Jessica Broganza
BE Comp 2
F17112151

PAGE NO :
DATE :

ICS Assignment 2:

1) What do you mean by polygraphic substitution cipher? List types of it.

Ans. Polygraphic substitution is a cipher in which a uniform substitution is performed on blocks of letters.

When the length of the block is specifically known, more precise terms are known and used: for instance, a ciphertext in which pairs ~~are~~ of letters are substituted is bigraphic.

Types:

i) Playfair cipher -

It replaces each pair of plaintext letters by another pair of plaintext letters by another pair of letters, determined by a single table.

ii) Two - square cipher -

It replaces each pair of plaintext letters by another pair of letters, determined by a single table.

iii) Four - square cipher -

It replaces each pair of plaintext letters by another pair of letters, determined by a single table.

iv) Hill cipher -

It is based on linear algebra. Each letter is represented by a number modulo 26.

2) Discuss Hill cipher in detail.

Ans. We can work on multiple letters at the same time using Hill cipher.

- When we use encryption algorithm, we take the 'm' successive plain letters and substitutes for them in 'm' cipher text letter.
- It is a polygraphic substitution cipher based on linear algebra.
- Each letter is represented by a number modulo 26.
- Often the simple scheme (A=0, B=1, C=2, ... Z=25) is used, but this is not an essential feature of the cipher.

- To encrypt a plaintext message, each block of 'm' letters is multiplied by inverse of the matrix used for encryption.

3) Discuss choosen plaintext attack on Hill cipher with example.

Ans. A chosen plaintext attack is an attack model for cryptoanalysis which presumes that the attacker can obtain the ciphertext for arbitrary plaintexts.

The goal of the attack is to gain information that reduces the security of the encryption scheme.

Because the Hill cipher is a linear cipher, it is vulnerable to a known plaintext attack. For a secret key K with shape nxn, we need a pair of known plaintext and ciphertext blocks, each of length n.

Let the ciphertext be encrypted with an unknown matrix k with shape 2x2 modulo 25 1.

$K_{P1} = C_1 \pmod m$

$K_{P2} = C_2 \pmod m$

Each pair adds one equation or two if we see them in an untalled way.

$K_{1,1}\ P_{1,1} + K_{1,2}\ P_{1,2} = C_{1,1} \pmod m$

$K_{2,1}\ P_{1,1} + K_{2,2}\ P_{1,2} = C_{1,2} \pmod m$

$K_{1,1}\ P_{2,1} + K_{1,2}\ P_{2,2} = C_{2,1} \pmod m$

$K_{2,1}\ P_{2,1} + K_{2,2}\ P_{2,2} = C_{2,2} \pmod m$

Also these equations can be seen as a single one if we see all the plaintext and ciphertext blocks / vectors as 2 matrices.

$KP = C \pmod m$

Find the secret key matrix K

Then : $K = C[P]^{-1} \pmod m$

when $[P]^{-1}$ is the inverse of the matrix P in (mod m)

So we cannot apply a standard inverse operation.

To decrypt the ciphertext, we need the inverse of k in (mod m)