**PRACTICAL-5**

**Aim: Prepare report on**

**Theory:**

**Example**

Use the additive cipher with key = 15 to encrypt the message “hello”.

**Solution**

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → W

Plaintext: e → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → T

Plaintext: l → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → A

Plaintext: l → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → A

Plaintext: o → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → D

The result is “WTAAD”. Note that the cipher is monoalphabetic because two instances of the same plaintext character (l’s) are encrypted as the same character (A).

**Example**

Use the additive cipher with key = 15 to decrypt the message “WTAAD”.

**Solution**

We apply the decryption algorithm to the plaintext character by character:

Plaintext: W → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → h

Plaintext: T → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → e

Plaintext: A → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → l

Plaintext: A → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → l

Plaintext: D → 07 encryption: (07 + 15) mod 26 cirphertext: 22 → o

The result is “hello”. Note that the operation is in modulo 26 (see Chapter 2), which means that a negative result needs to be mapped to Z (for example − 15 becomes 11).

**Shift Cipher:**

Historically, additive ciphers are called shift ciphers. The reason is that the encryption algorithm can be interpreted as “shift key characters down” and the encryption algorithm can be interpreted as “shift key character up”. For example, if the key = 15, the encryption algorithm shifts 15 characters down (toward the end of the alphabet). The decryption algorithm shifts 15 characters up (toward the beginning of the alphabet). Of course, when we reach the end or the beginning of the alphabet, we wrap around (manifestation of modulo 26).

**Caesar Cipher**

Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications. Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

**Program:**