A MODIFIED CEASER CIPHER

A. Hassan

Department of Mathematics,
Federal University Birnin Kebbi, Nigeria
Email: aliyu.hassan@fubk.edu.ng

Abstract:

The conventional Caesar cipher, traditionally reliant on alphabet letters, has undergone a modification in this undertaking. The innovation involves the incorporation of both alphabets and special characters, resulting in a robust cipher text. This alteration serves a dual purpose: facilitating uncomplicated decryption for the intended recipient while presenting a formidable challenge for potential intruders, by expanding the character set to encompass special characters, the cipher attains heightened complexity. This not only enhances the security of the encoded message but also fortifies the resilience against unauthorized deciphering attempts. The strategic utilization of special characters introduces an additional layer of intricacy, rendering the cipher less susceptible to conventional decryption methods. The primary objective remains to create a cryptographic system that strikes a delicate balance between accessibility and security. The intentional inclusion of special characters not only diversifies the encoding possibilities but also contributes to the creation of a dynamic cipher system. This adaptive approach ensures that the communication remains safeguarded against adversaries seeking to compromise the confidentiality of the information. In essence, this evolved Caesar cipher becomes a potent tool in the hands of the sender and a formidable enigma for those attempting unauthorized access.

Introduction

The Caesar Cipher, named after Julius Caesar who is reputed to have used it for secure communication, stands as one of the earliest and simplest encryption techniques. Dating back to ancient Rome, this substitution cipher operates by shifting each letter of the plaintext by a fixed number of positions down the alphabet. The key, known as the Caesar shift or cipher key, determines the magnitude and direction of the displacement. For example, with a shift of 3, 'A' would become 'D,"B' becomes 'E,' and so forth. Despite its historical significance, the Caesar Cipher is remarkably easy to decipher with modern computational power. Its vulnerability lies in the limited number of potential keys, only 25 possible shifts in the case of the Standard English alphabet. Consequently, it falls under the category of weak encryption methods and is more suitable for educational purposes or as a stepping stone to more sophisticated cryptographic techniques. Nevertheless, the Caesar Cipher exemplifies the fundamental concept of encryption through the alteration of character positions, laying the groundwork for more complex cryptographic algorithms that are integral to modern information security. Its historical relevance and simplicity make it an essential starting point for understanding the evolution of encryption techniques and the ongoing pursuit of secure communication.

Cryptographic techniques were used by different authors such as [7], [4] and [5] to investigate the security and uniqueness of algorithms and also in [17], [14], [10] and [1] different cryptographic ideas were used in order to have a text fully secured and prevents it from intruders which may likely use the information sent over communication channel in their favour, Ceaser cipher was extensively studied by [2], [3], [5], [6], [11], [12], [14] and [17] and discovered some weaknesses and power of the classical Ceaser cipher together with different modifications that may add security to the algorithm used in order to prevent unwanted access to the data being sent over media, Study on modified ciphers were conducted by [9], [15],[1] and [16] and consequently many results were obtained from the different studies, many recommendations were being derived from [1], [8], and [3] which gave rise to multiple researches in the field of cryptography.

Materials and Method

Terms used in cryptography

i. Plaintext: original message
ii. Cipher text: coded message
iii. Encryption: the process of converting plaintext into coded text
iv. Decryption: the process of converting coded text into plaintext
v. Key: a piece of information that is used for encryption and decryption
vi. Cryptography: the study of encryption and decryption principles
vii. Cipher: an algorithm used for encryption and decryption
viii. Key: a piece of information used by an encryption algorithm to transform plaintext into cipher text or vice versa
ix. Symmetric key cryptography: a type of cryptography where the same key is used for both encryption and decryption
x. Asymmetric key cryptography: a type of cryptography that uses a pair of keys (public and private) for encryption and decryption
xi. Frequency analysis: manually tracing the plaintext from cipher text using frequency of letters used in the cipher text.

Table 1: Frequency of English Letters

Letters	Frequency (%)	Letters	Frequency (%)
E	11.1607	M	3.0129
A	8.4966	H	3.0034
R	7.5809	G	2.4705
I	7.5448	B	2.0720
O	7.1635	F	1.8121
T	6.9509	Y	1.7779
N	6.6544	W	1.2899
S	5.7351	K	1.1016

L	5.4893	V	1.0074
C	4.5388	X	0.2902
U	3.6308	Z	0.2722
D	3.3844	J	0.1965
P	3.1671	Q	0.1962

Ceaser Cipher

The Caesar cipher is a substitution cipher that shifts the letters of the alphabet by a fixed number of positions. Here's how it works:

a. **Key Selection:** A key is chosen, which an integer is representing the number of positions each letter in the plaintext is shifted. For example, with a key of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.
b. **Encryption Process:** Each letter in the plaintext is shifted by the key value. If the alphabet is considered cyclic, meaning after 'Z' it wraps around to 'A', the shifting process remains consistent.
The cipher text is represented by "**C"** while the plaintext is represented by "**P"**

$$C = (P + k)_{\mathrm{mod}\,26}$$
$$P = (C - k)_{\mathrm{mod}\,26}$$

Where, **k** is the key value to be used for both the processes.

Example:

Using a key of **3**:

Plaintext: HELLO

Encryption: KHOOR

c. **Decryption Process**: To decrypt, the process is reversed. Each letter in the ciphertext is shifted backward by the key value.
d. **Security**: Caesar cipher is vulnerable to brute-force attacks due to its limited key space (only 25 possibilities for a Standard English alphabet). Frequency analysis can also be employed, as it doesn't alter the frequency distribution of letters.
e. **Variations**: Caesar cipher can be generalized with different shift values, not limited to integers. This leads to the creation of more complex substitution ciphers.
f. **Usage**: Despite its simplicity, Caesar cipher is a historical encryption method, allegedly used by Julius Caesar. However, it's not suitable for secure communication in modern contexts. Remember, it's a basic and easily breakable cipher. Modern cryptographic systems use more sophisticated algorithms to ensure secure communication.

Table 2: Plaintext alphabets and their corresponding values in Ceaser cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Example: code the text using cipher Ceaser cipher algorithm. “ATTACK IMMEDIATELY BY DOWN AND REPORT TO THE DIVISION IMMEDIATELY AFTER ATTACK”

Solution:

Plaintext:
“ATTACKIMMEDIATELYBYDOWNANDREPORTTOTHEDIVISIONIMMEDIATELYAFTERATTACK”

Cipher text:
“DWWDFNLPPHGLDWHOBEBGRZQDQGUHSRUWWRWKHGLYLVLRQLPPHGLDWHOBDIWHUDWWDFN”

Proposed Modification of the Ceaser Algorithm

The suggested cryptosystem enhances the traditional Caesar cipher by incorporating a modified table of letters and their associated numeric values. This modification introduces special characters in the ciphertext, adding complexity compared to the classical Caesar cipher that solely employs alphabets in the ciphertext, thereby making it more resistant to intrusion attempts.

Table 3: Plaintext and special characters modified Ceaser cipher

A	B	#	C	D	*	E	F	+	G	H	-	I	J	$	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

L	?	M	N	!	O	P	@	Q	R	%	S	T	>	U
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

V	<	W	X	^	Y	Z
31	32	33	34	35	36	37

The encryption algorithm is given by the relation below.

$$C = (P + K)_{\mathrm{mod}\,38}$$

Where:
C: is the cipher text
P: is the plaintext
K: is the key

The decryption algorithm is given by the relation below.

$$P = (C - K)_{\mathrm{mod}\,38}$$

Where:
C: is the cipher text
P: is the plaintext
K: is the key

Example: Encrypt the information using modified Ceaser cipher using a **key = 2** "ATTACK IMMEDIATELY BY DOWN AND REPORT TO THE DIVISION IMMEDIATELY AFTER ATTACK"

Solution. Using the encryption algorithm of the modified Ceaser cipher which is given by $C = (P + K)_{\mathrm{mod}\,38}$ the cipher text will be.

#UU#*?$!!+E$#U+MACAE@^O#OES+Q@SUU@UI+EW>$@O$!!+E$#U+MA#GU+S#UU

The intending recipient and also intruders will receive the code **#UU#*?$!!+E$#U+MACAE@^O#OES+Q@SUU@UI+EW>$@O$!!+E$#U+MA#GU+S#UU** as sent over communication media, the intending recipient will use the decryption algorithm and Table 3 above to decrypt the cipher text, while intruders will use frequency analysis or any available tools within their system to crack the code, and due to the inclusion of special characters, the frequency analysis will likely fail to work.

CONCLUSION

The research demonstrates that enhancements to the Caesar cipher yield remarkable outcomes, presenting a heightened level of complexity for potential attackers while maintaining simplicity for the intended recipient. The Caesar cipher, a classical encryption technique, has been refined to enhance its security features. The results reveal a significant advancement in thwarting information breaches. Through systematic modifications, the improved Caesar cipher achieves a

robust defense against unauthorized access. This heightened resilience makes it a formidable challenge for attackers attempting to decipher sensitive information. The encryption's intricacies act as a formidable deterrent, ensuring a higher level of confidentiality. Despite the heightened complexity introduced in the improved Caesar cipher, its user-friendliness remains intact for the intended recipient. This delicate balance between enhanced security and user accessibility marks a distinctive achievement in cryptographic research. The recipient experiences a seamless decryption process, ensuring efficient and timely access to the protected information. The findings underscore the practical applicability of the enhanced Caesar cipher in real-world scenarios where information security is paramount. The cipher's improved resistance to attacks positions it as a valuable tool in safeguarding sensitive data. This research not only contributes to the evolution of classical encryption methods but also highlights the importance of striking a balance between security and usability in cryptographic systems.

Acknowledgement

I wish to extend a special thanks to the mathematics department staff of Federal University Birnin Kebbi, for their invaluable assistance and contributions to the advancement of this manuscript. Their unwavering support has played a crucial role in the development and refinement of this work. I deeply appreciate the collaborative efforts and guidance provided by the dedicated members of the department, which have significantly enriched the content and quality of this manuscript.

References

[1] Hassan, A., Garko, A., Sani, S., Abdullahi, U and Sahalu, S (2023). Combined Techniques of Hill Cipher and Transposition Cipher, Journal of Mathematics Letters. **1**(822) pp 1-8, DOI:10.31586/jml.2023.822

[2] Sharma, s and Gupta, Y (2017). Study on Cryptography and Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, **2**(1)-ISSN: 2456-3307. pp 249-252

[3] Kasturia, P and Maheswa, K (2017). Critical Analysis of Various Cryptographic Algorithms. Journal of Ultra Computer & Information Technology. 8(1), pp 5-9

[4] Alhassan, M. J; Hassan, A; Sani, S. and Alhassan, Y. (2021). A Combined Technique of an Affine Cipher and Transposition Cipher *Quest Journals Journal of Research in Applied Mathematics Volume 7. Issue 10 (2021) pp: 08-12*

[5] Azzam A and Sumarsono (2017), A Modifying of Hill Cipher Algorithm with 3 Substitution Ceaser Cipher. Proceedings International Conference of Science and Engineering, Indonesia.**1**: 157-163.

[6] Fahrul I, K., Hassan F, S., Toras P and Rahmat W. (2017), Combination of Ceaser Cipher Modification with Transposition Cipher. Advances in Science Technology and Engineering Systems Journal. **2**(5): 22-25.

[7] Hassan, A; Alhassan, M. J; Alhassan, Y. and Sani, S. (2021). Cryptography as a Solution for a Better Security International Journal of Advances in Engineering and Management (IJAEM :3(12). pp: 849-853

[8] Badamasi, B. L., Sani, S., Ahmad, S. T and Hassan, A (2023). Using Big Data to Determine Potential Dropout of Students in Some Selected Tertiary Institutions in Kebbi State, Nigeria. International Journal of Innovative Science and Research Technology. ISSN: 2456-2165. **8**(10). Pp 1-6

[9] https://www3.nd.edu/~busiforc/handouts/cryptography/letterfrequencies.html

[10] Kuriakkottu A. R. (2021). Use of Transposition Cipher and its Types. International Journal of Research and Engineering, Science and Management 4(11), 164-165

[11] Kashish G and Supriya K. (2013) Modified Ceaser Cipher for a Better Security Enhancement. International Journal of Computer Application.**73**:26-31

[12] Mishra A. (2013), Enhancing security of Ceaser cipher using different methods. International Journal of Research in Engineering and Technology **2**(09):327-332.

[13] Massoud S., Sokouti B. and Saeid P. (2009), An Approach in Improving Transposition cipher System. Indian Journal of Science and Technology. **2**(8):9-15.

[14] Pooja S and Pintu S. (2017), Enhancing security of Ceaser cipher using "Divide and Conquer Approach". International Journal of Advance Research in Science and Engineering. **06**(02):144-150.

[15] Rajput Y., Naik D. and Mane C. (2014), An improved cryptographic technique to encrypt Text message using double encryption. International Journal of Computer Applications **86**(6):24-28.

[16] Sriramoju A. B (2017), modification affine ciphers algorithm for cryptography password, Programmer Analyst, Ramstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020, Pittsburgh, Pennsylvania -15222, USA.

[17] Shahid B. D. (2014), enhancing the security of Ceaser cipher using double substitution method. International Journal of Computer Science and Engineering Technology. **5**: 772-774.