AUTHENTICATION USING CAESAR CIPHER WITH RANDOMLY GENERATED KEY

MINI PROJECT REPORT

submitted in partial fulfilment of the requirements
for the award of the degree in

BACHELOR OF TECHNOLOGY
In
COMPUTER SCIENCE AND ENGINEERING

by

Y. RAJESH	**(201211101051)**
K. BHASKAR	**(201211101027)**
K. AADI DINAKAR	**(201211101029)**

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING

APRIL 2023

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DECLARATION

We **Y. RAJESH, K. BHASKAR, K. AADI DINAKAR** hereby declare that the Project Report entitled **"AUTHENTICATION USING CAESAR CIPHER WITH RANDOMLY GENERATED KEY"** is done by me under the guidance of **Dr. G. SONIYA PRIYATHARSINI** is submitted in partial fulfilment of the requirements for the award of the degree in BACHELOR OF TECHNOLOGY.

DATE :

PLACE : SIGNATURE OF THE CANDIDATE

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this mini project report is the bonafide work of

Y. RAJESH	**(201211101051)**
K. BHASKAR	**(201211101027)**
K. AADI DINAKAR	**(201211101029)**

Who carried out the mini project entitled **"AUTHENTICATION USING CAESAR CIPHER WITH RANDOMLY GENERATED KEY"** under our supervision from Dec 2022 to April 2023.

Mini Project Coordinator

Dr. G. Soniya Priyatharsini

Associate Professor (CSE)

Dr. MGR Educational and Research Institute
Deemed to be University

Department Head

Dr. S. Geetha

Professor & HOD (CSE)

Dr.MGR Educational and Research Institute
Deemed to be University

Submitted for Viva Voce Examination held on ____________________

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

We would like to thank our beloved Chancellor Thiru. Dr. A.C. Shanmugam, B.A., B.L., President Er. A.C.S. Arun Kumar, B.Tech., and Secretary Thiru A. Ravikumar for all the encouragement and support extended to us during the tenure of this project and also our years of studies in this wonderful University.

We express my heartfelt thanks to our Vice Chancellor Dr. S. Geethalakshmi in providing all the support of my Project.

We express my heartfelt thanks to our Head of the Department, Prof. Mrs. S. Geetha, who has been actively involved and very influential from the start till the completion of our Project.

Our sincere thanks to our Project Coordinators Dr. G. Soniya Priyatharisini and Project guide M. Chandran for their continuous guidance and encouragement throughout this work, which has made the project a success.

We would also like to thank all the teaching and non-teaching staff Computer Science and Engineering department, for their constant support and the encouragement given to us while we went about to achieving my project goals.

LIST OF FIGURES

TABLE OF CONTENTS

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 project aims to propose an enhanced version of Caesar cipher substitution technique which can overcome all the limitations faced by classical Caesar Cipher and we implemented more number of shifts and which is included with special characters, alphabet, numbers, and symbols. The proposed model is most reliable and secure with modern technologies.

KEYWORDS

Security, Encryption, Decryption, Cryptography, Substitution, Cipher, Random Number, Recursive, Primitive root, Plaintext, Ciphertext, Diffie-Hellman, Digital Signatures AES, RSA, Vigenère cipher algorithm.

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.

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 an encryption technique that was used by Julius Caesar to communicate with his generals. 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. The key for the cipher is the number of positions to shift.

Components of the cryptography are Plaintext and Cipher text, Ciphers, Secret Key, Encryption algorithm and Decryption algorithm. The information that is routed over the network is called as Plain text and after adding number of operations on Plaintext, a Cipher text is obtained. Encryption algorithm and decryption algorithm which are used for encrypt and decrypt the plaintext are called Ciphers. The number on which cipher is operated is called as key. In Encryption part, three elements are required i.e., Plaintext, Rule and Key.

When these elements are used along, they form cipher text. In decryption part, three elements which are required are Cipher text, Rule and Key. Sender shares the secret key only with the receiver so that the information should stay protected. Caesar cipher is also familiar with another name “Shift Cipher”. Caesar cipher is also known as Julius Caesar, by its inventor name. In Caesar cipher, all the characters of the plaintext are interchanged by a character, symbols, numbers, and special characters of some mounted variety of locations down the alphabet When the key value is 2, all the characters of plaintext are encrypted into cipher text by these characters, symbols, numbers, and special characters.

1.1. 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.

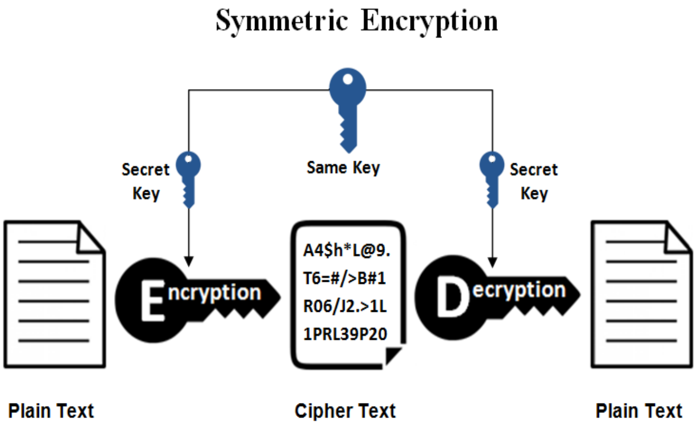


Fig. 1.1

1.2. 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).

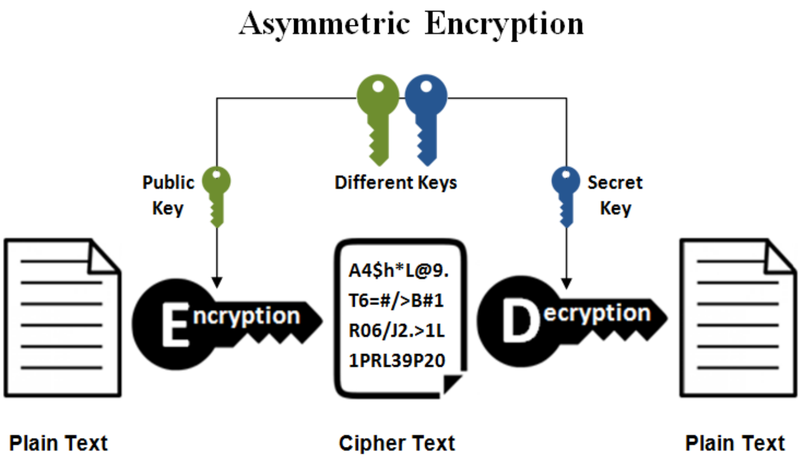


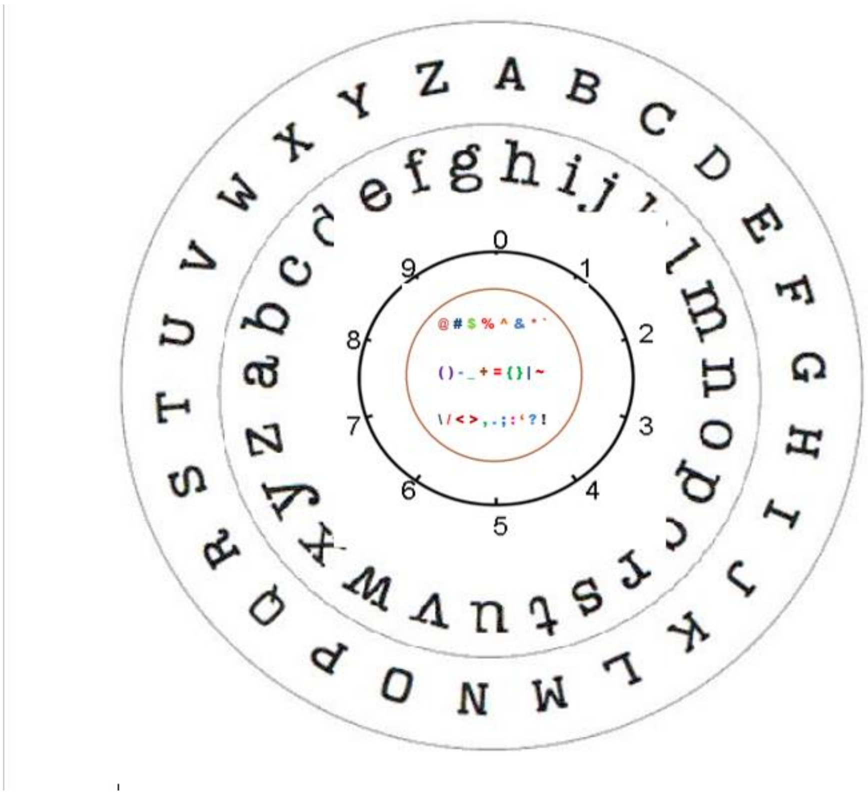
Fig. 1.2

1.3. CAESER-CIPHER (SUBSTITUTION TECHNIQUE)

The Caesar Cipher technique is one of the earliest methods of encryption technique. It is actually a type of substitution cipher, which is a method of encryption that replaces each letter in the plaintext with another letter, number, symbol. In the case of the Caesar Cipher, the substitution is a simple shift of the letters by a fixed amount

Other examples of substitution ciphers include the Atbash Cipher, which reverses the order of the letters in the alphabet (e.g., A becomes Z, B becomes Y, and so on), and the Polybius Square Cipher, which uses a grid to map each letter to a pair of numbers.

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.


Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9
@ # $ % ^ & * `
( ) - _ + = { } | ~
\ / < > , . ; : ' ? !

Caesar-cipher substitution wheel

Fig. 1.3

Plaintext: It is a simple message written by the user.

Ciphertext: It is an encrypted message after applying some technique.

The formula of encryption and decryption is:

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 100.

Encryption of a letter by a shift n can be described mathematically as.

$$Dn\ (x) = (xi + n)\ mod\ 100$$

(Encryption phase with shift n)

$$Dn\ (x) = (xi - n)\ mod\ 100$$

(Decryption phase with shift n)

Where ,

E denotes the encryption
D denotes the decryption
x denotes the letters value
n denotes the key value (shift value)

Examples: -

1. Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
   Shift: 23
   Cipher: XYZA@BCDE$FGHIJK^LMNO8&PQRS9TU*VW

2. Text: ATTACKATONCE
   Shift: 4
   Cipher: E3X#XEG^O6EX%SRGI

2. PROBLEM DEFINITION

The problem that the Caesar cipher aims to solve is that of secure communication between two parties. In ancient times, communication between military or political leaders needed to be kept secret, and the Caesar cipher provided a simple way to achieve this.

The problem with plain text communication is that it can be intercepted and read by unauthorized individuals, leading to sensitive information being compromised. The Caesar cipher provides a way to encrypt messages in a simple and straightforward manner, making it more difficult for unauthorized individuals to read or understand the message.

The challenge with the Caesar cipher, however, is that it is a relatively encryption method and can be easily cracked with modern tools and techniques. For one, the fixed shift used in the old Caesar-cipher model is easily detectable through frequency analysis, which involves analysing the frequency of letters in the ciphertext to determine the shift used. In previous models it is not securable against brute attacks which leads to information will be goes to wrong hands.

3. OBJECTIVE OF THE PROJECT

The objective of the Caesar cipher is to provide a encryption method for secure communication between two parties. By shifting each letter in the plaintext, a fixed number of positions down the alphabet, symbols, numbers, special characters, the Caesar cipher aims to make it more difficult for unauthorized individuals to read or understand the message.

The specific objectives of the Caesar cipher are:

1. **To provide a basic level of security for communications**: - The Caesar cipher aims to prevent unauthorized individuals from easily understanding the message, providing a basic level of security for communication between two parties.

2. **To be easy to use**: - The Caesar cipher is a simple encryption method that can be easily understood and used by individuals with no prior encryption experience.

3. **To be easily reversible**: - The Caesar cipher can be reversed by shifting each letter in the opposite direction, allowing the intended recipient of the message to decipher the ciphertext.

4. **To lay the foundation for modern encryption techniques**: - The Caesar cipher laid the foundation for modern encryption techniques and serves as an important historical encryption method that has contributed to the development of modern cryptography.

4. LITERATURE SURVEY

1. RAJAN (2019) et al. In paper entitled “ADVANCEMENT IN CAESAR CIPHER BY RANDOMIZATION AND DELTA FORMATION” discusses the Caesar cipher by involving the Delta formation method. By adding this algorithm, it’s not easy for attacker to crack the cipher because the character replaced is randomly generated. Brute force attacker will also not be able to crack it because the characters are replaced by the other character according to delta formation. This method makes the transmission of data more secure. These delta formation Caesar ciphers divide in three portions.

   A. Alphabetic order.
   B. Character can be made by the combination of characters.
   C. Delta formation.

   Computational complexity in this cipher is less then hill cipher and play fair cipher. ATM cards data are encrypted by using this cryptography.

2. P. Verma (2020) et al. In paper entitled “EXTENDED CAESAR CIPHER FOR LOW POWERED DEVICES” demonstrate the Caesar cipher by adding new function in basic Caesar cipher which strengthen its impact to withstand against severe attacks. This extended Caesar cipher has also three parts:

   A. Key generation Process
   B. Encryption Process
   C. Decryption Process

   Basic Caesar cipher has also similar parts but in this paper, the authors have added more operations in all the process. Like in key generation, factorial function is added and then key value is taken in binary form. In Encryption process, the XOR of key and plaintext is done. By adding these functions, this technique has higher avalanche effect and more equalization in frequency test.

3. P. Garg (2021) et al. In paper entitled “A Review Paper on Cryptography and Significance of Key Length” states the importance of the key length. In this paper, author explains number of algorithms. Public Key cryptography, secrete key cryptography, and Hash Function are these algorithms. A single key is used in secrete key cryptography for both encryption and decryption. Sender uses the key for encrypt the data and then send the key to receiver for decrypt the data. \For encryption and decryption of a message.

5. REQUIREMENT ANALYSIS

Requirement analysis of the Caesar cipher involves identifying the functional and non-functional requirements for the encryption method to meet its objectives. Here are some requirements for the Caesar cipher:

5.1. **Functional Requirements: -**

1. Encryption: - The Caesar cipher should be able to encrypt plaintext messages by shifting each letter a fixed number of positions down the alphabet.

2. Decryption: - The Caesar cipher should be able to decrypt ciphertext messages by shifting each letter in the opposite direction of the encryption process.

3. Reversibility: - The Caesar cipher should be easily reversible, allowing the intended recipient of the message to easily decipher the ciphertext.

4. 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.

5.2. Non-Functional Requirements: -

1. Security: - The Caesar cipher should provide a basic level of security for communications by making it more difficult for unauthorized individuals to read or understand the message.

2. Usability: - The Caesar cipher should be easy to use, even for individuals with no prior encryption experience.

3. Efficiency: - The Caesar cipher should be efficient, taking minimal time and resources to encrypt and decrypt messages.

4. Compatibility: - The Caesar cipher should be compatible with a variety of devices and platforms, allowing for widespread use.

5. 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.

6. Key management: - The shift value used in the Caesar cipher serves as the encryption key. The key must be kept secret and securely shared between the sender and recipient of the message.

6. EXISISTING SYSTEM

1. **Vulnerable to Brute Force Attack: -** The Caesar Cipher has a very limited number of possible keys (26), which makes it vulnerable to brute force attacks. With modern computing power, it is relatively easy to try all 26 possible keys and decode the message.

2. **Lack of Security: -** Because the Caesar Cipher uses a fixed shift value for each letter, it is not very secure. An attacker can easily use frequency analysis to deduce the shift value and decode the message.

3. **Limited Key Space:** - The key space of the Caesar Cipher is very small, as it is limited to the 26 possible shift values. This means that the cipher can be easily broken with basic cryptanalysis techniques.

4. **Not Suitable for Modern Communication:** - The Caesar Cipher is not suitable for modern communication, as it is too easy to break. In today's digital world, where security is of utmost importance, more advanced encryption techniques such as AES are required.

5. **Inability to Encrypt Numbers and Symbols: -** The Caesar Cipher is designed to encrypt only letters, which means that it cannot encrypt numbers or symbols. This limits its usefulness in many modern applications, such as online banking, where numbers and symbols are frequently used.

6. **Languages: -** Only English is the default language to encrypt and decrypt the message. So, its difficult to other country peoples

7. PROPOSED SYSTEM

1. In proposed system increased number of possible keys more than 100 and it is secure against brute force attacks. As it is not possible to decode the message.

2. Now Caesar-cipher is very fast and efficient, both in terms of encryption and decryption. It can be used to quickly encrypt short messages or to test other cryptographic algorithms.

3. Increased the key space of Caesar-cipher to large size with more than 100 possible shift values. Along with combination of alphabets, numbers, special characters and symbols as the shift values.

4. In proposed system the Caesar-Cipher is designed to encrypt with alphabets, numbers, special characters and symbols with a total of more than 1000 characters.

5. Include many different types of languages such as Englis, French, German, Italian, Portuguese, Spanish and Swedish used to encrypt and decrypt the message.

6. Now it is suitable for modern communication and it is not easy to decode the message.

7. It is more secure against modern technologies. By implementing some algorithms such as

   - **Advanced Encryption Standard (AES):** AES is a symmetric encryption algorithm that is widely used for securing data. It is a block cipher algorithm that uses a 128-bit block size and key sizes of 128, 192, or 256 bits. AES is considered to be one of the strongest encryption algorithms currently available.

   - **RSA**: RSA is an asymmetric encryption algorithm that is widely used for secure communication, digital signatures, and key exchange. It is based on the difficulty of factoring large integers, and uses a public key for encryption and a private key for decryption.

   - **Vigenère cipher**: The Vigenère cipher is a polyalphabetic substitution cipher that involves shifting each character by a different amount, depending on a secret keyword. The Vigenère cipher is considered stronger than the Caesar cipher, but is still vulnerable to cryptanalysis.

   - **Playfair cipher**: The Playfair cipher is a polygraphic substitution cipher that involves encrypting pairs of characters instead of single characters. The Playfair cipher also involves shifting characters, but is more complex than the Caesar cipher and offers better security.

8. Increased more secure and reliable communication between sender and receiver and also improved time efficiency while encoding and decoding the message

8. SOFTWARE / HARDWARE REQUIREMENTS

8.1. Software Requirements

1. A programming language (e.g., Python, HTML, CSS, JS)
2. Text editor or IDE to write and execute the code (e.g., VS code, Code Sand Box)
3. Operating Systems (e.g., Windows, Mac OS, Linux)

8.2. Hardware Requirements

1. Computer

   Specifications: -

   I. 512 Gb SSD

   II. 8 Gb Ram

   III. Core i5/i7 Processor

   IV. Standard 110 keys keyboard

9. DESIGN

9.1. UML DIAGRAMS

9.1.1. USE CASE DIAGRAM

In this use case diagram, the primary actor is the "User", who interacts with the system by entering a message, choosing a shift, and then either encrypting or decrypting the message. The "Caesar Cipher" system receives the input from the user and performs the encryption or decryption based on the selected shift. The system has two use cases: "encrypt message" and "decrypt message", which take as input a message and a shift, and return an encrypted or decrypted message, respectively.

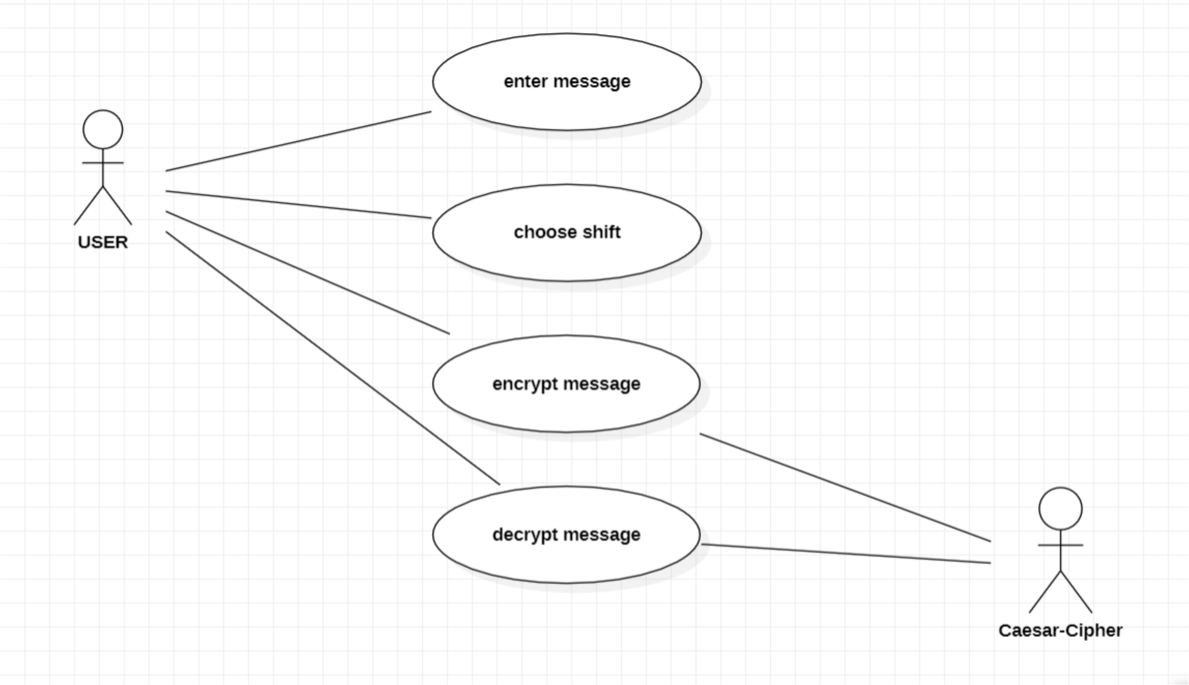


Fig. 9.1.1

9.2.2. ACTIVITY DIAGRAM

In this activity diagram, the process starts with getting the plaintext from the user. Then, the user is prompted to provide the shift value to be used in the encryption process. Next, the plaintext is encrypted using the shift value, and the resulting ciphertext is displayed. Then, the user is prompted to provide the ciphertext to be decrypted. The ciphertext is decrypted using the shift value, and the resulting plaintext is displayed. Finally, the process ends.

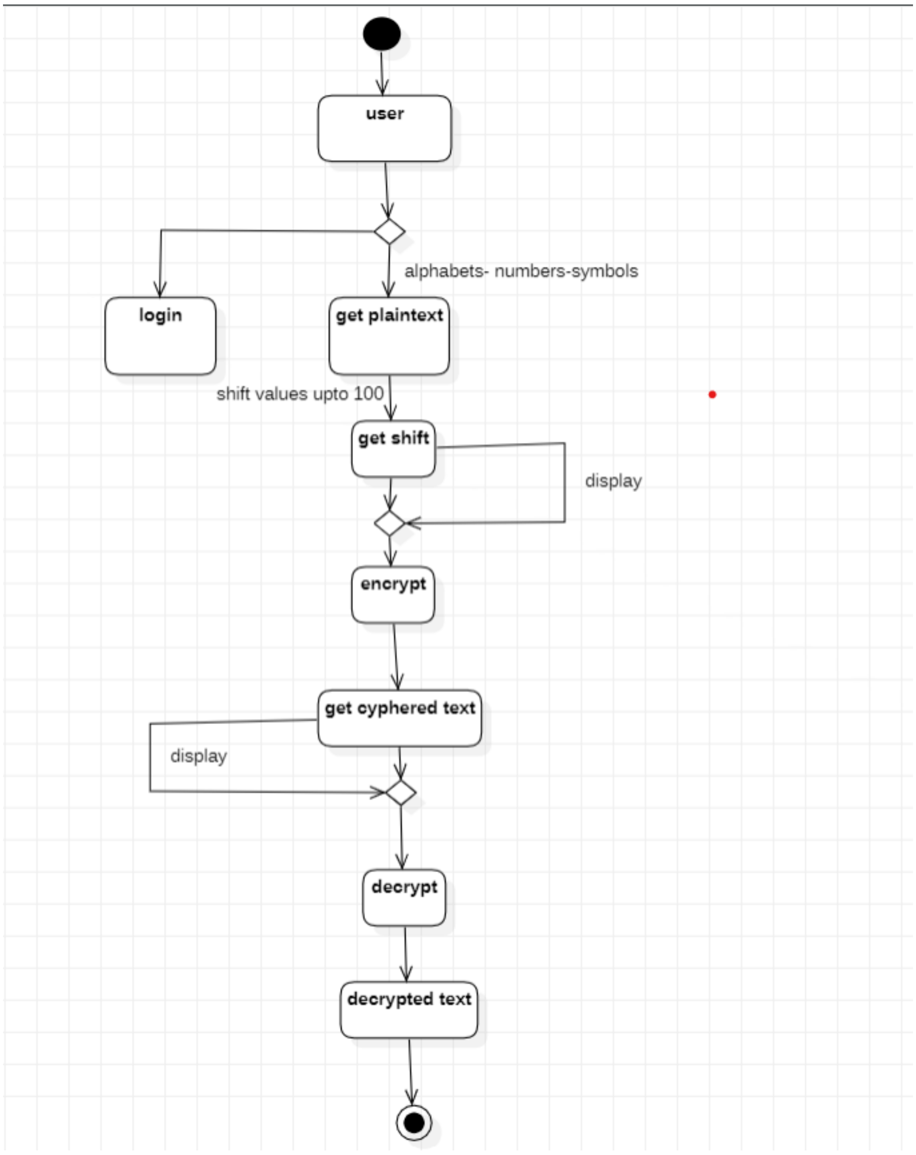


Fig. 9.1.2

9.2.3. SEQUENCE DIAGRAM

In this sequence diagram, the User object creates a new CaesarCipher object and passes a plaintext message to the encrypt () method of the CaesarCipher object. The encrypt () method returns the corresponding ciphertext message, which is then passed back to the User object. The User object then passes the ciphertext message to the decrypt () method of the CaesarCipher object, which returns the corresponding plaintext message.

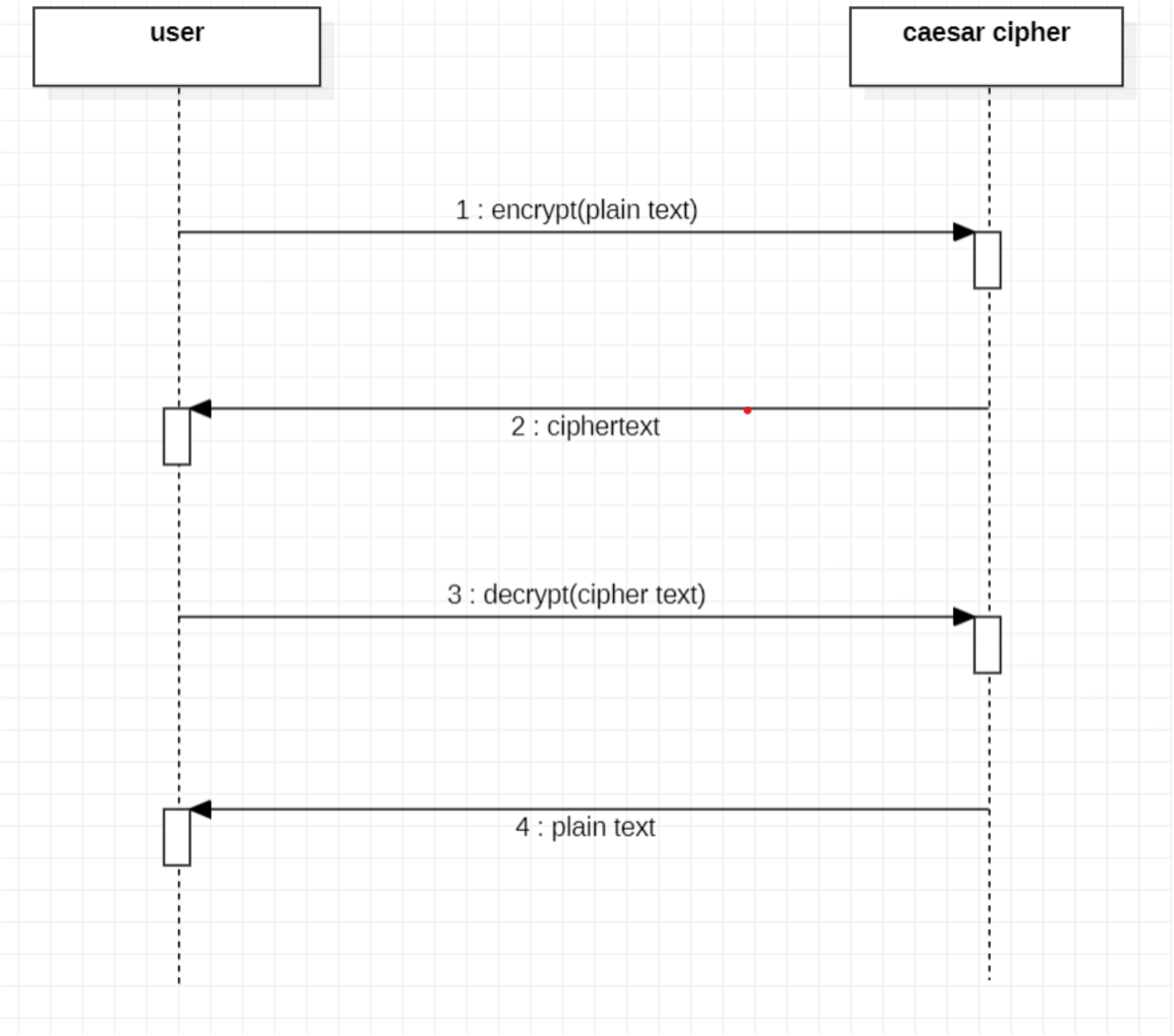


Fig. 9.1.3

9.24. CLASS DIAGRAM

In this class diagram, there are two classes: Caesar Cipher and User. The Caesar Cipher class represents the encryption and decryption algorithm, and the User class represents a user who interacts with the system.

The Caesar Cipher class has a private attribute called shift, which is the number of positions to shift each letter in the plaintext. The class has two constructors: Caesar Cipher () and Caesar Cipher (shift: int). The first constructor creates a Caesar Cipher object with a default shift of 3, while the second constructor allows the user to specify a custom shift value. The class also has two public methods: encrypt (plaintext: str) and decrypt (ciphertext: str). The encrypt () method takes a plaintext string as input and returns the corresponding ciphertext string, while the decrypt () method takes a ciphertext string as input and returns the corresponding plaintext string.

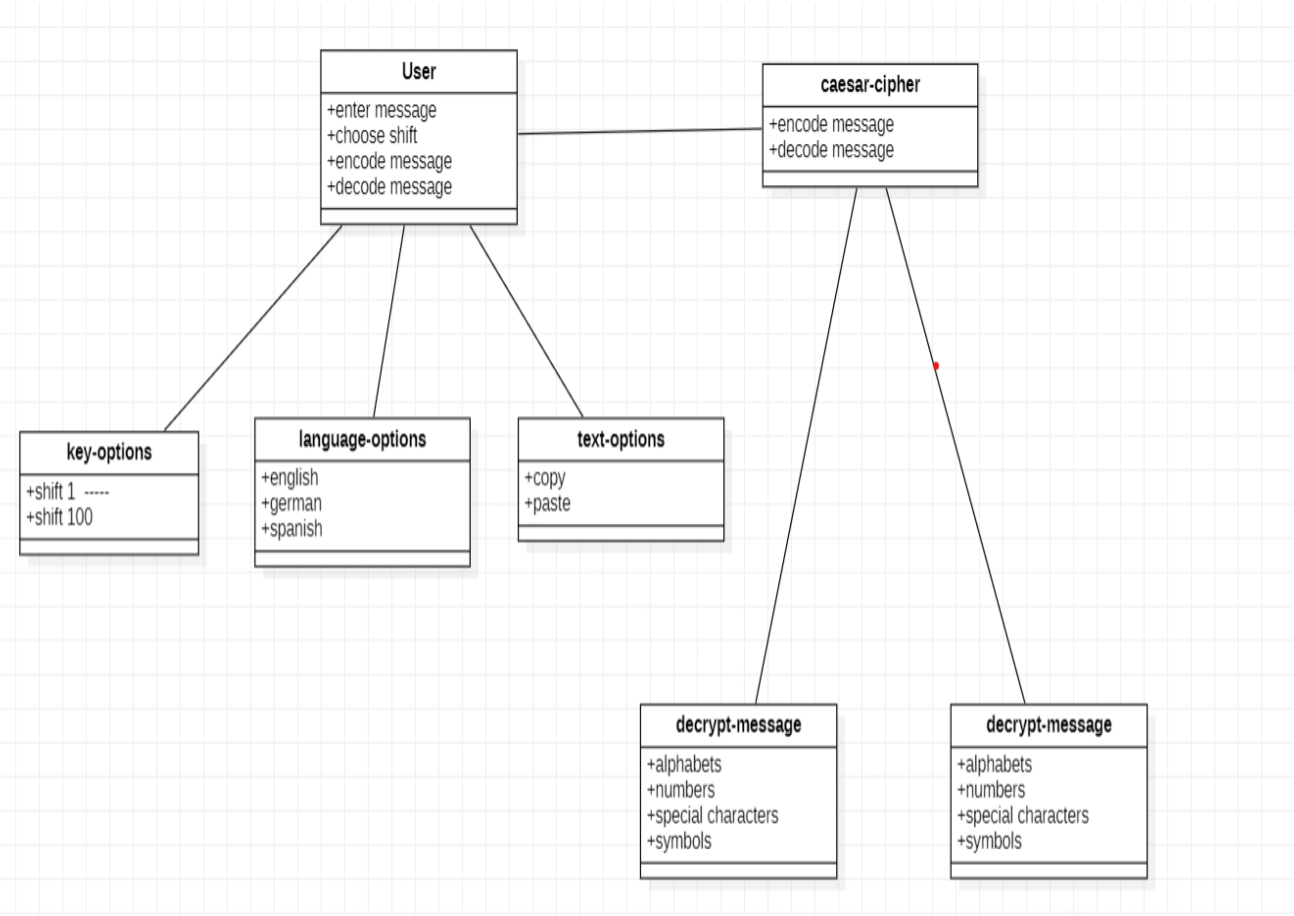


Fig. 9.1.4

9.2. ARCHITECTURE DIAGRAM

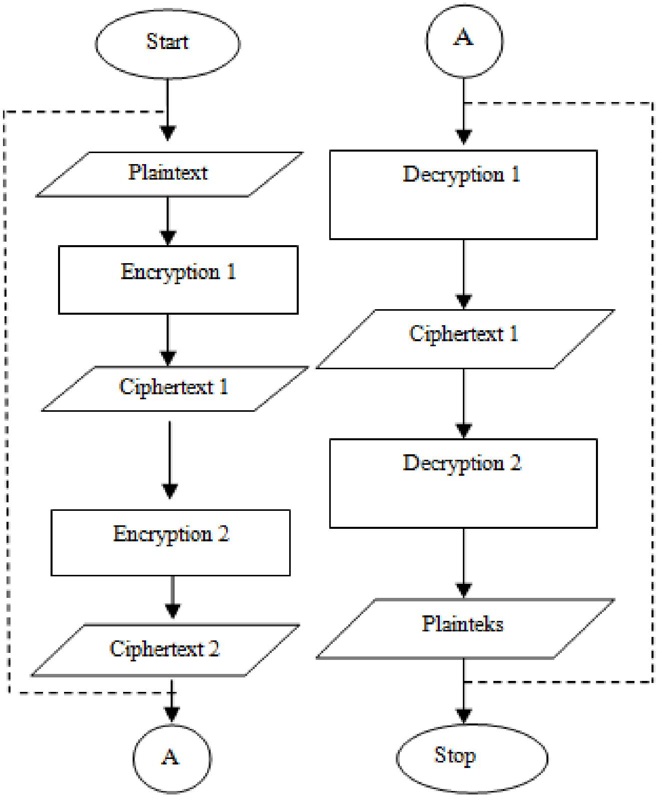


Fig. 9.2

1. **Plain Text**: The actual message is known as plain text.
2. **Cipher Text:** The random stream of data which is un understandable.
3. **Encryption Algorithm:** Process of converting from plain text to cipher text.
4. **Decryption Algorithm:** Process of converting cipher text to plain text.
5. **Key:** It is the algorithm used to encrypt and decrypt the data.

In this architecture diagram, the plaintext is the original message that is to be encrypted. The ciphertext is the encrypted message that is produced by the Caesar cipher. The encryption and decryption functions are represented by the "Encrypt" and "Decrypt" boxes in the diagram. These boxes take the plaintext or ciphertext, respectively, as input, along with a key. In the case of the Caesar cipher, the key is the number of positions to shift each letter.

The encryption function shifts each letter of the plaintext by the key number of positions down the alphabet, wrapping around to the beginning of the alphabet if necessary. The result is the ciphertext. The decryption function works in reverse: it shifts each letter of the ciphertext back up the alphabet by the key number of positions to recover the original plaintext.

Overall, the architecture diagram shows how the Caesar cipher works by taking plaintext as input, encrypting it with a key, producing ciphertext, and then decrypting the ciphertext with the same key to recover the original plaintext.

10. IMPLEMENTATION

10.1. Encryption Module:

This module takes a plaintext message and a key as input and produces the corresponding ciphertext message as output. The module involves shifting each letter of the plaintext message by the key number of positions down the alphabet, wrapping around to the beginning of the alphabet if necessary. This can be implemented using a simple loop that iterates over each character of the plaintext message and applies the key shift operation to each character.

10.2. **Decryption Module:**

This module takes a ciphertext message and a key as input and produces the corresponding plaintext message as output. The module involves shifting each letter of the ciphertext message back up the alphabet by the key number of positions to recover the original plaintext. This can be implemented using the same loop structure as the encryption module, but with the key shift operation in reverse.

10.3. **Key Generation Module:**

This module generates a random key for use with the encryption and decryption modules. In the case of the Caesar cipher, the key is simply a number that represents the number of positions to shift each letter. This can be implemented using a random number generator function that produces a number between 1 and 25, inclusive.

10.4. **Input/Output Module:**

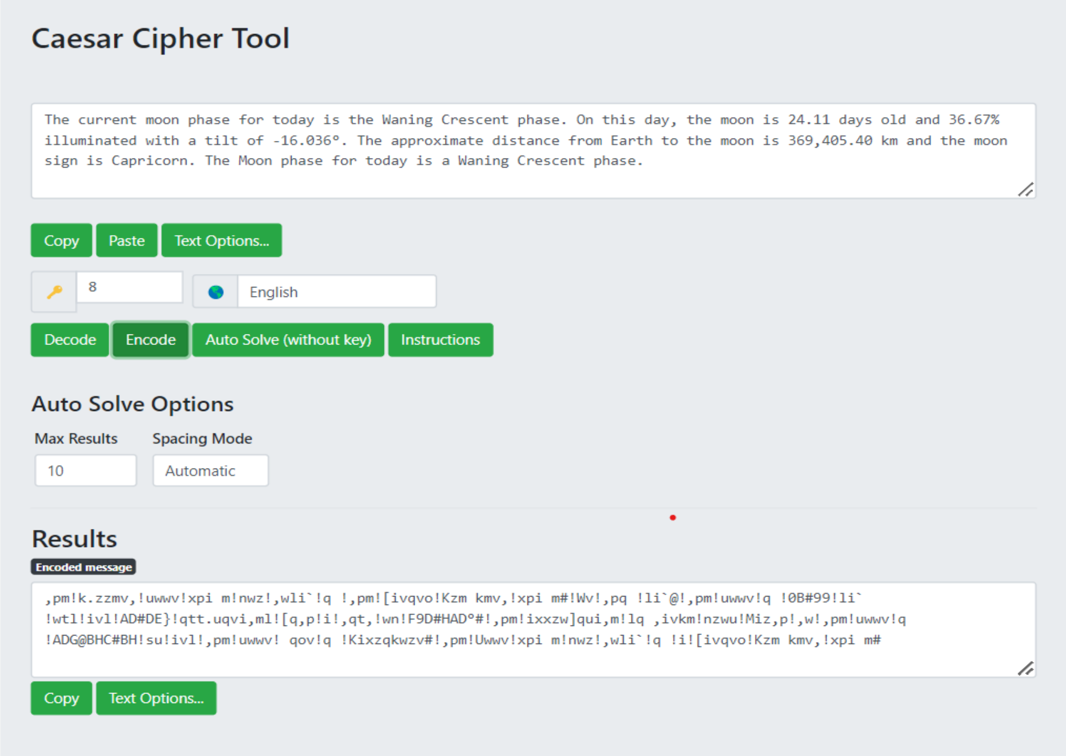
This module handles user input and output. It prompts the user to enter a message and a key for encryption or decryption, calls the appropriate module (encryption or decryption), and displays the result to the user. It can also handle errors such as invalid input (e.g., non-alphabetic characters in the message or an invalid key).

10.5. CODING:

```
#Encoding message

def caesar_cipher(text, shift):
    # Create a dictionary to map each character to its shifted counterpart
    shifted_dict = {}
    for i in range(256):
        shifted_dict[chr(i)] = chr((i + shift) % 256)

    # Add special characters to the dictionary
    shifted_dict[" @"] = "@ "
    shifted_dict["."] = "."
    shifted_dict[","] = ","
    shifted_dict["!"] = "!"
    shifted_dict["%"] = "%"
    shifted_dict["$"] = "$"
    shifted_dict["#"] = "#"

    # Apply the shift to each character in the input text
    ciphered_text = ""
    for char in text:
        ciphered_text += shifted_dict[char]

    return ciphered_text

# Encoding message
plaintext = "Gupta is good boy i like his guts"
shift = 8
encoded = caesar_cipher(plaintext, shift)
print(encoded)

#Decoding message
plaintext = "O}x|i(q{(owwl(jw⍰(q(tqsm(pq{(o}|{"
shift = 8

decoded = caesar_cipher(plaintext, -shift)
print(decoded)
```

10.6. OUTPUT:

#Encoding Message



Caesar Cipher Tool

```
The current moon phase for today is the Waning Crescent phase. On this day, the moon is 24.11 days old and 36.67%
illuminated with a tilt of -16.036°. The approximate distance from Earth to the moon is 369,405.40 km and the moon
sign is Capricorn. The Moon phase for today is a Waning Crescent phase.
```

8

English

Auto Solve Options

Max Results: 10

Spacing Mode: Automatic

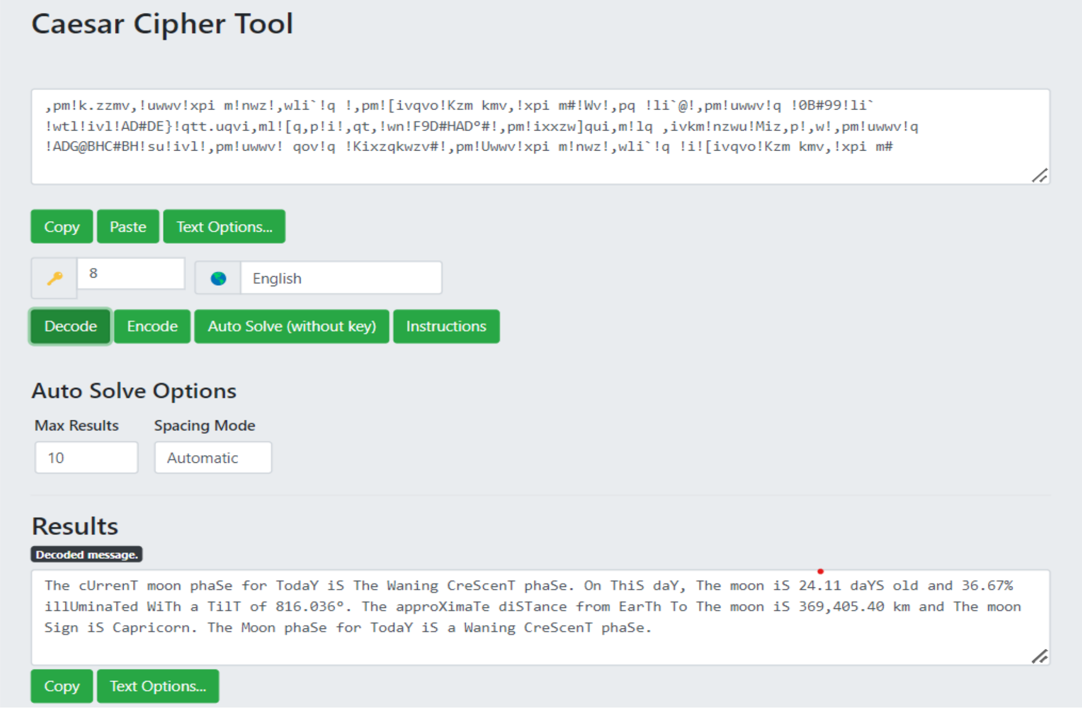
Results

Encoded message

```
,pm!k.zzmv,!uwwv!xpi m!nwz!,wli`!q !,pm![ivqvo!Kzm kmv,!xpi m#!Wv!,pq !li`@!,pm!uwwv!q !0B#99!li`
!wtl!ivl!AD#DE}!qtt.uqvi,ml![q,p!i!,qt,!wn!F9D#HAD°#!,pm!ixxzw]qui,m!lq ,ivkm!nzwu!Miz,p!,w!,pm!uwwv!q
!ADG@BHC#BH!su!ivl!,pm!uwwv! qov!q !Kixzqkwzv#!,pm!Uwwv!xpi m!nwz!,wli`!q !i![ivqvo!Kzm kmv,!xpi m#
```

Fig. 10.6.1

#Decoding Message



Caesar Cipher Tool

```
,pm!k.zzmv,!uwwv!xpi m!nwz!,wli`!q !,pm![ivqvo!Kzm kmv,!xpi m#!Wv!,pq !li`@!,pm!uwwv!q !0B#99!li`
!wtl!ivl!AD#DE}!qtt.uqvi,ml![q,p!i!,qt,!wn!F9D#HAD°#!,pm!ixxzw]qui,m!lq ,ivkm!nzwu!Miz,p!,w!,pm!uwwv!q
!ADG@BHC#BH!su!ivl!,pm!uwwv! qov!q !Kixzqkwzv#!,pm!Uwwv!xpi m!nwz!,wli`!q !i![ivqvo!Kzm kmv,!xpi m#
```

8

English

Auto Solve Options

Max Results: 10

Spacing Mode: Automatic

Results

Decoded message.

```
The cUrrenT moon phaSe for TodaY iS The Waning CreScenT phaSe. On ThiS daY, The moon iS 24.11 daYS old and 36.67%
illUminaTed WiTh a TilT of 816.036°. The approXimaTe diSTance from EarTh To The moon iS 369,405.40 km and The moon
Sign iS Capricorn. The Moon phaSe for TodaY iS a Waning CreScenT phaSe.
```

Fig. 10.6.2

11. 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 project, 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 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.

12. REFERENCES

[1] A.F.A.Abidin, O.Y. Chuan and M.R.K. ariffin-" A Novel enhancement Technique of the Hill Cipherfor 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- "Integrating 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 usingLinear feedback Shift Register "– IJCSNS, Vol.8, No.12, December 2008.