kriativ.tech

Edição Nº 9 – 22-01-2023
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2022-06-80

Enhancing Caesar's Cipher

Antonio Santos
Assistant Professor at ISTEC – asisanto@my.istec.pt

Abstract: *Before the invention of computers all methods were calculated manually, and as such the cryptographic methods developed during that period took this limitation into account. The Caesar Cipher method was one of the first to be used and disseminated in several countries. This method is very simple, which means that with current means you can break your security quickly and easily. However, it has a characteristic that, given its nature, any change to the method increases its safety, and like other authors in this article, it will be shown that a small change will imply some improvement in the method's safety; transforming the monoalphabetic substitution Caesar cipher into a polyalphabetic substitution cipher with a key created from the displacement element (key) supplied by the user.*

Keywords: *Encryption, Substitution cipher, Monoalphabetic, polyalphabetic, Caesar cipher, Vigenère cipher.*

I. Introduction

In current times, the pandemic has shown that the use of new communication technologies is a sustainable way of continuing to carry out their activities. It can even be said that the pandemic came to serve as a lever for some people and companies that were resisting to join the majority of companies and people who had already turned to the internet as a main communication channel for their business, learning and recreational. Teleworking, shopping, home banking, eLearning, text messages, games, streaming, etc., are already part of most people's vocabulary and everyday life. And as what is popular is always used by criminals who take advantage of the weaknesses of others to take economic advantage or not, communications companies and not only began to take measures to ensure this security and began to use/develop techniques that until then they were only used for military purposes and have now been placed at the service of the common citizen, cryptography. Referring [1], they refer that historically, the biggest users of cryptography were military organizations and governments, nowadays, it is everywhere. In other words, encryption is nothing new today but has been used for thousands of years to help provide confidential communications between mutually trusted parties [2].

On the other hand, when people communicate, and based on messages in text form, they can be transmitted in terms of their form: clear text, stenography and cryptography. The clear text as being the text in natural language, or according to Holden [3] states that the clear text is the text of the message in ordinary language, on the other hand, Kahate [4] defines this as the text that can be understood by anyone who knows the language, as long as the message is not encoded in any way. Stenography can be defined as the concealment of the message, Kipper [5] describes this as writing hidden in plain sight. Finally, Holden [3] writes that stenography consists in hiding the very existence of the message. With regard to cryptography, it is understood as the basic text encoding, so that unwanted people do not have access to the content. According to Kahate [4] cryptography is the art of obtaining security by encoding messages to make them unreadable, while Paar and Pelzl [6] go further, stating that nowadays cryptography is the science of secret writing with the objective to hide the meaning of a message. And last but not least, Delfs and

Knebl [7] define cryptography as the science of science of keeping secrets. Cryptography has moved from a heuristic set of tools concerned with ensuring secret communication between the military to a science that helps protect systems for ordinary people around the world. It also means that cryptography has become a central topic in computer science [1].

Cryptography, according to Aggarwal [8], is divided into two categories depending on the type of security keys used to encrypt/decrypt data, these techniques are: asymmetric and symmetric encryption. Symmetric or single-key encryption uses the same key to encrypt and decrypt. With this type of encryption, both the sender and the receiver know the same secret code, called a key. Messages are encrypted by the sender using the key and decrypted by the recipient using the same key [9]. Stallings [10] also writes that symmetric cryptography is a form of cryptosystem in which encryption and decryption are performed using the same key. Asymmetric cryptography according to Shrivastava et al. [9], also called public-key cryptography, uses a pair of keys to encrypt and decrypt. With public-key cryptography, keys work in combined public and private key pairs. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. As these keys only function as a pair, encryption initiated with the public key can only be decrypted with the corresponding private key.

Cryptography, in addition to being of the two types mentioned above, uses two techniques: transposition and substitution [11]. Transposition ciphers scramble the letters of the message in a way designed to confuse the attacker but can be undone by the intended recipient [12]. On the other hand, Singh [11] writes that in the transposition, the letters of the message are simply reorganized, effectively generating an anagram. Whereas Kahate [4] in the substitution technique, the characters of a plain text message are replaced by other characters, numbers or symbols.

The term cipher can be defined as another word for the definition of algorithm [13]. Generally speaking, ciphers are simpler forms of algorithms than those used today. Many of the initial cipher were very easy to decipher. Nowadays, the principles that were developed in the old ciphers are used, however, with evolution, a lot of complexity has been implemented in order to make the message safer and more difficult to break. In other words, Kahate [4] writes that ciphertext is the result when plain text is encoded using any suitable scheme.

II. Background

The art of cryptography was born hand in hand with the art of writing. As civilizations evolved, human beings organized themselves into tribes, groups and kingdoms. This led to the emergence of ideas such as: power, battles, supremacy and politics. These ideas further fueled people's natural need to secretly communicate with a selective recipient, which in turn ensured the continued evolution of cryptography as well. The roots of cryptography are found in civilizations: Roman and Egyptian [14].

a) Caesar’s Cipher

The "Caesar Cipher" is one of the earliest known ciphers, although according to Holden [3], Caesar was probably not the original inventor of what he now calls the Caesar cipher, but he certainly made it popular 110 BC [15]. Julius Caesar, a Roman military and political leader, used this writing technique to send secret messages to his generals and allies. For Julius Caesar, the security of his information was essential in order to guarantee his success. Caesar was responsible for developing a system in which it was intended to guarantee the security of his messages, which if intercepted by his enemies, could not be decrypted without the use of a key. In case one of your messages is intercepted, your opponent would not be able to read it. What at the time was a great advantage over opponents of the emperor and the empire. Despite the apparent simplicity of this cipher, even at the time, the messages intercepted by potential enemies were incomprehensible due to the high level of illiteracy that existed, often as they were incomprehensible those who intercepted them considered them to be written in a foreign language.

The Caesar cipher uses the substitution cipher, which involves replacing each letter of the alphabet with the letter that is three places to

the right in the alphabet, that is, for each letter or character there is a corresponding cipher letter/character. According to Stallings [10], in Caesar's original cipher, there is a replacement for the corresponding letter with a rotation of three characters. This rotation corresponds to the number of letters or characters that are traversed in the alphabet, starting from the letter to be encrypted. To decode a certain message, reverse rotation is applied. The recipient of the same would also have to have privileged access to information, the number of positions of the rotation, to proceed with its decryption. This number of positions in the rotation indicates the change or displacement of the letters, thus being the key to decrypt the message. This cipher is probably one of the best known in the world [13].

Cesar's base cipher is only defined for the 26 characters of the alphabet, hence and according to Trappe and Washington [16], spaces and punctuation are omitted, and they can be replaced by other characters, or even left as space characters, which makes easier its decryption, but also giving clues to possible opponents.

As the alphabet has 26 characters and in the encryption using the “original” Caesar cipher there is a three-position advance, the following is observed:

A→D (A becomes D), B→E, …, W→Z and the rest become the initials, that is: X→A, Y→B e Z→C.

If we represent each character by a decimal value according to the order of the character within the alphabet: A→0, B→1, …, X→23, Y→24, Z→25. Applying Caesar's cipher shift to these (add 3): A→0+3, B→1+3, …, X→23+3, Y→24+3, Z→25+3, would result: A →3, B→4, …, X→26, Y→27, Z→28; as position three represents D, so A→D, position four represents the E, B→E, and so on to the position 25 that represents the W→Z. From 26 onwards, the remainder of the division can be taken by 26, that is: 26=26*1+0, 27=26*1+1 e 28=26*1+2, taking the remains, one has to: X→0, Y→1, Z→2, which in turn: X→A, Y→B, Z→C. Based on this reasoning, E[x]=x+3 (mod 26) can be used, where mod 26 is the remainder of the division of x+3 by 26, x the decimal value to be transformed and E[x] represents the encryption of the character whose value is x, that is, x = 0, 1, 2, 3, 4, … , 25.

The reverse encryption process, in order to recover the original text of the message from its encrypted version, is called decryption or decryption [17]. According to Trappe and Washington [16], in Cesar's cipher, decryption is performed by shifting three spaces backwards (left).

To represent decryption, inverse to encryption, the same methodology will be used, but in reverse:

Taking: A→0, B→1, …, X→23, Y→24, Z→25. Applying to these, the inverse displacement of the Caesar cipher (subtract 3): A→0-3, B→1-3, …, X→23-3, Y→24-3, Z→25-3, would result: A→-3, B→-2, C→-1, D→0, …, X→20, Y→21, Z→22; as position 0 represents A, then D→A, 1 represents the B, then E→B, and so on to Z→W, missing the first three, then the A→X, B→Y e C→Z. Deducing the equation D[x]=x-3 (mod 26), where D[x] represents the decryption of the character with the decimal value x.

According to Easttom [18], he writes that although Caesar's cipher is reputed to have used a shift of three to the right/left, any shift pattern will work with this method, shifting right or left by any number. of spaces. Also Sinkov [19] mentions that the Caesar Cipher is a direct standard alphabet with the specific key three. On the other hand, Baldoni et al. [20] the Caesar cipher is a cipher whose cipher text is obtained from the plain text by moving each letter a fixed value of positions, that is, it is not limited to three positions. Bauer [21] also writes that it is not mandatory to apply a three-character change, any value can be used, although he emphasizes that only values strictly comprised between 0 and 26 offer different encryptions. This type of cipher is called a displacement cipher. According to Katz and Lindell [15], the shift cipher is similar to the Caesar cipher, but the displacement (k) is introduced and this k is a decimal between 0 and 25. From here, the following formulas can be drawn: encryption: E[x] = x + k (mod 26) and decryption: D[x] = x - k (mod 26).

According to Schneier [22], simple substitution ciphers such as this one can be easily broken because the cipher does not hide the underlying frequencies of different characters in plain text. On the other hand, Musa [23] states

that as the secret key is a value between 0 and 25, in this case three, a brute force attack can break the cipher scheme in a short period of time.

b) Vigenère Cipher

This cipher is named after the French cryptographer Blaise de Vigenère who, in the 16th century, developed the theory of polyalphabetic substitution cryptography. According to Stamp and Low [12], a polyalphabetic cipher is essentially a simple variable substitution cipher, that is, a different substitution alphabet is used for different parts of the message.

The basic version of the Vigenère cipher uses a table (Vigenère's Table) which in the first line contains the alphabet from A to Z, in the second line from B to Z followed by A, in the third line from C to Z and A to B, and so on until the first column has the alphabet from A to Z. Furthermore, to further protect the encrypted text, a password is inserted, which consists of a word or text repeated throughout the entire message to be encrypted. To encrypt, take the character to encrypt and look for this in the first line, when finding the column that starts with that character, it is selected and will cross with the line whose character corresponds to the key character, the existing character in that crossing is the selected one. To decrypt, logically you need to know the key and operate in reverse.

Another way to apply Vigenère's technique is to convert characters into numbers, both plain text and key, and add them one by one, that is, the first letter of the key is added to the first letter of the plain text, mod 26, the second letter of the brace is added to the second letter of the plaintext, and so on, by the first m letters of the plaintext, where m is the size of the brace always smaller than n is the length of the plaintext. For the next m letters of clear text, those in the key are repeated. This process continues until the entire plaintext string is encrypted. A general equation of the encryption process is:

$$C_i=(p_i+k_{(i \bmod m)}) \bmod 26.$$

Basically, each clear text character is encrypted as a different Caesar cipher depending on the corresponding key character. Similarly, decryption is:

$$p_i=(C_i-k_{(i \bmod m)}) \bmod 26.$$

To encrypt a message, there needs to be a key that is as long as the length of the message. Typically, the key is a repeated keyword.

Recall that a polyalphabetic substitution cipher uses several simple substitutions to encrypt a message. As this cipher, as it is a polyalphabetic substitution, does not preserve the letter frequencies of the plain text to the same degree as a monoalphabetic substitution (Cesar cipher). On the other hand, if we are facing a large number of alphabets in relation to the message size, the letter frequencies of the plain text will not be preserved at all [9]. The Vigerère cipher is based on the Caesar cipher, as if we look at substitution it follows the same pattern as the Caesar shift cipher.

III. Related Works

After some readings, some works that proposed to improve the security of the Caesar Cipher algorithm were selected.

Mathur et al. [24] proposed an algorithm for data encryption/decryption in which this algorithm is based on ASCII values of characters in plain text. This algorithm is used to encrypt data using ASCII values of the data to be encrypted. The secret used will be the modification of another string and that string is used as a key to encrypt or decrypt the data. This algorithm works when the input length and key length are the same.

Singh and Sen [25], proposed different methods that increase the security of the substitution cipher, focusing on the well-known classical techniques, the aim was to induce some force to these classical cryptographs. For that purpose, they mixed classical cryptography with some other techniques. Your proposed method has shown that it is better in terms of providing more security to any text message.

Jain et al. [26], to increase the strength of this classic encryption technique, the proposed modified algorithm uses the concepts of affine ciphers, transposition ciphers, and random substitution techniques to create ciphertext that is nearly impossible to decode. It also increases the range of characters the Caesar cipher algorithm can encrypt, including all extended ASCII and ASCII characters in addition to alphabets. A complex key generation technique that generates

two keys from a single key that is used to provide more security.

Singh et al. [27] proposed a Caesar cipher substitution method and rail fence transposition techniques are used individually, the ciphertext obtained is easy to crack. The authors present a perspective on the combination of substitution and transposition techniques. Combining the Caesar cipher with the rail fence technique can eliminate its fundamental weakness and produce a ciphertext that is difficult to decipher.

Senthil et al. [28] presented some improvements to the Vigenère and Caesar cipher technique using some rigorous mathematical tools that use a prime factor, its primitive roots and its generator. The changes and substitutions performed in both techniques of this cipher are not uniform, following a particular scientific procedure.

IV. Modified Caesar's Algorithm

The Caesar cipher is quite easy to break security as referred to by Schneier [22] and Musa [23], mentioned earlier. According to Jain et al. [26], a modification of the Caesar algorithm serves to overcome some of the weaknesses and limitations of the Caesar cipher, which can be improved using one or more different encryption algorithms. Therefore, the generic simple substitution attack (Caesar cipher) will not work in a polyalphabetic substitution, being only vulnerable to a statistical attack [9].

In this article we intend to make some modifications to Caesar's algorithm, based in part on the Vigenère cipher in order to bring some security.

a) Algorithm

Bowne [29], proposed Caesar's algorithm, which, when encrypting, advances three positions to the right in the alphabet, and moves back three places in the case of decryption. If the displacement can be chosen, we are faced with the displacement cipher, in which it advances or retreats as many places in the alphabet as the chosen value (k), with $0 \leq k \leq 25$. Using the uppercase characters of the alphabet for encryption, this for the present is not very viable, because if one intends to write a text with upper and lower case characters, spaces and numbers, it would be limited.

In this article, the algorithm proposes to use ASCII code characters as a basis. That is, first the read character will be converted to ASCII code and then the sum or subtraction of the displacement value modulo 256 is done, in which the displacement value varies between 0 and 255. Analytically representing:

Encryption: *C[i]=P[i]+k (mod 256) e i=0,1,2,…,n.*

Decryption: *P[i]=C[i]-k (mod 256) e i=0,1,2,…,n.*

Where E[X] is the transformation of the plaintext character X, k is the key chosen by the user between 1 and 255. To improve the security of this simple substitution encryption/decryption model, and to prevent the same character in different positions from having the same transformation, and thus avoid successful brute force attacks, it is intended to apply a polyalphabetic substitution technique as in case of the Vigenère cipher and having the same length as the plain text. In other words, the value of k is incremented as the plaintext is encoded. Finally, to further improve security, the ciphertext is inverted.

Encryption: C[i]=P[i]+(k+i)(mod 256) and i=0,1,2,…,n-1.

After going through the entire cycle, the resulting array will be inverted.

The encryption improvements are evident, because the first character takes an advance of k, which was stipulated by the user, the second character will take an advance of k+1, and so on.

Decryption: P[i]=C[i]-k+i (mod 256) and k=k+n-1 e i=0,1,2,3,…,n-1.

At the end of the cycle, the resulting array is inverted to arrive at the plain text. As the inversion in the array is only at the end, you will have to use the maximum value in the first substitution and decreasing it until the value k, introduced by the user as a key.

1) Encryption

The encryption algorithm can be translated/represented as follows:

k ← read (displacement k)
P ← read (Plain text)
N ← le←ngth (P)
for i←0 to n, do
C[i] ← ASCII code to character((Character to ASCII code(P[i]) + k + i) mod 256)

C ← invert (C)
Print(C)

In python you use the command C[i] = chr((ord(P[i])+k+i) %256), to encrypt each character, where chr() converts the ASCII code to a character and ord() converts a character to ASCII code.

As can be seen by the algorithm, the key entered by the user is used for the first transformation (shift), the second transformation will have a k+1 key, the third transformation will have a k+2 key, and so on until the last transform which will have a key of k plus the plaintext length minus one.

2) Decryption

To decrypt, the inverse of encryption is used. Taking this into account, decryption algorithm can be translated/represented as follows:

k← read (displacement k)
C← read (Cipher text)
n← length (C)+k-1
For i ← 0 to n, do
P[i] ← ASCII code to character((Character to ASCII code(C[i]) - k + i) mod 256}
P ← invert (P)
Print(P)

In python you use the command P[i]=chr((ord(C[i])-k+i)%256), being to decrypt each character, where ord() converts a character to ASCII code to a character and chr() converts ASCII code.

As the resulting text is only inverted at the end so that the plain text is readable, the transformation key for the first character is k, the key that the user specified for encryption, plus the length of the entered encrypted text minus one, the second character will use k plus length of ciphertext minus two, and so on until the last one uses a transform of k

b) Results

To verify the effectiveness of the method, two texts were used, the word: “Mississippi” and the phrase: “A trip on the Mississippi river”. The text was selected because of the frequency of the characters, in order to check the frequency of the output characters.

The first string to be used will be the word: “Mississippi”.

```
Enter the shift value: 5
Enter the message to encrypt: Mississippi
Encrypted message: x~}u~}r{zoR
```

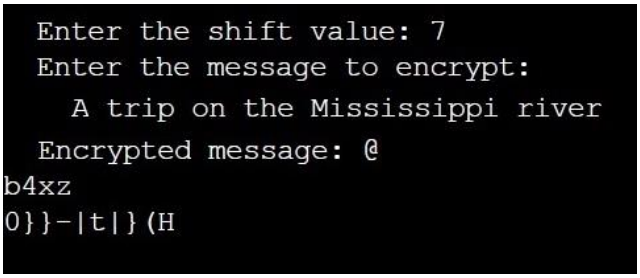
Picture 1: Encryption of the word: Mississipi.

Analyzing the transformation “M” corresponds to the value 77 of the ascii code, adding 5 and obtaining 82 corresponding to the character “R”. The next character is the “i” which corresponds to the value 105 of the ascii code, as it is the second character, it is added to the 105 o 5+1, and 111 is obtained, which is the character “o”. Then we have the third character “s” which represents the value 115 of the ascii code, adding to the value 115 the value 5+2, we get 122 which corresponds to the character “z”; and so on until the last character, which will result in “x”. When inverting the sequence obtained, the “R” that was the first character of the transformation becomes the last and the “x” that was the last becomes the first. As can be seen, equal characters in the plain text did not result equal in the cipher text, which happens in the cipher text with the Caesar cipher.

```
Enter the shift value: 5
Enter encrypted message: x~}u~}r{zoR
Plain text: Mississippi
```

Picture 2: Word decryption: x~}u~}r{zoR.

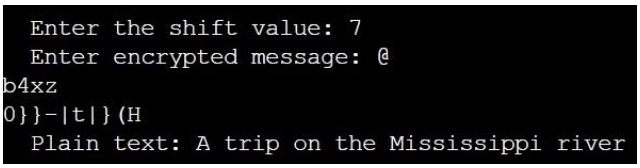
Analyzing the decryption, we have as input the character "x" that corresponds to the value 120 of the ASCII code, subtracting 11 (word length) + 5 (offset) - 1, that is, 120-11-5+1=105, and 105 represents the “i” according to the ASCII encoding. Going to the decryption of the second character which is the "~", which corresponds to the value 126 of the ASCII code, from this value we will subtract 11+5-2=14 and 126-14=112, and by the table of the ASCII code 112 corresponds to “p”. And so on until the last character, which is the "R", this corresponds to the value 82, and to decrypt it is subtracted from this 11+5-11=5 and 82-5=77, and by the encoding table ASCII it corresponds to the “M”. Finally, it reverses the word and results in the plain text word entered for encryption: Mississipi.



Picture 3: Encryption of a text string.

If you use a sentence whose length is greater than the word used in figure 1 and figure 2, we can observe that, when encrypting, even line breaks exist in the encrypted sentence, which does not happen in the plain text sentence. What is interesting from a reading point of view for those who are not authorized to read this. And in addition, the inversion, in a sentence with some dimension, ends up improving the encryption a lot, for the simple reason that the first character is almost always written with a capital letter and if the ok entered is low, the resulting letter ends up capitalized, if this goes to the end of the exit sentence ends up going unnoticed.

Picture 4: Decryption of a text string.



The decryption of the sentence took place as expected, although there was some difficulty in copying and pasting the resulting text in the encryption. It can be seen that although there are some repeated characters in the input sentence, they do not match the same in the output.

As you can see, the frequency of characters in plain text does not match the frequency of characters in encoded text. And with this it can be said that the implemented change brought a great benefit to the security of encrypted information. The final inversion also ends up creating greater confusion for those trying to decrypt the code, and like the Vigenère cipher, the brute force method does not work well, and only methods based on statistics can achieve decryption, as long as the users poorly intended do not know the algorithm.

V. Conclusion

Information security is essential nowadays and it is up to the programmer to analyze to what extent the data processed by the software under development should be encrypted. The programmer is always advised to encrypt the data before storing it in the databases, because if malicious users want to copy the tables they will be surprised to see that the data is not the way they intended. And companies can only gain from this improvement in their software because disgruntled employees when fired or when hired by competitors are unable to access business data.

This method started from Caesar's cipher method and inspired on Vigenère's cipher it expands the key from the key k, an integer between 1 and 255, and expands it to the length of the simple text, by incrementing the k plus the position of the character in plain text. In the case of decryption, the opposite is done, starting at the most k plus the ciphertext length and decreasing it until reaching k. At the end of encryption and decryption, the text produced is inverted.

This method has proven to be easy to implement and has high security at the level of the Vigenère cipher. On the other hand, as this technique works with only one cycle, it is quick to execute and does not need large machine resources, which makes it even more efficient. It should also be noted that the value of k does not need to be introduced, but rather use an existing value in the company's data, or one that the programmer finds interesting..

VI. References

[1] Katz J, Lindell Y. (2015). Introduction to Modern Cryptography. 2nd ed. Florida: Taylor & Francis Group, LLC, CRC Press.

[2] Stinson DR, Paterson MB. (2018). Cryptography: Theory and Practice. 4th ed. Textbooks in Mathemátics. Florida: CRC Press.

[3] Holden J. (2017). The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption. New Jersey: Princeton University Press.

[4] Kahate A. (2003). Cryptography and Network Security. New Delhi: Tata McGraw-Hill.

[5] Kipper G. (2004). Investigator´s Guide to Steganography. Florida: Auerbach Publications.

[6] Paar C, Pelzl J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Berlin: Springer-Verlag.

[7] Delfs H, Knebl H. (2007). Introduction to Cryptography: Principles and Applications. 2nd ed. Berlin: Springer-Verlag.

[8] Aggarwal S. (2016). A Review on Enhancing Caesar Cipher. International Journal of Research Science & Management. 3 (6): 14-20.

[9] Shrivastava M, Jain S, Singh P. (2016). Content Based Symmetric Key Algorithm, International Conference on Computational Modeling and Security, Procedia Computer Science. 85: 222-227.

[10] Stallings W. (2011). Cryptography and network security: Principles and Practice. 5th ed. New York: Prentice Hall.

[11] Singh S. (1999). The Code Book, Anchor Books: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Boks.

[12] Stamp M, Low RM. (2007). Applied Cryptanalysis - Breaking Ciphers in the Real World, San Jose: Wiley-Interscience, John Wiley & Sons, Inc..

[13] Cobb C. (2004). Cryptography for Dummies, New Jersey: Wiley Publishing.

[14] Kumari S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science. 6(4): 20915-20919.

[15] Katz J, Lindell Y. (2008). Introduction to Modern Cryptography. Florida: Taylor & Francis Group, LLC, CRC Press.

[16] Trappe W, Washington L. (2006). Introduction to Cryptography with Coding Theory. 2nd ed. New Jersey: Pearson Education Inc., Pearson-Prentice Hall.

[17] Churchhouse R. (2004). Codes and ciphers: Julius Caesar, the Enigma and the Internet. Cambridge: Cambridge University Press.

[18] Easttom W. (2021). Modern Cryptography Applied Mathematics for Encryption and Information Security. Cham: Springer Nature Switzerland AG, Springer.

[19] Sinkov A. (1966). Elementary Cryptanalysis - A Mathematical Approach. 5th Printing. Washington The Mathematical Association of America.

[20] Baldoni M.W, Ciliberto C. and Cattaneo G.M.P. (2009). Elementary Number Theory, Cryptography and Code. Roma: Springer-Verlag.

[21] Bauer C. (2013). Secret History: The Story of Cryptology. Filadelfia: Chapman and Hall/CRC.

[22] Schneier B. (1996). Applied Cryptography, 2nd ed. Illinois: John Wiley & Sons.

[23] Musa S.M. (2018). Network Security and Cryptography: A Self-teaching Introduction. Virgínia: Mercury Learning & Information.

[24] Mathur A. (2012). A Research paper: An ASCII value based dataencryption algorithm and its comparison with other symmetric data encryption algorithms. International Journal on Computer Science and Engineering (IJCSE). 4(9): 1650-1657..

[25] Singh P, Sen P. (2017). Enhancing Security of Caesar Cipher Using Divide and Conquer Approach. International Journal of Advance Research in Science and Enginheering. 6 (02): 144-150.

[26] Jain A, Dedhia R, Patil (2015). A. 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.

[27] 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. (12): 78-82.

[28] Senthil K, Prasanthi K, Rajaram R. (2013). A Modern Avatar Of Julius Caesar and Vigenere Cipher. Proceedings of IEEE International Conference on Computational Intelligence and Computing Research.

[29] Bowne S. (2018). Hands-On Cryptography with Python. Birmingham: Packt Publishing.