**ALLISON TEBRIMAM MAGAJI**

**16/SCI01/024**

1. Caesar cipher or Shift cipher

 This is one of the earliest and the simplest cryptosystems. A given plaintext is encrypted into a cipher-text by shifting each letter of the given plaintext by n positions. It is a special case of substitution wherein each alphabet in a message is replaced by an alphabet n places down the line. Caesar cipher is susceptible to a statistical cipher-text only attack. For example; let the message “hello” is encrypted with the key of 15. Then all characters in the cipher-text will be shifted from 15. Then the answer hello= WTAAD. Obviously, if a different key used, the cipher alphabet will be shifted a different amount.

1. **Mono-alphabetic cipher or Simple cipher**

 Mono-alphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. It relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. For example, if ‘a’ is encrypted as ‘R’, for any number of occurrence in that plaintext, ‘a’ will always replace it with ‘R’ in the cipher-text.

1. **Playfair cipher**

 The Playfair cipher was first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. In playfair cipher initially a key table is created. The key table is 5x5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 must be unique and one letter (usually J) of the alphabet is omitted from the table as we need only 25 alphabets instead of 26. If the plain text contains J, then it is replaced by I. For example, the key is **“grace”.** Thus the initial entries are **‘g’, ‘r’, ‘a’, ‘c’, ‘e’** followed by the remaining characters of **a-z (except ‘j’)** in that order.

1. **Vigenere cipher**

 The vigenere cipher uses a 26x26 table with A to Z as the row heading and column heading. This table is usually referred to Vigenere Tableau, Vigenere Table, or Vigenere square. The first row of this table has 26 English letters. Starting with the second row, each row has the letters shifted to the left position in a cyclic way. For example, when B is shifted to the first position on the second row, the letter A moves to the end. In addition to the plaintext, the vigenere cipher requires a keyword, which is repeated so that the total length is equal to that of the plaintext. For example, suppose the plaintext is MICHIGAN TECHNOLOGICAL UNIVERSITY and the keyword is HOUGHTON. Then, the keyword must be repeated as follows:

**MICHIGAN TECHNOLOGICAL UNIVERSITY**

**HOUGHTON HOUGHTONHOUGH TONHOUGNTO**

Remove all spaces and punctuation, converting all letters to upper case, and dividing the results into 5-letter blocks. As a result, the above plaintext and keyword become the following:

**MICHI GANTE CHNOL OGICA LUNIV ERSIT Y**

**HOUGH TONHO UGHTO NHOUG HTONH OUGHT O**

To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword, use the keyword letter and the plaintext as the row index and column index, respectively, and the entry at the row-column intersection is the letter in the ciphertext. For example, the first letter in the plaintext is **M** and its corresponding keyword letter is **H**. This means that the row of **H** and the column of **M** are used, and the entry **T** at the intersection is the encrypted result.



Repeating this process until all plaintext letters are processed, the ciphertext is **TWWNPZOA ASWNUHZBNWWGS NBVCSLYPMM**. The following has the plaintext, repeated keyword and ciphertext aligned together.

**MICHI GANTE CHNOL OGICA LUNIV ERSIT Y**

**HOUGH TONHO UGHTO NHOUG HTONH OUGHT O**

**TWWNP ZOAAS WNUHZ BNWWG SNBVC SLYPM M**

To decrypt, pick a letter in the ciphertext and its corresponding letter in the keyword, use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter. For example, to decrypt the first letter **T** in the ciphertext, we find the corresponding letter **H** in the keyword. Then, the row of **H** is used to find the corresponding letter **T** and the column that contains **T** provides the plaintext letter **M** (see the above figures). Consider the fifth letter **P** in the ciphertext. This letter corresponds to the keyword letter **H** and row **H** is used to find **P**. Since **P** is on column **I**, the corresponding plaintext letter is **I**.

1. **Polyalphabetic cipher**

 The development of Polyalphabetic Substitution Ciphers was the cryptographers answer to Frequency Analysis. The first known polyalphabetic cipher was the Alberti Cipher invented by Leon Battista Alberti in around 1467. He used a mixed alphabet to encrypt the plaintext, but at random points he would change to a different mixed alphabet, indicating the change with an uppercase letter in the ciphertext. In order to utilise this cipher, Alberti used a cipher disc to show how plaintext letters are related to ciphertext letters.



As an example we shall encrypt the plaintext "leon battista alberti". To keep with the convention of writing ciphertext in uppercase, we shall invert Alberti's own rule, and use lowercase letters to signify the change.

We start by referencing the starting position of the cipher disc, which in this case is "a" is encrypted as "V", so we start the ciphertext with a lowercase "v". We then encrypt the first few letters as a Caesar Shift, using the ciphertext alphabet given below.

The first shift used, as shown in the disc above.

Plaintext:  leonbat...
Ciphertext: vGZJIWVOg...

The uppercase letters above encrypt the plaintext letters given. The "v" indicates the starting position of the disc, and the "g" indicates that we need to change the position so that "G" is beneath "a". We then get the new ciphertext alphabet as shown below.



The second shift used, when "a" is encrypted to "G".

Plaintext:   ...tistaa...
Ciphertext:  ...gZOYZGGm...

This time the plaintext letters are encrypted to the ciphertext letters using the ciphertext alphabet above, and the "m" indicates that we are changing alphabet again to get the final ciphertext alphabet below.



The final shift used which maps "a" to "M".

Plaintext:...lberti
Ciphertext:        ...mXNQDFU

So we get the final ciphertext "vGZJIWVOgZOYZGGmXNQDFU". Notice how the letter "t" is encrypted to "O" first of all, then "Z" and finally "F". This is the essence of a polyalphabetic cipher, that the same plaintext letter is encrypted to a different ciphertext letter each time.

1. **One Time cipher**

 One-time pad cipher is a type of Vigenere cipher which includes the following features −

* It is an unbreakable cipher.
* The key is exactly same as the length of message which is encrypted.
* The key is made up of random symbols.
* As the name suggests, key is used one time only and never used again for any other message to be encrypted.

Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

**Why is it Unbreakable?**

The key is unbreakable owing to the following features −

* The key is as long as the given message.
* The key is truly random and specially auto-generated.
* Key and plain text calculated as modulo 10/26/2.
* Each key should be used once and destroyed by both sender and receiver.
* There should be two copies of key: one with the sender and other with the receiver.

**Encryption**

To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the plain text. It is described in the example below −



**Decryption**

To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.