CYBER SECURITY REPORT

Prepared For :

Dr.Mohammed Abdelhammed

by :

1-hassan marwan hassan
2-mohammed hamdy taher
4-mohammed ehab
3-ahmed mohammed sayed
5-david farid
6-peter beshoy

GUI

THE GUI IS CREATED BY USING LIBRARY CALLED TKINTER IN PYTHON

BACKEND

1- Caesar Cipher
Cryptography Algorithm For the Caesar Cipher
Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.
For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:
Write down the plaintext message: HELLO
Choose a shift value. In this case, we will use a shift of 3.

2-Substitution
A Substitution Cipher is one of the oldest and simplest methods of encryption. In this type of cipher, each letter in the plaintext (original message) is replaced with a different letter or symbol according to a fixed system.

Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

BACKEND

3-ROT13 :
ROT13 cipher(read as – “rotate by 13 places”) is a special case of the Ceaser cipher in which the shift is always 13

4-rail fence cipher :
The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.
In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence. When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

So every letter is shifted 13 places to encrypt or to decrypt the message.

BACKEND

5-Play Fair:
Generate the key Square (5×5):
The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order

6-RSA cipher:
RSA Algorithm is based on factorization of large number and modular arithmetic for encrypting and decrypting data. It consists of three main stages
Key Generation: Creating Public and Private Keys
Encryption: Sender encrypts the data using Public Key to get cipher text.
Decryption: Decrypting the cipher text using Private Key to get the original data.

.

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

BACKEND

7-Vigenere Cipher :
is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.
The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

The alphabet used at each point depends on a repeating keyword.

BACKEND

8-affine cipher
Last Updated : 07 Mar, 2023
The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which.
The whole process relies on working modulo m (the length of the alphabet used). In the affine cipher, the letters of an alphabet of size m are first mapped to the integers in the range 0 ... m-1.

The 'key' for the Affine cipher consists of 2 numbers, we'll call them a and b. The following discussion assumes the use of a 26 character alphabet (m = 26). a should be chosen to be relatively prime to m (i.e. a should have no factors in common with m).