AUTHENTICATION USING CAESAR CIPHER WITH RANDOMLY GENERATED KEY

Y. Rajesh **K. Bhaskar** **K. Audi Dinakar**

Students of B. Tech CSE(AI), Department of CSE, Dr. M.G.R Educational & Research Institute

ABSTRACT

The Caesar cipher is a historic encryption method that involves shifting each letter of a message a certain number of positions to the right or left of the alphabet. The key to the cipher is the number of positions that the letters are shifted. The Caesar cipher is a simple and easy-to-understand encryption technique that was used by Julius Caesar to communicate with his generals. It can be implemented quickly and is easily reversible, making it an attractive option for simple data encryption. Encryption at the sending end and decryption at the receiving end of the communication system are required for secure communication. To provide data security, numerous cyphers have been created. The effectiveness of the utilised cyphers is mostly influenced by their memory requirements and throughput. Large key spaces, a big number of rounds, and numerous complex processes may increase security, but they can slow down operations. As a result, we have suggested a way in this study to enhance the Caesar cypher by using a random number generation technique for key generation operations. Alphabets, integers, and symbols are now included in the Caesar Cipher. This paper aims to propose an enhanced version of Caesar cipher substitution technique which can overcome all the limitations faced by classical Caesar Cipher.

KEYWORDS

Security, Encryption, Decryption, Cryptography, Substitution, Cipher, Random Number, Recursive, Primitive root, Plaintext, Ciphertext, Diffie-Hellman, Digital signatures.

1. INTRODUCTION

Cryptography is the practice of securing communication and data using mathematical algorithms and protocols. It involves techniques for encryption, decryption, authentication, and digital signature. The goal of cryptography is to ensure confidentiality, integrity, and authenticity of the data and communication.

Encryption involves transforming plain text into a cipher text, which can only be read by someone who has the key to decrypt it. Decryption is the process of converting the cipher text back into plain text using the key. Cryptographic algorithms are designed to make it difficult to decrypt the cipher text without the key.

Authentication is the process of verifying the identity of a person or system. Cryptographic protocols are used to authenticate the identity of users or systems to prevent unauthorized access to data or communication.

Digital signatures are used to verify the authenticity of digital messages or documents. They provide a way to verify

the identity of the sender and the integrity of the message or document.

Cryptography is widely used in many applications, such as secure communication, e-commerce, and online banking. It is also used in the storage of sensitive information, such as passwords and credit card information. Cryptography plays a critical role in modern information security, protecting sensitive information from unauthorized access and ensuring the privacy of communication.

The Caesar cipher works by shifting each letter in the plaintext by a fixed number of positions down the alphabet. The key for the cipher is the number of positions to shift.

2.LITERATURE SURVEY

1. A research Paper for Symmetric and Asymmetric Cryptography done by Akshay Kekunnaya, Rajeshwari Gundla, Siddharth Nanda

We have learned the type of cryptography that is symmetric and asymmetric cryptography. Cryptography is used to ensure that the message sent by the people is secured or not.

2. A study on symmetric and asymmetric key encryption algorithms done by S.Suguna, Dr.V.Dhanakoti, R. Manjupriya.

This paper tells about the study of symmetric and Asymmetric key encryption algorithm like AES, DES, TRIPLE DES, RC4, Multiphase encryption, RSA, Elgamal cryptosystem, Digital signature and Diffie Hellman.

3. Comparison study of symmetric key and asymmetric key algorithm done by Priasnyomo Prima Santoso, Elkin Rilvani, Ahmad Budi Trisnawan.

This paper discusses various key symmetric cryptographic algorithms and asymmetric keys from several related literature review article

3. FOLLOWING ARE THE VARIOUS GOALS OF CAESER-CIPHER

A. Confidentiality

Data that resides in computer is transmitted and that isto be accessed only by the legal person and that data can't be accessed by anyone else.

B. Authentication

The data that is seen by any system has to check the identity of the sender, whether the data is appear from a legal person or illegal person.

C. Data Integrity

To verify the information has not been changed by illegal or unknown person. Only the sender and receiver can modify the message. No others have the rights to access the message (or) Data.

D. Non-Repudiation

It does not allow repudiation by the sender or receiver. The receiver proves the identification of the sender in case of denial by the sender. The sender proves theidentification of the receiver in case of denial by the receiver.

E. Access Control:

It is to ensure that only the authorized person can have the rights to access the transmitted information.

4. BASIC TERMINOLOGY USED IN CAESER-CIPHER CRYPTOGRAPHY

A. Plain Text

The data is in the original form is called plaintext. The sender sends the plaintext to the receiver. At the time of encryption process this plaintext is taken as input. Example: Seetha wants to send the message “How are you”to Priya. Then the message “How are you” is called plaintext.

B. Cipher Text

The data is in an understandable form is called cipher text. At the time of encryption process the plain text is converted into cipher text. The cipher text is can’t be understood by anyone. It is the outcome of the encryption process. For example: The plain text “How are you” is converted into cipher text as “* @97k&A%L".

C. Encryption

The method of translating the plain text into cipher text with the help of algorithm and the encryption key is called encryption algorithm.

D. Decryption:

The method of translating the cipher text back in to its original form that is plain text with the help of decryption key and algorithm is called decryption algorithm.

E. Keys

The numeric, alpha numeric or special symbol are used as key. During the encryption and decryption process the key plays a major role. The information security directly depends on the selection of key.

5.1 SYMMETRIC KEY CRYPTOGRAPHY

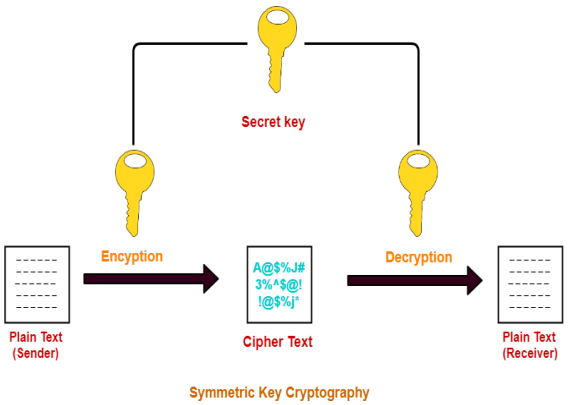
Symmetric key cryptography, also known as secret key cryptography, is a type of encryption method that uses a single secret key for both encryption and decryption of data. The same key is used by both the sender and receiver to encrypt and decrypt messages.

In symmetric key cryptography, the sender and receiver must agree on a shared secret key before any secure communication can take place. Once the key is established, the sender uses the key to encrypt the message, and the receiver uses the same key to decrypt the message.

One of the main advantages of symmetric key cryptography is its speed and efficiency. Because only one key is used for both encryption and decryption, the process is faster than asymmetric key cryptography, which requires two separate keys.

However, a major challenge with symmetric key cryptography is the secure distribution of the secret key. The sender and receiver must have a secure way to exchange the key without it being intercepted by a third party. Once the key is compromised, all communications using that key are no longer secure.

Symmetric key cryptography is widely used in many different applications, including secure communication over the internet, data encryption, and authentication. Examples of symmetric key cryptography algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish.



Symmetric Key Cryptography

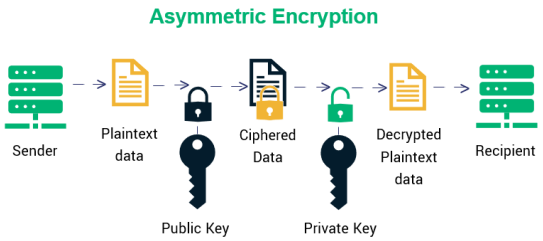
5.2 ASSYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography, also known as public key cryptography, is a type of encryption method that uses two different but mathematically related keys to encrypt and decrypt data. One key, the public key, is freely distributed and available to anyone, while the other key, the private key, is kept secret by the owner.

In asymmetric key cryptography, the public key is used to encrypt data, while the private key is used to decrypt it. This means that anyone can encrypt data using the public key, but only the owner of the private key can decrypt it.

This method of encryption has several advantages over symmetric key cryptography, which uses the same key for both encryption and decryption. One major advantage is that it eliminates the need to securely share the same key between parties, which can be difficult to achieve in some situations. Instead, only the public key needs to be shared, and the private key can be kept secure by its owner.

Asymmetric key cryptography is widely used in many different applications, including secure communication over the internet, digital signatures, and secure key exchange. Examples of asymmetric key cryptography algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC).



6. METHOD & SOFTWARE

CAESER-CIPHER (SUBSTITUTION TECHNIQUE)

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

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.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

Examples: -

1. **Text**:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ

   Shift: 23

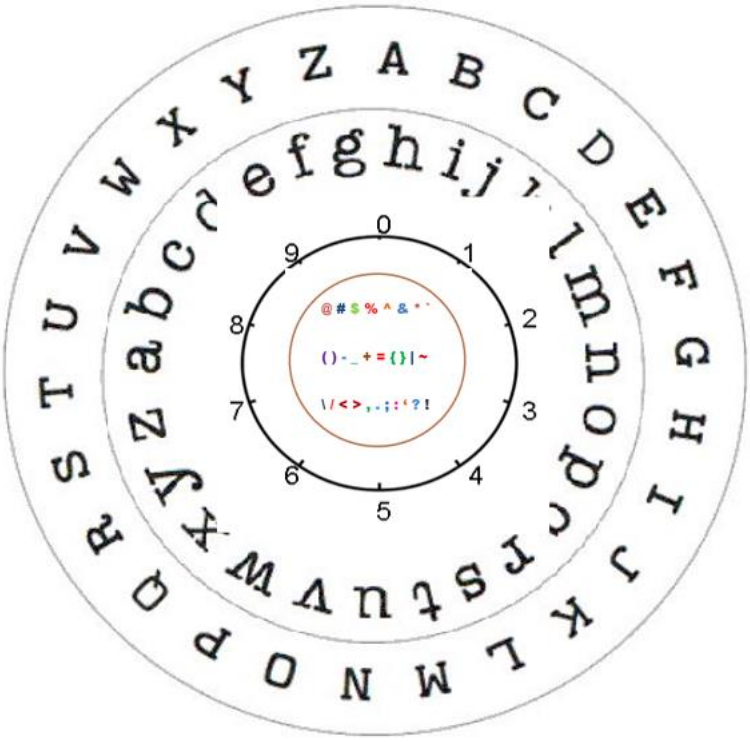
   Cipher:

   XYZA@BCDE$FGHIJK^LMNO&PQRSTU*VW

2. **Text**: ATTACKATONCE

   Shift: 4

   Cipher: EX#XEG^OEX%SRGI



7. Diffie-Hellman Algorithm

The Diffie-Hellman algorithm is a cryptographic protocol used to establish a shared secret between two parties without actually exchanging the secret over a communication channel. Here's an overview of the algorithm:

1. Agree on a prime number p and a base g (where g is a primitive root modulo p).

2. Each party, Alice and Bob, privately choose a random number (a for Alice and b for Bob) that is less than p.

3. Alice computes A = g^a mod p and sends this value to Bob.

4. Bob computes B = g^b mod p and sends this value to Alice.

5. Both Alice and Bob now compute a shared secret key K using the following formula: K = (B^a) mod p (Alice) or K = (A^b) mod p (Bob).

The security of the Diffie-Hellman algorithm relies on the fact that computing K requires knowledge of a or b, which are kept secret by Alice and Bob, respectively. An attacker who intercepts A and B cannot easily compute K without knowing either a or b

8. PROPOSED SYSTEM

In this approach, developed 256 combinations of alphabets, numbers and symbols which are included in the system.

Improved Brute force attack requires 93! Attempts, which makes the algorithm more robust and also works very fast with 1 µS / byte.

Key length of the Algorithm is 100-bits. The proposed algorithm includes rich character set compare to Caesar cipher. The algorithm occupies memory approximately equal to 5 Kb.

Enhanced the security to a greater extent because of the fact that in order to decrypt the cipher text one needs to have access to keys in both the steps.

9. ALGORTHIM

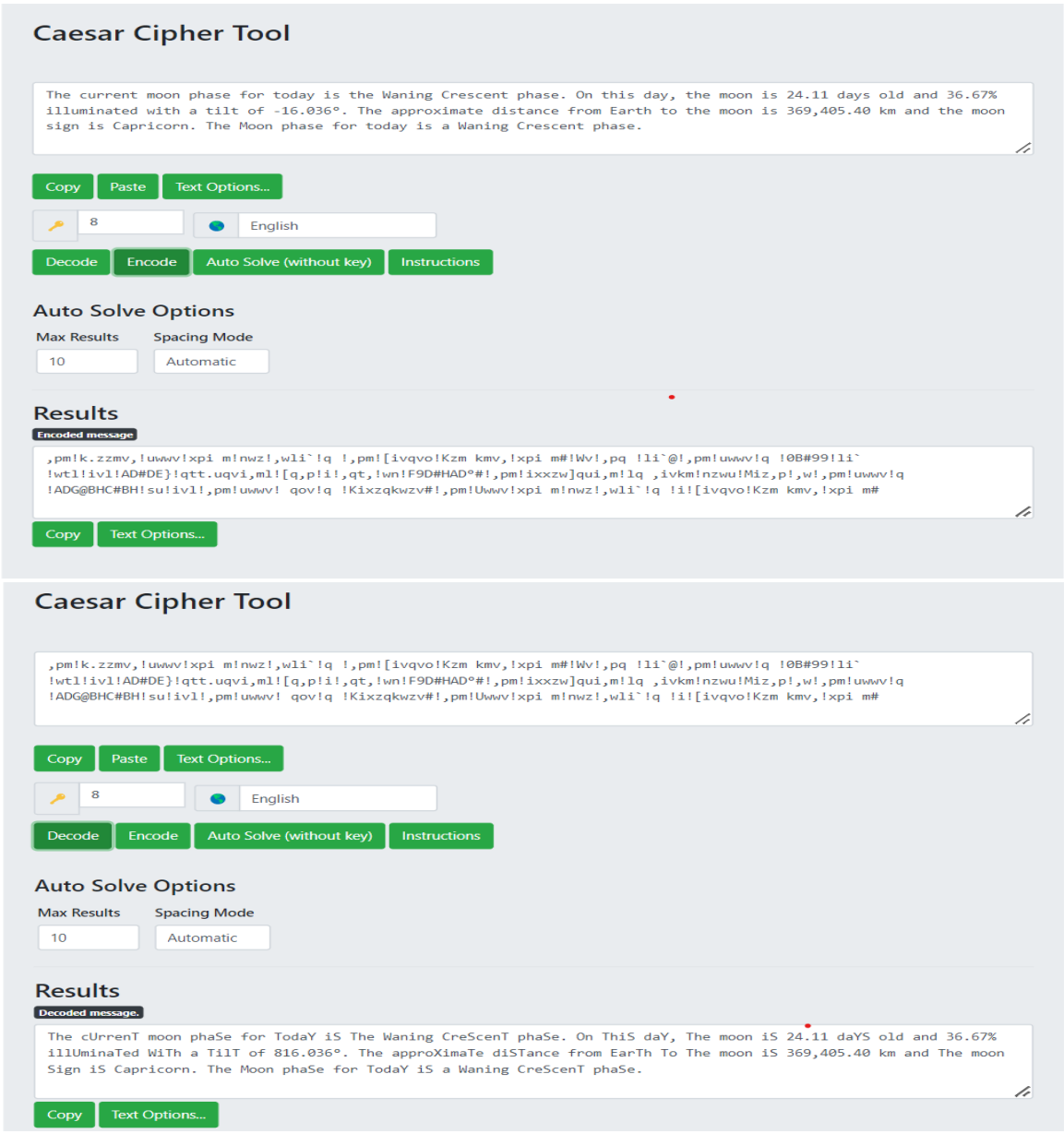
9.1. ENCRYPTION

1. Initialize a variable to hold the plaintext message.
2. Ask the user for the number of positions to shift the letters by (this is known as the "key").
3. Initialize a variable to hold the ciphertext message.
4. Loop through each character in the plaintext message: a. If the character is a letter, shift it by the key number of positions down the alphabet. If the resulting character goes past the end of the alphabet, wrap around to the beginning (e.g., if the key is 3 and the character is 'z', shift it to 'c'). b. If the character is not a letter, leave it as-is. c. Add the resulting character to the ciphertext message.
5. Return the ciphertext message.

9.2. DECRYPTION

1. Initialize a variable to hold the ciphertext message.
2. Ask the user for the number of positions that the letters were shifted by (this is known as the "key").
3. Initialize a variable to hold the plaintext message.
4. Loop through each character in the ciphertext message:
   a) If the character is a letter, shift it back by the key number of positions up the alphabet. If the resulting character goes past the beginning of the alphabet, wrap around to the end (e.g., if the key is 3 and the character is 'a', shift it to 'x').
      b. If the character is not a letter, leave it as-is.
      c. Add the resulting character to the plaintext message.
5. Print the plaintext message.

OUTPUT:



CONCLUSION

Security plays a major role in wireless type of medium because when we transmit our data wirelessly, it can be access by the third party or an outsider. Cryptography plays an important role for safe transmission of data. Data is encrypted and decrypted by many techniques. Caesar cipher is important technique which has less complex, limited power consumption and less memory consumption . In this paper, the limitations and weaknesses of classical encryption algorithms like Caesar cipher and Transposition cipher are described. Then a modified Caesar algorithm is proposed to overcome all the weaknesses and limitations of Caesar cipher. The proposed algorithm uses a randomized approach for substitution which is then combined with double for

substitution which is then combined with double columnar transposition technique to increase the strength. On performing cryptanalysis on the modified algorithm, it is found impossible to break it by frequency analysis. It is practically impossible to decode the algorithm by brute force approach since the attacker would have to try a total of key length raised to 256 different combinations of keys. Security provided by this algorithm can be enhanced further by using it with one or more different encryption algorithms or by using asymmetric key approach instead of symmetric key.

REFERENCES

[1] A.F.A.Abidin, O.Y. Chuan and M.R.K. ariffin-“ A Novel enhancement Technique of the Hill Cipher for effective Cryptographic Purposes ‘- Journal of Computer science , 7(5): 785- 789, 2011

[2] Dharmendra Kumar Gupta, Sumit Kumar Srivastava, Vedpal Singh- “New Concept of encryption algorithm A hybrid approach of Caesar Cipher and Columnar transposition in multi stages “– Journal of Global Research in Computer Science, Volume 3, No. 1, January 2012, P. No. 60-66

[3] Fauzan Saeed, Mustafa Rashid- “I n t e g r a t i n g Classical Encryption with Modern Technique “ IJCSNS, Volume 10, No. 5, May 2010

[4] Prof.K.Govinda , Dr.E. sathiyamoorth- “Multilevel Cryptography Technique Using Graceful Codes “- JGRCS, Volume 2, No.7, July 2011

[5] Monodeep Banerjee, Saptarshi Naskar, krishnendu Basuli, Samar Sen Sarma- “A Novel scheme forText data encryption “- JGRCS, Volume 3, No.1, January 2012

[6] Phillip I Wilson and Mario Garcia – “A Modified Version of the Vigenere Algorithm “- IJCSNS, Vol. 6, No.3B, march 2006

[7] Packirisamy Murali and Gandhi doss Senthil Kumar – “Modified Version of Playfair cipher using Linear feedback Shift Register “– IJCSNS, Vol.8, No.12, December 2008