CS 154 Project :

Cryptographic Security and Hacking Fundamentals

A Project Report By -

1. Amey Patil - 160050006
2. Abhro Bhuniya - 160050017
3. Vinod Shekokar - 160050016

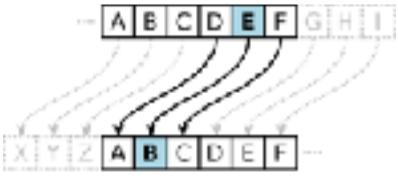
Introduction

Our Project is about implementation of Cryptographic Ciphers and Cipher attacks (for ciphers easier to break). So we have implemented following 6 Cryptographic ciphers and a Hacker algorithm :

1. Caesar Shift Cipher
2. Scytale Cipher
3. Viginère Cipher
4. One-Time-Pad Cipher
5. Enigma Cipher
6. Advanced Encryption Standard (A.E.S.)
7. Hacker

And to combine them we made a very simple GUI interface to make the whole project user friendly and interactive. Basically our whole project is all about implementing the Encryption and Decryption Algorithms in Racket .To see the implementation of the project please run the the main.rkt file

Caesar Shift Cipher



- This is a old age encryption algorithm .
- For a given message it shifts all the letters by a Key .
- This was pretty easy to implement and easy to hack also.
- To decrypt the message we just have to reverse the shift process.

Scytale Cipher

- It breaks the message into lengths equal to a Key , and then the corresponding elements of each group are taken to get cipher text
- This is also a easy algorithm , And caab be hacked too.

Viginere Cipher

- Viginere Cipher uses a secret Key word and using the transformations for the letters it changes the given message into a cipher text
- The letters of the message are transformed by taking a known transform with the letters off keyword.
- If the message is longer than key the key is repeated.

One-Time-Pad Cipher

- One-Time-Pad works on the basic fact that XOR function is reversible .
- It generates a Random Key of length same as the Message length .
- Then XOR function is applied to Message and Key to get a cipher text.
- And for decryption, because XOR is reversible the cipher text is again put into XOR function with Key and original message is recovered .
- This is mathematically proven that for sufficiently long messages OTP can not be hacked .

ENIGMA Cipher

- As you may know Enigma is used in World War II by Germans , It is actually a electric machine that connects the specific electric circuits for given Rotor settings .
- We have simulated the whole Enigma machine in a racket program by making the rotors as list of functions to direct the input signal.
- Here the initial rotor settings is the Secret Key for the the encryption method.

Advanced Encryption Standard

- It is based reversibility of matrix multiplication and linear transformations .
- We convert our message into 4X4 matrices of hexadecimal representation , and apply the encryption procedure.
- Encryption procedure is a 10 round (for 128 bit) application of simple matrix transformation {SubBytes , ShiftRows , MixColumns , AddRoundKey}.
- the key is a matrix with hexadecimal entries , which also changes by specific key schedule over the rounds .
- Basically AES is just a algorithm which transforms the given matrix with lots of permutations and also keeping the reversibility of the process.
- For decryption we just reverse the whole process .

HACKER

- Hacker is only implemented for Caesar shift and Scytale ciphers.
- It checks all possible keys to decrypt a message and gives the message which is best written in English .
- Basically we have implemented nice-text? function which uses the frequency analysis for english letters ,double-letters to give the message that is most meaningful in English .

INPUT AND OUTPUT

1. Ideally for every text message for all the algorithms should give the same message as input.
2. For successfully implementing the Hacker we need to give the input as nicely written text
   Input = output =
   "TRUE LOVE IS POSSIBLY THE MOST FULFILLING OF LIFE'S SECRET TREASURES. BUT LOVE BY A LESSER STANDARD IS STILL EXTREMELY IMPORTANT FOR THE HUMAN EXPERIENCE.”.

LIMITATIONS

- The Interface is not very attractive .
- Hacker doesn’t recognise the messages that are not in good English