JCBD
JOURNAL OF COMPUTERS AND DIGITAL BUSINESS
Volume 4, Number 3, September 2025, pp. 138-145
Homepage: https://jurnal.delitekno.co.id/index.php/jcbd

Securing Private Text Messages Using a Modified ASCII-256 Caesar Cipher and Avalanche Effect Assessment

Maghfira Aida[1*], Yulia Alfi Sinaga[2], Afthar Kautsar[3]

[1, 2, 3]*Universitas Islam Negeri Sumatera Utara, Indonesia*

* maghfira0701212205@uinsu.ac.id

https://doi.org/10.56427/jcbd.v4i3.765

ARTICLE INFO

Article History
Accepted : April 27, 2025
Revised: August 10, 2025
Approved: September 26, 2025

Keywords
Modified Caesar Cipher,
ASCII-256 Encryption,
Avalanche Effect,
Character Error Rate,
Cryptographic Security

ABSTRACT

Cryptography is a scientific discipline used to protect information by transforming readable messages into forms that are unintelligible to unauthorized parties. One of the earliest and simplest cryptographic techniques is the Caesar Cipher, which remains relevant for academic exploration, particularly in understanding fundamental concepts of substitution ciphers. This study proposes a modified version of the Caesar Cipher by incorporating the full ASCII-256 character set, thereby expanding the substitution space and increasing the complexity of the encryption process. To evaluate the effectiveness of this modification, two measurement techniques were applied: the Avalanche Effect, which assesses the sensitivity of the cipher to small input changes, and the Character Error Rate (CER), which examines the accuracy and distortion level during decryption. The experimental results demonstrate that the modified cipher achieves an average Avalanche Effect exceeding 10% and a CER value above 50%, indicating enhanced resistance to simple cryptanalytic approaches and improved confidentiality of encrypted data. The implementation and simulations were performed using MATLAB R2013a to provide a controlled environment for testing and analysis. This study offers a deeper conceptual understanding of how classic ciphers can be strengthened through structural modifications and serves as a reference for introductory cryptographic research as well as educational demonstrations.

1. Introduction

The development of digital technology in the Industry 4.0 era has had a significant impact on various aspects of life. Information can now be accessed and disseminated very quickly, including personal, educational, financial, and other important data [1]. This convenience also creates new risks, one of which is the rise of cybercrime. Digital crimes such as data theft often occur due to security gaps in systems, and this can have serious impacts on data privacy and integrity [2]. Cybercriminals typically exploit data that has significant value, so protective measures are needed to maintain the confidentiality of this information.

One widely used approach to data security is cryptography. The term cryptography comes from the Greek words crypto, meaning secret, and graphy, meaning writing. Cryptography is the study of how to encode data so that it can only be accessed by authorized parties [3]. Messages sent via digital media are converted into a form that cannot be read by just anyone, and can only be returned to their original form through a decryption process with a specific key.

The Caesar Cipher is a classic cryptographic algorithm that is still widely used in education due to its simplicity. Although its security is no longer considered strong enough for use in modern systems, this algorithm remains highly relevant as a foundation for understanding the basic principles of cryptography [4].

Several previous studies have attempted to develop the Caesar Cipher to increase the algorithm's security level. One example was conducted modified this algorithm with the Linear Congruent method to create more

random encryption patterns [5]. However, this approach is still limited to the alphabetic character space, so the algorithm's complexity has not increased significantly. Meanwhile, compared the Caesar Cipher with other algorithms such as the Vigenère Cipher, and note the Caesar Cipher's weakness against frequency-based attacks due to its overly linear nature [6]. Neither algorithm considers the possibility of expanding the character space to include all ASCII characters, which could pose additional challenges to the cipher-breaking process.

Considering the shortcomings of previous studies, this research attempts to implement a modified Caesar Cipher using the 256-character ASCII representation. This approach is taken to increase the complexity of the encryption pattern while minimizing the possibility of brute-force attacks and frequency analysis. Testing software is also needed to analyze this logic [7]. The entire implementation and testing process was conducted using MATLAB R2013a software. This software was selected based on its ability to perform efficient numerical and algorithmic simulations, which supports analysis of character changes and algorithm sensitivity levels using the Avalanche Effect and Character Error Rate methods [8].

2. Research methodology

This study uses a quantitative approach with a structured and clear experimental design. The main objective of this study is to test the effectiveness and security of a modified encryption algorithm, specifically one that uses the Caesar Cipher method with 256 ASCII character representation. This study relies on mathematical methods to analyze the encryption and decryption results and the effect of the modification on the security of the messages sent [9]. Encryption is the process of extracting cipher text from plain text. Decryption is the opposite [10]. The encryption and decryption processes in this study were carried out using MATLAB R2013a software. MATLAB was chosen because of its ability to efficiently simulate numerical algorithms.

To make it easier to understand the concepts of encryption and decryption in cryptography, consider Figure 1. This figure illustrates how plaintext is first encrypted into ciphertext using the Caesar Cipher algorithm and then decrypted back into the original plaintext. This process illustrates how cryptography works to maintain the confidentiality of sent messages.

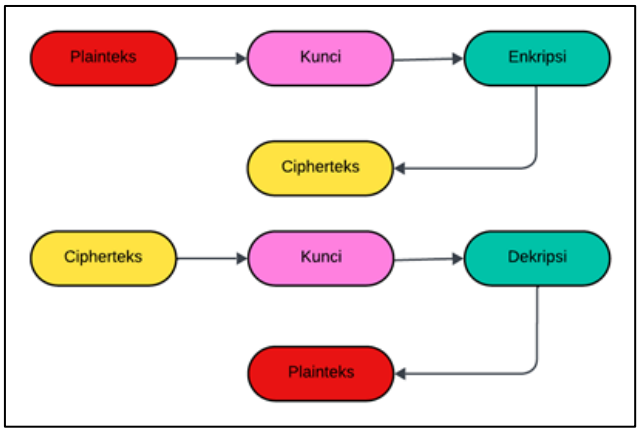

Figure 1. Cryptography Encryption and Decryption Diagram

The experimental process begins by determining the characteristics of the plaintext to be encrypted, which consists of plaintext converted into ciphertext using the Caesar Cipher algorithm. Each character in the plaintext will be processed based on a specific shift determined by the key. Character shifting is carried out by utilizing the ASCII 256 system to replace characters in the original text (plaintext) with characters that are in specific positions after the shift is performed. This algorithm changes the position of each character in the text sequence based on a predetermined shift value [11].

The Avalanche Effect test aims to measure how much the output (ciphertext) changes when the input (plaintext) undergoes a small change. Meanwhile, the Character Error Rate measures the extent to which the characters in the decrypted ciphertext deviate from the characters in the original plaintext. Both methods are important for evaluating an algorithm's robustness to small changes and character errors during the decryption process. Testing was performed over several iterations to analyze the consistency of the encryption and decryption results. Each iteration was tested with varying plaintext sizes, ranging from short to long, to ensure the algorithm could handle a wide range of input types effectively.

3. Results and Discussion

Currently, with the very rapid development of technology, this test can be carried out using the MATLAB R2013a application so that readers can understand and comprehend what happens if a method is applied to solve a problem. Manual encryption and decryption testing by entering a message “Maghfira and Yulia UINSU Students” and changing 1 word “Maghfira and Yulia UINSU Students” with a key shift of 125. Then change the message and key characters to decimal form such as M = 77 by matching them to the ASCII table. Repeat the same thing on the message changes.

From the initial message calculate the key shift by 45.
C1 = (P1 + K) mod 256
= (77+125) mod 256
= 202 (character Ê)
C2 = (P2 + K) mod 256
= (97+125) mod 256
= 222 (character Þ)
Repeat the calculation until the last message.

Table 1. Initial Message Encryption Process

Original Message	Original Message Decimal	Key Shift	Ciphertext Characters	Decimal Ciphertext
M	77	125	Ê	202
a	97	125	Þ	222
g	103	125	ä	228
h	104	125	å	229
f	102	125	ã	227
i	105	125	æ	230
r	114	125	ï	239
a	97	125	Þ	222
d	100	125	a	225
a	97	125	Þ	222
n	110	125	ë	235
Y	89	125	Ö	214
u	117	125	ò	242
l	108	125	e	233
i	105	125	æ	230
a	97	125	Þ	222
M	77	125	Ê	202
a	97	125	Þ	222
h	104	125	å	229
a	97	125	Þ	222
s	115	125	ð	240
i	105	125	æ	230
s	115	125	ð	240
w	119	125	ô	244
a	97	125	Þ	222
U	85	125	Ò	210
I	73	125	A	198
N	78	125	Ë	203
S	83	125	Đ	208
U	85	125	Ò	210

From the initial encryption, 5 lines were produced, the first line contained the original message "Maghfira and Yulia UINSU Students", the second line contained the decimal form of the original message (77, 97,

etc.), the third line contained the key shift (125), the fourth line contained the results of the ciphertext in the form of characters that correspond to the ASCII table (Ê, Þ, etc.)and the fifth line contains the results of the ciphertext in decimal form (202, 222, etc.).

Table 2. Second Message Encryption Message

Original Message	Original Message Decimal	Key Shift	Ciphertext Characters	Decimal Ciphertext
M	77	125	Ê	202
a	97	125	Þ	222
g	103	125	ä	228
h	104	125	å	229
f	102	125	ã	227
i	105	125	æ	230
r	114	125	ï	239
a	97	125	Þ	222
d	100	125	a	225
a	97	125	Þ	222
n	110	125	ë	235
Y	89	125	Ö	214
u	117	125	ò	242
l	108	125	e	233
i	105	125	æ	230
a	97	125	Þ	222
m	155	125	ê	24
a	97	125	Þ	222
h	104	125	å	229
a	97	125	Þ	222
s	115	125	ð	240
i	105	125	æ	230
s	115	125	ð	240
w	119	125	ô	244
a	97	125	Þ	222
U	85	125	Ò	210
I	73	125	A	198
N	78	125	Ë	203
S	83	125	Ð	208
U	85	125	Ò	210

From the second encryption, 5 lines are produced, the first line contains the original message "Maghfira and Yulia are UINSU students", the second line contains the decimal form of the original message (77, 97, etc.), the third line contains the key shift (125), the fourth line contains the results of the ciphertext in the form of characters that correspond to the ASCII table (Ê, Þ, etc.)and the fifth line contains the results of the ciphertext in decimal form (202, 222, etc.).

Table 3. Initial Message Decryption Process

Ciphertext Characters	Decimal Ciphertext	Key Shift	Original Message	Original Message Decimal
Ê	202	125	M	77
Þ	222	125	a	97
ä	228	125	g	103
å	229	125	h	104
ã	227	125	f	102
æ	230	125	i	105

ï	239	125	r	114
Þ	222	125	a	97
a	225	125	d	100
Þ	222	125	a	97
ë	235	125	n	110
Ö	214	125	Y	89
ò	242	125	u	117
e	233	125	l	108
æ	230	125	i	105
Þ	222	125	a	97
Ê	202	125	M	77
Þ	222	125	a	97
å	229	125	h	104
Þ	222	125	a	97
ð	240	125	s	115
æ	230	125	i	105
ð	240	125	s	115
ô	244	125	w	119
Þ	222	125	a	97
Ò	210	125	U	85
A	198	125	I	73
Ë	203	125	N	78
Đ	208	125	S	83
Ò	210	125	U	85

From the first decryption, 5 lines of content are produced, the first line contains the results of the previous ciphertext in the form of characters that correspond to the ASCII table (Ê, Þ, etc.), the second line contains the results of the ciphertext in decimal form (202, 222, etc.), the third line contains the key shift (125), the fourth line contains the original message "Maghfira and Yulia UINSU Students" and the fifth line contains the decimal form of the original message (77, 97, etc.).

Table 4. Second Message Decryption Process

Ciphertext Characters	Decimal Ciphertext	Key Shift	Original Message	Original Message Decimal
Ê	202	125	M	77
Þ	222	125	a	97
ä	228	125	g	103
å	229	125	h	104
ã	227	125	f	102
æ	230	125	i	105
ï	239	125	r	114
Þ	222	125	a	97
a	225	125	d	100
Þ	222	125	a	97
ë	235	125	n	110
Ö	214	125	Y	89
ò	242	125	u	117
e	233	125	l	108
æ	230	125	i	105
Þ	222	125	a	97

ê	24	125	m	155
Þ	222	125	a	97
å	229	125	h	104
Þ	222	125	a	97
ð	240	125	s	115
æ	230	125	i	105
ð	240	125	s	115
ô	244	125	w	119
Þ	222	125	a	97
Ò	210	125	U	85
A	198	125	I	73
Ë	203	125	N	78
Ð	208	125	S	83
Ò	210	125	U	85

From the second decryption, 5 lines are produced, the first line contains the results of the previous ciphertext in the form of characters that correspond to the ASCII table (Ê, Þ, etc.), the second line contains the results of the ciphertext in decimal form (202, 222, etc.), the third line contains the key shift (125), the fourth line contains the original message "Maghfira and Yulia are UINSU students" and the fifth line contains the decimal form of the original message (77, 97, etc.). After manually encrypting and decrypting both messages, the results can be proven using Matlab R2013a.

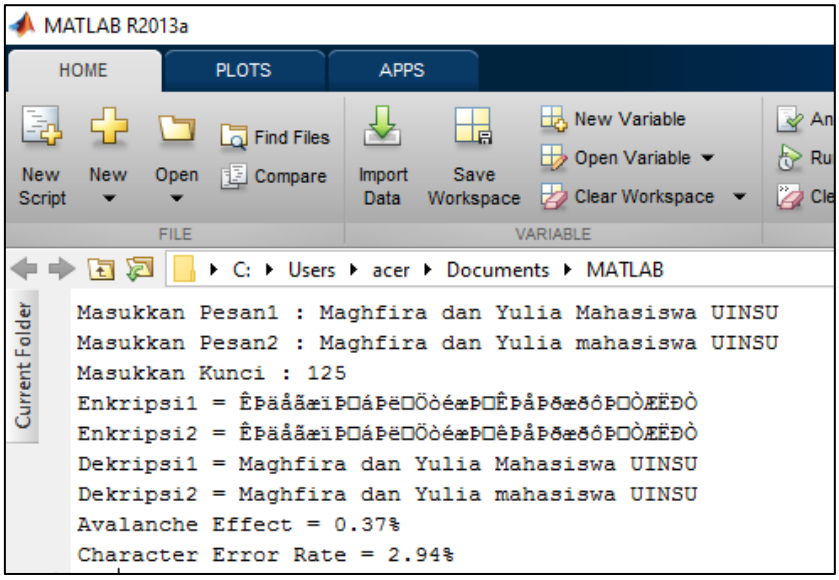

Figure 2. Program View

To ensure whether Caesar Cipher is safe to use for securing private texts, a test was conducted on 5 test texts.

Table 5. Avalanche Effect and Character Error Rate Testing

Plaintext	Key	Avalanche Effect	Character Error Rate
Perken@lk4n Name S4ya M4ghf$$ira A1da	150	13.51%	43.24%
pErKen@LkAn N4m4 SaY2 MaghF$$irA AiD4	150	13.51%	43.24%
Yulia ALFI sin@g@ bERasal Dari LABura	75	12.16%	51.35%
YuL!A AlF1 S!n#G@ BeR4saL D4rI lAbuR4	75	12.16%	51.35%
P##G*I Cer%aH	50	12.50%	76.92%

p**G#i cER%Ah	50	12.50%	76.92%
P##G*I Cer%aH Bers@ma Kelu5RGA	60	10.42%	63.33%
p**G#i cER%Ah bERS$Ma Kelu3Rga	60	10.42%	63.33%
Hopefully BetAH S@MP@IT@maT. SUCCESS S##lalu 21	200	2.78%	15.56%
Hopefully BetaH S@MP@i T@m@T. sUkSeS S%#lalu 21	200	2.78%	15.56%

Based on the tests conducted, 5 trials were used with 10 texts with different key shift variations. In the third experiment, the average Avalanche Effect value reached 12.50% and the Character Error Rate reached 76.92%. An Avalanche Effect value exceeding 10% can be considered sufficient for simple security systems, such as in non-critical applications or for educational purposes. The use of 256 ASCII characters including uppercase letters, lowercase letters, numbers, and symbols can increase the possible key space, thereby extending the brute force time in cracking the ciphertext. Encrypted characters such as "Ê" appear due to the ASCII representation that exceeds the standard alphabetic characters. This is because small changes in the plaintext only result in small changes in the ciphertext due to the linear nature of the substitution.

4. Conclusion

Based on the research conducted, it can be concluded that the Caesar Cipher method can be used for simple applications such as encrypting private text messages. In the research conducted, the Caesar Cipher method obtained a fairly good average Avalanche Effect value, with a value above 10%. The greater the number of differences in the message, the greater the impact on the Avalanche Effect value. For further development, Caesar Cipher can be combined with other classical algorithms to further secure private text messages.

Thank You

We would like to express our sincere gratitude to all those who contributed to this research. First, we would like to thank our colleagues in the Computer Science Study Program, Faculty of Science and Technology, State Islamic University of North Sumatra, Medan, for their support and cooperation throughout this research process. We would also like to thank the reviewers and colleagues who provided valuable input during the review process. Finally, we would like to thank our family and friends for their continued support. We hope that the results of this research will be beneficial for the future development of cryptography.

Reference

[1] Mulyani F and Haliza N, "Analisis Perkembangan Ilmu Pengetahuan dan Teknologi (Iptek) Dalam Pendidikan," *J. Pendidik. Dan Konseling*, vol. 3, no. 1, pp. 101–109, 2021.

[2] S. A. Rahmah, "Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web," *J. Comput. Digit. Bus.* , vol. 2, no. 3, pp. 112–119, 2023.

[3] D. Alameka, "SYSTEMATIC LITERATURE REVIEW: SEKTOR SERANGAN SIBER DAN METODE PENDETEKSI SERANGAN SIBER PADA WEBSITE PELAYANAN PUBLIK DI KALIMANTAN TIMUR," 2023.

[4] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.

[5] S. D. Nasution, "Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data," *J. Inform.*, vol. 01, no. 03, pp. 95–101, 2024.

[6] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *J. Educ.*, vol. 5, no. 3, pp. 8563–8573, 2023, doi: 10.31004/joe.v5i3.1647.

[7] J. S. Permana, H. Hendrana, and R. Murnir, "Mengamankan File Rahasia Menggunakan Hybrid Kriptografi," *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 2449–2460, 2024.

[8] Muslih Muslih and Lekso Budi Handoko, "Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher," *Semin. Nas. Teknol. dan Multidisiplin Ilmu*, vol. 2, no. 1, pp. 127–

134, 2022, doi: 10.51903/semnastekmu.v2i1.162.
[9] B. G. & R. P. Ritwiyan, "Implementasi Kriptografi Pada Web Service Dengan Metode Caesar Cipher," *Skanika*, vol. 4, no. 1, pp. 39–44, 2021.
[10] A. M. Fajrin, J. R. Benedict, and H. J. Kusuma, "Analisis Performa dari Algoritma Kriptografi RSA dan ElGamal dalam Enkripsi dan Dekripsi Pesan," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 1, pp. 91–98, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik
[11] R. Silalahi, S. Iin Parlina, I. Gunawan, and W. Saputra, "Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data," vol. 1, no. April, pp. 282–293, 2021.