FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 5, May, 2025, pp 180 - 186
DOI: https://doi.org/10.33003/fjs-2025-0905-3494

A MODIFIED CAESAR CIPHER ENCRYPTION TECHNIQUE FOR SECURED INFORMATION SHARING

***[1]Olanrewaju, Babatunde Seyi, [1]Eguavoen, Victor Osasu and [3]Okunade, Oluwasogo Adekunle**

[1]Department of Computer Science, Wellspring University, Benin City, Edo State, Nigeria.
[2]Department of Computer Science, Faculty of Computing, National Open University of Nigeria, Abuja, Nigeria

*Corresponding authors' email: babatunde_olanrewaju@wellspringuniversity.edu.ng Phone: +2348028320321

ABSTRACT

The need to ensure the confidentiality of data in a shared environment triggered the implementation of cryptography, where data is transformed into an unintelligible format. In modern cryptography, complex mathematical concepts create a strong encryption system. This paper developed an encryption method based on the Caesar cipher method. The developed method modified the Caesar cipher method by adding a second layer of encryption. In the developed method, after the first encryption using the Caesar cipher substitution method, an alphanumeric table for Caesar cipher text was formulated to generate the final cipher text, which leaves no resemblance to the Caesar cipher encryption. The encryption was implemented using the Python programming language. Both the Caesar cipher and the modified methods were simulated in a Python Integrated Development Environment and tested using a brute force attack. The results showed the Caesar cipher method broken without the shift key available, while the modified method could not be broken. The result demonstrated that a strong encryption technique could be developed with less complexity.

Keywords: Cryptography, Caesar cipher, Python Programming language, Brute force attack

INTRODUCTION

The insatiable need for a higher volume of data transmission at the highest possible transmission speed is increasingly driving wireless communication researchers to innovate technologies that could handle low latency and high-speed communications of such data(Delfs & Knebl, 2015; Odijie et al., 2024). However, network administrators have adopted cryptography whereby secret keys are used to accomplish the transformation of the original message to an unintelligible format (Ugwunna et al., 2024). Only recipients of such messages with the secret key have access to convert the unintelligible message back to a readable format (Stanislav & Maurizio, 2020). The actual message to be transmitted is called the plaintext, while the message that has been transformed into an unintelligible format is known as the ciphertext (Delfs & Knebl, 2015). The drive to transform textual information is to shield messages meant to be transmitted or stored through computing devices and networks from those who should not have access to the content of the messages, even if the unintended recipients get in contact with the messages (Bishop, 2005).

The encryption method has been adopted in the early century. An example of the foremost encryption method is the Caesar cipher, where the shifting of the positions of the alphabet turns a plain text into ciphertext (Satish & Shinde, 2024). Julius Caesar used this method of encryption by transmitting his instructions to his army to deny his enemies the ability to comprehend his messages, even if they were intercepted. This encryption method is simple to implement but not strong considering the capability of modern computing devices in the cryptanalysis of messages encrypted with this method (Mogollon, 2007). The implication of this is that Caesar's cipher method of encryption could not be considered in this modern computing era. Numerous algorithms have been developed after the Caesar substitution cipher, all of which come with higher complexities in implementation (Verma et al., 2017). This paper leverages the simplicity of the Caesar cipher to develop a simple yet stronger encryption technique.

Information sharing is a significant aspect of human existence because it touches every critical sector of human life (Olanrewaju & Osunade, 2018). Therefore, the need to ensure confidentiality of classified information that could lead to financial loss or loss of lives or properties, or even personality damage, has been the concern of whoever is security conscious. Given this, concerned individuals adopted different methods to make messages unreadable to whom the message is not meant in a process of encryption. Thus, a real message that is to be protected is transformed into an unreadable text. Among the earlier methods that could be deployed to convert plain text data to unreadable data is the Caesar Cipher algorithm. This method is so-called after the Roman ruler, Julius Caesar, who encrypted his instructions using this algorithm. He shifted by some amount the letters of the alphabet in case the messages got to the enemies by chance, they would not understand them (Satish & Shinde, 2024). The Caesar cipher method could be easily implemented however, it can easily be broken, which makes it not acceptable for many applications by today's standard (Dar, 2014). Recent cryptographic methods employ mathematical principles to produce stronger ciphers that are difficult to break. However, these mathematical methods posed a very high level of complexity in their implementations (Olanrewaju et al., 2024).

Modern cryptography is founded on complexity theory, describing the simplicity or difficulty of performing cryptanalysis on ciphertext (Talbot & Welsh, 2006). This implies that for an encryption system to be considered strong, it must be hard to break. With this assumption in mind, it is possible to develop an encryption system with various degrees of complexity. The complexities of cryptography will be greatly reduced by producing an easy way of transforming messages to a non-readable format that will still be difficult to decrypt. The Caesar cipher method is simple to design however, it is also simple to break when cryptanalysis is applied to its encrypted text. A brute force attack will easily decipher the Caesar cipher text (Olanrewaju et al., 2024).

The simplicity of breaking Caesar cipher text is viewed as the limitation of this method (Hassan, 2024). This research developed a modified Caesar cipher algorithm for making cryptography stronger and, at the same time, reducing the complexities of developing a strong encryption system. This research is aimed at developing a cryptosystem of low complexity and yet a strong encryption system through the modification of the existing Caesar cipher encryption algorithm.

MATERIALS AND METHODS

Fundamentals of security encompass a broad range of principles and practices to protect assets such as data, information, systems, and resources on the web or information-sharing platforms from various threats (Simson & Spafford, 2002; Odijie et al., 2025). Network confidentiality is among the core aspects that constitute information security. Confidentiality is fundamental to information security, ensuring data is accessible only to authorized individuals, systems, or processes. It aims to prevent unauthorized access, disclosure, or exposure of sensitive information (Bishop, 2005). Confidentiality safeguards sensitive messages like personal information, financial records, trade secrets, and classified documents from being accessed by unintended recipients. Maintaining confidentiality fosters trust between individuals, organizations, and their stakeholders by assuring them that their private or sensitive information is secure and will not be exploited (Simson & Spafford, 2002). Many industries and jurisdictions have guidelines like the General Data Protection Regulation (GDPR) that mandate the protection of classified information. Ensuring confidentiality helps organizations conform to these legal requirements (Bellovin, 2008).

Confidentiality is important for maintaining trust with stakeholders. By implementing robust security measures, such as encryption, access controls, and secure transmission protocols, organisations can effectively safeguard confidential data against unauthorised access, disclosure, or exploitation. Continual vigilance, adherence to best practices, and staying abreast of emerging threats are critical to ensuring confidentiality in today's digital landscape (Stanislav & Maurizio, 2020).

While primarily used for confidentiality, encryption also promotes information integrity by protecting data from unauthorized modifications during transmission or storage. Authorized users with contact with messages may intentionally or unintentionally alter data, compromising its integrity. Data integrity is important for ensuring the reliability and trustworthiness of information. By implementing comprehensive cryptographic principles, establishments can ease the risks associated with data tampering and maintain the integrity of their confidential information. Continual monitoring, adherence to best practices, and proactive response to emerging threats are critical to preserving data integrity in today's dynamic and interconnected digital environments (Sinclair & Smith, 2008).

Cryptography is fundamental to the sanctity of communications in modern information systems. As technology advances and security threats evolve, the importance of cryptography in safeguarding confidential data and maintaining trust in digital interactions cannot be overemphasised (Delfs & Knebl, 2015). An understanding of cryptographic principles is essential for effective protection against cyber threats (Tanenbaum & Wetherall, 2011). Cybersecurity threats continue to evolve, with cryptography playing an important part in shielding confidential information, securing communications, and ensuring privacy (Vogel, 2011).

Caesar cipher is one of the earliest known encryption techniques, named after Julius Caesar, who encrypted his private correspondence (Mogollon, 2007; Dar, 2014; Jain et al., 2015; Asoronye et al., 2019; Sahni & Mapari, 2024). It is one of the categories of substitution ciphers in which each letter of the alphabet is shifted using a desired number of places known as the key shift. The Caesar cipher encryption process chooses a fixed integer shift key. In the plaintext, letters will be shifted forward using any desired shift positions. Non-alphabetic characters (such as punctuation, spaces, or numbers) remain unchanged (Jain et al., 2015; Sahni & Mapari, 2024). To retrieve the original plaintext of a Caesar ciphertext, each letter in the encrypted message should be shifted backward by the same amount used to shift it forward during encryption. This method is easily breakable through brute-force attacks. There are 25 possible keys (for a 26-letter alphabet), thereby making it weak to simple frequency analysis attacks. The Caesar cipher illustrates the basic principles of encryption and has historical significance as one of the earliest recorded methods of cryptography. Its simplicity and ease of implementation make it a valuable teaching tool for introducing cryptographic concepts. Historically significant and conceptually simple, yet several weaknesses that make it unsuitable for secure modern communication are noticeable. With 25 possible keys (excluding the trivial case of no encryption), a brute force attack can easily be applied by trying all possible shifts. Caesar Cipher does not adhere to modern cryptographic standards like those defined by AES or RSA (Rivest-Shamir-Adleman) (Gunawan et al., 2019). It lacks the complexity necessary to protect confidential data in today's digital environment.

Asoronye et al. (2019) designed a system that achieved cryptanalysis of the Caesar cipher encryption technique. In the research, a decryption formula that performs the cryptanalysis of the ciphertext was successfully deployed. The original message is recovered with the use of a random key. The algorithm was developed in the C programming language. The work shows the ineffectiveness of the Caesar cipher as it could easily be decrypted.

In the paper titled "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages", (Gunawan et al., 2019) developed an encryption system to enhance the Caesar cipher by combining it with the Rivest Shamir Adleman (RSA) algorithm. Adding the RSA technique to the Caesar cipher method gives another layer of encryption, which improves the level of security of the ciphertext produced. To use the RSA algorithm, it is necessary to have considerable knowledge of mathematics, just as with any other cryptographic technique; this raises the level of complexity in the execution of the system.

Verma et al. (2017) also improved the security of the Caesar cipher encryption method by developing an encryption technique using the matrix concept. This method is developed to change characters, digits, and symbols, using a character value table. The use of the matrix concept also brings a sort of higher complexity to the implementation of this technique.

Jain et al., (2015) also enhanced the Caesar Cipher Substitution Method. The work used a randomized approach to strengthen the Caesar cipher method. The paper proposed a modified algorithm using the ideas of randomized substitution techniques to produce encrypted messages. However, a complex key generation technique that generates two keys from a single key was used to provide the enhancement to the Caesar cipher method. This also increases the complexity of the implementation of this method.

Goyal and Kinger (2013) also modified the Caesar cipher encryption technique to improve the Caesar cipher text. Goyal and Kinger (2013) modified the traditional Caesar cipher by fixing the key size to one, and also the alphabet index is checked. This modified method, though, enhances the traditional Caesar cipher method, is still very weak because only one layer of encryption is used, just as in the Caesar cipher method. With a brute force attack, it will be easily deciphered.

To overcome the limitations of the existing system described in the preceding section, an enhancement is made to the system. The primary objective of this modified Caesar cipher is to develop a not-too-complex and yet stronger encryption system. A model for the existing Caesar cipher is presented in Figure 1.

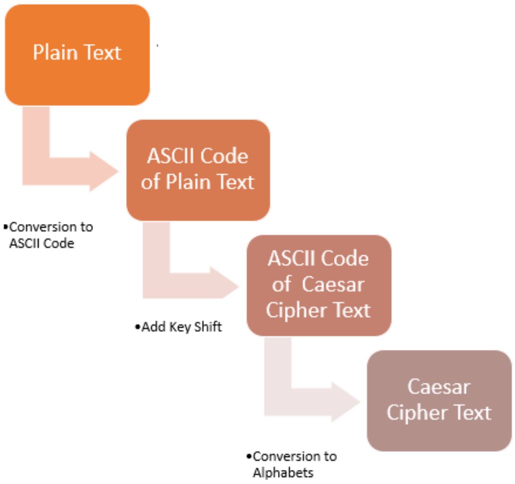


Figure 1: Implementation Model for Caesar Cipher Encryption

In the figure, the plaintext to be encrypted is converted into ASCII code; thereafter, a desired key shift is added to the ASCII code generated to form another ASCII code, which represents the ciphertext to be produced. Finally, the ASCII code produced after a key shift has been added is converted to an alphabet to represent the ciphertext generated from the Caesar cipher encryption model.

To enhance this weak Caesar ciphertext, another layer of text transformation is then included in the system. In the model for the enhanced encryption technique shown in Figure 2, the ciphertext produced using the Caesar cipher is converted to a stronger ciphertext using an alphanumeric conversion method. The final ciphertext, which is in the form of alphanumeric characters, does not show any trace of the Caesar cipher encryption method for any hacker to try cryptanalysis of the transformed text using the Caesar cipher.

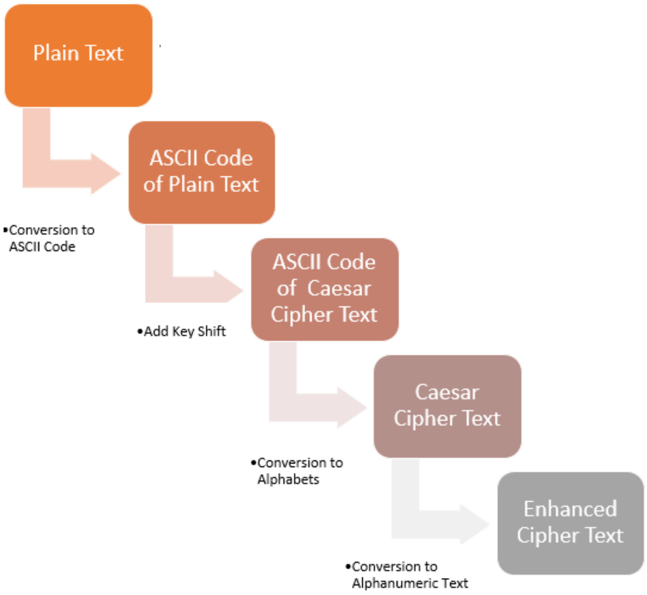


Figure 2: Implementation Model for Modified Caesar Cipher Encryption

Figure 3 below shows the algorithm of the modified Caesar cipher encryption method. In the algorithm, the character in the information 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 guarantee the range of recognised ASCII codes for alphabets. If the new ASCII code is greater than 90, the code for the last alphabet ‘Z’, 26, will be subtracted from it to get a code within the range of the alphabet. If the code generated is not up to 65, which is the code for the first alphabet ‘A’, 26 is added. The new character code after the addition or subtraction of 26, as the case may be, is then converted to the character that now represents the encrypted message.

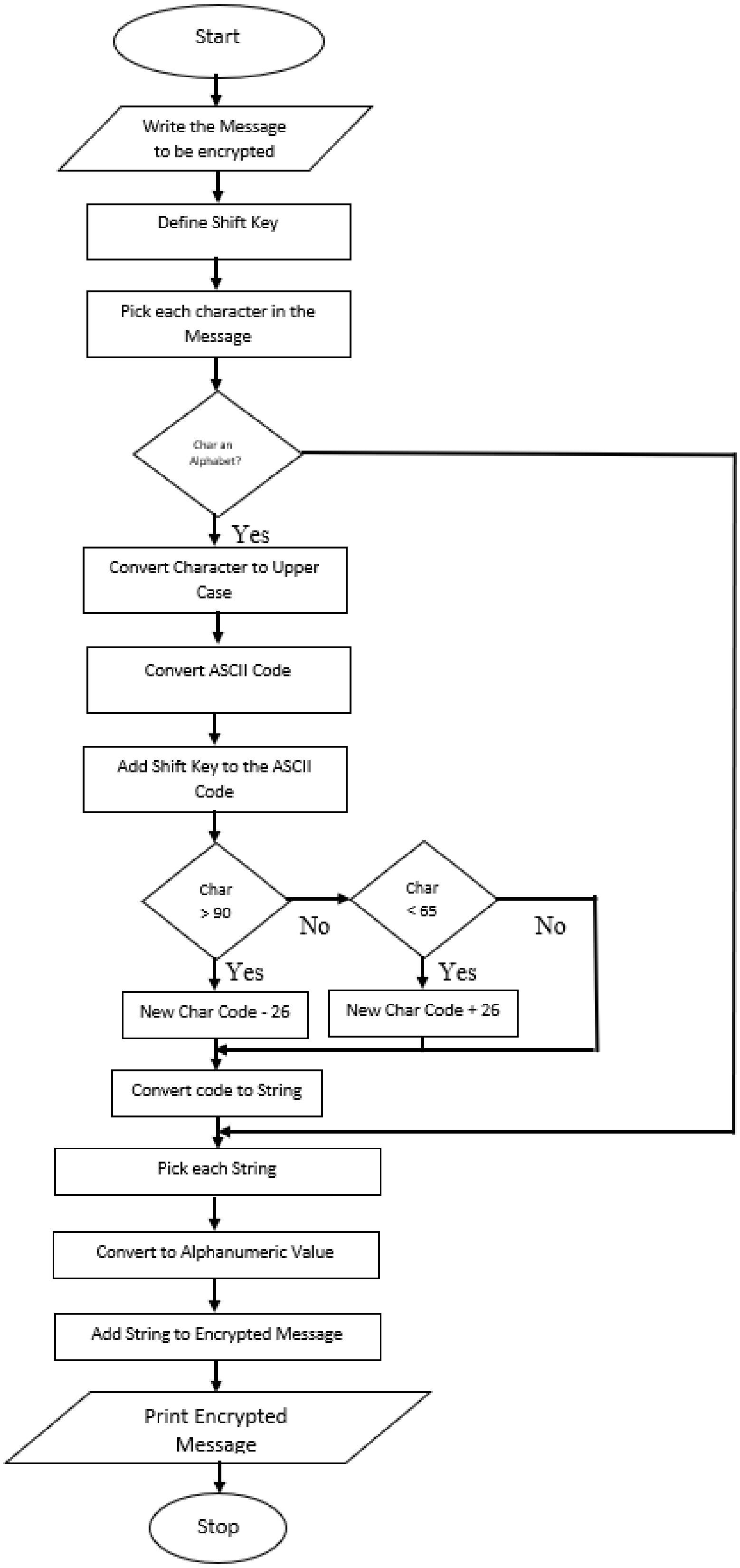

Start
Write the Message to be encrypted
Define Shift Key
Pick each character in the Message
Char an Alphabet?
Yes
Convert Character to Upper Case
Convert ASCII Code
Add Shift Key to the ASCII Code
Char > 90
No
Yes
Char < 65
No
Yes
New Char Code - 26
New Char Code + 26
Convert code to String
Pick each String
Convert to Alphanumeric Value
Add String to Encrypted Message
Print Encrypted Message
Stop

Figure 3: Flowchart for the Modified Caesar Cipher Encryption Method

Formulation of An Alphanumeric Table

The conversion of the final encrypted message to an alphanumeric value needs a conversion table as formulated in Table 1. An arbitrary method was used to select the corresponding alphanumeric value for the Caesar cipher text. This is to make cryptanalysis more difficult.

Table 1: Alphanumeric Value of Caesar Cipher Text

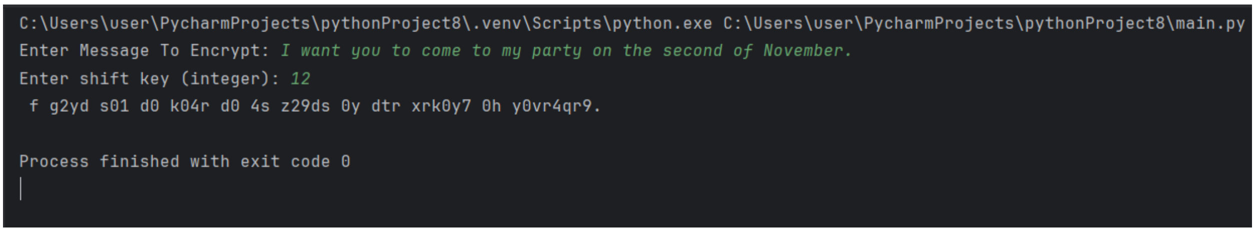
Caesar Cipher Text	Alphanumeric Value
A	0
B	z
C	b
D	9
E	x
F	d
G	1
H	v
I	g
J	8
K	s
L	j
M	2
N	q
O	k
P	7
Q	r
R	h
S	3
T	t
U	f
V	6
W	w
X	c
Y	4
Z	y

From the table, each encrypted Caesar cipher text, which is in uppercase, is converted to the corresponding alphanumeric value. The alphanumeric values of the Caesar cipher text will now be the final output of the modified method. This means that for this enhanced method, two layers of encryption are used. The shift key method and the conversion to alphanumeric values, which represent the final ciphertext text make up the two layers.

RESULTS AND DISCUSSION

The ciphertext for the enhanced Caesar cipher encryption method is generated from a two-layer encryption. The first encryption applies the Caesar cipher method, while the second encryption converts the Caesar cipher text to alphanumeric form.

Figure 4 shows the output of the encryption of the plain text message "*I want you to come to my party on the second of November*" using a shift key equal to "12". The ciphertext generated was *"f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9."*

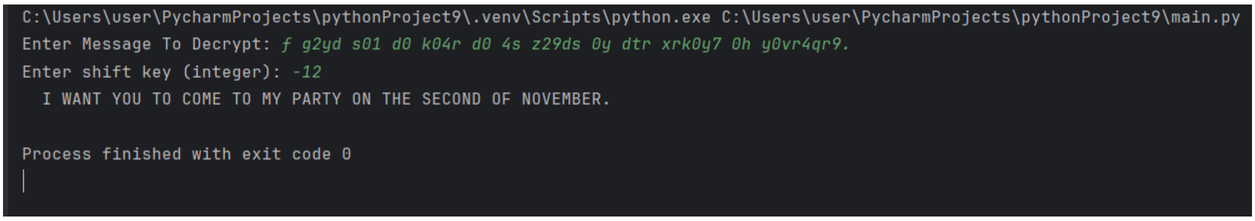


```
C:\Users\user\PycharmProjects\pythonProject8\.venv\Scripts\python.exe C:\Users\user\PycharmProjects\pythonProject8\main.py
Enter Message To Encrypt: I want you to come to my party on the second of November.
Enter shift key (integer): 12
 f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.

Process finished with exit code 0
```

Figure 4: Modified Caesar Cipher Encryption of Plain Text

To decipher the ciphertext generated in the modified encryption, a reverse system that performs the deciphering was used. Figure 5 shows the modified Caesar cipher decryption of cipher ciphertext produced by the encryption system. The decryption system first converts the alphanumeric form of the encrypted message to the Caesar cipher text in the first layer of deciphering before applying the reverse shift key (-12) to recover the original message.



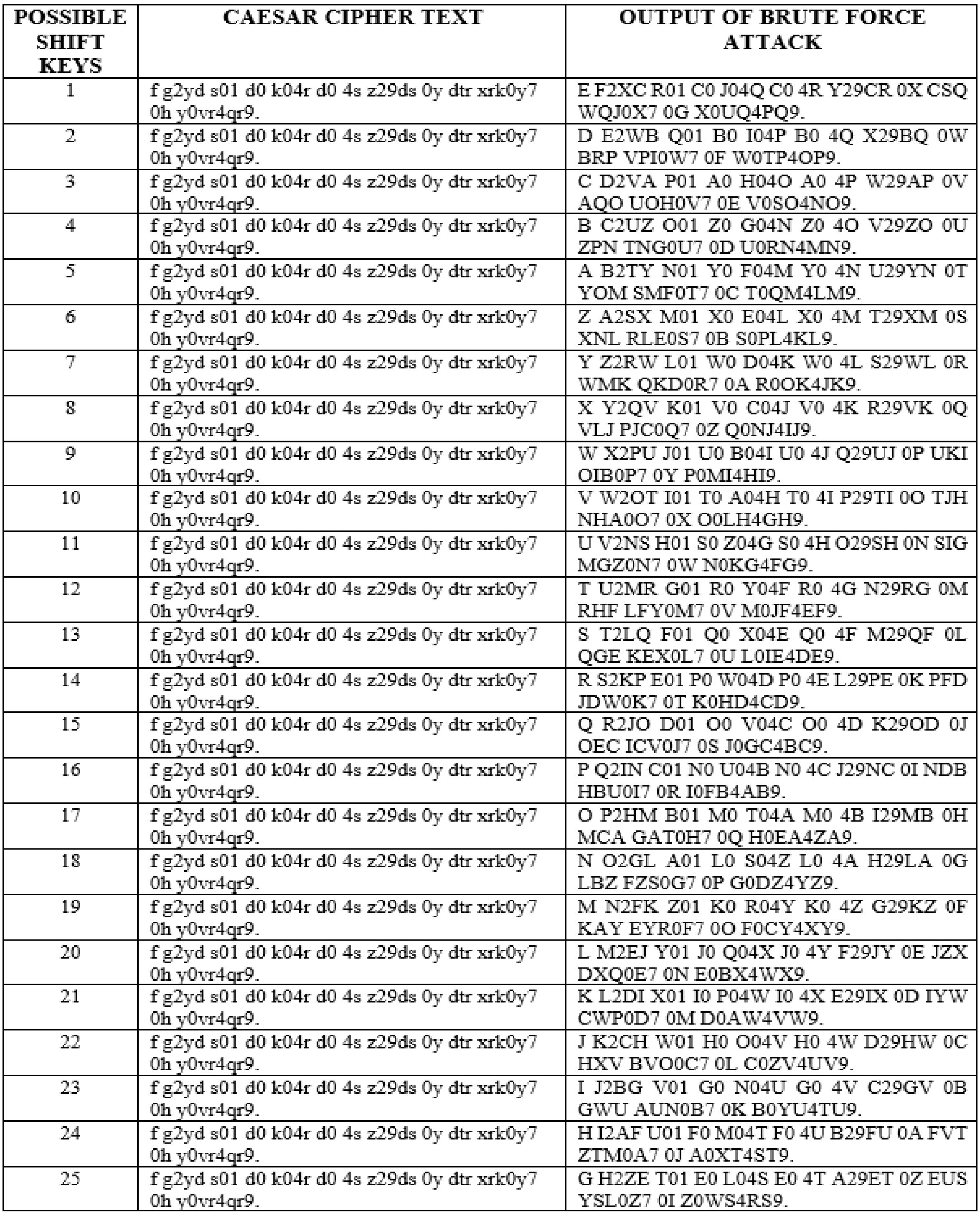
```
C:\Users\user\PycharmProjects\pythonProject9\.venv\Scripts\python.exe C:\Users\user\PycharmProjects\pythonProject9\main.py
Enter Message To Decrypt: f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.
Enter shift key (integer): -12
  I WANT YOU TO COME TO MY PARTY ON THE SECOND OF NOVEMBER.

Process finished with exit code 0
```

Figure 5: Modified Caesar Cipher Decryption of Cipher Text

In comparing the Caesar cipher encryption technique and the modified Caesar cipher encryption technique, the brute force approach was used to attempt to break the two encryption methods. From the viewpoint of an attacker, by examining the structure of the ciphertext of the Caesar cipher encryption technique, it will be easier to break using the brute force attack. For the modified Caesar cipher encryption technique, an attacker may not likely consider the ciphertext generated for breaking using the Caesar cipher shift key because of its alphanumeric nature. If an attacker wants to attempt to break the ciphertext of the modified Caesar cipher encryption technique, it will be difficult. Using the ciphertext generated from the modified Caesar cipher encryption for the same plain text, Table 2 shows the brute force attack using all the possible shift keys of the Caesar cipher. From the table, it is shown that trying all the Caesar cipher shift keys will not yield any intelligible text. Also, with no clearly defined mathematical function used, it is difficult for the code to be broken compared with the existing Caesar cipher encryption method. The only option available for an attacker to be successful in recovering the message is to have access to the alphanumeric table for conversion of the ciphertext.

Table 2: Brute Force Attack on Modified Caesar Cipher Encryption Technique



POSSIBLE SHIFT KEYS	CAESAR CIPHER TEXT	OUTPUT OF BRUTE FORCE ATTACK
1	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	E F2XC R01 C0 J04Q C0 4R Y29CR 0X CSQ WQJ0X7 0G X0UQ4PQ9.
2	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	D E2WB Q01 B0 I04P B0 4Q X29BQ 0W BRP VPI0W7 0F W0TP4OP9.
3	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	C D2VA P01 A0 H04O A0 4P W29AP 0V AQO UOH0V7 0E V0SO4NO9.
4	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	B C2UZ O01 Z0 G04N Z0 4O V29ZO 0U ZPN TNG0U7 0D U0RN4MN9.
5	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	A B2TY N01 Y0 F04M Y0 4N U29YN 0T YOM SMF0T7 0C T0QM4LM9.
6	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	Z A2SX M01 X0 E04L X0 4M T29XM 0S XNL RLE0S7 0B S0PL4KL9.
7	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	Y Z2RW L01 W0 D04K W0 4L S29WL 0R WMK QKD0R7 0A R0OK4JK9.
8	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	X Y2QV K01 V0 C04J V0 4K R29VK 0Q VLJ PJC0Q7 0Z Q0NJ4IJ9.
9	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	W X2PU J01 U0 B04I U0 4J Q29UJ 0P UKI OIB0P7 0Y P0MI4HI9.
10	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	V W2OT I01 T0 A04H T0 4I P29TI 0O TJH NHA0O7 0X O0LH4GH9.
11	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	U V2NS H01 S0 Z04G S0 4H O29SH 0N SIG MGZ0N7 0W N0KG4FG9.
12	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	T U2MR G01 R0 Y04F R0 4G N29RG 0M RHF LFY0M7 0V M0JF4EF9.
13	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	S T2LQ F01 Q0 X04E Q0 4F M29QF 0L QGE KEX0L7 0U L0IE4DE9.
14	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	R S2KP E01 P0 W04D P0 4E L29PE 0K PFD JDW0K7 0T K0HD4CD9.
15	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	Q R2JO D01 O0 V04C O0 4D K29OD 0J OEC ICV0J7 0S J0GC4BC9.
16	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	P Q2IN C01 N0 U04B N0 4C J29NC 0I NDB HBU0I7 0R I0FB4AB9.
17	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	O P2HM B01 M0 T04A M0 4B I29MB 0H MCA GAT0H7 0Q H0EA4ZA9.
18	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	N O2GL A01 L0 S04Z L0 4A H29LA 0G LBZ FZS0G7 0P G0DZ4YZ9.
19	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	M N2FK Z01 K0 R04Y K0 4Z G29KZ 0F KAY EYR0F7 0O F0CY4XY9.
20	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	L M2EJ Y01 J0 Q04X J0 4Y F29JY 0E JZX DXQ0E7 0N E0BX4WX9.
21	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	K L2DI X01 I0 P04W I0 4X E29IX 0D IYW CWP0D7 0M D0AW4VW9.
22	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	J K2CH W01 H0 O04V H0 4W D29HW 0C HXV BVO0C7 0L C0ZV4UV9.
23	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	I J2BG V01 G0 N04U G0 4V C29GV 0B GWU AUN0B7 0K B0YU4TU9.
24	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	H I2AF U01 F0 M04T F0 4U B29FU 0A FVT ZTM0A7 0J A0XT4ST9.
25	f g2yd s01 d0 k04r d0 4s z29ds 0y dtr xrk0y7 0h y0vr4qr9.	G H2ZE T01 E0 L04S E0 4T A29ET 0Z EUS YSL0Z7 0I Z0WS4RS9.

CONCLUSION

The use of the encryption method has been adopted in the early century. An example of the foremost encryption method is the Caesar cipher, where the shifting of the positions of the alphabet turns a plaintext into ciphertext. Julius Caesar used this method of encryption by transmitting his instructions to his army to deny his enemies the ability to comprehend his messages, even if they were intercepted. This code is simple to implement but not strong considering the capability of modern computing devices in the cryptanalysis of ciphertext (Mogollon, 2007). The implication of this is that Caesar's cipher method of encryption could not be considered in this modern computing era. Numerous algorithms have been developed after the Caesar substitution cipher, all of which come with higher complexities in implementation (Verma et al., 2017). This paper leverages the simplicity of the Caesar cipher method of encryption to develop a simple yet stronger encryption technique.

REFERENCES

Asoronye, G. O., Emereonye, G. I., Onyibe, C. O., & Agha, I. A. (2019). An Efficient Implementation for the Cryptanalysis of Caesar's Cipher. In *Melting Pot* (Vol. 5).

Bellovin, S. M. (2008). The Insider Attack Problem Nature and Scope. *Advances in Information Security*, *39*. https://doi.org/10.1007/978-0-387-77322-3_1

Dar, S. B. (2014). Enhancing The Security of Caesar Cipher Using Double Substitution Method. *International Journal of Computer Science & Engineering Technology (IJCSET)*, *5*(7).

Delfs, H., & Knebl, H. (2015). Introduction to cryptography: Principles and applications: Third edition. In *Introduction to Cryptography: Principles and Applications: Third Edition*. https://doi.org/10.1007/978-3-662-47974-2

Goyal, K., & Kinger, S. (2013). Modified Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications*, *73*(3). https://doi.org/10.5120/12722-9558

Gunawan, I., Sumarno, Tambunan, H. S., Irawan, E., Qurniawan, H., & Hartama, D. (2019). Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages. *Journal of Physics: Conference Series*, *1255*(1). https://doi.org/10.1088/1742-6596/1255/1/012077

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). https://doi.org/10.5120/ijca2015907062

Odijie, C. H., Olanrewaju, B. S., & Odijie, B. O. (2025). THE EMERGING TECHNOLOGIES, USE CASES, PROSPECTS, AND CHALLENGES OF 6G WIRELESS SYSTEMS. *International Journal Of Novel Research And Development*, *10*(1), 989–996.

Odijie, C. H., Olanrewaju, & Olayinka. (2024). 6G WIRELESS SYSTEM: PAVING THE PATH FOR THE FUTURE OF CONNECTIVITY. In *Wellspring University Journal of Science and Computing* (Vol. 1, Issue 1). https://ORCID.org/0009-0006-7450-9485

Olanrewaju, B. S., Oghene, F. B. ;, & Akilo, B. E. (2024). Implementation of Caesar Cipher Encryption Using Python Programming Language. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(5), 533–539.

Olanrewaju, B. S. , & Osunade, O. (2018). Design of a Mathematical Model for Spectrum Utilisation in Cognitive Radio. *International Journal of Computer Applications*, *180*(19). https://doi.org/10.5120/ijca2018916436

Sinclair, S., & Smith, S. W. (2008). Preventative Directions For Insider Threat Mitigation Via Access Control. *Advances in Information Security*, *39*. https://doi.org/10.1007/978-0-387-77322-3_10

Ugwunna, C. O., Okimba, P. E., Alabi, O. A., Orji, E. E., Olowofeso, E. O. & Ayomide, S. O (2025). ADVANCED ENCRYPTION STANDARD (AES) IMPLEMENTATION EFFICIENCY USING JAVA AND NODE.JS PLATFORMS. *FUDMA Journal of Sciences (FJS), 8(6) pp 42-49.* : https://doi.org/10.33003/fjs-2024-0806-2832

Verma, P., Gaba, G. S., & Miglani, R. (2017). Diversified Caesar Cipher for Impeccable Security. *International Journal of Security and Its Applications*, *11*(2). https://doi.org/10.14257/ijsia.2017.11.2.04

Vogel, M. (2011). Quantum Computation and Quantum Information, by M.A. Nielsen and I.L. Chuang. *Contemporary Physics*, *52*(6). https://doi.org/10.1080/00107514.2011.587535

©2025 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.