CAESAR CIPHER

A COURSE PROJECT REPORT

By

S. Surya Prakash (RA2011030010137)

Under the guidance of

Mrs. Mary Subaja Christo

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

In **Networking and Communication**

FACULTY OF ENGINEERING AND TECHNOLOGY SRM

INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chenpalpattu District

NOVEMBER 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "**CAESAR CIPHER**" is the bonafide work of **S. Surya Prakash(RA2011030010137)** who carried out the project work under my supervision.

Signature of the Faculty

Mrs. Mary Subaja Christo

Assistant Professor

Department of NWC

SRM Institute of Science and Technology

TABLE OF CONTENTS

Abstract

- The Caesar Cipher algorithm for cryptography is one of the oldest algorithms. Now much newer algorithms have arrived that are much more secure, however in terms of speed of execution Caesar cipher algorithm is still the fastest owing to its simplicity.

- However the algorithm is extremely easy to crack. This is because in this algorithm each character of a message is always replaced by the same fixed character that has been predetermined. To improve the algorithm and enhance it's security feature, a few changes can be added.

- This paper proposes an enhancement to the existing algorithm by making use first of a simple Diffie-Hellman key exchange scenario to obtain a secret key and later using simple mathematics to ensure the encryption of data is much more safer.

- Once a private shared key is obtained by making use of the Diffie-Hellman method, the key is subject to the mod operation with 26 to obtain a value less than or equal to 26, then the current character is taken and to this the key value obtained is added to obtain a new character.

- For any character in the `x' position the key is simply first multiplied with `x' and then mod is done to obtain the encrypted character. So 2nd character of the message is multiplied with 2, third character with 3 and so on.

- This enhances the security and also does not increase the time of execution by a large margin.

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor Dr.Annapurani Panaiyappan, Professor and Head, Department of Networking and Communications** and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our my Course project Faculty **<Faculty Name> , <Designation> , <Department>,** for his/her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD Dr. Annapurani Panaiyappan ,Professor and Head ,Department of Networking and Communications** and **Course Coordinators** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

Introduction

- In cryptography, a Caesar cipher, also known as **Caesar's cipher**, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.
- The method is named after Julius Caesar, who used it in his private correspondence.
- The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system.
- As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communications security.
- 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.

Literature Survey

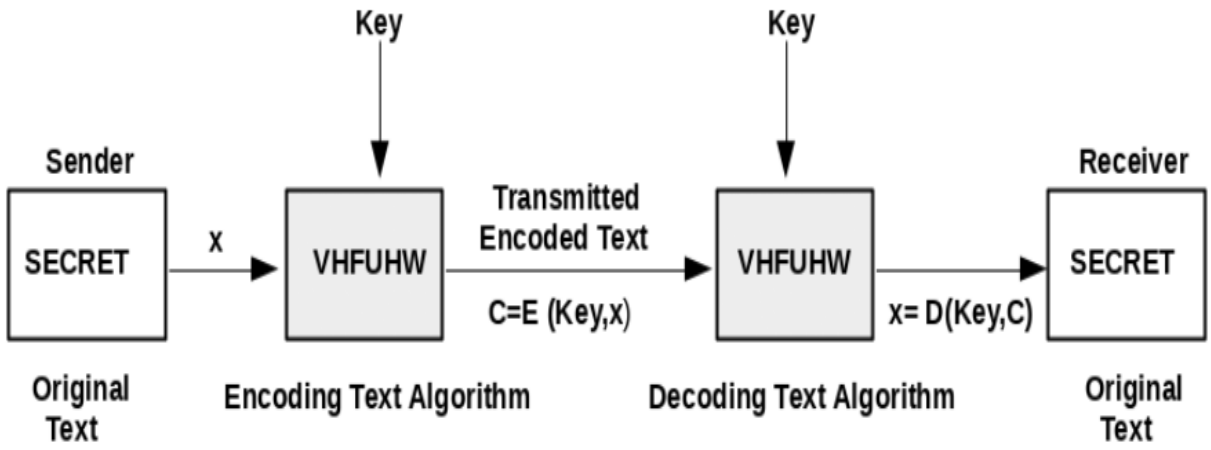
In 2011 Uttam Kr. Mondal Satyendra Nath Mandal proposed “Frame Based Symmetric Key Cryptography”. They proposed symmetry key block cipher algorithm to encrypt plain text into cipher text or vice versa using a frame set. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with Chi-square value, frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with the well-known existing algorithms .

In 2012 Aarti Soni, Suyash Agrawal proposed “Using Genetic Algorithm for Symmetric key Cryptography”. Genetic algorithms are a class of optimization algorithms. Many problems can be solved using genetic algorithms through modelling a simplified version of genetic processes. They proposed a method based on Genetic Algorithm which is used to generate key by the help of pseudo random number generator. Random number will be generated on the basis of current time of the system. Using Genetic Algorithm they keep the strength of the key to be good, still make the whole algorithm good enough. Symmetric key algorithm AES has been proposed for encrypting the image as it is very secure method for symmetric key encryption .

In 2012 Somdip Dey proposed “An Integrated Symmetric Key Cryptographic Method”. They proposed a new integrated symmetric-key cryptographic method, named SJA, which is the combination of advanced Caesar Cipher method, TTJSA method, Bit wise Rotation and Reversal method. The encryption method consists of three basic steps Encryption Technique using Advanced Caesar Cipher, Encryption Technique using TTJSA Algorithm, and Encryption Technique using Bit wise Rotation and Reversal

In2014 Saranya K Mohanapriya R proposed “A Review on Symmetric Key Encryption Techniques in Cryptography”. They proposed a study on various symmetric key encryption techniques, its comparison and the attacks to which they are vulnerable to.

Architecture Diagram



Block diagram of the classic Caesar system

Here in this architecture, we can see that we will be encoding the given plain text with the desired algorithm (Caesar cipher) and the proposed key.

First, we will be encrypting the plain text into a cipher text and it will be transmitted from the sender to the receiver and on the receiver's end the cipher is decoded using the key known to the receiver (symmetric encryption) and on the decryption we will again receive the plain text

(original message).

EXPLANATION

In cryptography, a Caesar cipher is categorized as a substitution cipher in which the alphabet in the plain text is shifted by a fixed number down the alphabet.

A Caesar cipher is one of the simplest and most well-known encryption techniques.

Named after Julius Caesar, it is one of the oldest types of ciphers and is based on the simplest monoalphabetic cipher. It is considered a weak method of cryptography, as it is easy to decode the message owing to its minimum security techniques.

For the same reason, a Caesar cipher is often incorporated only in parts of other complex encryption schemes.

Mathematical Description :-

First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25. We can now represent the caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

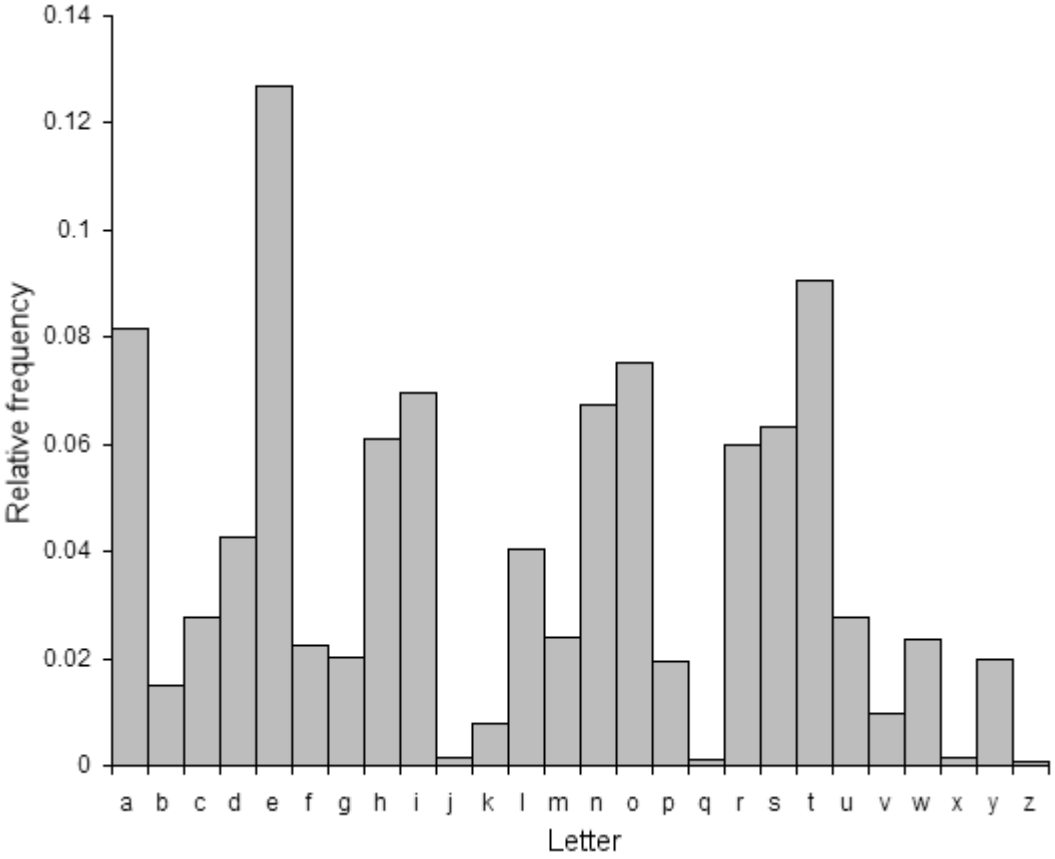
Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is :

$$e(x) = (x - k) \pmod{26}$$

Cryptanalysis is the art of breaking codes and ciphers. The Caesar cipher is probably the easiest of all ciphers to break. Since the shift has to be a number between 1 and 25, (0 or 26 would result in an unchanged plaintext) we can simply try each possibility and see which one results in a piece of readable text. If you happen to know what a piece of the ciphertext is, or you can guess a piece, then this will allow you to immediately find the key.

If this is not possible, a more systematic approach is to calculate the frequency distribution of the letters in the cipher text. This consists of counting how many times each letter appears. Natural English text has a very distinct distribution that

can be used help crack codes.



For a method that works well on computers, we need a way of figuring out which of the 25 possible decryptions looks the most like English text. The key (or shift) that results in a decryption with the highest likelyhood of being English text is most probably the correct key. Of course, the more ciphertext you have, the more likely this is to be true (this is the case for all statistical measures, including the frequency approach above). So the method used is to take the ciphertext, try decrypting it with each key, then see which decryption looks the best. This simplistic method of cryptanalysis only works on very simple ciphers such as the Caesar cipher and the rail fence cipher, even slightly more complex ciphers can have far too many keys to check all of them.

Advantages of using a Caesar cipher include:

- One of the easiest methods to use in cryptography and can provide minimum security to the information
- Use of only a short key in the entire process
- One of the best methods to use if the system cannot use any complicated coding techniques
- Requires few computing resources

RESULTS

CODE(Encryption):-

```
#include<stdio.h>


#include<ctype.h>


int main()
{
  char text[500], ch;
  int key;
  // taking user input
  printf("Enter a message to encrypt: ");
  scanf("%s", text);
  printf("Enter the key: ");
  scanf("%d", & key);
  // visiting character by character
  for (int i = 0; text[i] != '\0'; ++i) {
    ch = text[i];
    // check for valid character
    if (isalnum(ch)) {


      // lower case characters
      if (islower(ch)) {
        ch = (ch - 'a' + key) % 26 + 'a';
      }
      // uppercase characters
```

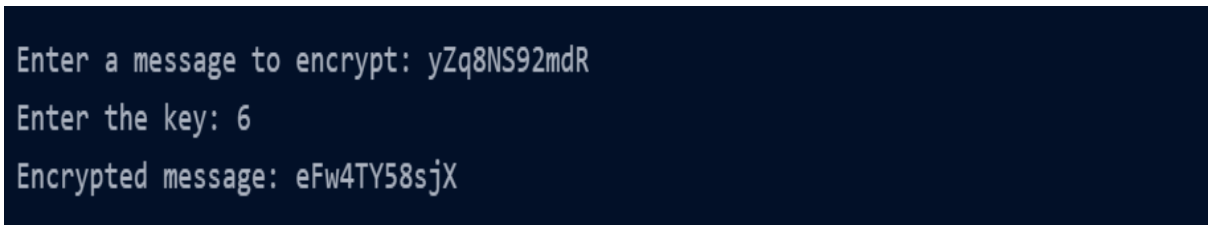
```
    if (isupper(ch)) {
      ch = (ch - 'A' + key) % 26 + 'A';
    }
    // numbers
    if (isdigit(ch)) {
      ch = (ch - '0' + key) % 10 + '0';
    }
  }
  // invalid character
  else {
    printf("Invalid Message");
  }
  // adding encoded answer
  text[i] = ch;

 }

 printf("Encrypted message: %s", text);

 return 0;
}
```

RESULT:-



CODE(Decryption):-

```
#include<stdio.h>
#include<ctype.h>
int main(
{
  char text[500], ch;
  int key;
  // taking user input
  printf("Enter a message to decrypt: ");
  scanf("%s", text);
  printf("Enter the key: ");

  scanf("%d", & key);

  //visiting each character
  for (int i = 0; text[i] != '\0'; ++i) {

    ch = text[i];
    // check for valid characters
    if (isalnum(ch)) {
      // lower case characters
      if (islower(ch)) {
        ch = (ch - 'a' - key + 26) % 26 + 'a';
      }
      // uppercase characters
      if (isupper(ch)) {
        ch = (ch - 'A' - key + 26) % 26 + 'A';
```

```
    }
    // numbers
    if (isdigit(ch)) {
      ch = (ch - '0' - key + 10) % 10 + '0';
    }
  }
  // invalid characters
  else {
    printf("Invalid Message");
  }
  // asding decoded character back
  text[i] = ch;
 }
 printf("Decrypted message: %s", text);
 return 0;

}
```

OUTPUT:-

```
Enter a message to decrypt: eFw4TY58sjX
Enter the key: 6
Decrypted message: yZq8NS92mdR
```

Conclusion

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

Caesar cipher algorithm can be implemented in many encryption projects to make data secure and better. Security is one of the important aspects in computing. In data transfer, security must be considered as one of the method implemented to ensure secure data transfer.

References

- https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/#:~:text=The%20Caesar%20Cipher%20technique%20is,of%20positions%20down%20the%20alphabet.
- https://www.researchgate.net/figure/Block-diagram-of-the-classic-Caesar-system_fig1_339340318
- https://ieeexplore.ieee.org/document/7749010
- https://www.scaler.com/topics/caesar-cipher-program-in-c/