International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-3, February 2022

An Enhancement to Caesar Cipher using Euler Totient Function

Rajalaxmi Mishra, Jibendu Kumar Mantri

Abstract*: In this modern world every communication including financial transactions are taking place through the open unsecured network. In order to communicate securely through open networks the messages need to be concealed by using the cryptographic methods. The mono alphabetic traditional Cipher is Caesar cipher is the simplest and fairly popular among the available cryptographic algorithms but it is prone to brute force attack and frequency analysis test. In this paper we propose an enhancement to Caesar cipher by using the Euler Totient function to generate the key to encrypt a text file. The Euler Totient function is applied on the total number of lines of the plain text file. The key value is generated from the plain text hence for different plain text the key value is different; this makes it difficult for the adversary to guess the key thus making the encryption scheme robust. It needs to design secured key distribution schemes to be taken up as the extension work of this scheme.

Keywords*: Caesar Cipher, Euler Totient Function, Key Generation Process, Modular Arithmetic.

I. INTRODUCTION

Now a days it becomes essential in our day-today life to exchange information through the open network i.e., Internet. The advancement of technology and digitization facilitates the banking and e-commerce transactions to take place digitally. Consequently the prime concern of the modern digital world is to safe guard the important information from the intruders. The information transmitted through the vulnerable open network can easily be obtained and tampered by the intruders. The messages sent over the open network can be disguised by the help of cryptographic techniques so that the received enciphered message can only be deciphered by the intended recipient [7]. The cryptographic techniques ensure confidentiality of messages along with integrity, authorization and non repudiations. It is the need of the hour to come up with novel efficient methods of cryptography to shield the sensitive and confidential information from the intruders while transmitting through open vulnerable network. Many researchers have proposed amazingly secure and strong cryptographic schemes like Advanced Encryption Standard AES [10,23], Data Encryption Standard (DES) [4,10], Blowfish[11], 3DES[16,17], RSA[10]. These ciphers consume more resources and also the implementation complexity is relatively high. Among the several available cryptographic schemes, the additive cipher also called shift cipher [5] is the most significant, simplest, mono-alphabetic substitution cipher. Caesar cipher is the additive cipher with key value 3, adopted by Julius Caesar to send secret messages to his troops. These ciphers are susceptible to attacks like brute force attack and cipher text only attack since the size of the domain of the key value is too small. The intruder can easily get the key value as the key can take one of the 25 (1-25) values [22].

Numerous researchers have carried out their research work to strengthen the security of Caesar Cipher and proposed several encryption schemes. Atish Jain et. al., proposed [2] which uses a randomized approach to enhance the Security of Caesar cipher. They utilized the concept of randomized substitution along with affine ciphers and transposition ciphers. A complex key generation method is employed to generate two keys from only one key to ensure improved security. B. Bazith Mohammed proposed an encryption scheme [3] which is a combination of Caesar cipher and rail fence cipher. A key generation technique is used to generate the key automatically for the Caesar cipher. It is capable of encrypting the data containing case sensitive alphabets, numbers and special characters. Benni Purnama and Hetty Rohayani AH proposed the method which modifies the Caesar cipher [6] to generate readable cipher text. The alphabet is divided into two groups; the vowels and consonants. The vowels were substituted with vowels and the consonants were replaced with consonants. The crypt-analyst would not get apprehensive of the cipher text as it is readable. Fahrul Ikhsan Lubis et. al., proposed an encryption scheme [9] which combines a modification of Caesar cipher along with the transposition cipher. The operation of encryption was carried out thrice. The Caesar modification cipher is first applied on the plain text then the resultant cipher text is processed with the transposition cipher, and then the Caesar modification cipher is applied again to the encrypted text resulted from the previous step. The Caesar cipher is modified to use the ASCII characters i.e., characters of value between 32 to 126 in ASCII table and the key value is dynamically calculated since the ASCII value of one of the plaintext character is taken as the key value.

Manuscript received on January 15, 2022.
Revised Manuscript received on January 24, 2022.
Manuscript published on February 28, 2022.
* Correspondence Author
Rajalaxmi Mishra, Faculty, College of IT & Management Education CIME, Bhubaneswar (Odisha), India.
Dr. Jibendu Kumar Mantri*, Department of Computer Application, North Orissa University, Baripada, (Odisha), India. Email: jkmantri@gmail.com

For different plaintext, key value is different. Greetta Pinheiro and Shruti Saraf proposed an encryption system [12] by generating the key value from the ASCII value and position value of the corresponding character for encryption and decryption process. It employed multistage encryption on the plain text which certainly improves the security of the plain text and prevents it from brute force attack. Kashish Goyal and Supriya Kinger proposed an encryption scheme in [13] that modifies the Caesar cipher which fixes the key value to one. If the index of the alphabet in the message is even number then alphabet value is incremented by one otherwise the value is decremented by one. A symmetric key encryption method based on modified Caesar cipher [16] was proposed by M. Ilayaraja et. al. It used mathematical principles to translate the plain text message which includes several special characters into secret information. The modification to traditional Caesar cipher algorithm proposed by Prachi Patni [17] used variable key for each character. The encryption process used the variable length key based on the string length, place of character and time of file. At the receiver side, the original message can be generated only if the receiver possesses appropriate decryption key. An encryption scheme [20] was proposed by Shahid Bashir Dar which used the basic encryption techniques of transposition and substitution to encrypt. On Caesar cipher it applied a single columnar transposition and subsequently a double substitution in order to produce a cipher with improved security.

In order to strengthen the Caesar cipher encryption scheme to make it robust, prime importance must be given to the key generation process. The keys can be generated from the plain text by using some mathematical principles. The brute force attack to get the key can be prevented if for different plain text the key values are different. The Caesar cipher method may be enhanced by adding more complexity to the system. In this paper to get better the security of Caesar cipher we proposed an enhanced Caesar cipher which generates the key value from the plain text by using the Euler totient function.

Sh.Ali, M.KhalidMahmood in [19] introduce the notion of totient and hypertotient numbers. It explores the potential links of totient, super totient and hyper totient numbers. A.P. Madushani and P.G.R.S. Ranasinghe in [1] proposed two methods of encryption by using modular arithmetic. It used the Euler's totient function with its intrinsic properties to propose the symmetric ciphers schemes, where the sender and the receiver share a secret key. Sanjeev Kumar Mandal and A R Deepti proposed an encryption scheme [18] which generates the key by using the Euler Totient function.

II. PROCEDURE FOR PAPER SUBMISSION

A. Theoretical backdrop

The key value is same for encryption and decryption in the symmetric key cryptography. The secret key requires to be shared between the communicating parties through a secured channel. The encryption algorithm is applied by the sender to produce the ciphered text C, from the plain text P by using the key K. Then the ciphered text can be transmitted through the open network to the intended recipient. The sender needs to share the secret key with the receiver. At the receiver side the decryption algorithm is applied along with the shared secret key on the cipher text to generate the plain text.

Encryption Algorithm:

Cipher text=Encptionkey (Plain text)

Decryption Algorithm:

Plain-Text = Decryptionkey (Cipher-Text) = Decryptionkey (Encptionkey (Plain -ext))

The classical symmetric key ciphers are largely classified into transposition ciphers and substitution ciphers. The substitution cipher is yet again classified as mono alphabetic substitution cipher and poly alphabetic substitution cipher.

The additive cipher is the mono-alphabetic substitution cipher also called as shift cipher. It uses modular arithmetic for both the encryption and decryption processes.

If the plain text is P, the cipher text is C and K is the secret key shared between sender and receiver, then the Encryption process which generates the ciphered text is

$C=(P + K) \bmod 26$

and the Decryption process which generates the plain text is

$P=(C – K) \bmod 26$

Caesar cipher is an additive cipher which uses 3 as the key value. The encryption process of Caesar cipher to generate the ciphered text is $C = (P + 3) \bmod 26$ and the decryption process of Caesar cipher which produces the plain text is

$P = (C – 3) \bmod 26$

For instance, the plain text "cryptography" is encrypted as "fubswrjdskb"

Euler's phi function also called Euler's totient function is denoted as $\phi(n)$ for the given integer n, it counts number of relative prime integers to n which are positive and less than n.

$\phi(n)$ =count of integers k, for $1 \leq k \leq n$ such that the GCD (n,k) =1

Definition1: For the positive integer $n \geq 1$, $\Phi(n)$ counts the no. of integers which are positive, less than n and also relatively prime to n.

Definition2: The Greatest Common Divisor, GCD(a, b) of two non zero integers a and b is calculated as the largest of all common divisors of a and b. When GCD(a, b) = 1, the non zero integer values a and b are said to be relatively prime.

Definition 3: For $n \geq 1$, $\Phi(n)$ computes the no. of positive integers k, such that k is less than n and GCD (n ,k) = 1 i.e., n and k are relatively prime.

Example1: $\Phi(9) = 6$ because there are the six integers 1, 2, 4, 5, 7 and 8 are relatively prime to 9 also less than 9. Since GCD(9 , 6) = 3, GCD(9 , 3) = 3 and GCD(9 9) = 9, the numbers 3, 6, and 9 are not relatively prime to 9.

Example2: $\Phi (1) = 1$ because the only positive non zero integer less than equal to 1 is 1 itself, and GCD(1, 1) = 1.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Theorem 1: For a prime number p, Φ(p) = p – l, and on the contrary, if for any positive integer p with Φ(p) = p - l, then p is a prime number.

Proof: For a prime number p, each of the positive integer less than p is relatively prime to p.

Φ(p)=p – l as there are p -1 integers less than p and are relatively prime to p.

On the contrary, for any composite number p, d is a divisor of p where 1 < d <p hence p and d are not relatively prime. Out of the p - 1 integers 1 , 2, ..., p – l, there exists at least one integer d which is the divisor of p hence it not relatively prime to p, Φ(p) ≤ p - 2

Therefore, if Φ(p) = p - l , then p ought to be a prime number.

Theorem 2 : Let a be a positive integer and p be a prime.

Then $\Phi(p) = p^a - p^{a-1} = p^{a-1}(p-1)$

Proof: The count of positive integers which are less than p^a and not relatively prime to p is exactly p^{a-l} .The prime number p divides these integers. Hence there are ($p^a - p^{a-1}$) integers relative prime to p^a and less than p^a. Therefore $\Phi(p) = p^a - p^{a-1} = p^{a-1}(p-1)$

Corollary 1: For any two relatively prime positive integers m and n, Φ(m.n)=Φ(m).Φ(n)

Corollary 2: Let $n = p_1^{a1}\, p_2^{a2} \ldots p_k^{ak}$ be the factorization of the positive integer n with prime powers. Then $\Phi(n) = n\left(1-\frac{1}{p1}\right)\left(1-\frac{1}{p2}\right)\ldots\left(1-\frac{1}{pk}\right)$

These results are used in our scheme to calculate the key value i.e Φ(total no. of lines)

B. The proposed Scheme

The key generation method in this scheme involves the calculation of Euler Totient function (Euler phi function) by using theorem 1 and corollary 2 . It also used the line number, word length of the respective word and the position of the plain text character to encrypt the character by extending the concepts of [9],[12] and [17] .

The text file has to be selected for encryption and then the encrypted text file has to be sent to the receiver along with the secret key.

Key Generation Process

The Key generation method first counts the number of lines of the text files. Then it calculates the Euler's Totient function Φ(line_count).

$\text{Key}=\Phi(n) = n\left(1-\frac{1}{p1}\right)\left(1-\frac{1}{p2}\right)\ldots\left(1-\frac{1}{pk}\right)$

Where n=line_count and

n =p1a1 p2a2 ….pkak is factorization of n with prime powers, for n ≥ 0

Encryption Process

The encryption process encrypts the entire text file character by character and creates a cipher text file.

P denoted as the plain text character and C denoted as the cipher text character.

Each character of the plain text file is encrypted by adding its value to its position in the line, word length of the corresponding word, line number.

C1=(P+pos) mod 256

C2=(C1+word_len) mod 256

C3=(C2+line_no.) mod 256

Then the encrypted value C3 is again added with Φ(line_count).

C=(C3+Φ(line_count)) mod 256

Φ(line_count) is the shared secret key.

The cipher text file is then sent to the receiver.

Decryption Process

Each character of the ciphered text file is decrypted by subtracting Φ(line_count) from its value.

P1= (C- Φ(line_count)) mod 256

Then from the computed value from the previous step, its position in the line, word length of the corresponding word, line number is subtracted to get the original plain text character.

P2=(P1 - line_no.) mod 256

P3=(P2 - word_len) mod 256

P=(P3 - pos) mod 256

Φ(line_count) is the shared secret key.

III. RESULT AND DISCUSSION

This scheme encrypts each character of the text file by using the line number, word length, and position along with Φ(line_count) as the key value. As the key value is generated from the plain text, the key is different for different plain text. It is not possible for the attacker to obtain the plain text from the cipher text by guessing the key value.

Frequency Analysis

The crypt analysts carry out the frequency analysis method on the cipher text. To test the effectiveness of our scheme, the frequency analysis of letters is closely observed.

The content of the plain text file is : 1111 2222 333333 44444

The frequency graph of the plain text is given below

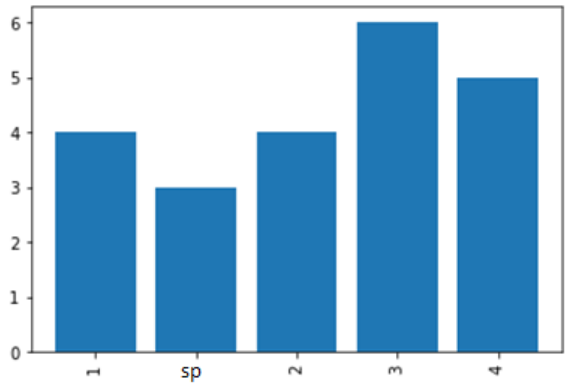

Figure 1: Frequency of plain text

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The content of the ciphered text file is: 789: =>?@ EFGHIJ LMNOP

The frequency graph is

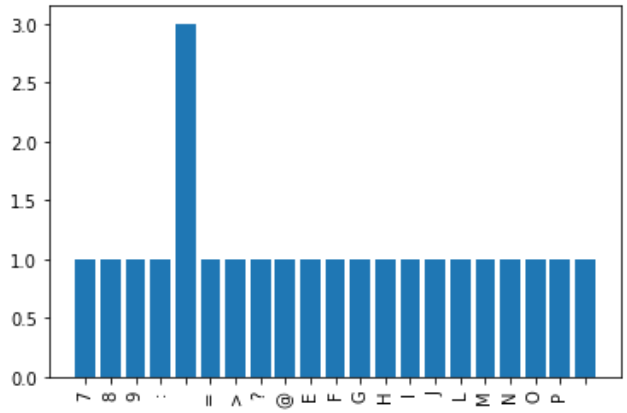

Figure 2 : Frequency of ciphered Text

Another example: figure 3 is the frequency graph of the plain text file

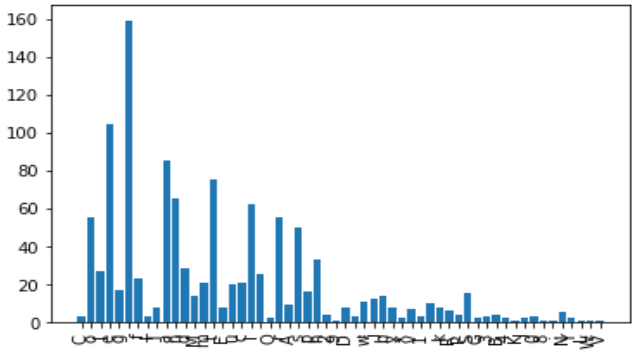

Figure 3: Frequency of plain text

And figure 4 is the frequency graph of the corresponding cipher text file

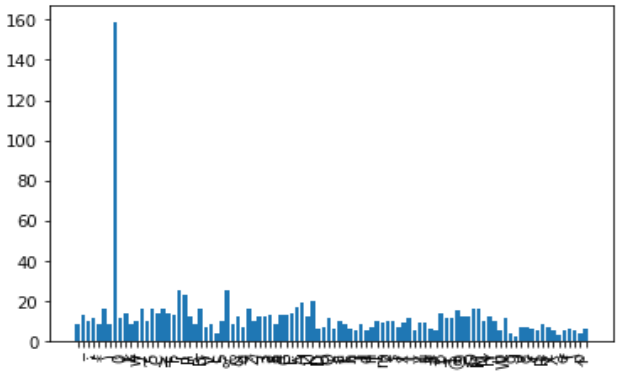

Figure 4: Frequency of ciphered text

From the frequency analysis it is clear that the proposed method eliminates repetition and no trace of it is provided in the cipher text.

IV. CONCLUSION AND FUTURE WORK

This paper proposes an enhancement to Caesar cipher by using modular arithmetic and Euler Totient function. The text in encrypted by using the key which is computed from the plain-text. For different plain-text the key is different. Consequently it is not possible for the intruder to guess the correct key to decrypt. From frequency analysis it is evident that this method eliminates repetition of characters. The key needs to be shared secretly, secure schemes must be proposed for secure key distribution as our future work.

REFERENCES:

1. A.P. Madushani and P.G.R.S. Ranasinghe, (2019) "A symmetric and a transposition cipher using the Euler's totient function", Ceylon Journal of Science 48(4) 2019: 327-330
2. Atish Jain, Ronak Dedhia, Abhijit Patil (2015) "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication", International Journal of Computer Applications (0975 – 8887) Volume 129 – No.13
3. B. Bazith Mohammed (2013) "Automatic Key Generation of Caesar Cipher",International Journal of Engineering Trends and Technology (IJETT) – Volume 6 , ISSN: 2231-538
4. B.Murali Krishna, Habibulla Khan, G.L.Madhumati, K.Praveen Kumar, G.Tejaswini, M.Srikanth, P.ravali (2017) "FPGA Implementation of DES Algorithm Using DNA Cryptography",Journal of Theoretical and Applied Information Technology, Vol.95. No 10, ISSN: 1992-8645
5. Behrouz A. Ferozan, Debdeep Mukhopadhyay (2013) "Cryptography and Network Security",2nd Edition, McGrawHill Education (India) Private Limited.
6. Benni Purnama, Hetty Rohayani.AH (2015) "A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted" Procedia Computer Science, 59, 195 – 204.
7. Bernard Menezes (2011) "Network Security and Cryptography", Cengage Learning, 2nd Edition
8. Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, Tanvi Madhekar, B.S. Thakare (2015) "Brief History of Encryption", International Journal of Computer Applications,Volume 131 – No.9, ISSN: 0975 – 8887.
9. Fahrul Ikhsan Lubis, Hasanal Fachri Satia Simbolon, Toras Pangidoan Batubara, Rahmat Widia Sembiring,(2017) "Combination of Caesar Cipher Modification with Transposition Cipher" Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 22-25.
10. G. Singh(2013) "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security". International Journal of Computer Applications, Vol. 67, No. 19.
11. G. Singh, A.Kumar, K. S. Sandha (2011) "A Study of New Trends in Blowfish Algorithm". International Journal of Engineering Research and Application.
12. Greetta Pinheiro, Shruti Saraf (2016)IJCST Vol. 7, Issue 1, Jan – March, ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print).
13. Kashish Goyal, Supriya Kinger (2013) "Modified Caesar Cipher for Better Security Enhancement", International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013
14. Kenneth H. Rosen (1986)"Elementary Number Theory and lts pplications", Addison-Wesley Publishing Company
15. M. Ilayaraja, K.Shankar, G. Devika(2017) "A Modified Symmetric Key Cryptography Method for Secure Data Transmission", International Journal of Pure and Applied Mathematics, Volume 116 No. 10, 301-308, ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version), Special Issue.
16. Murtada Mohamed Abdelwahab (2018) ,"A Compact Cryptosystem Design of Triple-DES",U of K E J Vol. 8 Issue 1, pp. 25-29
17. Omar G. Abood, Shawkat K. Guirguis "A Survey on Cryptography Algorithms"International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 495 ISSN 2250-3153.
18. Prachi Patni (2013) "A Poly-alphabetic Approach to Caesar Cipher Algorithm " International Journal of Computer Science and Information Technologies, Vol. 4 (6), 954-959, ISSN:0975-9646.
19. Sanjeev Kumar Mandal, A R Deepti (2018) "A Secure Cryptosystem by using Euler Totient Function and Modified RSA" IOSR Journal of Engineering (IOSRJEN, Vol. 08, Issue 10, PP 01-07, ISSN (e): 2250-3021, ISSN (p): 2278-8719
20. Sh.Ali, M.KhalidMahmood (2020) "New Numbers on Euler's Totien tFunction with Applications", Journal of Mathematical Extension, Vol.14, No.1, 61-83, ISSN: 1735-8299.
21. Shahid Bashir Dar (2014) "Enhancing The Security of Caesar Cipher Using Double Substitution Method", International Journal of Computer Science & Engineering Technology Vol. 5 No. 07 Jul 2014, ISSN : 2229-3345
22. Williams Stallings (2000) "Cryptography and Network Security", 4th Edition, Prentice Hall. Pearson.

23. Z. J. Chowdhury,D. Pishva and G. G. D. Nishantha(2010) "AES and Confidentiality from the Inside Out", Advanced Communication Technology (ICACT), 2010 The 12th International Conference on IEEE, Vol. 2, 1587-1591.

AUTHORS PROFILE

Rajalaxmi Mishra, a faculty member in CIME, Bhubaneswar, Odisha, India. Qualification: M.Sc (Statistics), M.Phil(Statistics), M.Tech (Computer Science), Perusing PhD in Computer Application in North Orissa University, Odisha, India. Research Interest is Cryptography and Network Security.

Dr. Jibendu Kumar Mantri, Associate Prof Dept. of Computer Application, North Orissa University. Odisha, India. Qualification: M.Sc M.Phil M.Tech Ph.D. 68 no. of research papers and 8 books already published. Areas of Interest: AI, Business Process Re-engineering, Computer Security. Life Member ISTE, and ISCA. His mailed is: jkmantri@gmail.com