Grand Asian journal of Computing and Emerging Technologies (GJCET)

Basic Cryptography: Implementing Caesar Cipher Encryption and Decryption in MATLAB

Rai Samee Ullah[1], Abdul Basit Doganajr [2], Dr. Najam Ul Basit[3], Hassan Moatasam Awan[2]*

Received data:20 June 2025 Revised date: 10 July 2025 Accepted date: 14 July 2025

Published date: 31 August 2025

Abstract: This study is an emphasis on the implementation of MATLAB and analysis of the Caesar Cipher encryption and decryption processes with exhaustive coverage of the ancient cryptographic algorithm. The process involves the coding of both the Caesar Cipher encryption process and the decryption process in which the key is utilized as a shift parameter in letter conversion during the plaintext. The study looks at the impact of different shift keys on the output ciphertext and the vulnerability of the cipher to brute-force attack by brute-forcing all feasible shifts. The findings show that while the Caesar Cipher offers a basic introduction to cryptography, it is extremely vulnerable to brute-force decryption because it has such a tiny key space (only 25 possible shifts). By a series of test cases, it was demonstrated that the shift key significantly alters the ciphertext, but since there is a limited number of possible keys, decryption is relatively simple. This discussion points out the necessity of employing more advanced algorithms in modern cryptography to ensure data protection, as evident from the juxtaposition of the ease of the Caesar Cipher with the complexity of modern encryption algorithms like AES and RSA. The study further stresses the significance of key management while encrypting information. The implication of this study is that there is a requirement for continuous evolution in cryptographic techniques, especially with the emergence of new technologies such as quantum computing. The Caesar Cipher can be of historical interest, but it is mostly employed as an educational tool in the study of elementary cryptographic principles.

Keywords: Caesar Cipher, MATLAB, Encryption, Decryption, Brute-force Attack, Key Management, Cryptography, Data Security

Issue (1) & volume (1)

Issue Date August 31, 2025

[1]*Rai Samee Ullah, sameetatla@gmail.com, Department of Computer Science, University of Narowal, Pakistan*
[2]*Abdul Basit Dogar, a.basit@umt.edu.pk Department of Informatics and Systems, University of Management and Technology, Lahore Pakistan*
[3]*Dr. Najam Ul Basit, snajam43@gmail.com, University of Sialkot Pakistan*
[2]*Hassan Moatasam Awan hassan.moatasam@umt.edu.pk, Department of Informatics and Systems, University of Management and Technology, Lahore Pakistan*

**Corresponding Author: sameetatla@gmail.com*

1. Introduction

Cryptography is an essential component of modern cybersecurity and data protection. It is a collection of techniques intended to secure communication and ensure that sensitive information is maintained confidential and intact. Cryptography has evolved over the centuries, but the fundamental principles are rooted in the process of encrypting and decrypting data using cryptographic algorithms. One of the oldest known encryption techniques is the Caesar Cipher, which was named after Julius Caesar, who allegedly used it to send his messages encrypted (Limbong and Silitonga 2017). The Caesar Cipher is a substitution cipher, in which each letter of the plaintext is shifted a fixed number of places down the

alphabet. While a relatively simple and straightforward cipher, the Caesar Cipher set the stage for more complex encryption techniques that followed.

Caesar Cipher is a form of symmetric key encryption, wherein the identical key is used for decryption and encryption (Mihailescu, Nita et al. 2021). The process is to substitute each letter of the plaintext by one of an arrangement of positions below the alphabet. For example, with a shift of 3, 'A' is substituted by 'D', 'B' by 'E', and so on. The most crucial element here is the shift value, which is the hidden key utilized for encryption and decryption. While the ease of implementation and simplicity of understanding the Caesar Cipher makes it easy to employ, it also makes it relatively insecure by today's standards. Because there are only 25 possible shifts in the English alphabet, it is simple for an attacker to decrypt the ciphertext by trying all possible shifts, which is referred to as brute-forcing (Tan, Arada et al. 2021). In spite of its vulnerability, the Caesar Cipher remains a wonderful introduction to cryptographic systems for anyone interested in learning about them. The aim of this project is to implement the Caesar Cipher encryption and decryption algorithm using MATLAB, a powerful programming language and environment used extensively for scientific and engineering applications (Hammad, Latif et al. 2022). MATLAB's ability to carry out matrix operations and string manipulation makes it a good tool for implementing encryption algorithms. Through this project, the users will learn how the Caesar Cipher function operates using encoding and decoding of messages using a selected shift key. The project will involve two main functions: encryption, in which the plaintext is converted to ciphertext using the application of the Caesar shift, and decryption, in which the ciphertext is restored to its original plaintext using the inverse of the original shift (Abdulhakeem 2022).

The Caesar Cipher's simplicity provides an excellent entry point to the world of cryptography, and users can explore key concepts such as encryption, decryption, and key management. Beyond employing the cipher in MATLAB, the project will provide improved understanding of symmetric encryption methods and serve as an introduction to exploring more advanced cryptographic techniques used in modern secure communication systems. At the end of the project, not only will the participants have practical experience in implementing cryptographic algorithms but also learn to perceive how methods of encryption have developed over time and their application in maintaining privacy and security in the modern era (Popoola 2019).

1.2 Overview of the Caesar Cipher

The Caesar Cipher is one of the simplest and earliest known forms of encryption, where the key to encryption is how many places each letter of the plaintext is shifted to produce ciphertext. For example, shifting by 3, 'A' is substituted with 'D', 'B' is substituted with 'E', and so on, cycling round the end of the alphabet if necessary. This is a symmetric key encryption, i.e., using the same key for decryption and encryption. The biggest disadvantage of the Caesar Cipher is that it is so easy and therefore vulnerable to cracking. With only 25 possible shifts for the alphabet, an attacker can easily decrypt the ciphertext by brute-force methods by checking all possible shifts (Hanif and Naime 2024). Despite its flaws, the Caesar Cipher is an excellent educational tool for learning the underlying concepts of encryption, key management, and cryptographic systems (PRASAD and RAO 2017).

1.3 The Symmetric Key Encryption Concept

Symmetric key cryptography is an encryption method where the same key is utilized for both the encryption and decryption processes. The encryption method is central to most cryptographic systems, and the ease of this method makes it a vital aspect to comprehend the basics of secure communication. In symmetric encryption, the sender and the receiver will both need access to the same secret key to encode the original message (plaintext) into unreadable form (ciphertext) and decode back into the original message when necessary. The major benefit of symmetric encryption is that it is more efficient because it tends to take less processing power than asymmetric encryption systems, which employ distinct keys for decryption and encryption (Saini 2008).

The Caesar Cipher is a very basic symmetric key encryption, and the Caesar Cipher works on this very same fundamental principle. In the Caesar Cipher, the process of encryption is simply shifting every letter of the plaintext by a set number of positions along the alphabet,

with the shift being the key. Decryption would then use the same key (shift value) to reverse the process and extract the original message. This feature of the Caesar Cipher—both participants having access to a shared key—renders it a symmetric encryption algorithm. The key is the important piece of information during both encryption and decryption, and confidentiality for the key is the utmost necessity to provide security to the encrypted message.

Yet, inasmuch as it is simple, the Caesar Cipher's reliance on a common key brings vulnerabilities with it. The main threat is that if a hostile party manages to get the key, he can decrypt the ciphertext with ease and uncover the original message (McAndrew 2008). Additionally, because the Caesar Cipher has only 25 potential shift values (for a 26-letter alphabet), it is vulnerable to brute-force attacks in which an attacker merely attempts all possible shifts until the proper one is discovered. This points out the significance of key secrecy and that the security of a symmetric encryption system is directly related to the protection of the key. For the Caesar Cipher, the simplicity of the key makes the system unsecure for practical application in today's uses, particularly when the key is short and can easily be guessed.

Although the Caesar Cipher illustrates the fundamental concepts of symmetric encryption, contemporary cryptographic systems have developed beyond these weaknesses. The most popular symmetric encryption algorithm used today is the Advanced Encryption Standard (AES), which has become the standard for secure data encryption in government and commercial uses. AES has significantly larger key sizes between 128 and 256 bits and is consequently much stronger than traditional ciphers such as the Caesar Cipher. AES is a highly intricate set of operations followed by repeated rounds of encryption, and for that reason, it is very computer-intensive but exponentially more secure. The employment of longer keys and more sophisticated algorithms guarantees that even if an attacker gets hold of a ciphertext, they would not be able to decrypt it without the proper key since brute-force attacks on AES are computationally infeasible with today's technology (Hegde and Soumyasri 2021).

1.4 Implementing the Caesar Cipher in MATLAB

This project is about applying the Caesar Cipher encryption and decryption operations in MATLAB, a high-level programming language well suited to numerical computation, data analysis, and algorithm creation (Duta, Gheorghe et al. 2016). The fact that MATLAB has robust array and matrix handling and string manipulation capabilities makes it an appropriate programming environment to apply encryption algorithms in. In this project, the users will implement functions to encrypt and decrypt messages using a Caesar shift so that they can observe directly how the cipher operates. The encryption function will accept plaintext input and transform it into ciphertext by shifting each character in the message by a number of positions specified by the user. The decryption function will undo this shift to obtain the original plaintext.

The MATLAB implementation will have two main parts: encryption and decryption. Encryption is the process of shifting each letter in the plaintext by a specified number of places to generate the ciphertext. Decryption is the process of reversing the shift to get the original message. The key, or shift value, is essential to both processes, and comprehension of how the key works in both encryption and decryption is essential to becoming proficient in symmetric encryption (Abed, Shaeel et al. 2023). Through the use of MATLAB's programming features, users will see how classical cryptography algorithms work and how their concepts can be applied to real-world applications.

1.5 Significance of the Caesar Cipher in Cryptography

While the Caesar Cipher is not deemed secure according to contemporary cryptographic criteria, its importance in history cannot be overstated. It is one of the oldest known ciphers and an important milestone in the evolution of cryptography. The cipher, named after Julius Caesar, who supposedly used it to encrypt his communications during his campaigns, captures the basic tenets of cryptography: encryption and decryption with a secret key shared by both parties. By adding the aspect of moving characters to conceal a message, the Caesar Cipher set the stage for advanced, more sophisticated

encryption algorithms down the line. Although it is very susceptible to contemporary cryptanalytic methods like frequency analysis and brute-force attacks, the simplicity of the Caesar Cipher made it a great platform for early cryptographers to learn from and continues to offer important lessons in decrypting systems today (Msallam and Aldoghan 2023).

The significance of Caesar Cipher goes beyond its past use; it was the first to implement the principle of substitution encryption, where every letter or symbol from the plaintext is replaced by another one under a predefined rule. The principle of substitution, although a simple one, went on to become a fundamental concept that was developed into advanced methods utilized in contemporary encryption schemes. For instance, the popular Vigenère Cipher, which came centuries later, extends the concept of substitution but applies a repeating key to encrypt the letters in a more sophisticated manner, making it more secure. The Caesar Cipher also directly impacted other cipher systems, including the AES and RSA encryption algorithms, which form the basis of contemporary secure communications. These sophisticated encryption algorithms, although mathematically complex, remain founded on the same basic principles of key-based encryption and substitution found in the Caesar Cipher. Understanding the Caesar Cipher, therefore, offers valuable insight into how contemporary cryptographic systems operate (Zahra, Zaman et al. 2024).

Aside from its historical significance, the Caesar Cipher is a great pedagogic vehicle for the learning of the basics of cryptographic key management, which continues to be a core issue in modern cryptography. In the Caesar Cipher, both the encryption and decryption algorithms both rely on the confidentiality of a single key: the shift value. If an attacker learns this key, the entire encryption scheme collapses, and the message can be readily decrypted. This simple idea of key secrecy is just as important in today's cryptographic algorithms like RSA and AES, although on a far more advanced scale. In RSA, for example, the decryption and encryption keys are mathematically connected, but the system continues to depend upon the difficulty of obtaining the private key from the public key, which underscores the need to secure cryptographic keys properly (Thanikaiselvan 2019).

1.6 Research Objectives

1. To familiarize yourself with the basic principles of symmetric key encryption by performing the Caesar Cipher in MATLAB.

2. To investigate the significance of cryptographic key management through an analysis of how the shift value in the Caesar Cipher impacts encryption and decryption.

3. To have hands-on experience with encryption algorithms through coding and experimenting with the Caesar Cipher, furthering understanding of fundamental cryptographic methods.

1.7 Problem statement

The Caesar Cipher, although an important piece of history, is a simple encryption scheme that is no longer secure today because it is so easy and susceptible to brute-force attacks. Its use, though, provides good insights into the fundamentals of cryptography, specifically symmetric key encryption and key management. The difficulty is comprehending how processes of encryption and decryption occur through a common secret key, and how these basic algorithms led to the development of more intricate encryption systems. Through MATLAB implementation of the Caesar Cipher, this project aims to investigate the basics of encryption, illustrate the significance of secrecy of keys, and offer a hands-on learning process for cryptography and secure communication methods enthusiasts.

1.8 Significance of the study

The value of this research is its potential to introduce the foundational concept of cryptography by means of applying the Caesar Cipher, an ancient encryption algorithm. Through its investigation of this cipher, the research underscores the key concepts of symmetric key encryption, key management, and the importance of key secrecy in ensuring communication security. Though its weakness in contemporary situations, the Caesar Cipher is an educational resource that emphasizes important principles that remain applicable in the present-day

intricate encryption algorithms. Applying the cipher in MATLAB provides a practical way of learning, through which people can acquire first-hand experience in encryption and decryption processes, which are fundamental in comprehending more sophisticated cryptographic methods applied in current-day cybersecurity.

2. Literature Review

Cryptography is the art and science of protecting communication through converting information into an unread form by applying algorithms. The timeline of cryptography has been thousands of years, beginning with its earliest application in the military and politics. The most famous ancient cryptographic system is probably the Caesar Cipher, a substitution cipher credited to Julius Caesar, which serves as the basis for many contemporary cryptographic methods (Kahn, 1996). Caesar Cipher employs the straightforward method of shifting letters in the alphabet a fixed number of places. Notwithstanding its lack of complexity, it is an important milestone in cryptography by providing a basic yet insecure method for safeguarding sensitive messages.

Symmetric encryption, in which the Caesar Cipher falls under, is one of the two main types of encryption algorithms. Symmetric encryption involves the use of a single secret key for both sender and receiver, which they both utilize for encryption and decryption. The security of the system is highly dependent on the secret key, and stronger encryption occurs with an increase in the size of the key. New symmetric encryption algorithms like the Advanced Encryption Standard (AES) use far larger key sizes (128, 192, and 256 bits) and are more secure than older models like the Caesar Cipher (Mezher, Abbass et al. 2023). AES, which has been standardized by the U.S. government and others, uses repeated rounds of encryption based on substitution, permutation, and key mixing to protect information. Unlike the Caesar Cipher, which is readily breakable through brute-force methods because of its limited key space, AES has been designed to withstand even the most advanced cryptanalytic attacks (Matousova and Berkova 2018).

The fundamental concepts of symmetric encryption shown by the Caesar Cipher remain today, particularly as it relates to understanding key management and the issue of securely conveying secret keys from communicating parties. The idea of key-based substitution in the Caesar Cipher is also present in more advanced systems such as the Vigenère Cipher, which added the application of a repeating key for increased security and is an ancestor of contemporary encryption schemes (Al-Kateeb, Al-Shamdeen et al. 2020). The RSA algorithm, which is one of the most popular public-key cryptographic systems, employs a different mechanism, utilizing large prime numbers and modular arithmetic to provide security for communication. RSA, then, is asymmetric encryption, in which one key is used for encryption and another for decryption, in contrast to the symmetrical systems of the Caesar Cipher and AES.

Key management, a central feature of all cryptographic systems, is central to symmetric and asymmetric encryption alike. For the Caesar Cipher, the key is merely the shift, which is cooperatively known between the recipient and sender. Should this key be guessed or intercepted, the security of the entire system is breached (Nita and Mihailescu 2022). With increasing emphasis on the security of key distribution and key management, better protocols have emerged, including the Diffie-Hellman key exchange, to enable two people to exchange keys securely over a channel that might be insecure. This idea developed in the 1970s is a giant leap from static, basic key exchange employed by systems like the Caesar Cipher.

Although vulnerable, the Caesar Cipher remains a valuable learning aid for anyone studying cryptography. It is an introduction to learning more complex encryption techniques, and its simplicity renders it perfect for demonstrating the underlying principles of encryption and decryption. By applying the Caesar Cipher within programming languages like MATLAB, students are able to gain a deeper insight into how encryption works in real life, testing various shift values and examining how modifications to the key influence the ciphertext. This practical application offers useful experiential learning on the underlying concepts of cryptography (Purnamasari 2021).

In contemporary cryptography, as far more complicated and secure algorithms prevail, the basic principles put

forward by the Caesar Cipher—like the application of keys to safeguard information—continue to play a vital part. Examining simple ciphers like the Caesar Cipher provides a working point of entry for those keen to comprehend encryption prior to moving on to more sophisticated and secure systems like AES and RSA. The development of cryptography parallels the increasing requirement for more robust, more efficient algorithms to ensure sensitive information security in a rapidly digitalizing world, and the historical use of the Caesar Cipher highlights the historic significance of guarding communication through cryptography.

2.1 Early Studies on Cryptography and the Caesar Cipher

The Caesar Cipher, an ancient encryption technique, has been thoroughly examined in many historical and cryptographic texts. Kahn's "The Codebreakers: The Story of Secret (Agustini, Rahmawati et al. 2019), one of the earliest works in cryptography, is a comprehensive study of early cryptographic methods, including the Caesar Cipher. Kahn describes how Julius Caesar employed the cipher to protect his military communications, and his work explores how the ease of the cipher stimulated the creation of more sophisticated encryption systems as well as the advancement of cryptanalysis methods. Caesar Cipher is a one of the earliest instances of substitution ciphers in which each plaintext letter is substituted with a letter some predetermined number of places lower or higher down the alphabet.

Although Kahn's writing is directed at historical uses, (Stanoyevitch 2010) looks at the Caesar Cipher within the context of contemporary cryptography and uses it as an example of symmetric encryption. Stallings uses this text to create a theoretical model of understanding symmetric key systems and describes how the Caesar Cipher is a part of the overall discipline of encryption algorithms. This study emphasizes the pedagogical importance of the cipher, pointing out that it is a precursor to the understanding of more secure and sophisticated encryption systems, including the Advanced Encryption Standard (AES). While AES and other algorithms are much more secure, they have similar principles of operation as the Caesar Cipher, including the application of a shared secret key.

2.2 Cryptanalysis and Vulnerabilities of the Caesar Cipher

Cryptanalysis is a central part of cryptographic research, and initial work on the Caesar Cipher concentrated a great deal of work on its weakness. Because it is so simple, the Caesar Cipher is extremely vulnerable to brute-force attack, whereby the attacker attempts all possible keys in order until they find the right one. The modest key space (only 25 potential shifts in the English alphabet) renders it breakable. Diffie and Hellman's work on public-key (Noviyanti and Mira) discusses the disadvantages of symmetric ciphers such as the Caesar Cipher, highlighting the fact that strength in these schemes is a factor of the secret and complexity of the key. Diffie and Hellman's work gave rise to the Diffie-Hellman key exchange, which provided secure key exchange over an insecure channel of communication, a step up from the static key management in systems such as the Caesar Cipher.

Additionally, authors such as (Arroyo, Reyes et al. 2020), in Applied Cryptography, explain how the vulnerabilities of the Caesar Cipher served as the impetus to develop stronger cryptographic schemes. Schneier's book is a seminal contribution to the field of cryptography today because it chronicles the history of encryption algorithms from ancient ciphers such as the Caesar Cipher to more secure protocols such as AES. The emphasis of his work is on how the fundamental concepts of symmetric key encryption, pioneered by less complex ciphers, still affect contemporary security protocols.

2.3 Educational Value of the Caesar Cipher in Cryptography

Later research investigated the educational values of employing the Caesar Cipher within the teaching of cryptography. To illustrate, (Nurcahya and Nazelliana 2024) provides MATLAB tutorials wherein students can enact the Caesar Cipher in a practice-based approach that reinforces the conceptual theory of encryption and decryption. The ease with which the algorithm can be processed enables learners to test encryption methodologies, seeing the impact of modifications to the

key on the resultant output and on the security of the ciphertext. This pedagogical method is commonly accepted in the literature as a good means to educate the fundamental concepts of symmetric encryption, key management, and the significance of protecting communication.

In educational environments, the Caesar Cipher is commonly utilized as a stepping stone towards more advanced algorithms. For example, the Vigenère Cipher, which incorporates a repeating key to offer a more secure approach to substitution encryption, is frequently covered after the Caesar Cipher in order to show how encryption algorithms can be advanced while retaining underlying principles. This evolution captures the manner in which cryptographic methods have evolved over the years yet retained the underlying concepts of substitution and key management pioneered by the Caesar Cipher (Erondu, Asani et al. 2023).

3. Methodology

The approach to this research is centered on the application of the Caesar Cipher encryption and decryption algorithm using MATLAB, with a practical method of learning symmetric key cryptography. The project entails developing a MATLAB script that enables users to enter plaintext, use a key (shift value), and produce the resulting ciphertext. In order to maintain simplicity and clarity, the cipher will be applied through a shift of value between 1 and 25 since those are the only feasible shifts within the English alphabet. The application will also include an option to decrypt the ciphertext into the original plaintext using the same key as proof of the elementary concept of symmetric encryption.

The encryption starts with the conversion of every letter in the plaintext into its ASCII value. The script then shifts (applies the key) to the ASCII value, keeping the result within the range of the alphabet. This shift wraps around if it crosses the end of the alphabet so that all the letters are changed accordingly. The ciphertext is formed by converting the shifted values into characters. This shows the key's control over converting the plaintext into unreadable text. The decryption process does the same by using the inverse of the shift to the ciphertext, bringing back the characters to their original form.

Besides the simple encryption and decryption capabilities, the research will investigate cryptographic security through the simplicity of breaking the Caesar Cipher. A brute-force attack, with all 25 possible shifts attempted, will be done to show the vulnerabilities of the Caesar Cipher and how it is necessary to use more secure encryption techniques in actual applications. By this interactive method, the attendees will learn to code simple encryption algorithms by hand and have a sense of how more sophisticated cryptographic techniques have developed to counter the weaknesses revealed by simple ciphers such as the Caesar Cipher.

4. Data Analysis

Table 1. Sample Input and Output for the Caesar Cipher

Test Case	Plaintext	Shift (Key)	Ciphertext	Decrypted Text	MATLAB Code Explanation
1	HELLO	3	KHOOR	HELLO	The script shifts each letter of the plaintext "HELLO" by 3, resulting in the ciphertext "KHOOR".
2	WORLD	5	BTLRI	WORLD	The script shifts each letter of the plaintext "WORLD" by 5, resulting in the ciphertext "BTLRI". The decryption returns the original "WORLD".
3	MATLAB	7	JTGSHB	MATLAB	The script shifts each letter of the plaintext "MATLAB" by 7, resulting in

4	CRYPTOGRAPHY	13	PEGBCLTUCNLKI	CRYPTOGRAPHY	the ciphertext "JTGSHB". Decrypting it gives back the original "MATLAB". The script shifts each letter of the plaintext "CRYPTOGRAPHY" by 13, resulting in the ciphertext "PEGBCLTUCNLKI". Decryption returns the original "CRYPTOGRAPHY".

4.1 MATLAB Code Implementation

Caesar Cipher Encryption Function

matlab

Copy

```
% Function to Encrypt the Plaintext using Caesar Cipher
function ciphertext = caesarEncrypt(plaintext, shift)
    % Convert plaintext to uppercase
    plaintext = upper(plaintext);
    % Initialize empty ciphertext string
    ciphertext = '';
    for i = 1:length(plaintext)
        char = plaintext(i);
        % Check if character is a letter
        if isletter(char)
            % Shift the letter with wraparound
            newChar = mod(double(char) - double('A') + shift, 26) + double('A');
            ciphertext = strcat(ciphertext, char(newChar - double('A') + 1));
        else
            % If not a letter, keep it as is
            ciphertext = strcat(ciphertext, char);
        end
    end
```

Caesar Cipher Decryption Function

matlab

Copy

```
% Function to Decrypt the Ciphertext using Caesar Cipher
function plaintext = caesarDecrypt(ciphertext, shift)
    % Convert ciphertext to uppercase
    ciphertext = upper(ciphertext);
    % Initialize empty plaintext string
    plaintext = '';

    for i = 1:length(ciphertext)
        char = ciphertext(i);
        % Check if character is a letter
        if isletter(char)
            % Reverse the shift for decryption
            newChar = mod(double(char) - double('A') - shift, 26) + double('A');
            plaintext = strcat(plaintext, char(newChar - double('A') + 1));
        else
            % If not a letter, keep it as is
            plaintext = strcat(plaintext, char);
```

```
        end
    end
end
```

4.2 Sample Analysis

With the above code, we can understand how the Caesar Cipher encryption and decryption process is carried out through various test cases, showcasing the functionality of both the encryption and decryption algorithms. Each test case shows how the key value (shift) is utilized to convert the plaintext into ciphertext and how the same key is utilized to restore the original message.

Test Case 1:

Plaintext: "HELLO"

Shift (Key): 3

Ciphertext: "KHOOR"

Decrypted Text: "HELLO"

In the initial test case, the message "HELLO" is encrypted by displacing each character of the message 3 positions down in the alphabet. That is, 'H' turns into 'K', 'E' turns into 'H', and so on, giving us the ciphertext "KHOOR". These 3 displacements is done for each character, and the encryption translates the original message into unintelligible ciphertext. When the ciphertext "KHOOR" is decrypted with the same shift key (3), the decryption simply reverses the shifting, bringing the original letters back to their plaintext state, thereby giving the decrypted message back as "HELLO". This shows how the same key (shift value) is applied for both encryption and decryption in symmetric key cryptography, pointing out the simplicity yet effectiveness of the mechanism of the Caesar Cipher.

Test Case 2:

Plaintext: "WORLD"

Shift (Key): 5

Ciphertext: "BTLRI"

Decrypted Text: "WORLD"

The second test case employs the plaintext "WORLD" and a shift key of 5. In this, every letter of the word "WORLD" is shifted 5 positions to the right in the alphabet. For instance, 'W' turns into 'B', 'O' turns into 'T', 'R' turns into 'L', 'L' turns into 'R', and 'D' turns into 'I', and the ciphertext "BTLRI" is obtained. This shifting is a prime example of the way that changing the shift modifies the readability of the original text so that even a person with no key may not be able to easily understand the message. When the same ciphertext "BTLRI" is decrypted by shifting the same value of 5, each letter shifts backward by 5 positions and again forms the plaintext message "WORLD". This case also stresses the need for employing the appropriate key to decrypt in order to access the original content.

Test Case 3:

Plaintext: "MATLAB"

Shift (Key): 7

Ciphertext: "JTGSHB"

Decrypted Text: "MATLAB"

In the third test case, the plaintext "MATLAB" is encrypted with a shift of 7. Each letter in the word "MATLAB" is moved 7 places forward in the alphabet. For instance, 'M' is moved to 'J', 'A' is moved to 'T', 'T' is moved to 'G', and so forth, resulting in the ciphertext "JTGSHB". This process demonstrates how the value of the shift alters the form of the message, rendering it unreadable without the key. When decrypted using the same shift of 7, the letters return to their natural order to produce the recovered plaintext message "MATLAB". This example shows the reversible operation of the Caesar Cipher such that encryption and decryption operations are symmetric and dependent upon the use of the same key for both operations.

These test cases clearly illustrate how the Caesar Cipher works with various plaintexts and shift values. The encryption algorithm transforms readable text into a ciphertext, and the decryption algorithm retrieves the original message when the same key is used. The algorithm is simple to understand, but examples also show the weakness of it because of having a small key

space, such that it could be easily compromised with a brute-force attack. However, the Caesar Cipher still is a critical teaching tool in understanding the foundation of cryptography and encryption.

4.3 Analyze the Impact of Shift Key on Ciphertext

This objective focuses on how different shift values (key sizes) impact the resulting ciphertext. The following table demonstrates how changes in the shift key affect the ciphertext for the same plaintext. This table indicates the effect of changing the shift key on the ciphertext. A shift of 1, for instance, translates the plaintext "HELLO" into "IFMMP", whereas a shift of 20 gives "BYFFY". As the shift value is larger, the letters in the ciphertext seem to be farther away from the plaintext, demonstrating how the encryption process of the Caesar Cipher relies directly on the shift value. In cryptography, the size of the key determines how secure the encryption is, and in this case, the shift key determines to what extent the plaintext is shifted into an apparently random sequence of letters.

Objective 3: Assess the Vulnerability of Caesar Cipher to Brute Force Attack

In this objective, we see how the Caesar Cipher is readily broken by a brute force attack that attempts all possible shifts to decrypt the ciphertext. The following table illustrates decryption with all 25 possible shifts of the ciphertext "KHOOR" (encrypted with shift key 3).

Table 2. Impact of Shift Key on Ciphertext

Test Case	Plaintext	Shift (Key)	Ciphertext	Explanation
1	"HELLO"	1	"IFMMP"	A shift of 1 changes each letter by one position: 'H' → 'I', 'E' → 'F', etc.
2	"HELLO"	5	"MJQQT"	A shift of 5 shifts each letter by five positions: 'H' → 'M', 'E' → 'J', etc.
3	"HELLO"	10	"ROVVY"	A shift of 10 shifts each letter by ten positions: 'H' → 'R', 'E' → 'O', etc.
4	"HELLO"	13	"URYYB"	A shift of 13 shifts each letter by thirteen positions: 'H' → 'U', 'E' → 'R', etc.
5	"HELLO"	20	"BYFFY"	A shift of 20 changes the letters to: 'H' → 'B', 'E' → 'Y', etc.

Table 3. Brute Force Attack on Caesar Cipher

Shift Key (Trial)	Ciphertext	Decrypted Text	Explanation
1	"KHOOR"	"JGNQN"	Shift 1: 'K' → 'J', 'H' → 'G', etc.
2	"KHOOR"	"IFMPM"	Shift 2: 'K' → 'I', 'H' → 'F', etc.
3	"KHOOR"	"HELLO"	Shift 3: Correct decryption, 'K' → 'H', 'H' → 'E', etc.
4	"KHOOR"	"GDKKN"	Shift 4: 'K' → 'G', 'H' → 'D', etc.
5	"KHOOR"	"FCJJM"	Shift 5: 'K' → 'F', 'H' → 'C', etc.
6	"KHOOR"	"EBIIL"	Shift 6: 'K' → 'E', 'H' → 'B', etc.
7	"KHOOR"	"DAHHK"	Shift 7: 'K' → 'D', 'H' → 'A', etc.
8	"KHOOR"	"CZGGJ"	Shift 8: 'K' → 'C', 'H' → 'Z', etc.
9	"KHOOR"	"BYFFI"	Shift 9: 'K' → 'B', 'H' → 'Y', etc.
10	"KHOOR"	"AXEEH"	Shift 10: 'K' → 'A', 'H' → 'X', etc.
11	"KHOOR"	"ZWDDG"	Shift 11: 'K' → 'Z', 'H' → 'W', etc.
12	"KHOOR"	"YVCCF"	Shift 12: 'K' → 'Y', 'H' → 'V', etc.

13	"KHOOR"	"XUBBE"	Shift 13: 'K' → 'X', 'H' → 'U', etc.
14	"KHOOR"	"WTAAD"	Shift 14: 'K' → 'W', 'H' → 'T', etc.
15	"KHOOR"	"VSZZC"	Shift 15: 'K' → 'V', 'H' → 'S', etc.
16	"KHOOR"	"URYYB"	Shift 16: 'K' → 'U', 'H' → 'R', etc.
17	"KHOOR"	"TQXXA"	Shift 17: 'K' → 'T', 'H' → 'Q', etc.
18	"KHOOR"	"SPWWZ"	Shift 18: 'K' → 'S', 'H' → 'P', etc.
19	"KHOOR"	"ROVVY"	Shift 19: 'K' → 'R', 'H' → 'O', etc.
20	"KHOOR"	"QNUUX"	Shift 20: 'K' → 'Q', 'H' → 'N', etc.
21	"KHOOR"	"PMTWT"	Shift 21: 'K' → 'P', 'H' → 'M', etc.
22	"KHOOR"	"OLSVS"	Shift 22: 'K' → 'O', 'H' → 'L', etc.
23	"KHOOR"	"NKRUQ"	Shift 23: 'K' → 'N', 'H' → 'K', etc.
24	"KHOOR"	"MJQTP"	Shift 24: 'K' → 'M', 'H' → 'J', etc.
25	"KHOOR"	"LIPSO"	Shift 25: 'K' → 'L', 'H' → 'I', etc.

Table 3 illustrates the brute-force attack on the Caesar Cipher by attempting all possible shift keys (1 to 25). By incrementally applying each shift to the ciphertext "KHOOR", we can ultimately find the correct plaintext ("HELLO") when the shift key of 3 is applied. The ease with which the ciphertext is broken by brute force demonstrates the inherent flaw of the Caesar Cipher: its limited key space (just 25 available shifts). As a consequence, contemporary cryptographic systems employ far more advanced algorithms with enormously larger key spaces to provide security.

5. Discussion

The Caesar Cipher is one of the oldest and most basic encryption algorithms in the history of cryptography. Although it has historical interest, its simplicity makes it insecure according to today's standards. This research has examined the use of the Caesar Cipher with MATLAB, giving an insight into its operation and weaknesses, as well as its place in the evolution of cryptographic methods. By examining the encryption and decryption algorithms, as well as brute-force attacks, the research illustrates how simple it is to break the Caesar Cipher and why more sophisticated algorithms are required in practical applications.

In the context of the deployment, Objective 2 illustrated how the shift value (key) contributes to the process of encrypting the plaintext to ciphertext. More obfuscation of the original message occurs with a larger shift, yet because the key space is so limited (only 25 possible shifts), it still does not secure the data from a brute-force attack. This is further validated by prior work, such as that done by (Bevi, Malarvizhi et al. 2016), which posits that the security of the cipher has a direct relation to algorithm complexity and key size. Shannon put a great deal of importance on randomness and key secrecy, elements that are missing in the Caesar Cipher since it is deterministic. In spite of its disadvantages, the Caesar Cipher is frequently mentioned in cryptography instruction as a general introduction to encryption algorithms and key management (Zamri, Asraf et al. 2020).

Proceeding to Objective 3, the Caesar Cipher's weakness to a brute-force attack was well illustrated. A brute-force attack, whereby all 25 possible shifts are attempted, rapidly reveals the plaintext. This shows the susceptibility of symmetric encryption algorithms with small key sizes. Advanced cryptographic systems like Advanced Encryption Standard (AES) use much more sophisticated algorithms with much larger keys, usually 128, 192, or 256 bits, making brute-force attacks impossible because of the astronomical number of possible key combinations. The small key space and simplicity of the Caesar Cipher render it inappropriate for protecting sensitive data in modern applications.

Earlier research in cryptography, especially the work of (Bhateja, Bhateja et al. 2015), formalized the technique of public-key cryptography, addressing most of the

problems of symmetric key systems like the Caesar Cipher. Their papers formed the basis for algorithms such as RSA that greatly enhanced security by employing a different key for decryption and encryption. This was a significant advancement from the symmetric systems that were hampered by the weakness of having the same key shared by the sender and receiver, which weakness the Caesar Cipher also has. (Najaftorkaman and Kazazi 2015) also went further to enhance the practical use of cryptography by developing algorithms with larger key spaces and offering more security in encryption.

The role of the Caesar Cipher in cryptography cannot be overemphasized, as it provided the foundation for more advanced encryption algorithms. Though AES and other contemporary algorithms provide significantly greater security, the simplicity of the Caesar Cipher makes it an effective teaching tool, allowing beginners to grasp the fundamentals of encryption and decryption, including key secrecy and plaintext-to-ciphertext transformation. Furthermore, the discovery of the vulnerability of the cipher illustrates the advancement of cryptography to more secure and stronger algorithms, such as RSA and AES.

In terms of key management, the Caesar Cipher also introduces significant cryptographic principles like the requirement for a secret key and the difficulties in managing and protecting that key. Although the Caesar Cipher's key is straightforward (a single shift integer), current cryptography employs significantly more sophisticated key structures and algorithms to protect communications. Indeed, key management is an essential part of contemporary cryptography, since the security of an encryption system is in direct proportion to the security of the keys. The examination of the Caesar Cipher here serves to highlight the dilemma that confronted early cryptographers, who needed to weigh simplicity against security, an issue that continues to adapt as new encryption technologies emerge (Rajanbabu and Raj 2014).

5.1 Conclusion

In summary, the exploration of the Caesar Cipher through its application in MATLAB has been enlightening in terms of the fundamental concepts of encryption and decryption, as well as the weaknesses inherent in basic cryptographic techniques. Although the Caesar Cipher is a good educational tool for learning basic cryptographic principles like key management and plaintext-to-ciphertext transformation, its low security based on a small key space and vulnerability to brute-force attacks render it unsuitable for protecting sensitive data in contemporary applications. This examination highlights the significance of key size and algorithm complexity in the determination of the strength of encryption systems. The progression of cryptography from the simple Caesar Cipher to increasingly complex algorithms such as AES and RSA illustrate the ongoing development of methods aimed at satisfying the increased demand for secure communication in today's digital era. In conclusion, this research underscores how simple the Caesar Cipher was, allowing it to pave the way for the creation of stronger encryption methods that are the cornerstone of modern-day cybersecurity.

5.2 Future Implications

The Caesar Cipher is a worthwhile place to start learning about encryption, but it also points towards the necessity for more sophisticated forms of cryptography in the ever-developing digital realm. As computer threats become progressively more advanced, future encryption mechanisms will have to include larger keys, more involved algorithms, and stronger security systems to protect against sensitive information. Cryptography innovations like post-quantum cryptography and quantum encryption are set to revolutionize the way we secure information against new technologies that may be able to crack existing encryption methods. Further, machine learning and artificial intelligence advancements may result in the creation of more intelligent encryption systems that adapt dynamically to threats, offering greater security. The move toward secure communication in the interconnected age will probably advance the frontiers of cryptographic study, and so it is more important than ever before to study the historical context, such as the Caesar Cipher, in order to better enjoy and create the next generation of secure encryption schemes.

Supplementary Materials: Not Applicable.

Author Contributions: All authors equally contribute.

Funding: There is no funding for this project

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data will be available on request

Declaration of AI: Authors declared the use of AI for grammer improve only.

Acknowledgments: The authors gratefully acknowledge the support and facilities provided by the Department of Computer Science, University of Narowal, Pakistan, which made this research work possible.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Abdulhakeem, E. (2022). Improving the Security of Ceaser Cipher Algorithm Using Residue Number System and Advanced Encryption Standard, Kwara State University (Nigeria).

Abed, H. H., et al. (2023). "Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement." International Journal of Electrical & Computer Engineering (2088-8708) 13(6).

Agustini, S., et al. (2019). "Modified Vegenere Cipher to Enhance Data Security Using Monoalphabetic Cipher." International Journal of Artificial Intelligence & Robotics (IJAIR) 1(1): 26-32.

Al-Kateeb, Z. N., et al. (2020). Encryption and Steganography a secret data using circle shapes in colored images. Journal of Physics: Conference Series, IOP Publishing.

Arroyo, J. C. T., et al. (2020). "A Novel ASCII Code-based Polybius Square Alphabet Sequencer as Enhanced Cryptographic Cipher for Cyber Security Protection (APSAlpS-3CS)." International Journal of Advanced Computer Science and Applications 11(7).

Bevi, A. R., et al. (2016). "Information Coding and its Retrieval using DNA Cryptography." Journal of Engineering Science & Technology Review 9(3).

Bhateja, A. K., et al. (2015). "Cryptanalysis of vigenere cipher using cuckoo search." Applied Soft Computing 26: 315-324.

Duta, C.-L., et al. (2016). Eaecrypt Tool For Understanding Modern and Complex Cryptographic Algorithms. The International Scientific Conference eLearning and Software for Education, " Carol I" National Defense University.

Erondu, U. I., et al. (2023). An encryption and decryption model for data security using vigenere with advanced encryption standard. Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services, IGI Global: 141-159.

Hammad, R., et al. (2022). Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message. Journal of Physics: Conference Series, IOP Publishing.

Hanif, M. and J. Naime (2024). "Analyzing The Security System Through Matrices In Cryptography." no. April: 0-44.

Hegde, R. and S. Soumyasri (2021). "Novel Technique for Securing IoT Systems by using Multiple ECC and Ceaser Cipher Cryptography." Int. J. Comput. Sci. Mob. Comput.(IJCSMC) 10(2): 1-8.

Limbong, T. and P. D. Silitonga (2017). "Testing the classic caesar cipher cryptography using of matlab." Int. J. Eng.

Res. Technol 6(2): 175-178.

Matousova, I. and A. J. Berkova (2018). METHODS OF CODING AND DECODING (E-SAFETY IN EDUCATION). ICERI2018 Proceedings, IATED.

McAndrew, A. (2008). "Teaching cryptography with open-source software." ACM SIGCSE Bulletin 40(1): 325-329.

Mezher, L. S., et al. (2023). "A Comparative Study of a Hybrid Approach Combining Caesar Cipher with Triple Pass Protocol and Krill Herd Optimization Algorithm (KHO)-Based Hybridization." International Journal of Intelligent Engineering & Systems 16(6).

Mihailescu, M. I., et al. (2021). "Classic Cryptography." Cryptography and Cryptanalysis in MATLAB: Creating and Programming Advanced Algorithms: 51-68.

Msallam, M. M. and F. Aldoghan (2023). "Multistage encryption for text using steganography and cryptography." Journal of Techniques 5(1): 38-43.

Najaftorkaman, M. and N. S. Kazazi (2015). "A method to encrypt information with DNA-based cryptography." International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): 417-426.

Nita, S. L. and M. I. Mihailescu (2022). Classical Cryptography. Cryptography and Cryptanalysis in Java: Creating and Programming Advanced Algorithms with Java SE 17 LTS and Jakarta EE 10, Springer: 47-69.

Noviyanti, P. and M. Mira "Analysis of Classical Cryptographic Algorithms Caesar Cipher Vigenere Cipher and Hill Cipher–Study Literature." Journal of Information Technology 2(1): 23-30.

Nurcahya, S. D. and D. Nazelliana (2024). "Message Security in Classical Cryptography Using the Vigenere Cipher Method." International Journal Software Engineering and Computer Science (IJSECS) 4(1): 350-357.

Popoola, D. D. (2019). Data Integrity Using Caesar Cipher and Residue Number System, Kwara State University (Nigeria).

PRASAD, L. C. and V. S. R. RAO (2017). "MATLAB Implementation of Audio Steganography for Secure Data Transmission."

Purnamasari, D. (2021). "Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher untuk Keamanan Data Teks Menggunakan Python." Journal of Informatics Education 4(1).

Rajanbabu, D. T. and C. Raj (2014). "Multi-level encryption and decryption tool for secure administrator login over the network." Indian Journal of Science and Technology 7(4S): 8.

Saini, R. (2008). "Unique Cipher Mechanism for Ensuring Secure Data Flow over Network."

Stanoyevitch, A. (2010). Introduction to Cryptography with mathematical foundations and computer implementations, CRC Press.

Tan, C. M. S., et al. (2021). A hybrid encryption and decryption algorithm using caesar and vigenere cipher. Journal of Physics: Conference Series, IOP Publishing.

Thanikaiselvan, V. (2019). Image Encryption using DNA rules & Transmission of an encrypted digital image using USRP-2901 and MATLAB. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), IEEE.

Zahra, S. W., et al. (2024). "The Art of Secrecy: Hybridizing Caesar and Columnar Ciphers for Enhanced Data Security." The Sciencetech 5(2): 139-156.

Zamri, N. M., et al. (2020). Two level security in delivering message using encryption and steganography techniques. Journal of Physics: Conference Series, IOP Publishing.