to form the ciphertext.

For example, to encrypt the message 'WE ARE DISCOVERED' with 3 "rails":

W				E				C				R		
	E		R		D		S		O		E		E	
		A				I				V				D

(Spaces and punctuation are omitted.)

Then the text is read horizontally: WECR ERDSOEE AIVD

Here the no of rails is 3. It is decided by the key given

Affine Cipher

The Affine Cipher is a monoalphabetic substitution cipher, each letter in the plaintext is mapped to exactly one letter in the ciphertext.

It's based on a simple mathematical formula using modular arithmetic.

Encryption Formula:

For each letter x (where A=0, B=1, …, Z=25):

$$E(x)=(ax+b) \bmod 26$$

Where:

- a= multiplicative key (must be coprime with 26)
- b= additive key (any number between 0–25)

Example: MIST

M	12
I	8
S	18
T	19

Taking a=5, b=8: E(x)=(5x+8) mod 26

x	5x+8	(5x+8) mod26	Cipher Letter
12	68	16	Q
8	48	22	W
18	98	20	U
19	103	25	Z

Ciphertext = **QWUZ**