Jessica Braganza
BE Comp 2
F17112151

PAGE NO.:
DATE:

Ics Assignment 1

1) What do you mean by shift cipher? Discuss various shift ciphers available.

Ans 1) Shift cipher is one of the earliest and simplest cryptosystems.

2) A given plaintext is encrypted into a ciphertext by shifting each letter of the given plaintext by n positions.

3) An example of encrypting the plaintext by shifting each letter by 3 places.

Plaintext: Shift cipher is simple.

Ciphertext: VkliwFishkhulvVlpsoh

4) Mathematically, the shift cipher encryption process is taking a letter and move it by n positions. Let x be the position number of a letter from the alphabet, n be an integer such that $0 \leq n \leq 25$.

5) It is the key for encryption and decryption of shift cipher cryptosystem.

6) Any number (mod 26) will result in an integer less than 26 and greater than 0.

7) Caesar ~~thi~~ cipher is a type of shift cipher.

2) Discuss caesar cipher in detail.

Ans. In caesar cipher technique, each letter is replaced by the letter / alphabet which is three places next to that letter which is to be substituted or in caesar cipher technique, each alphabet of a plaintext is replaced with another alphabet but 3 places down the one as mentioned below.

plaintext - sunrises in the east.

ciphertext - NXSULVHVLSWKHHDVW

Mathematically, the caesar cipher algorithm can be expressed as

$C = E(3, P) = (P+3) \bmod 26$

$P = D(3, C) = (C-3) \bmod 26$

DATE :

where, C = ciphertext / or alphabet

P = plaintext / alphabet

E = Encryption

D = Decryption

MOD 26: because in English there are total 26 alphabets.

3) What do you mean by monoalphabetic and polyalphabetic ciphers? Give an example of each of them.

Ans Monoalphabetic cipher

- In caesar cipher, the attacker can easily guess the plaintext as it is easily recognizable.
- In this cipher substitutes one letter of the alphabet with any random letter from the alphabet.
- It is not necessary that if A is substituted with B then compulsorily B has to be substituted with C.
- It can be replaced with any other letter of the alphabet.
- The only weakness in the algorithm is that if more repetition occurs then attacker can easily guess the plaintext.
- This random substitution is just done to have uniqueness
- In this the substitution of characters are random permutation of the 26 letters of the alphabet

Plaintext - East or West

Ciphertext - aesy xk taay

Polyalphabetic cipher

- It is more secure and hard to be broken
- more than one alphabet is used for substitution
- In a polyalphabetic cipher, the substitution rule changes continuously from letter to letter according to the elements of the encryption key.
- In polyalphabetic or particular alphabet, different substitution can be done using vignere table.

4) what are different substitution ciphers ?

Ans. A substitution is a technique in which each letter or bit of the plaintext is substituted or replaced by some other letter, number or symbol to produce ciphertext substitution means replacing an alphabet of ~~cipher~~ plaintext with an alphabet of ciphertext. It is also called confusion. The best example of substitution cipher is caesar cipher.

Types:

i) Caesar cipher:

In this technique each letter is replaced by the ~~letter~~ alphabet which is three places next to that letter / ~~which~~ is to be substituted.

ii) Monoalphabetic cipher:

In this cipher, substitutes one letter of the alphabet with any random letter from the alphabet.

iii) Polyalphabetic cipher:

In this more than one word / alphabet is used for substitution, the substitution rule changes continuously from letter to letter according to the elements of the encryption key.

iv) Playfair cipher:

It is a multiple letter encryption technique which uses 5×5 matrix table to store the letters of the phrase given for encryption which later on becomes key for encryption and decryption.

v) Verman cipher:

This uses a random key of the same length of the message, so that the key is not repeated. The case happens here is sender is generating new key for every new message while sending the message to the receiver called as one-time pad. The key is used to encrypt and decrypt a single message.

vi) Hill cipher:

It is a polygraphic substitution cipher based on linear

DATE :

algebra. Each letter is represented by a number modulo 26. Often the simple scheme (A=0, B=1, C=2, ... Z=25) is used, this is not an essential feature of the cipher.