Caesar Cipher :

The Caesar cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down the alphabet.

The Caesar cipher works by choosing a number between 1 and 25, which is used as the "key" for the encryption. Let's say the key is 3. To encrypt a message, each letter in the plaintext is shifted three places down the alphabet. For example, A becomes D, B becomes E, and so on.

To decrypt the message, the recipient simply shifts each letter in the ciphertext three places up the alphabet. For example, D becomes A, E becomes B, and so on.

Let's say we want to encrypt the message "HELLO" using a key of 3. First, we write out the alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

Next, we shift each letter in the plaintext message "HELLO" three places down the alphabet:

H -> K

E -> H

L -> O

L -> O

O -> R

So the encrypted message would be "KHOOR".

To decrypt the message, the recipient would simply shift each letter in the ciphertext three places up the alphabet:

K -> H

H -> E

O -> L

O -> L

R -> O

So the decrypted message would be "HELLO" again.

Advantages:

- Easy to implement and use thus, making suitable for beginners to learn about encryption.
- Can be physically implemented, such as with a set of rotating disks or a set of cards, known as a scytale, which can be useful in certain situations.
- Requires only a small set of pre-shared information.

- Can be modified easily to create a more secure variant, such as by using a multiple shift values or keywords.

Disadvantages:

- It is not secure against modern decryption methods.
- Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
- The small number of possible keys means that an attacker can easily try all possible keys until the correct one is found, making it vulnerable to a brute force attack.
- It is not suitable for long text encryption as it would be easy to crack.
- It is not suitable for secure communication as it is easily broken.
- Does not provide confidentiality, integrity, and authenticity in a message.

Affine Cipher:

The Affine cipher is a type of monoalphabetic substitution cipher, herein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

It uses a mathematical formula to transform each letter in the plaintext into a corresponding letter in the ciphertext.

The formula used in the affine cipher is:

$$C = ((P * K_1) + k_2) \bmod 26$$

Where:

- C is the ciphertext letter
- P is the plaintext letter
- K_1 and k_2 are integers (i.e keys) that determine the transformation

mod 26 means to take the result of the calculation and divide it by 26, then take the remainder. This ensures that the result is always a number between 0 and 25, which correspond to the letters of the alphabet.

To decrypt the message, we use the inverse of the formula:

$$D = (C+(-k_2)*k^{-1}) \bmod 26$$

Where k^{-1} is the modular inverse of a, which is a number such that a multiplied by its inverse equals 1 (mod 26).

Let's say we want to encrypt the message "HELLO" using a key of k_1 =5 and k_2 =7.
First, we write out the alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

Next, we apply the Affine cipher formula to each letter in the plaintext message "HELLO":

$C = ((P * K_1) + k_2) \text{ mod } 26$

H -> (5*7 + 7) mod 26 = 12 -> M

E -> (5*4 + 7) mod 26 = 9 -> J

L -> (5*11 + 7) mod 26 = 10 -> K

L -> (5*11 + 7) mod 26 = 10 -> K

O -> (5*14 + 7) mod 26 = 19 -> T

So the encrypted message would be "MJKKT".

To decrypt the message, the recipient would apply the inverse of the Affine cipher formula:

M -> (21*(12-7)) mod 26 + 7 = 19 -> T

J -> (21*(9-7)) mod 26 + 7 = 4 -> E

K -> (21*(10-7)) mod 26 + 7 = 11 -> L

K -> (21*(10-7)) mod 26 + 7 = 11 -> L

T -> (21*(19-7)) mod 26 + 7 = 14 -> O

So the decrypted message would be "HELLO" again.

Vigenere Cipher :

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

Encryption and Decryption Using Vigenere Cipher:

let's say we want to encrypt the message "HELLO" using the keyword "LEMON" with the Vigenere Cipher.

Step 1: Write the message and the keyword above each other, repeating the keyword as many times as necessary to match the length of the message.

Message: H E L L O

Keyword: L E M O N

Step 2: Assign each letter a numerical value according to its position in the alphabet, using A=0, B=1, C=2, and so on.

Message: 7 4 11 11 14

Keyword: 11 4 12 14 13

Step 3: Add the numerical values of each letter in the message and the keyword, using modular arithmetic (i.e., if the sum is greater than 25, subtract 26 to wrap around to the beginning of the alphabet).

Message: 7 4 11 11 14

Keyword: 11 4 12 14 13

Result: 18 8 23 25 1

Step 4: Convert the numerical values back to letters using the same mapping as in step 2 (i.e., 0=A, 1=B, 2=C, and so on).

Result: S I X A B

Therefore, the encrypted message for "HELLO" with the keyword "LEMON" using the Vigenere Cipher is "SIXAB".

To decrypt the message, we can simply reverse the process by subtracting the numerical values of the key from the corresponding numerical values of the ciphertext, modulo 26, to obtain the original numerical values of the plaintext.

CipherText : S I X A B

18 8 23 25 1

Keyword : L E M O N

11 4 12 14 13

```
Substitution :   18   8  23  25   1
                -11   4  12  14  13
                ---------------------
                  7   4  11  11  14
                  H   E   L   L   O      -------> Plain Text.
```

Hill Cipher

The Hill cipher is a polyalphabetic substitution cipher based on linear algebra.

Encryption: P*K mod 26
Decryption : $C*k^{-1}$ mod 26

<u>We will Encrypt and Decrypt the Word "PAY"</u>

First. Choose a matrix key, which is a square matrix with a determinant that is relatively prime to the length of the alphabet being used. Let's use the 3x3 matrix key:

$$K=\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

PT= P A Y

15 0 24

$$\text{Encryption: } \begin{vmatrix} 15 & 0 & 24 \end{vmatrix} * \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \mod 26$$

$$\begin{vmatrix} 303 & 303 & 531 \end{vmatrix} \mod 26$$

$\begin{vmatrix} 17 & 17 & 11 \end{vmatrix}$ = R R L ----> Cipher Text

$K^{-1} = 1/|k| * Adj(k) \quad \mod 26$

$|k| = 23$

$$Adj(k) = \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 3 \\ 6 & 0 & 1 \end{vmatrix}$$

$$K^{-1} = 1/23 * \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 3 \\ 6 & 0 & 1 \end{vmatrix} \mod 26$$

$$= 23^{-1} * \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 3 \\ 6 & 0 & 1 \end{vmatrix} \mod 26$$

$$= 17 * \begin{vmatrix} 14 & 25 & 7 \\ 7 & 1 & 3 \\ 6 & 0 & 1 \end{vmatrix} \mod 26$$

(17 is multiplicative inverse of 23 mod 26)

$$= \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 14 & 0 & 17 \end{vmatrix}$$

Decryption :

$$\begin{vmatrix} 17 & 17 & 11 \end{vmatrix} * \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 14 & 0 & 17 \end{vmatrix} \mod 26$$

$= \begin{vmatrix} 265 & 610 & 425 \end{vmatrix} \mod 26$

$= \begin{vmatrix} 15 & 0 & 24 \end{vmatrix}$ = P A Y -----> Plain Text

Playfair Cipher

In Playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

ALGORITHM

1) create 5X5 Matrix that is called grid of letters.
2) The matrix is made by inserting the value of the key and remaining alphabets into The Matrix where I and J will be combined.
3) convert the text into pair of letters e.g. HEYA ----> HE YA
   3.1) pair can`t be made with same letters ; break the letters in single and add 'x' to the previous letters.
   3.2) If the letter is standing alone in the process of pairing a at Z with the letter.
4) Code will be formed using 3 rules :-
   4.1) if both of the letters are in the same row replace them with the letters to their immediate right.
   4.2) if both letters are in the same column replace them with the letters immediate below to them.
   4.3) if not in the same row or column replace them with the letters in the same row respectively but at the other pair of corners.

Example:
Encrypting and Decrypting the message "HELLO" using the key "PLAYFAIR"

Key Generation:
The key "PLAYFAIR" is used to generate the Playfair matrix:

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

Encryption:
Message: HELLO
Plaintext pairs: HE, LL, OX (if message length is odd, X is added at the end)

Pair 1: HE

Find the position of each letter in the Playfair matrix: H (row 3, column 2), E (row 1, column 3)

If the letters are in the same row, replace them with the letters to their right (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Encrypted pair: RB

Pair 2: LL

Find the position of each letter in the Playfair matrix: L (row 2, column 2)
If the letters are in the same row, replace them with the letters to their right (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Encrypted pair: IR

Pair 3: OX

Find the position of each letter in the Playfair matrix: O (row 4, column 4), X (row 4, column 5)
If the letters are in the same row, replace them with the letters to their right (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Encrypted pair: ST

Encrypted message: RB IR ST

Decryption:
Encrypted message: RB IR ST

Pair 1: RB

Find the position of each letter in the Playfair matrix: R (row 2, column 3), B (row 0, column 4)
If the letters are in the same row, replace them with the letters to their left (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Decrypted pair: HE

Pair 2: IR

Find the position of each letter in the Playfair matrix: I (row 1, column 0), R (row 2, column 3)
If the letters are in the same row, replace them with the letters to their left (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Decrypted pair: LL

Pair 3: ST

Find the position of each letter in the Playfair matrix: S (row 3, column 3), T (row 3, column 4)
If the letters are in the same row, replace them with the letters to their left (circularly). Otherwise, replace each letter with the letter in the same row, but in the column of the other letter.
Decrypted pair: OX

Decrypted message: HELLO

The Playfair cipher algorithm replaces each pair of letters with another pair of letters based on their positions in the Playfair matrix. This provides a simple but effective way to encrypt and decrypt messages.