



Sparkling Light Publisher

Sparklinglight Transactions on Artificial Intelligence and Quantum Computing (STAIQC)



Website: <https://sparklinglightpublisher.com/> ISSN (Online):2583-0732

A Novel Approach to Strengthen Additional Layer of Security to Caesar Cipher

Vyshak R^{a,#}, Abdul Shareef Pallivalappil^b.

^{a*} Student in MSc Forensic Science, Jain Deemed to be University, Bengaluru- 560027, Karnataka, India.

^bDigital Forensic Consultant, TalFor, Palace Road, Bangalore, India.

Abstract

We are living in the world of technology where we share our messages to the sender via several messaging applications. While we share the information, we are not aware about how secure our messages are and whether any person can hack the private messages or not. It is obvious when the messaging applications with no security pose great risk to our private information. Cryptography is a technique which is used to hide the information in the form of encryption. This preserves confidentiality, integrity and availability and also provides security and privacy of data to the users. In this study, we have developed a simple approach with an additional layer of security to be added over the Caesar Cipher to enhance the security that can be incorporated with messaging applications.

© 2022 STAIQC. All rights reserved.

Keywords: Messaging, Cryptography, Encryption, Security, Caesar cipher.

1. Introduction

The Caesar Cipher is a type of substitution cipher plain text's alphabet is shifted down by a set amount, with other characters, symbols, and objects being replaced [1]. This method uses a key that moves all of the letters in a piece of text by a specific number of positions. The key to this cypher is a letter that represents the number of shift positions, and this is one of the most basic and extensively used encryption methods. Because each letter is typed in plain text before being replaced by a set number of letters down the alphabet, it's also known as a substitution cipher. Cipher can be easily broken, even in a ciphertext-only context. There are two possibilities can be considered: one attacker is aware that a straightforward swap although cipher has been employed, it is ignorant that it is part of the Caesar scheme, while the other attacker is aware that the Caesar cipher has been used, but has no idea how to pick it.

E-mail address of authors: E-mail: vyshakrj4@gmail.com, abdulshareef.777333@gmail.com.

© 2022 STAIQC. All rights reserved.

Please cite this article as: Vyshak R., Abdul Shareef Pallivalappil., (2022). A Novel Approach to Strengthen Additional Layer of Security to Caesar Cipher. *Sparklinglight Transactions on Artificial Intelligence and Quantum Computing (STAIQC)*, 2(2), 1-7. ISSN (Online):2583-0732. Received Date: 2022/07/20, Reviewed Date: 2022/07/26, Published Date: 2022/08/24.

First, consider the following situation, the techniques can be used to break the encryption similar to those that were previously used to crack a simple substitution cipher where frequency analysis or word pattern analysis are two examples of this type of analysis. An attacker might notice the regularity in the answer while solving and determine what a Caesar cypher is and what algorithm is used. Whereas breaking the approach in the second circumstance is even easier. Because the number of possible shifts is restricted, a brute force assault can be used to test them one by one. One method is to enter a portion of the encrypted text into a table that includes all potential shifts. Another way to look This approach entails supposing that beneath each letter of the ciphertext, starting with that letter, the whole letter is written backwards. These attacks are often accelerated with a set of strips with the alphabet printed backwards. After that, the strips are placed in one row to generate the ciphertext, stand in one of the opposite rows.

Matching the letters' frequency distribution is another brute-force strategy. By graphing the number of times each letter appears in the ciphertext and understanding the plaintext's original language's anticipated distribution of those letters, a person can quickly recognize the monetary worth of the shift by observing the relocation of specific graph's characteristics. Frequency analysis are the terms for this. Computers may also do this by using chi-squared statistics to see how effectively the frequency distribution actually works in accordance with the predicted distribution. There will usually be just one probable decryption for natural language plaintext, while numerous options are possible for extremely short plaintexts. Encrypting a text many times with the Caesar cipher adds no additional security. These are because two encryption schemes (shift A and shift B) are identical confined to one shift encryption with A and B [10].

Various sensitive data is exchanged through the internet, including banking transactions, credit information, and confidential data. There is a huge need for security to protect this type of data. Cryptography is a science and an art producing unreadable only the intended recipients have access to data or ciphers recipient can read them. Encryption is the process of converting data into an unreadable format, and decryption is the opposite of encryption. The original message is Plaintext, and the coded message is Ciphertext. Substitution Technique and Transportation Technique are two encryption approaches that is discussed here. The letters in the simple text are swapped out with new ones, other symbols, or letters in replacement technique. Caesar cipher, hill cipher, monoalphabetic cipher, and so on. On the other hand, in transportation mode, some type of permutation on plaintext is preferred. For instance, the rail fence method, the columnar method, and so on.

These are the main objectives in this study;

- To understand the history of Caesar cipher.
- To understand the usage of Caesar cipher for encryption.
- To show procedures to strengthen the Caesar cipher.

2. Related Work

Several research investigations have been conducted within order to analyzed as well as reduce the attack vector on websites and platforms for social networking, such as WhatsApp, Email, and others, such as Facebook. These studies were successful in raising public awareness about cyber-attacks that occur as a result of insufficient security. These related efforts have contributed to a better knowledge of the situation by impacting security lapse that have made Caesar cipher assaults easier to carry out, such as security, sustainability, motivational factors, and so on.

(Renuka, 2019) This paper uses the columnar transposition cipher and the Caesar cipher are used to encrypt, examine, and differentiate the forwarded data to determine which method is the finest for securely transmitting data [9]. (Lubis, 2017) Modifications to the Caesar cipher will be made combined using cipher for transposition, resulting in thrice enciphers in the observations: first, transposition will be used to protect the produced encipher, later using the second Caesar modification, the transposition result will be encrypted once more, and finally, with respect to second Caesar change, the transposition result will be encrypted again. The transfer of alphabets is determined by the ASCII table rather than the alphabet, before encryption the deciphered will be augmented with characters, the new deciphered text will then be separated into two halves after the addition of characters, deciphered text to be protected and deciphered in the moderation in the Caesar cipher (no encryption). (Singh, 2020) One of the most well-known instances is the Caesar cipher of encryption techniques. The Brute Force Attack, Avalanche Effect, and Frequency Test are all used to analyzed the Delta formation, XOR and Basic type of Caesar cipher [7]. (Limbong, 2017) In the science of encrypting messages, the

Caesar cipher is a traditional and extremely basic approach. This approach has limitations, such as the fact that spaces cannot be encrypted because the algorithm utilizes mod 26, and if the rest of the results are also counted, the output will no longer require encryption. However, learning a fundamental technique of modern cryptography is critical. After that, employing software testers to verify the conversion of plaintext to encrypted text and encrypted text to plaintext (decryption) such as R2010a MATLAB is required in order to make it easier to figure out how cryptography works [6]. (Ismael Imran, 2014) Encryption will be used to make information more difficult to read and secure. In fact, one of the most basic and widely used encryption methods is the Caesar cipher. The encipher employs three steps, each of them involves replacing every single alphabet in the normal text with a predetermined number of alphabetical positions. This ends with the output of this project is enciphered data that can be decoded and made viewable. To summarize, the Ciphertext technique can be used in a variety of ways of encrypted applications which improve quality and safety of data [4]. (Gul) They show in this work how to use multiple keys to improve the security of the Caesar cipher. They don't keep track of the letters in ordinary Caesar cipher, but they will here by using counters equal to the number of English alphabets. They must also find a technique to alert the recipient to the fact that some letters in the plain text have been repeated. This can be accomplished simply counting the letters in plain text [3]. (Omolar, 2014) This study aims to add the corpus of information in the world of traditional encryption through proposing the novel plaintext encrypting with a tweaked proposed method. Utilizing a significant number of cycles and a high range of additional spaces to do several complicated procedures may be required give safety, yet it slows down process. As a consequence, a revised combination of Caesar and Vigenere Cipher is created in this study, Classical ciphers lack the spread and complexity that modern ciphers have [8]. (Verma, 2017) This work proposes a new improved Caesar cipher algorithm in which encryption is not limited to alphabets. The Caesar cipher is a versatile cipher that can encrypt symbols, letters, and numerals. In addition, a new character value table is proposed, which specifies the symbol, character, and digit places in the table. Furthermore, the Caesar cipher is made more complex using the matrix concept, making it difficult for brute force attackers to find the key value [12]. (Jain, 2015) This study contributes to the field by using traditional encryption presenting a reworked and enlarged form of the Caesar cipher that makes use of information science and math skills. To strengthen the effectiveness of this traditional encryption software, the recommended revised method computes randomized ciphers, affine ciphers, and transposition replacement techniques to create a cipher text which is extremely difficult to decipher. In addition to alphabets, it expands all ASCII and enlarged ASCII characters are included in the variety of characteristics which the Ciphertext Technique can encode. The goal of this study is to offer an enhanced Caesar cipher replacement solution that overcomes all of the conventional Caesar Cipher's drawbacks [5]. (Education, 2021) They developed a modified multiple encryption technique for safe communications using Classical Ciphers, Affine Ciphers, and Caesar Ciphers in this study [2]. (Chhabra, 2017) The research of several encryption strategies for data and information security has been conceded in this work [1]. (Suri, 2016) This work acknowledges the investigation of different encryption algorithms for data and information protection. The updated technique is based on the last section's mix of substitution and transposition procedures. The cipher that resulted was given the initials SY, which are the initials of the article's author [11].

3. Purpose

The goal of this document is to offer various ways for improving cipher that substitutes security. We will discuss this in this article on a famous classical procedure with a goal of adding additional layer of security to them. To accomplish this, we combined classical encryption with other techniques. Our recommended solution proved to be superior in terms of increasing the security of any text message. We have used Caesar Ciphers as a representation of Classical Techniques in our investigations. We utilized various ways to make it more secure, such as the divide and conquer approach.

4. Methodology

The source of this study is referred from journals, conference papers, and research articles. The plan of research is how to convert a simple Caesar cipher to more secured, by adding additional layer of security by applying the Divide and Conquer Strategy.

5. Problem faced

After studying several methods, we discovered that encrypting a message with this method is easily exploitable due to the fact that only a few digits' letters are skipped and they're added at the last. However, if we add a few more to it, it becomes a lot more interesting, it is going to prove to be the best technique for encrypting the message.

Substitution Cipher, also known as Simple Caesar Cipher, is a method of encrypting a message by replacing certain characters with others in ordered alphabetically. This study employs a secondary technique in which data is gathered from a variety of international publications published by a variety of writers.

- The alphabets are twisted, the letter after Z is A, here will characterize transformation by making a list of all possible outcomes:

Plain text: - 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

Cipher text: - X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

- Now let's do it numerically.

Plain text: - 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

Cipher text: - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

6. Solution

We noticed in the Caesar cipher a method that we merely delete the numbers of digits 1 to 3, abcd... alphabets etc. However, because it is freely accessible, we use a divide and conquer strategy to secure them after completing the previous steps.

7. Algorithms for Encryption

Use the Caesar cipher approach from before. (Shift 23).

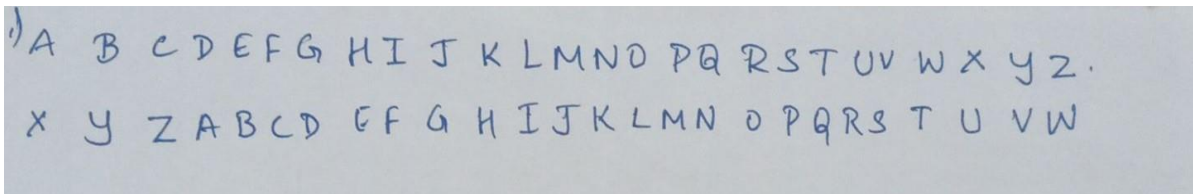


Fig. 1.1

Now do the opposite of what we did before.

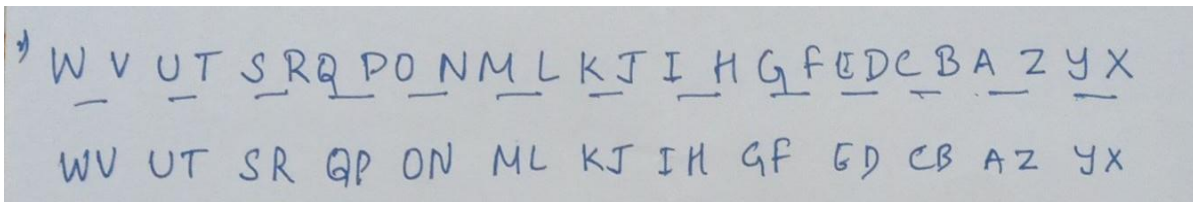


Fig. 1.2

Now scramble this back letter with 2-2 other letters.

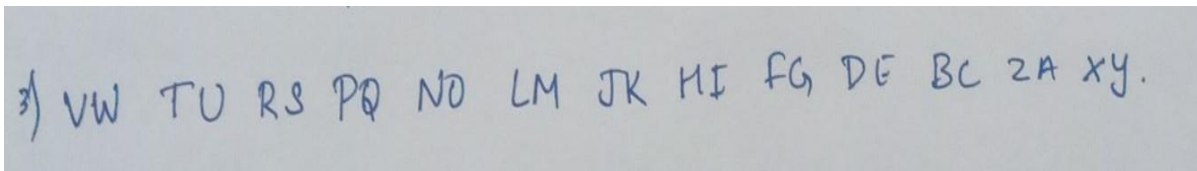


Fig. 1.3

Combine the scrambled letters into a three-letter group and jumble it once more.

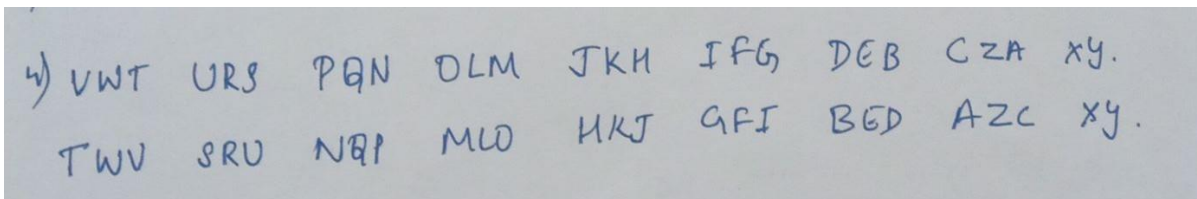


Fig. 1.4

Once completing the step 4 compare with the scrambled letters that it, abcde... further can be analyzed for further coding with applications.

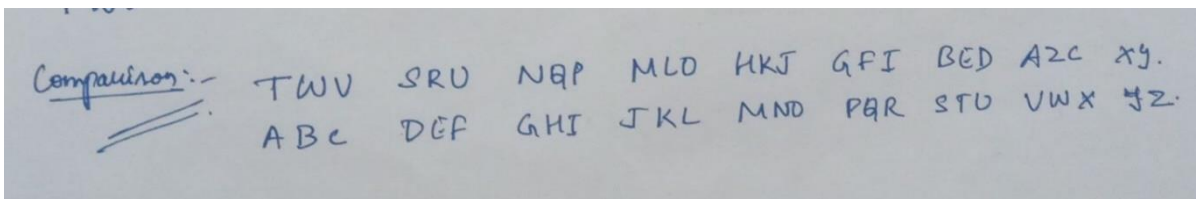
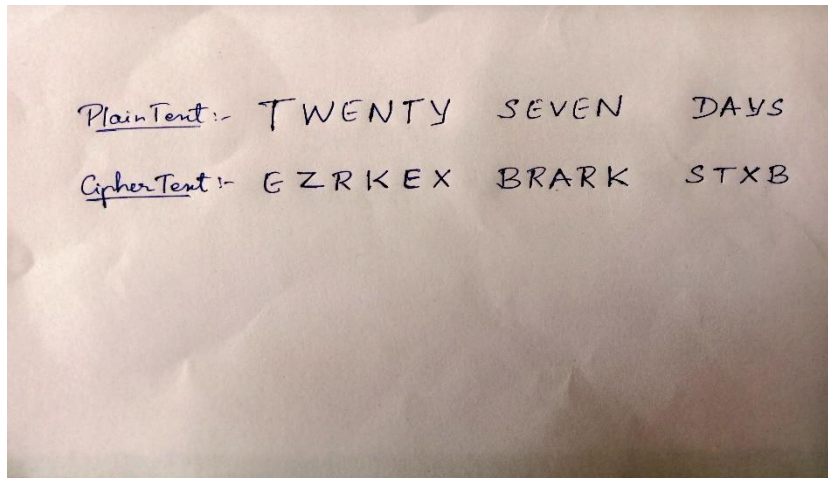


Fig. 1.5

8. Decryption Algorithm

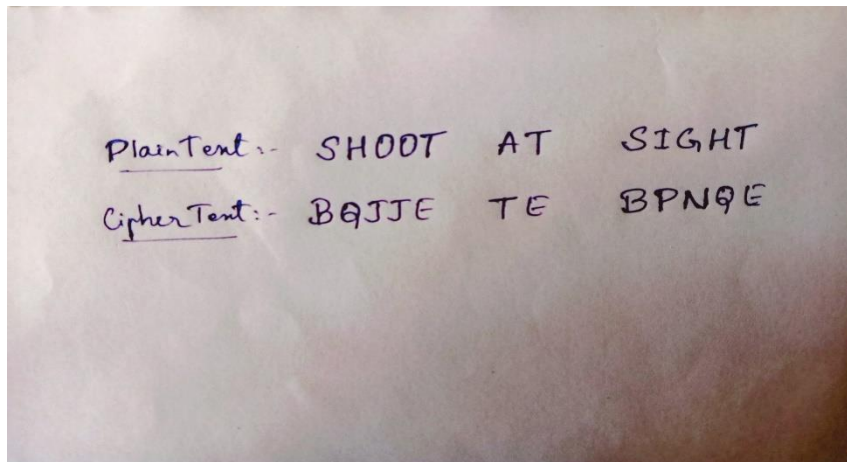
Text and an encryption key are required to encrypt a text using the suggested approach. The encryption key is an integer value that defines the substitution alphabet. It uses to verify that integers are preserved, use modulo twenty-six arithmetic values wrap around when the encryption key is greater than twenty-six. During the encryption process, formed performs reverse operations, which are then followed by decryption. It necessitates the use of a decryption key as well as encrypted content. To achieve reverse character replacement, it is recommended that the decipher key is complementary with respect to encipher key.



Plain Text:- TWENTY SEVEN DAYS
Cipher Text:- EZRKEX BRARK STXB

Fig. 2

In the above image it is observed that Plain text is “TWENTY SEVEN DAYS” and when it is converted to cipher text by using the encryption algorithm which has been explained in the earlier the result would be “EZRKEX BRARK STXB”. So, in this the plain text is converted by using an additional layer of security over the old version of Caesar Cipher.



Plain Text:- SHOOT AT SIGHT
Cipher Text:- BQJJE TE BPNQE

Fig. 3

In the above second image it is observed that the Plain text is “SHOOT AT SIGHT” and when it is converted to cipher text by using the encryption algorithm which has been explained in the earlier the result would be “BQJJE TE BPNQE”. So, in this the plain text is converted by using an additional layer of security over the old version of Caesar Cipher.

9. Importance

One of the most crucial components of computers is security. The best practice is to ensure data transfers are encrypted. The movement of data from one place or host to another host or server is known as data transfer. To provide the essential data transfer security is very crucial in the present times.

10. Conclusion

The study has demonstrated the technique to add additional layer of security to one of the earliest known ciphers in the world, i.e.: the Caesar cipher. This method allows the user to select the decipherable algorithm swiftly and without much difficulty. Adding few additional layers of security will further enhance the security of this cipher technique and can be easily incorporated with several tools. This will also serve as a good resource for easy understanding of cryptography and adding additional layers to existing cipher techniques to enhances security as well.

References

- [1] Chhabra, P. (2017). A Survey on Classic Cipher in Cryptography. 7416-7421.
- [2] Education, M. (2021). A Study on some modified Classical Ciphers for Secure Crypto-System. 5316-5319.
- [3] Gul, N. (n.d.). Enhancing Ceaser Cipher by Using Multiple Keys. 41-46.
- [4] Ismael Imran, P. E. (2014). Enhancement Caesar Cipher for Better Security. *IOSR Journal of Computer Engineering*, 1(1), 01-05.
- [5] Jain, A. (2015). Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. *International Journal of Computer Applications*, 1(1), 6-11.
- [6] Limbong, T. (2017). Testing the Classic Caesar Cipher Cryptography using of Matlab. *International Journal of Engineering Research & Technology*, 1(1), 175-178.
- [7] Lubis, F. I. (2017). Combination of caesar cipher modification with transposition cipher. *Advances in Science, Technology and Engineering Systems*, 1(!), 22-25.
- [8] Omolara, O. E. (2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication Omolara Computer Engineering and Intelligent Systems. *Computer Engineering and Intelligent System*, 1(1), 34-46.
- [9] Renuka, K. (2019). Analysis and Comparison of Substitution and Transposition Cipher. 549-555.
- [10] Singh, R. (2020). A Review Paper on Cryptography of Modified Caesar Cipher.
- [11] Suri, S. (2016). A Proposed Cipher Technique with a Study of Existing Cryptography Techniques. *International Journal of Computer Science and Mobile Computing*, 1(1), 46-53.
- [12] Verma, P. (2017). Diversified Caesar Cipher for Impeccable Security. *International Journal of Security and Its Applications*, 1(1), 33-40.
