**Roll\_No : 068464.**

**Name : Nabila Naz “ CC\_312”**

**BS(IT) : 5th(sem).**

**Submitted to: Mam Sehrish Khan.**

# Caesar Cipher:

**The Caesar Cipher, also known as the Shift Cipher, is a simple and ancient encryption technique. It is a substitution cipher where each letter in the plain-text is shifted a certain number of places down or up the alphabet. This shift is determined by a key, which is typically a single digit.**

**For example, with a shift of 3:**

**- A becomes D**

**- B becomes E**

**- C becomes F**

Rendered by QuickLaTeX.com

**(Encryption Phase with shift n)**

Rendered by QuickLaTeX.com  
 **(Decryption Phase with shift n)**

**The method is named after Julius Caesar, who is rumored to have used it to communicate with his generals. The Caesar Cipher is a basic and easily crack-able encryption method, as there are only 25 possible ways to decrypt a message (since shifting by 26 positions is equivalent to no shift at all).**

**While the Caesar Cipher is not secure for serious applications, it is often used in puzzle games and educational exercises to introduce the concept of encryption.**

#### 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 scythe, 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-plaint ext attacks, where an attacker has access to both the encrypted and encrypted 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.

**Features of Caesar cipher:**

1. Substitution cipher: The Caesar cipher is a type of substitution cipher, where each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
2. Fixed key: The Caesar cipher uses a fixed key, which is the number of positions by which the letters are shifted. This key is known to both the sender and the receiver.
3. Symmetric encryption: The Caesar cipher is a symmetric encryption technique, meaning that the same key is used for both encryption and decryption.
4. Limited keyspace: The Caesar cipher has a very limited keyspace of only 26 possible keys, as there are only 26 letters in the English alphabet.
5. Vulnerable to brute force attacks: The Caesar cipher is vulnerable to brute force attacks, as there are only 26 possible keys to try.
6. Easy to implement: The Caesar cipher is very easy to implement and requires only simple arithmetic operations, making it a popular choice for simple encryption tasks.

**Rules for the Caesar Cipher:**

1. Choose a number between 1 and 25. This will be your “shift” value.
2. Write down the letters of the alphabet in order, from A to Z.
3. Shift each letter of the alphabet by the “shift” value. For example, if the shift value is 3, A would become D, B would become E, C would become F, and so on.
4. Encrypt your message by replacing each letter with the corresponding shifted letter. For example, if the shift value is 3, the word “hello” would become “khoor”.
5. To decrypt the message, simply reverse the process by shifting each letter back by the same amount. For example, if the shift value is 3, the encrypted message “khoor” would become “hello”.