American Journal of Electronics & Communication

Abhishek Tripathi et. al., American Journal of Electronics & Communication, Vol. I (4), 13-15

A new Modified method of Cryptography using Caesar Cipher

Abhishek Tripathi
Department of Computer Science
University of Engineering and Management
Kolkata, India
abhishek161199@gmail.com

Jhilam Chakraborty
Department of Computer Science
University of Engineering and Management
Kolkata, India
jhilamchakraborty.2001@gmail.com

Sadia Anzum
Department of Computer Science
University of Engineering and Management
Kolkata, India
anzum.sadia@gmail.com

Sudipta Basu Pal
Department of Computer Science
University of Engineering and Management
Kolkata, India
Sudipta_basu68@yahoo.com

Abstract

Nowadays the modern world depends on connections through the internet brings different teams together. The essential components of communication are sender, medium, and receiver. Data transmission over the internet is not possible without any encryption method due to security issues. Different types of areas like corporate sectors, banking sectors, government sectors, and many other sectors share their data through the internet. Hackers always try to attack the transmitted data and try to recover the data. Various techniques are developed for providing data security. Cryptography is used for the safe transmission of data. Encryption is done at the sender side in cryptography, and decryption is done at the receiver side. In the encryption technique, Caesar cipher is one of the best examples. The analysis of Basic Caesar cipher, Delta formation Caesar cipher, and XOR Caesar cipher is done based on many parameters like Avalanche Effect, Frequency Test, and Brute force attack. The authors of this paper have tried to modify the caesar cipher method, which produces ciphertext that can be read. After that with the new ciphertext that can be read, then cryptanalysis not suspicious of the ciphertext.

Keywords

Substitution, Plaintext, Cryptography, Caesar Cipher, Ciphertext

I. Introduction

The meaning of cryptography is simply hiding of data or information. Hiding mainly provides the security from the attackers [1,2,3].In the case of encryption the Caesar Cipher is one of the simplest and earliest methods of cryptography which was first used by the Roman Emperor Julius Caesar to send secret messages to his army generals[4,5,6]. It is a simple replacement cipher where the plaintext is shifted for a pre-defined number of times. This pre-defined number becomes our key. For instance, with a shift of 1, A would be replaced by B, B would be replaced by C, and so on. The main disadvantage of this cipher is the limited number of keys available. With each language coming with a finite set of letters of the alphabet, the resolution also becomes finite for this reason. So with the English language, there are only 26 keys possible. This way a code breaker will try out each possible key and get the exact plaintext.

In this paper authors have applied a modified approach, instead of conventionally shifting the characters linearly, the characters will be shifted arbitrarily[7,8,9,10]. For this case, the substitution permutation box method will be used. A substitution box would be generated by performing the process of Affine Ciphers [Cipher text = (key1*Plain text)+ key2]. Then the characters would be substituted by their corresponding equivalent values. Also, the Ciphertext is scrambled by alternating the position of the characters randomly to conceal the features of the language. This operation is done using double columnar transposition on the plaintext to be encrypted. This algorithm can encrypt the special characters which the conventional Caesar cipher cannot encrypt.

II. Background Work

Roman dictator Julius Caesar was known to use a method of encryption (currently known as *Caesar Cipher)* to convey confidential messages to his army generals.

In the nineteenth century, it was noticed that the advertisement section in newspapers were used to exchange the encrypted message using this method. Caesar cipher was still in use even as late as 1915. It was also used as a replacement of more complex ciphers that were too difficult to decode.

A. ROT-13:

ROT-13 is a kind of Caesar Cipher that was developed in ancient Rome wherein the shift implemented to encrypt is equal to 13. This cipher, however, does not offer any safety

and hence, can be decoded very easily using the hill-climbing technique.

B. Some Modifications:

Some methods have been proposed by the researchers to improve the security level of the traditional Caesar cipher.
The general monoalphabetic method of encryption is mentioned in the book "A Manuscript of Deciphering Cryptographic Messages" written by scientist Abu Alkindi.
In 2013, Dr. A Padmapriya and Dr. P. Subhasri proposed the method of reverse Caesar cipher encryption using all the 256 ASCII characters.

C. Caesar Cipher and Brute-Force Attack

The Brute force attack is a cryptanalytic method where the cryptanalysis makes a guess of the key and decrypts the ciphertext and if the key is incorrect he simply shifts to the next key in consideration [11,12,13,14]. This method is gone by trial and error.
In 2013 a new method was considered that used a two-level transposition which would employ two-level encryption and decryption. Here the Brute force attack is not conceivable because two different key levels have been used during the process of encryption.

III. Result Analysis

A. Implementation of the modified approach

1) The user enters the password and plaintext in the input.
Plaintext: We will be attacked today
Password: advert

2) The two subkeys will be created key A and Hkey B. At the start the Hkey A is set to 0, and password "advert" is converted into its ASCII equivalent.

3) The Hkey A is updated using the following formula,and this step is continued for all values until the final Hkey A obtained is 1367456.

4) We will takethe mod 5 of ASCII equivalent and add1 to it gives Hkey B:
Hence, Hkey A becomes equal to 1367456 and Hkey B becomes equal to 18465.

5) For the next satep, two substitution tables are created by calling initialize function(). 'Table' and 'inverse table' are the names given to them.

6) Substituting the characters of of plain texrt by the assigned values of the 'table' table the ciphertexts generated.
Plaintext: We will be attacked today
Ciphertext: Q^GBaCzzCNY{Yw\fAXy.

B. Result analysis

For performing cryptanalysis on this caesar cipher algorithm, a message with encryption key 'advert' is taken This algorithm is used for the encryption process and the resultant ciphertext is shown as the output. The decryption can be achieved by using the same encryption key. Now, we are assuming that if someone gets this encrypted text but doesn't know the encryption key. Hence, to decrypt the message he uses many cryptanalysis methods.He uses frequency analysis to decode and decrypt the text. Already we have done frequency analysis with 200 different samples on the text which is encrypted therefore the frequency analysis gives incorrect answers protecting out encrypted text. The characteristics of the English language also have been successfully hidden (like the two or three letter words frequently occurring together, like-is, an, he, she, the, etc.) by using the transposition method, making the level of security, even more, stronger for an the person to take advantage of language characteristics to decipher, as well as the range of each character in the key is increased to 255, therefore it is almost impossible to decipher the text using the brute force attack as instead of only 26 possible key combinations, the possible number of combinations of keys is increased to (key length) ^256.

The comparation with the conventional Caesar Cipher with the modified approach of the same technique is shown in table 1. The following table shows the comparison result between the two methods clearly.

TABLE I. Comparison between Classical Caesar Cipher and the Modified Caesar Cipher when used to encrypt and decrypt a text in English.

Classical Caesar Cipher	**Modified Caesar Cipher**
All the characters are shifted linearly by a constant key.	Each character is shifted by a random number using affine cipher.
The characteristics of the language is respected and maintained.	Characters are spread throughout the cipher text. So the characteristics of the language remains hidden
Easy to implement.	It is more complex hence is comparatively difficult to execute.
Prone to attacks like the frequency analysis attacks.	Impossible to attack using the frequency analysis attack method.
Takes only 26 key combinations, hence it is easy to break using the Bruce Force attack.	It takes (key length) ^256 as the possible key combinations. Hence it becomes difficult to break using Brute Force attack.

IV. CONCLUSION

In this paper, the authors have tried to modify the basic caesar cipher method that produces ciphertext that can be read. The advantage of the new method is with the ciphertext can be read, then cryptanalysis is not considered as suspicious of the ciphertext. This algorithm uses a random approach for the substitution of characters present in the sample text. By performing the methods of cryptanalysis on the new algorithm, it was seen impossible to break it by the methods in question (Frequency analysis and the Brute Force technique). Security provided by this modified algorithm of Caesar Cipher can be further enhanced by using it with one or more different encryption algorithms or by using asymmetric key tactics instead of the symmetric key ones.

ACKNOWLEDGMENT

The authors wish to thank all the professors of the Computer Science Engineering Department UEM, Kolkata, India, for a numbers of fruitful discussions and valuable suggestion to perform the analysis.

REFERENCES

[1] S G Srikantaswamy, Dr. H D Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.

[2] L .c han, n.m. mahyuddin , ”an implementation of caesar Cipher and xor encryption technique in a secure wireless Communication”,ieee confer,encepp.111-116, 2014.

[3] Goyal,Khasis. Kinger, Supriya.Modified Caesar Cipherfor Better Security Enhancement. International Journal of Computer Aplications (975-8887) Volume 73 - No.3 July 2013.

[4] Practical Cryptography Niels Ferguson and Bruce Schneier, John Wiley & Sons, 2003

[5] Applied Cryptography, 2nd edition Bruce Schneier, John Wiley & Sons, 1996

[6] The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography Simon Singh, Doubleday, 1999

[7] Atul Kahate (2009), Cryptography and Network Security, 2nd edition,

[8] McGraw-Hill. http://searchsecurity.techtarget.com/definition/cipher

[9] Stallings, W. (2006), Cryptography and Network Security 4/E., Pearson Education India.

[10] Behrouz A Fourouzan, Debdeep Mukhopadhyay (2010), Cryptography and Network, 2nd edition, McGraw-Hill.

[11] Goyal, Kashish, and SupriyaKinger. "Modified Caesar Cipher for Better Security Enhancement." International Journal of Computer Applications (0975–8887) Volume (2013).

[12] Singh, Ajit, Aarti Nandal, and Swati Malik. "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 2.12 (2012).

[13] Omolara, O. E., A. I. Oludare, and S. E. Abdulahi. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication." Computer Engineering and Intelligent Systems 5.5 (2014): 34-46.

[14] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on. IEEE, 2013.

[15] Disina, Abdulkadir Hassan. "Robust Caesar Cipher against frequency cryptanalysis using bi-directional shifting." Diss. Universiti Tun Hussein Onn Malaysia, 2014.

[16] Purnama, Benni, and AH Hetty Rohayani. "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to be Encrypted." Procedia Computer Science 59 (2015): 195-204.