**INFORMATION SECURITY**

**(CC\_312)**

**Roll\_No : 068464.**

**Name : Nabila Naz**

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

**Submitted to: Mam Sehrish Khan.**

**SHIFT CIPHER**

The shift cipher, also known as the Caesar cipher, is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. It's one of the simplest and oldest known encryption techniques. The method is named after Julius Caesar, who is reputed to have used it to communicate with his generals.

**Encryption:**

1. Choose a shift value, often denoted as "k."
2. Replace each letter in the plaintext with the letter that is k positions to the right in the alphabet.
3. Wrap around to the beginning of the alphabet if necessary.
4. **For example, with a shift of 3:**
5. **A becomes D**
6. **B becomes E**
7. **C becomes F**
8. **...**
9. The transformation is the same for both uppercase and lowercase letters.

**Decryption:**

1. To decrypt, use the opposite shift value.
2. Replace each letter in the cipher-text with the letter that is k positions to the left in the alphabet.
3. Decryption essentially involves reversing the encryption process.

**Example#1.**

1. **Original: HELLO**
2. **Shift: 3**
3. **Encrypted: KHOOR**
4. **Decrypted (with shift 3): HELLO**

**Example#2.**

**use your last name and the last last digit of your roll number in shift cipher.**

### **Shift Cipher Encryption:**

using a shift cipher with a key of 4, here's the encryption:

Original: N A Z

Shift: 4

Encrypted: R E D

So, "Naz" encrypted with a shift of 4 becomes "Red."

Decrypted:

Original: R E D

Shift: 4

Decrypted: N A Z

So, "RED" decrypted with a shift of 4 becomes "Naz."