International Journal of Multidisciplinary Research and Growth Evaluation.

Implementation of Caesar Cipher Encryption Using Python Programming Language

Olanrewaju, Babatunde Seyi [1*], Oghene Freddinnand Best [2], Akilo, Babalola Eyitemi [3]
[1-3] Department of Computer Science, Wellspring University, Benin City, Edo State, Nigeria

* Corresponding Author: **Olanrewaju, Babatunde Seyi**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 05
September-October 2024
Received: 22-07-2024
Accepted: 26-08-2024
Page No: 533-539

Abstract
Information security is a vital aspect of data communication that is of great concern while using computing devices. It is therefore not out of place in introducing cryptography at the early stage of the study of computer security. Many modern cryptographic methods are deeply rooted in mathematical principles and this makes it a little difficult to comprehend by some students who are deficient in mathematics in learning cryptography. An example of a simple and foremost technique used in cryptography is the Caesar cipher substitution method. This method is considered very weak in this modern day of quantum computing whereby the cipher text could be easily be deciphered. However, introducing cryptography principles using the Caesar cipher method would likely spur the interest of learners interested in computer security because of its simplicity. This paper was aimed at providing an easy approach to learning cryptographic principles at the introductory stage using the Caesar cipher encryption technique. An easy to comprehend algorithm was developed and implemented in Python programming language. The result produced the cipher text of the plain text encrypted. Also, a brute force attack was used to decipher the cipher text to expose the weakness of the method. This result would make learners to have an increased interest in modern cryptographic techniques.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.5.533-539

Keywords: information security; cryptography; Caesar Cipher method; Python programming language; brute force attack

1. Introduction

Communication is a vital aspect of human existence whereby messages are sent to the desired recipients in different forms [1]. Communication, especially in verbal or written form will be desired to be made private for different reasons, either positive or negative [2]. Information communication technologies have been adopted to limit the barriers that could impede successful and securely transmitted messages. The means of using information technologies to transmit messages whether verbal or written, could be compromised to retrieve secret messages.

In social or organisational media networks or platforms where information sharing is the basis of such networks, there may be a need to send a confidential message to only one or a group of recipients. To ensure data or information privacy in such an environment, there is a need to put measures in place to provide every means of confidentiality of private data [3, 4]. There are several measures put in place to guarantee data confidentiality; a popular approach is data encryption. The changing of the textual format or representation of data is generally known as data encryption. Data encryption is a cryptographic principle whereby a proven mathematical concept is used to transform a message into a non-readable format [5].

Anyone who desires to practice network security must have adequate knowledge of cryptography. In learning cryptography, an in-depth knowledge of mathematics is required. According to [6], knowing certain basic mathematical concepts would aid the understanding of cryptography. Mathematical concepts like counting techniques, permutations, plotting a curve, raising a number to a power, modular arithmetic, and congruence would be needed. Introducing these complex mathematical concepts at the onset of studying cryptography to those who are not well-grounded in mathematics, could frustrate their ambitions.

This paper presented the implementation of a simple cryptographic technique in a way to stimulate interest in the study of cryptography.

2. Literature review

According to [5] and [7], the most widely known encryption technique in cryptography is Caesar Cipher. In Caesar's cipher, characters of plaintext are replaced with a fixed number of locations down the alphabet [8]. It is also called 'shift cipher'. This method was used by Julius Caesar to communicate with his generals and it works only on shifting of characters based on the key value [9]. Julius Caesar used shift cipher with a constant left shift of three (3) as shown in Table 1 to encrypt important military messages during the war [10].

Table 1: Julius Caesar's Shift Cipher with Shift 3

Plain Text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher Text	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

The Caesar Cipher is an ancient and widely used cipher that is easy to encrypt and decrypt. It works by shifting the letters of the alphabet over to create an entirely new alphabet [11]. For example, to implement Caesar cipher using a key shift of one (1), the plaintext and the corresponding ciphertext will be as shown in Figure 1.

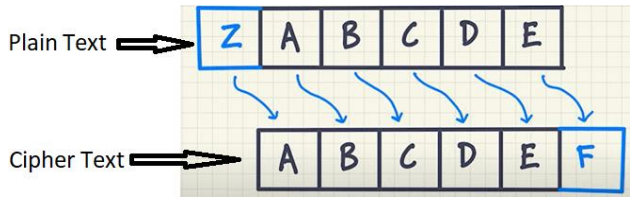

Fig 1: Caesar Cipher with Key 1

From the above figure, the plaintext *'HELLO WORLD'* will be encrypted as *'IFMMP XPSME'* as shown in Figure 2 below.

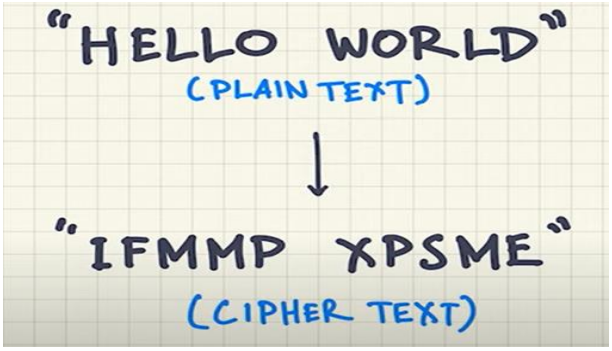

Fig 2: Plaintext and the Corresponding Ciphertext using Caesar Cipher with Key 1

If different shift key is used, the same plaintext will be encrypted to produce different ciphertext. As an illustration, if the same *'HELLO WORLD'* is to be encrypted with a shift key of 12, the ciphertext that will be produced as shown in Figure below will be different from the one produced with a key shift of 1 in Figure 2.

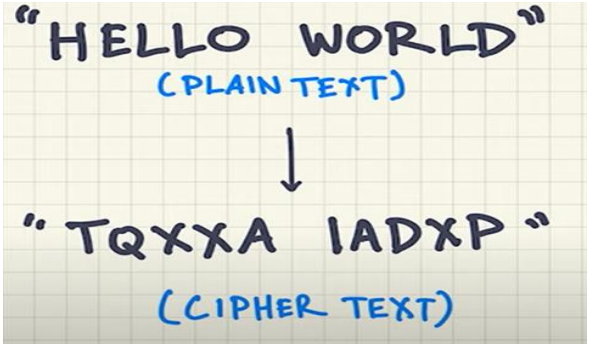

Fig 3: Plaintext and the Corresponding Ciphertext using Caesar Cipher with Key 12

This *Caesar substitution cipher* is very weak because if the quantity of displacement is known, privacy is no longer achievable. Without the knowledge of the displacement, the plaintext could still be discovered very easily because the quantity of possible cipher solutions is only 25. The issues identified in this system are:

1. It is more prone to attacks because the key ranges between 1 to 26. Brute force attackers try all the conceivable combinations of keys and gets the message in a very easy way. So, the key should be more and more complex to create hindrance in brute force attacks.
2. Too simple and easy to decrypt by an unauthorized user. It can be easily hacked. It means the message encrypted by this method can be easily decrypted. The pattern of letters provides a clue to the hacker about the possible cipher shift [12].
3. Provides the minimum layer of security. If the number of possible keys in any encryption system is not large enough, an attacker could attempt every one of the likely keys and guess right with little effort in a few trials [13]. This would make the system not to be properly secured. The Caesar-cipher encryption system is based

only on a shift in keys and in this modern computing this is not too difficult because there is no additional layer of security to the system.

3. Methodology

An algorithm of the Caesar cipher encryption technique as represented by a flowchart is shown in Figure 4. In the flowchart, the message to be encrypted is written and a shift key to be used is defined. The system then picks each of the characters in the message, and checks if it is an alphabet, if yes it will be converted to upper case otherwise, it will be added directly to the encrypted message. The characters are converted to upper cases to avoid errors in the representation of characters in different cases using ASCII codes. In other words, both the encrypted and the resultant decrypted message are represented in upper cases.

The character in the message that has been converted to ASCII code is added to the already defined shift key to produce a new character in ASCII code. A test is performed on the new ASCII code to ensure that it is within the range of recognised ASCII codes for alphabets. If the new ASCII code is greater than 90 which is the code for the last alphabet 'Z', 26 which is the range of the alphabet will be subtracted from it to get a code within the range of the alphabet. If the code is less than 65 which is the code for the first alphabet 'A', 26 is added to the new code. The new character code after the addition or subtraction of 26 as the case may be applied is then converted to character in which now represents the encrypted message.

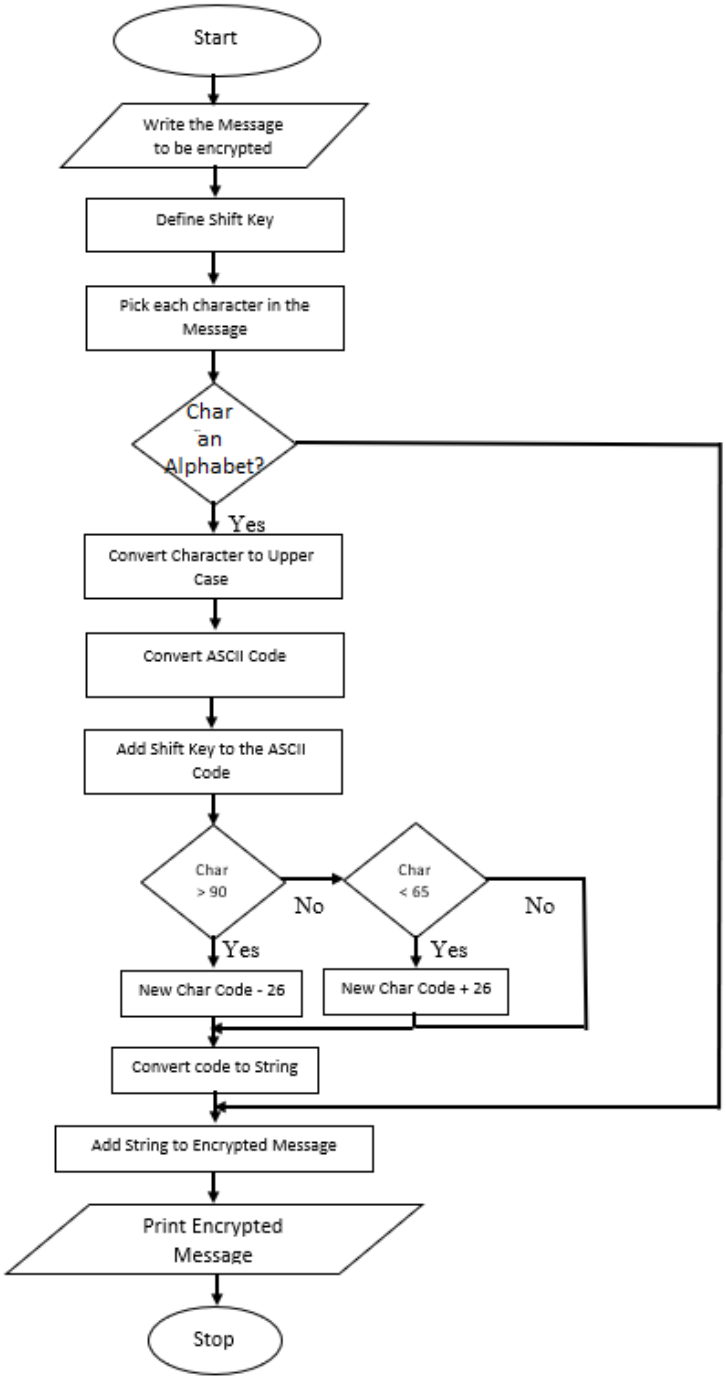

Fig 4: Flowchart for Caesar Cipher Encryption Method

The Caesar cipher encryption method was implemented in Python Programming language using the ASCII table. The Python code is presented below.

```
FIRST_CHAR_CODE= ord("A")
LAST_CHAR_CODE = ord("Z")

def caesar_shift(message, shift):
    # Output
    result= " "

    #Go through each of the letters in the message
    for char in message.upper():
        if char.isalpha():FIRST_CHAR_CODE = ord("A")
LAST_CHAR_CODE = ord("Z")
CHAR_RANGE = (LAST_CHAR_CODE - FIRST_CHAR_CODE) +

def caesar_shift(message, shift):
    # Output
    result= " "
```

```
    #Go through each of the letters in the message
    for char in message.upper():
        if char.isalpha():
            #convert character to ASCII code
            char_code = ord(char)
            new_char_code = char_code + shift
            if new_char_code > LAST_CHAR_CODE:
                new_char_code -= CHAR_RANGE
            if new_char_code < FIRST_CHAR_CODE:
                new_char_code += CHAR_RANGE
            #convert ASCII code back to character as encrypted
            new_char = chr(new_char_code)
            #Add encrypted character to the encrypted message
            result += new_char
        else:
            result += char
    print(result)

user_message = input("Enter Message To Encrypt: ")
user_shift_key =int(input("Enter shift key (integer): "))
caesar_shift(user_message, user_shift_key)
```

The internal coding system of the computer is capable of representing the letters of the alphabet. Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. The American National Standards Institute (ANSI) developed a code known as the American Standard Code for Information Interchange (ASCII). The ASCII codes for the letters of the alphabet in upper case are shown in Table 2.

Table 2: ASCII Codes for Alphabet in Upper Cases

Alphabet	ASCII Code
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

4. Result discussion

The Caesar cipher and the enhanced encryption methods were implemented and run from the console of the Python programming language's Integrated Development Environment (IDE). To perform encryption, the system asks the user to enter the message to be encrypted thereafter, the desired shift to be used for the Caesar cipher encryption is entered. Figure 5 shows the Caesar cipher encryption of the message "*I want you to come to my party on the second of November.*". The encryption was done using a key shift of "12" resulting in the cipher text "*U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.*"

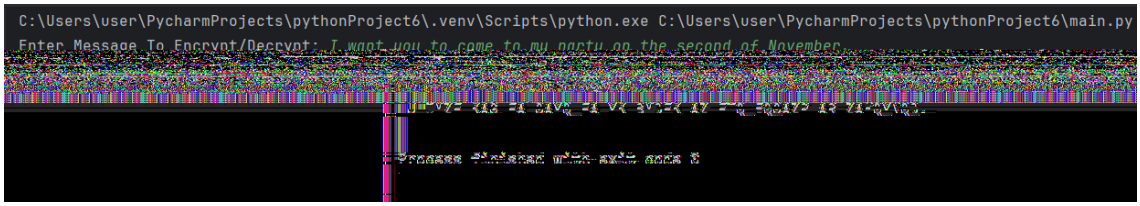

Fig 5: Caesar Cipher Encryption of Plain Text

To perform the decryption of the cipher text for Caesar cipher encryption, the same application was used. The cipher text was entered as a message to be decrypted and the negation of the shift key used to encrypt was entered to decipher the cipher text.

Figure 6 shows the decryption of the cipher text "*U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.*" produced from the encryption process performed earlier. The deciphering was achieved by using "-12" as the shift key that represents the reverse of the encryption operation. The plain text was recovered as *"I WANT YOU TO COME TO MY PARTY ON THE SECOND OF NOVEMBER."*

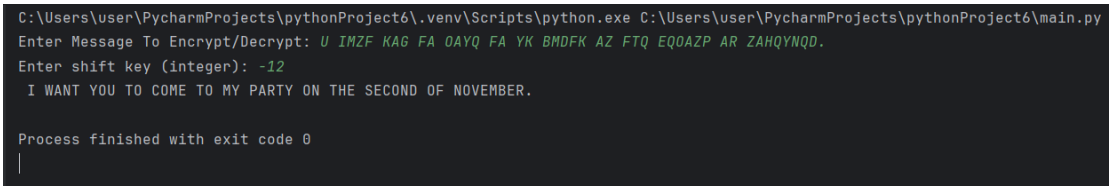

Fig 6: Caesar Cipher Decryption of Cipher Text

Using the cipher text generated from the plain text encrypted earlier in Figure 5, Table 3 shows the brute force attempts using all the possible shift keys. From the table, it is shown that trying the correct shift key (-12) will reveal the plain text. This shows the weakness of the Caesar cipher encryption technique.

Table 3: Brute Force Attack on Caesar Cipher Encryption Technique

POSSIBLE SHIFT KEYS	CAESAR CIPHER TEXT	OUTPUT OF BRUTE FORCE ATTACK
1	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	T HLYE JZF EZ NZXP EZ XJ ALCEJ ZY ESP DPNZYO ZQ YZGPXMPC.
2	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	S GKXD IYE DY MYWO DY WI ZKBDI YX DRO COMYXN YP XYFOWLOB.
3	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	R FJWC HXD CX LXVN CX VH YJACH XW CQN BNLXWM XO WXENVKNA.
4	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	Q EIVB GWC BW KWUM BW UG XIZBG WV BPM AMKWVL WN VWDMUJMZ.
5	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	P DHUA FVB AV JVTL AV TF WHYAF VU AOL ZLJVUK VM UVCLTILY.
6	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	O CGTZ EUA ZU IUSK ZU SE VGXZE UT ZNK YKIUTJ UL TUBKSHKX.
7	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	N BFSY DTZ YT HTRJ YT RD UFWYD TS YMJ XJHTSI TK STAJRGJW.
8	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	M AERX CSY XS GSQI XS QC TEVXC SR XLI WIGSRH SJ RSZIQFIV.
9	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	L ZDQW BRX WR FRPH WR PB SDUWB RQ WKH VHFRQG RI QRYHPEHU.
10	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	K YCPV AQW VQ EQOG VQ OA RCTVA QP VJG UGEQPF QH PQXGODGT.
11	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	J XBOU ZPV UP DPNF UP NZ QBSUZ PO UIF TFDPOE PG OPWFNCFS.
12	**U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.**	**I WANT YOU TO COME TO MY PARTY ON THE SECOND OF NOVEMBER.**
13	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	H VZMS XNT SN BNLD SN LX OZQSX NM SGD RDBNMC NE MNUDLADQ.
14	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	G UYLR WMS RM AMKC RM KW NYPRW ML RFC QCAMLB MD LMTCKZCP.
15	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	F TXKQ VLR QL ZLJB QL JV MXOQV LK QEB PBZLKA LC KLSBJYBO.
16	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	E SWJP UKQ PK YKIA PK IU LWNPU KJ PDA OAYKJZ KB JKRAIXAN.
17	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	D RVIO TJP OJ XJHZ OJ HT KVMOT JI OCZ NZXJIY JA IJQZHWZM.
18	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	C QUHN SIO NI WIGY NI GS JULNS IH NBY MYWIHX IZ HIPYGVYL.
19	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	B PTGM RHN MH VHFX MH FR ITKMR HG MAX LXVHGW HY GHOXFUXK.
20	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	A OSFL QGM LG UGEW LG EQ HSJLQ GF LZW KWUGFV GX FGNWETWJ.
21	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	Z NREK PFL KF TFDV KF DP GRIKP FE KYV JVTFEU FW EFMVDSVI.
22	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	Y MQDJ OEK JE SECU JE CO FQHJO ED JXU IUSEDT EV DELUCRUH.
23	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	X LPCI NDJ ID RDBT ID BN EPGIN DC IWT HTRDCS DU CDKTBQTG.
24	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	W KOBH MCI HC QCAS HC AM DOFHM CB HVS GSQCBR CT BCJSAPSF.
25	U IMZF KAG FA OAYQ FA YK BMDFK AZ FTQ EQOAZP AR ZAHQYNQD.	V JNAG LBH GB PBZR GB ZL CNEGL BA GUR FRPBAQ BS ABIRZORE.

5. Conclusion

There is sometimes a need to ensure some kinds of information are received only by the intended recipients. This need involves data encryption for transforming a written message to a non-readable format. This principle known as cryptography is an important aspect of information security. This paper aims to stimulate a desire to study cryptography by presenting its implementation in the simplest possible way. The paper hides the complexities of mathematical concepts needed to develop a very strong cryptographic system. This research used a simple Programming language to implement a simple encryption technique called Caesar cipher. The result shows how messages could be encrypted and decrypted. The weakness of the Caesar cipher was demonstrated by applying a brute-force attack. The result is to show that stronger mechanisms are needed if information security is highly desired. Therefore, whosoever aspires to be a network administrator needs to have a good knowledge of mathematics. When such concepts are presented there will still be interest in the study of cryptography while using complex mathematical principles.

6. References

1. Tanenbaum AS, Wetherall DJ. Computer Networks. 5th ed. Prentice Hall; c2011. ISBN-13: 978-0-13-212695-3.
2. Nwankwo W, Olanrewaju B, Chinedu P, Olayinka TC.

National Social Information Technology Infrastructure: A Potent Mechanism for Waging Anti-Corruption War. American Journal of Embedded Systems and Applications. 2018;6(1):56-68.
3. Bishop M. Introduction to Computer Security. Pearson Education, Inc.; c2005. ISBN 0-321-24744-2.
4. Bellovin SM. The Insider Attack Problem: Nature and Scope. In: Jajodi S, editor. Insider Attack and Cyber Security: Beyond the Hacker. Advances in Information Security Series. Springer Science+Business Media, LLC. 2008;39:1-4.
5. Gupta G, Chawla R. Review on Encryption Ciphers of Cryptography in Network Security. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(7):1-26.
6. Mogollon M. Cryptography and Security Services: Mechanisms and Applications. CyberTech Publishing; c2007. ISBN 978-1-59904-839-0.
7. Dar SB. Enhancing the Security of Caesar Cipher Using Double Substitution Method. International Journal of Computer Science & Engineering Technology. 2014;5(7):772-774.
8. Delfs H, Knebl H. Introduction to Cryptography: Principles and Applications. 2nd ed. Springer New York; c2007. ISBN-13: 978-3-540-49243-6.
9. Priya V, Gurjot SG, Rajan M. Diversified Caesar Cipher for Impeccable Security. International Journal of Security and Its Application. 2017;11(3):33-40. doi: 10.14257/ijsia.2017.11.2.04.
10. Atish J, Ronak D, Abhijit P. Enhancing the Security of Caesar Cipher Substitution. International Journal of Computer Applications. 2015;129(13):1-4.
11. Asoronye GO, Emereonye GI, Onyibe CO, Agha IA. An Efficient Implementation for the Cryptanalysis of Caesar's Cipher. Melting Pot. 2019;5(2):101-109.
12. Talbot J, Welsh D. Complexity and Cryptography: An Introduction. Cambridge University Press; c2006. ISBN-13: 978-0-511-14070-9.
13. Stanislav A, Maurizio M. Cyber Arms Security in Cyberspace. CRC Press Taylor & Francis Group; c2020. Available from: https://www.taylorfrancis.com/books/mono/10.1201/9780367853860/cyber-arms-stanislav-abaimov-maurizio-martellini