Received: 29 May 2022 | Revised: 18 July 2022 | Accepted: 16 August 2022 | Published online: 23 August 2022

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2024, Vol. 3(1) 8–14
DOI: 10.47852/bonviewJCCE2202261

BON VIEW PUBLISHING

Revisiting Shift Cipher Technique for Amplified Data Security

Raksha Verma[1,*], Anjali Kumari[1], Adarsh Anand[2] and V. S. S. Yadavalli[3]

[1]*Department of Mathematics, University of Delhi, India*

[2]*Department of Operational Research, University of Delhi, India*

[3]*Department of Industrial and Systems Engineering, University of Pretoria, Republic of South Africa*

Abstract: Ever since manual work is overtaken by technology, the rapid advancement in the technologies for performing all kinds of work online has created new possibilities for the organizations and institutions of all types. But this has also created opportunities for attackers and opponents by reducing the powers of existing controls over data sharing. All private, public, and any other sectors are using the internet for sharing their data. Transmission of unencrypted data over the internet is not secure as it poses many privacy concerns as they can be easily hacked and misused by any unintended person. So, everyone is concerned about safe and secure ways of data transmission in order to avoid leak of private data, as hackers always try to chase the transmitted data and to recover it, and therefore various different techniques are developed in order to make data transmission more secure. Encryption is essential to protect and prevent such lapses in the transmission of sensitive information over the internet and any other networks. In this paper, the author has worked on a better version of Caesar cipher and invented a method in which modular arithmetic is used to convert plaintext into ciphertext in order to amplify and to bolster up the security of the sensitive data or information, and the author composed the decryption method in such a way that it is no way related to encryption by involving the divisibility tests and arithmetic modulo.

Keywords: decryption, private key encryption, public key encryption, number theory

1. Introduction

Cryptography is linked with the protection of information communicated through the use of various techniques so that only the right person, whom the data is meant for, can read and process the transmitted data (Pradipta, 2016). It is a way to avoid unauthorized access. It is basically a process which is used to convert the plaintext into a form which is incomprehensible to others except the authorized persons and vice versa (Sharma & Kakkar, 2012). The major need to maintain the confidentiality and integrity of the data which is sent over the network has made it popular nowadays. It emerged from the Greek words "kryptos" and "graphein" which symbolize "secretly hidden" and "to write," respectively (Goyal & Kinger, 2013). In cryptography, the technique of converting the original message into incomprehensible form is known as encryption (Crampton, 2011), whereas decryption is the technique of converting back ciphertext into plaintext (Stallings, 2006).

Using this technique, the transmitted message can be augmented to such an extent that it cannot be altered or misused by any unauthorized person. For example, security of data in the internet banking system is an important issue nowadays that needs to be solved. To augment such type of data, a secured system is needed and encryption–decryption method can be used to protect such data whereby the message is encrypted by the sender by the secret key, which is known only to the receiver (Basu & Ray, 2012). The data is converted into unreadable at sender's side and converted back to readable at the receiver's side (Cao et al., 2006). Confidentiality is the major concern of any type of service that should not be compromised at any cost, i.e. unauthorized people should not be able to alter and misuse the data (Dey et al., 2012). So, in order to maintain the privacy and confidentiality in their communications, government institutions and organizations use different cryptography methods (Koblitz, 1994). Original message can be converted to unreadable form by using several tools of number theory like congruence, properties of primes, and modular arithmetic (Rosen, 2011). Divisibility tests can also play an important role in the encryption of messages.

There are numerous techniques for encryption and decryption that can be categorized into two main groups: symmetric key and asymmetric key cryptography (Dey, 2012). Same key is used for both encryption and decryption in symmetric key cryptography as presented in Figure 1, and DES, 3DES, etc., are its most important algorithms (Thakur & Kumar, 2011). In this technique, users can make changes in the keys, improve them with the help of some algorithms, and can use them in designing new keys, whereas in asymmetric key cryptography, both encryption and decryption are done by two different and independent keys as presented in Figure 2, such as RSA. Furthermore, the asymmetric key encryption techniques are 1000 times slower than symmetric key cryptography, that is, for designing two different keys, they require more evaluative processing power (Kahate, 2003).

*Corresponding author: Raksha Verma, Department of Mathematics, University of Delhi, India. Email: raksha.verma@rajguru.du.ac.in

Figure 1
Private key cryptography

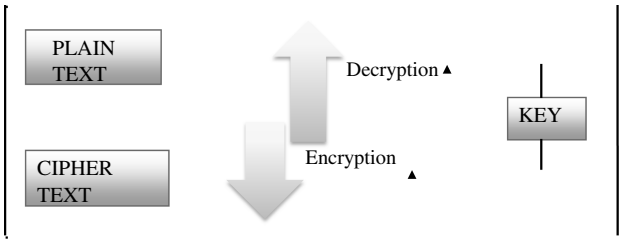
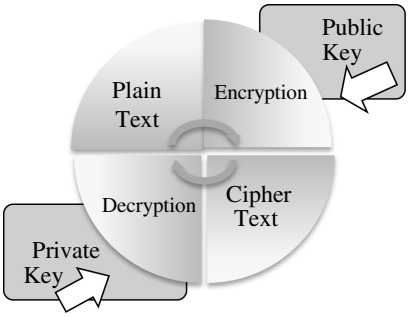


Figure 2
Public key cryptography



The Figure 1 illustrates the private key cryptography as well as the overall process of cryptography where the plaintext is encrypted at the sender side by using an algorithm and key, whereas the ciphertext is deciphered at the receiver's end by using the reverse process.

2. Literature Review

The Caesar cipher technique has a great name and is one of the most popular manual encryption–decryption techniques and is the origin of cryptography (Mishra, 2013). It is manual and the easiest example of a substitution method. In this technique, each alphabet of the given message is substituted by another alphabet which is far from it just by some number of positions in the alphabetic order that will be fixed (Alanazi et al., 2010). This method is named after Julius Caesar. So, to communicate with his officials, he used this method to protect the message and to prevent it from getting leaked in between by any intruder. But, the directness of encryption and decryption of this cipher is its major drawback as one can easily find the algorithm used for encryption without knowing the encryption key and cannot be used in this technology-based 21st century. Another security concern is that there are only 25 possible options of encryption key in this technique which cannot be able to bear the brute force attack (Srikantaswamy & Phaneendra, 2012).

Traditional Caesar cipher technique is very weak which can be easily broken by the brute force attack and accessed by intruders. So, it cannot be used to secure the data and maintain the confidentiality of data over the internet and various networks in this technological era. Nowadays, cryptographers are busy in producing an intelligent cipher, whereas cryptanalysts try to decipher them illegally. The strength, success, and competence of a cryptographic technique fully depend on the fact that how difficult it is to be broken or accessed by an unauthorized person.

So, to innovate a strong and complex cryptographic technique which cannot be altered, misused, and hacked by an unintended person, in the field of data encryption, a lot of work has been done. Below are some proposed algorithms that will give some possibilities regarding the performance of different data encryption algorithms and ideas of combining two different algorithms to make an effective and powerful encryption algorithm.

- (Alanazi et al., 2010) presented an informative comparison between DES, 3DES, and AES and differentiated them on the basis of nine vital factors.
- Saroha et al. (2012) discussed how he has applied the double columnar transposition method on Caesar cipher to strengthen and to make it hard bitten (Goyal & Kinger, 2013).
- Singh et al. (2012) has proposed a method which is a combination of Caesar cipher substitution and rail fence transposition techniques.
- Mathur (2012) has proposed an algorithm that is based on ASCII values of the characters for encryption and decryption. This algorithm is implemented only when the length of key used for encryption and length of input are the same. This method cannot be used for the case where the length of the original message that has to be encrypted and the length of the key used to encrypt the message are not the same which is its major drawback.
- Garg (2012) has stated the need and importance of cryptography for the secure communication of data over various networks and the internet. He has suggested various cryptographic algorithms like public key algorithms and symmetric key algorithms which are used for encryptions.
- Goyal and Kinger (2013) proposed an algorithm which is a betterment of Caesar cipher and where key size is one which is fixed. Firstly in this proposed algorithm, the alphabet index is checked, and if the alphabet index is even, then one needs to either raise the value of the alphabet index by "one" or else reduce its value by "one." The limitation of this algorithm is that if one letter with an even index number and one letter with an odd index number should be deciphered if it is already known, then it will become easy for anyone to determine the encryption algorithm used.
- Goyal (2013) describes cloud computing security issues. In this paper, the authors gave information about the various security issues like confidentiality, web security and email security.
- Senthil et al. (2013) suggested some more additions in the Caesar cipher and Vigenere cipher technique by using some magical tools of mathematics like prime factors, their roots, and their generators.
- Rajan and Balakumaran (2014) has proposed a method which is slightly a modification of Caesar cipher by involving delta formation method. By adding delta formation method to Caesar cipher, it is not easy for the unauthorized person to crack the ciphertext as the character replaced is randomly generated. Brute force attackers will also not be able to crack it.
- Disina (2014) has proposed an encryption method that depends on the position of the bit in the message. According to this method, the sender will transpose the bits of the message by shifting the characters at the even position to the right and characters at the odd position to the left.
- Dar (2014) has demonstrated that by making the function complex, we can enhance its security of the message and protect it from severe attacks. In his paper, he has proposed a method in which double substitution is applied on Caesar cipher to make it secure and protect it from various attacks like brute force attack.
- Gupta (2012) has proposed an algorithm in which he changed the traditional Caesar cipher by interbreeding it with columnar

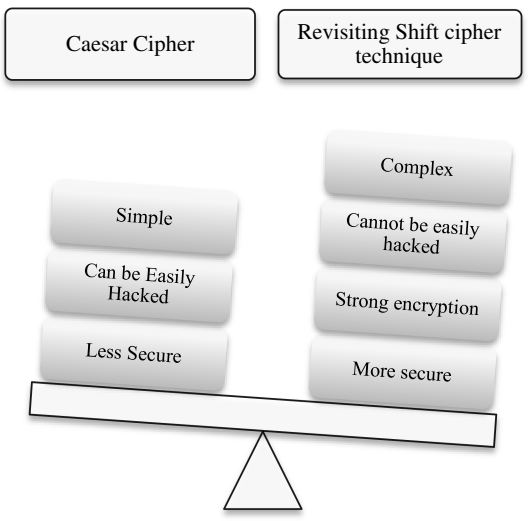
transposition to create a new method to encrypt a message. In this method, he used two different encryption keys for Caesar cipher and for the transposition method. Here, the transformation is done on the encrypted text which is received after applying the traditional Caesar cipher on the original message.

- Omolara et al. (2014) has proposed a modified version of Caesar cipher which is a hybrid of traditional Caesar cipher and Vigenere cipher to increase the diffusion and confusion of ciphertext by using various techniques like xoring keys.
- Purnama and Hetty Rohayani (2015) has proposed a method which is a modification of traditional Caesar cipher where she uses such a method of encryption that the ciphertext generated is legible that will leave the unauthorized users in dilemma whether the text has been encrypted or not.
- Jain et al. (2015) has proposed a method of Caesar cipher substitution in which the characters are shifted randomly by using the substitution and permutation box which is used in DES, etc.
- Verma and Gaba (2016) has represented a modified version of Caesar cipher by adding a new function in it that has strengthened its impact and made it more secure.

3. Comparision Between Caesar Cipher and Revisiting Shift Cipher Technique

Caesar cipher is so effortless as it shifts the encrypted character by a number of positions ahead of it. Another security concern is that there are only 25 possible options of encryption key in this technique which can be easily broken by brute force attack. If we differentiate them on the basis of security, then we will find that the revisiting shift cipher technique is much more efficient in keeping the data secure than the Caesar cipher technique due to its complexity illustrated in Figure 3. The major advantage of revisiting shift cipher over traditional Caesar cipher is that the algorithms used during encryption and decryption of the message are different; they are not converse to each other. So, if the encryption algorithm is leaked by any source, then that would not affect the security of the ciphertext as a different approach is required to decrypt it, whereas in traditional Caesar cipher encryption and decryption processes are converse to each other. As a result, an unauthorized person with the encryption algorithm can easily decode the ciphertext. Revisiting the shift cipher method involves rigorous mathematical tools like modular arithmetic and divisibility tests. Ciphertext produced by this algorithm is strong enough to compete against various attacks by intruders. Its complexity makes it more secure that it can bear the brute force attack without getting hacked.

Figure 3
Comparison between Caesar Cipher and Revisiting Shift cipher technique



4. Proposed Algorithm

Considering the limitations of all algorithms proposed so far, the author has invented a method "Revisiting Shift Cipher Technique" involving the divisibility tests and modular arithmetic and proposed this algorithm to make data more secure and to prevent it from getting hacked.

4.1. Revisiting shift cipher technique

The proposed algorithm requires a plaintext to encrypt the message. It is based on the concept of modulo 26 arithmetic to ensure that the integer value repeats itself in case the key supplied for encryption exceeds 26 (Mishra, 2013). In this method, the private key is "*n*". Decryption follows a different approach and is different from the converse of the process of encryption and requires encrypted text to extract the original message from it. In the proposed method, firstly the alphabet index is multiplied by 3, then shifted by the "*n*" number of positions down the alphabets, and then the encrypted character is replaced by the additive inverse of its index number in Z_{26}. Furthermore, if a hack attempt is made to decode the ciphertext, it would not be easy for the intruder to understand and hack the algorithm involved in encryption.

4.1.1. Encryption algorithm

Step 1: Take the plaintext as input.
Step 2: Multiply the alphabet index by three then shift it by n number of positions ahead of it.
Step 3: Find its additive inverse in Z_{26}.
Step 4: Get the encrypted key as presented in Figure 4 and an example is illustrated in Figure 6 with n =2.

MATHEMATICALLY:

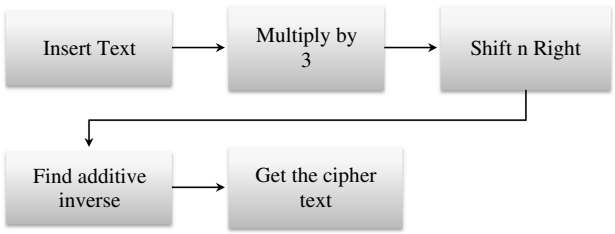
$$C = E(p) = additive\ inverse\ of\ (3p + n) in\ Z_{26}$$

4.1.2. Decryption algorithm

Step 1: Insert the ciphertext.

Step 2: Find the additive inverse of the alphabet index in Z_{26} and decrease the value by n.

Figure 4
Encryption process



Step 3: Then check the alphabet index if the alphabet index is a multiple of three then divide it by three, else if alphabet index is one less than the multiple of three then multiply it by 9 else add twenty six to it and divide by three as presented in Figure 5.

MATHEMATICALLY:

$$P = D(c) = \frac{((-C - n))}{3}$$

$$C \text{ is a multiple of } 3$$

$$D(C) = 9(-C - n)$$

$$\text{if } C \text{ is one less than the multiple}$$

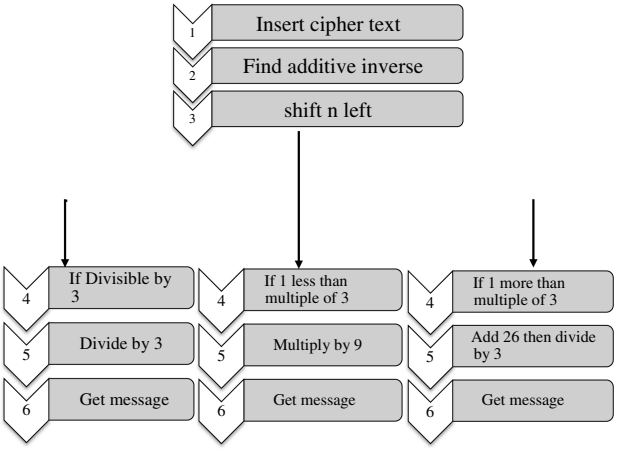
$$\text{of } 3$$

else

$$D(C) = \frac{(-C - n) + 26}{3}$$

$$\text{where} - C \text{ is the additive inverse of } C \text{ in } Z_{26}$$

Figure 5
Decryption process



4.2. Mappings

Table 1
The mapping of numbers with uppercase letters

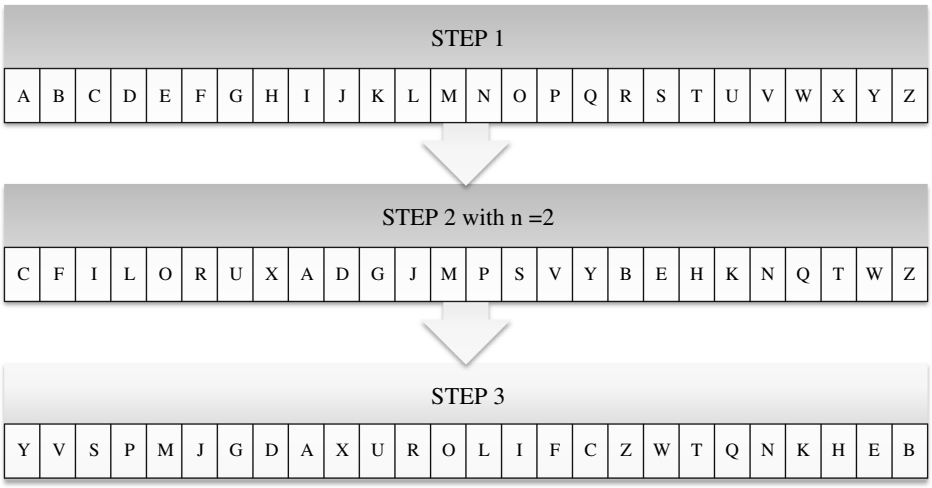
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2
The mapping of numbers with lowercase letters

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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The above Table 1 and Table 2 show the index numbers of alphabets starting from A = 0 to Z = 25.

Figure 6
Steps for encrypting a message with $n = 2$



The Figure 6 shows the steps that need to be followed for encrypting a message. In step-1, the alphabet's index number is multiplied by 3 and $n = 2$ is added to it in step-2, then in step-3 its additive inverse was calculated.

Figure 7
Cipher text for uppercase and lowercase letters for $n = 2$

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
Y	V	S	P	M	J	G	D	A	X	U	R	O	L	I	F	C	Z	W	T	Q	N	K	H	E	B
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
y	v	s	p	m	j	g	d	a	X	u	r	o	l	i	F	c	z	w	t	q	n	k	h	e	b

The Figure 7 shows the cipher text for each uppercase and lowercase letters after encrypting it with the revisiting shift Caesar cipher method for $n = 2$.

5. Experimental Results

5.1. Examples

5.1.1. Encryption

Example 1 with $n = 2$

Plaintext : Computer
Ciphertext: Siofqtmz

We get "Siofgtmz" as ciphertext since by the algorithm the value "C" that is 2, is multiplied by 3, and we have to add 2 and find its additive inverse using the algorithm and we get "S" as ciphertext of "C". In the same way, "i" became the ciphertext of "o", "o" became the ciphertext of "m", "f" became the ciphertext of "p", "q" became the ciphertext of "u", "t" became the ciphertext of "t", "m" became the ciphertext of "e", and "z" became the ciphertext of "r".

Example 2 with $n = 3$

Plaintext :	Number
Ciphertext :	kpnulc

We get "Crlgfs" as ciphertext since by the algorithm the value "N" that is 13, is multiplied by 3, and we have to add 3 and find its additive inverse using the algorithm and we get "k" as ciphertext of "N". In the same way, "p" became the ciphertext of "u", "n" became the ciphertext of "m", "u" became the ciphertext of "b", "l" became the ciphertext of "e", and "c" became the ciphertext of "r".

Example 3 with $n = 1$

Plaintext :	Good
Ciphertext :	Hjjq

We get "Hjjq" as ciphertext since by the algorithm the value "G" that is 6, is multiplied by 3, and we have to add 1 and find its additive inverse in z_{26}. Using the algorithm, we get "H" as ciphertext of "G". In the same way, "r" became the ciphertext of "u", "j" became the ciphertext of "o", and "q" became the ciphertext of "d".

Example 1 with $n = 2$

Ciphertext : Siofqtmz
Plaintext: Computer

5.1.2. Decryption

We get "Computer" as plaintext because according to algorithm "S" that is 18, we have to find its additive inverse in z_{26} which is "H" that is 8 and we have to subtract 2 as per algorithm and we get 6 which is a

multiple of 3 so we have to divide it by 3, and we get 2 that is "C" as the plaintext of "S". When we apply the algorithm on "I" that is 8, we get "q" that is 18 as its additive inverse in z_{26} then we subtract 2 from it and we get 16 which is one more than the multiple of 3. So, according to the algorithm, we added 26 to it and then divide the sum by 3 and get "o" that is 14 as the plaintext of "i". Similarly, we got "m" as the plaintext of "o", "p" as the plaintext of "f", "u" as the plaintext of "q", "t" as the plaintext of "t", "e" as the plaintext of "m", and "r" as the plaintext of "z".

Example 2 with $n = 3$

Ciphertext : Jpnulc	
Plaintext : Number	

We get "Number" as plaintext because according to algorithm "k" that is 10, we have to find its additive inverse in z_{26} which is "O" that is 16 and we have to subtract 3 as per algorithm and we get 13 which is one more than the multiple of 3 so we have to add 26 to it and divide it by 3, and we get 13 that is "N" as the plaintext of "J". In the same way, "u" became the plaintext of "r". When we apply the algorithm on "p" that is 15, we get "l" that is 11 as its additive inverse in z_{26} then we subtract 3 from it and we get 8 which is one less than the multiple of 3. So, according to the algorithm we multiply it by 9 and reduce it in modulo 26 and get "u" that is 20 as the plaintext of "p". Similarly, we got "m" as the plaintext of "n", "b" as the plaintext of "u", "e" as the plaintext of "l", and "r" as the plaintext of "c".

Example 3 with $n = 1$

Ciphertext :	Hjjq
Plaintext :	Good

We get "Good" as plaintext because according to algorithm "H" that is 7, we have to find its additive inverse in z_{26} which is "T" that is 19 and we have to subtract 1 as per algorithm and we get 18 which is a multiple of 3 so we have to divide it by 3, and we get 6 that is "G" as the plaintext of "J". When we apply the algorithm on "j" that is 9, we get "r" that is 17 as its additive inverse in z_{26} then we subtract 1 from it and we get 16 which is one more than the multiple of 3. So, according to the algorithm we added 26 to it and then divide the sum by 3 and get "o" that is 14 as the plaintext of "j". Similarly, we got "d" as the plaintext of "q".

6. Conclusion and Scope of Future Work

The important aspect of data transmission is the security of the data that should not be compromised. This paper presents a remodeled shift cipher which is a slight transformation of the Caesar cipher to vanquish all the weaknesses and drawbacks of the Caesar cipher. The use of the internet and network is rapidly growing. So, it has become mandatory that the transmission of data over various networks using different services should be secure. The proposed algorithm uses the modular arithmetic and divisibility tests to encrypt and decrypt the data to increase the strength of security that ultimately reduces the chances of message to be decoded by any unauthorized body. On performing the cryptanalysis on the modified algorithm, it is found impossible to break it using frequency analysis. This algorithm is strong enough that it cannot be decoded by the brute force approach as there is a high percentage of confusion of use of divisibility tests that make it a strong cipher and unbreakable. It provides a higher degree of secure data encryption of data than Caesar cipher. The security provided by this algorithm can be increased by using it with one or more different algorithms like Playfair which is one of the strongest encryption techniques that is based on the matrix approach. Combination of revisiting shift cipher and Playfair cipher no doubt will make a strong algorithm for cryptography, and a lot of work can be done to enhance them as well. Future work will explore various developments in Playfair cipher and Caesar cipher for a better and crack-proof encryption scheme.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

References

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. *arXiv Preprint*:1003.4085. https://doi.org/10.48550/arXiv.1003.4085

Basu, S., & Ray, U. K. (2012). Modified playfair cipher using rectangular matrix. *International Journal of Computer Applications*, *46*(9), 28–30.

Cao, J., Liao, L., & Wang, G. (2006). Scalable key management for secure multicast communication in the mobile environment. *Pervasive and Mobile Computing*, *2*(2), 187–203. https://doi.org/10.1016/j.pmcj.2005.11.003

Crampton, J. (2011). Time-storage trade-offs for cryptographically-enforced access control. In *Computer Security–ESORICS 2011: 16th European Symposium on Research in Computer Security*, *16*, 245–261. https://doi.org/10.1007/978-3-642-23822-2_14

Dar, S. B. (2014). Enhancing the security of Caesar cipher using double substitution method. *International Journal of Computer Science & Engineering Technology, 5*(7), 772–774. http://www.ijcset.com/docs/IJCSET14-05-07-033.pdf

Dey, S., Nath, J., & Nath, A. (2012). An advanced combined symmetric key cryptographic method using bit manipulation, bit reversal, modified Caesar cipher (SD-REE), DJSA method, TTJSA method: SJA-I algorithm. *International Journal of Computer Applications*, *46*(20), 46–53.

Dey, S. (2012). SD-AREE: An advanced modified Caesar Cipher method to exclude repetition from a message. *International Journal of Information & Network Security*, *1*(2), 67–76.

Disina, A. H. (2014). *Robust Caesar Cipher against frequency cryptanalysis using bi-directional shifting.* Master's Thesis, Universiti Tun Hussein Onn Malaysia.

Garg, P. (2012). A review paper on cryptography and significance of key length. *International Journal of Computer Science and Communication Engineering*.

Goyal, K., & Kinger, S. (2013). Modified caesar cipher for better security enhancement. *International Journal of Computer Applications*, *73*(3), 26–31. https://doi.org/10.5120/12722-9558

Goyal, K. (2013). Security concerns in the world of cloud computing, *International Journal of Advanced Research in Computer Science*, *4*(2), 230.

Gupta, D. K. (2012). New concept of symmetric encryption algorithm: A hybrid approach of Caesar cipher and columnar transposition multi stages. *Journal of Global Research in Computer Science*, *3*(1), 60–66.

Jain, A., Dedhia, R., & Patil, A. (2015). Enhancing the security of Caesar cipher substitution method using a randomized approach for more secure communication. *International Journal of Computer Applications*, *129*(13), 6–11. https://doi.org/10.5120/ijca2015907062

Kahate, A. (2003). *Cryptography and network security.* USA: McGraw-Hill, Inc.

Koblitz, N. (1994). *A course in number theory and cryptography.* Germany: Springer-Verlag.

Mathur, A. (2012). A research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. *International Journal on Computer Science and Engineering*, *4*(9), 1650–1657.

Mishra, A. (2013). Enhancing security of caesar cipher using different methods. *International Journal of Research in Engineering and Technology, 2*(9), 327–332.

Omolara, O. E., Oludare, A. I., & Abdulahi, S. E. (2014). Developing a modified hybrid Caesar cipher and Vigenere cipher for secure data communication. *Computer Engineering and Intelligent Systems*, *5*(5), 34–46.

Pradipta, A. (2016). Implementation methods Caesar cipher alphabet compound in cryptography for information security. *Indonesian Journal on Networking and Security*, *5*, 16–19.

Purnama, B., & Hetty Rohayani, A. H. (2015). A new modified caesar cipher cryptography method with legible ciphertext from a message to be encrypted. *Procedia Computer Science 59*, 195–204. https://doi.org/10.1016/j.procs.2015.07.552

Rajan, A., & Balakumaran, D. (2014). Advancement in Caesar cipher by randomization and delta formation. In *International Conference on Information Communication and Embedded Systems, 1–4. https://doi.org/10.1109/ICICES.2014.7033998*

Rosen, K. H. (2011). *Elementary number theory*. UK: Pearson Education.

Saroha, V., Mor, S., & Dagar, A. (2012). Enhancing security of Caesar Cipher by double columnar transposition method. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(10), 86–88.

Senthil, K., Prasanthi, K., & Rajaram, R. (2013). A modern avatar of Julius Ceasar and Vigenere cipher. In *2013 IEEE International Conference on Computational Intelligence and Computing Research*, 1–3. https://doi.org/10.1109/ICCIC.2013.6724170

Sharma, G., & Kakkar, A. (2012). Cryptography algorithms and approaches used for data security. *International Journal of Scientific & Engineering Research*, *3*(6), 1–6.

Singh, A., Nandal, A., & Malik, S. (2012). Implementation of Caesar cipher with rail fence for enhancing data security. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(12), 78–82.

Srikantaswamy, S. G., & Phaneendra, H. D. (2012). Improved Caesar cipher with random number generation technique and multistage encryption. *International Journal on Cryptography and Information Security*, *2*(4), 39–49.

Stallings, W. (2006). *Cryptography and network security*. UK: Pearson Education.

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International Journal of Emerging Technology and Advanced Engineering*, *1*(2), 6–12.

Verma, P., & Gaba, G. S. (2016). Extended Caesar cipher for low powered devices. *International Journal of Control Theory and Applications*, *9*(11), 5391–5400.

How to Cite: Verma, R., Kumari, A., Anand, A., & Yadavalli, V. S. S. (2024). Revisiting Shift Cipher Technique for Amplified Data Security. *Journal of Computational and Cognitive Engineering, 3*(1), 8–14. https://doi.org/10.47852/bonviewJCCE2202261