**PRACTICAL-4**

**Aim: Prepare report on**

**Theory:**



**Fig 4.1**

**Categories of Traditional Ciphers:**

We can divide traditional symmetric-key ciphers into two broad categories: substitution ciphers and transposition ciphers. In a substitution cipher, we replace one symbol in the ciphertext with another symbol; in a transposition cipher, we reorder the position of symbols in the plaintext.

**SUBSTITUTION CIPHERS:**

A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace letter A with letter D, and letter T with letter Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6. Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

A substitution cipher replaces one symbol with another.

**Monoalphabetic Ciphers:**

We first discuss a group of substitution ciphers called the monoalphabetic ciphers. In monoalphabetic substitution, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text. For example, if the algorithm says that letter A in the plaintext is changed to letter D, every letter A is changed to letter D. In other words, the relationship between letters in the plaintext and the ciphertext is one-to-one.

In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

**Example of :**

The following shows a plaintext and its corresponding ciphertext. We use lowercase characters to show the plaintext; we use uppercase characters to show the ciphertext. The cipher is probably monoalphabetic because both l’s (els) are encrypted as O’s.

Plaintext: hello Ciphertext: KHOOR

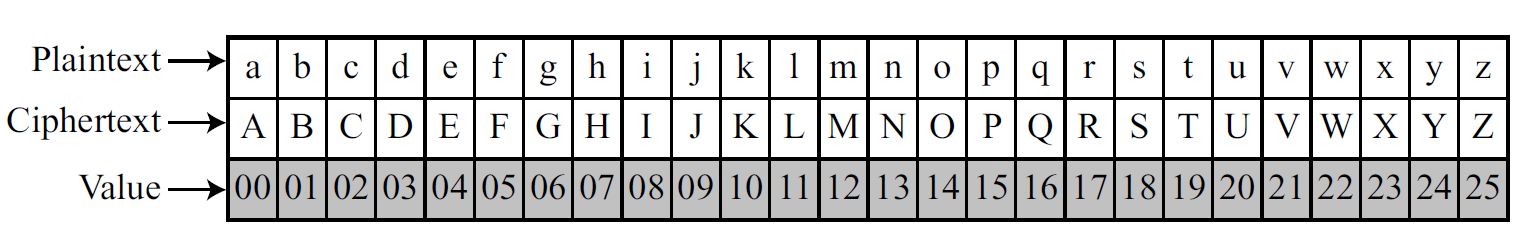
**Example of :**

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each l (el) is encrypted by a different character. The first l (el) is encrypted as N; the second as Z.

Plaintext: hello Ciphertext: ABNZF

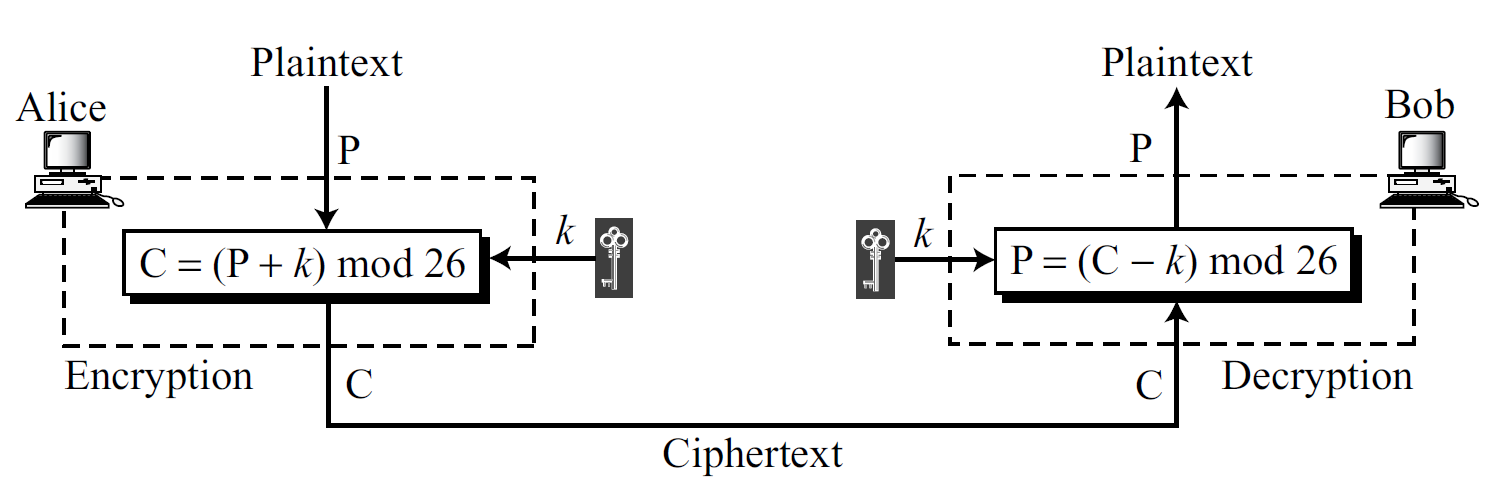
**Additive Cipher**

The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature. Assume that the plaintext consists of lowercase letters (a to z), and that the ciphertext consists of uppercase letters (A to Z). To be able to apply mathematical operations on the plaintext and ciphertext, we assign numerical values to each letter (lower- or uppercase), as shown in Figure 5.1.

****

**Fig 5.1 Representation of plaintext and ciphertext characters in Z26**

In Figure 5.1 each character (lowercase or uppercase) is assigned an integer in Z26. The secret key between Alice and Bob is also an integer in Z26. The encryption algorithm adds the key to the plaintext character; the decryption algorithm subtracts the key from the ciphertext character. All operations are done in Z26. Figure 5.2 shows the process.



**Fig 5.2 Additive cipher**

We can easily prove that the encryption and decryption are inverse of each other because plaintext created by Bob (P1) is the same as the one sent by Alice (P).

P1 = (C − k) mod 26 = (P + k − k) mode 26 = P

When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

**Example for encryption**

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 → 04 encryption: (04 + 15) mod 26 cirphertext: 19 → T

Plaintext: l → 11 encryption: (11 + 15) mod 26 cirphertext: 00 → A

Plaintext: l → 11 encryption: (11 + 15) mod 26 cirphertext: 00 → A

Plaintext: o → 14 encryption: (14 + 15) mod 26 cirphertext: 03 → D

**Table5.1: convert plaintext to ciphertext**

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 for decryption**

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

Plaintext: T → 19 encryption: (19 + 15) mod 26 cirphertext: 04 → e

Plaintext: A → 00 encryption: (00 + 15) mod 26 cirphertext: 11 → l

Plaintext: A → 00 encryption: (00 + 15) mod 26 cirphertext: 11 → l

Plaintext: D → 03 encryption: (03 + 15) mod 26 cirphertext: 14 → o

**Table5.2: convert ciphertext to plaintext (using same key)**

To decrypt the message “WTAAD”. Use the additive inverse of key 15 is 11.

Plaintext: W → 22 encryption: (22 + 11) mod 26 cirphertext: 07 → h

Plaintext: T → 19 encryption: (19 + 11) mod 26 cirphertext: 04 → e

Plaintext: A → 00 encryption: (00 + 11) mod 26 cirphertext: 11 → l

Plaintext: A → 00 encryption: (00 + 11) mod 26 cirphertext: 11 → l

Plaintext: D → 03 encryption: (03 + 11) mod 26 cirphertext: 14 → o

**Table5.3: convert ciphertext to plaintext (using additive inverse of key)**

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.