SECURITY ANALYSIS AND MODIFICATION OF A CEASER CIPHER

Article *in* Journal of Mathematical Sciences & Computational Mathematics · July 2024

DOI: 10.15864/jmscm.5305

1 author:

Aliyu Hassan

Federal University Birnin Kebbi, Kebbi State, Nigeria

16 PUBLICATIONS **42** CITATIONS

SECURITY ANALYSIS AND MODIFICATION OF A CEASER CIPHER

[1,*]Hassan. A and [2]Abdullahi. U

[1]Department of Mathematics,
Federal University Birnin Kebbi, Nigeria

[2]Teachers Service Board Sokoto, Nigeria

[*]Corresponding Author. Email: aliyu.hassan@fubk.edu.ng

Abstract:

This work presents a new Caesar algorithm that contains alphabet and special characters presents in QWERTY keyboard combination, within the modified Caesar table. Unlike traditional implementations of Ceaser table that contains alphabets only, the algorithm employs Modulo 40 instead of Modulo 26 of the classical Ceaser algorithm, resulting in a ciphertext that includes both alphabetic and special characters. This modification aims to increase the security of encrypted data by diverting the attention of cyber attackers using frequency analysis of English letters. The introduced special characters from the QWERTY keyboard provide an additional layer of complexity, making the encryption more complex to decryption techniques. The proposed method offers a new perspective on cryptographic algorithms, contributing to the ongoing efforts to boost cyber security measures against continues attacks.

Keywords: *Ceaser cipher, Encryption, Algorithm, Security analysis, Cyber security.*

1. INTRODUCTION

The Caesar Cipher is a substitution encryption algorithm, which works in a way that, each letter in the plaintext is shifted to a certain number of positions moving right or left of the alphabets. Named after Julius Caesar, who reportedly used it to protect military messages, the algorithm involves a fixed key, the shift value. For example, with a shift of 2, `A` becomes `C`, `B` becomes `D` and so on. It operates on a modular arithmetic basis, wrap around to the beginning of the alphabet when necessary. The Ceaser cipher offers limited security against modern day cryptographic analysis software. And in this work a modification of the classical Ceaser cipher will be discussed based on the literatures that works on different improvement of a classical Ceaser cipher method which leads to different cryptographic algorithms and each algorithm has a unique responsibility in attaining a maximum security when sending data over any communication channel such as Short Message Service (S.M.S), Electronic Mail (Email) etc.

2. LITERATURE REVIEW

Cipher algorithms were used by different researchers such as [7], [4], [19] and [5] to check level of security and diverse a way to make the security of the cipher more secure in the context of communication (Short Message Service (SMS), Electronic Mail (Email), FAX, Post Office Box (P.O.BOX) etc),

In [1], [14], [10], [20] and [17] a different cryptographic ideas in order for the data to be fully secured along any communication channel. The study of Ceaser cipher was conducted by [2], [3], [5], [6], [11], [12], [14] and [17] and discovers its vulnerability to attacks by intruders, and comes up with different ways that may add security to the algorithm used in order to prevent unwanted access to the data being sent through communication channels.

Study on modified ciphers were conducted by [9], [21], [15],[1] and [16] and consequently many results were obtained from the different studies, many recommendations were being derived also from [1], [22], [8], and [3] which gave rise more researches on Ceaser algorithm in the field of cryptography for the safety of the information being conveyed into the media via which the communication will be made.

3. METHODS

3.1 Terms used in the work.

i. Plaintext: The message intended to be sent.
ii. Cipher text: The message to which receiver will receive.
iii. Encryption: The process of changing plaintext into cipher text.
iv. Decryption: The process of changing cipher text into plaintext
v. Cryptography: The study of encryption and decryption principles
vi. Cipher: an algorithm used for encryption and decryption
vii. Key: a piece of information used by an encryption algorithm to transform plaintext into cipher text or vice versa
viii. 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

Samuel Morse (1791-1872)

3.2 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
b. **Encryption Process:** Each letter in the plaintext will be shifted by the key value. The cipher text is represented by "**C"** while the plaintext is represented by "**P"**

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

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

Example 1:

Using a (k= **2,** implies each letter will moved ahead by two positions**)** and using the algorithm below

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

Plaintext: WELCOME

Cipher text: YGNEQOG

c. **Decryption Process**: To decrypt, the process is reversed.

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

Cipher text: YGNEQOG

Plaintext: WELCOME

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

Table 2 above was used for the example 1. And the result was alphabets only (the real classical Ceaser cipher).

4. RESULTS

4.1 Proposed Modification of the Ceaser Algorithm

The proposed algorithm uses a classical Ceaser table with modifications, where the special characters were used to add more security to the key system and cipher text which is to be sent over communication channels. This modification adds complexity for unwanted users compared to the classical Caesar cipher only depends on alphabets characters in the ciphertext and this add a layer of complexity to intrusion attempts.

Table 3: Plaintext and Special Characters Modified Ceaser Cipher

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

.	K	@	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	31	32

<	V	W	X	^	Y	Z
33	34	35	36	37	38	39

4.2 The encryption algorithm is given by the relation below.

$$C = (P + K)_{\text{mod } 40}$$

4.3 The decryption algorithm is given by the relation below.

$$P = (C - K)_{\text{mod } 40}$$

Where:
C: Ciphertext
P: Plaintext
K: Key

Example: Use **Table 3** and secure the command "Attention troops, Operation Ironclad is underway. Intel confirms bandits' stronghold at grid coordinates XYZ. Execute a synchronized assault at 3am. Alpha and Bravo teams secure the perimeter, Charlie team approaches from the south. Air support will engage upon visual confirmation. Neutralize threats swiftly, prioritize hostage safety if encountered. Maintain radio silence, except for essential communications.

Evacuate wounded promptly. Report any unforeseen developments immediately." using **key = 3**

Solution. Using the encryption algorithm of the Modified Ceaser Cipher Algorithm which is given by

$$C = \left(P + K\right)_{\mathrm{mod}\,40}$$

CIPHER TEXT: "*WW$QW@, QWU,,R<T,R$U*W@,QQU, QEO*-@<XQ-$UZ*#M@ QW$ OE,QH@U P< D*Q@W< <WU,QI.,O-*WI U@-E,,U-@Q*W$<AHCM$A$ EW$ *< #QE. U, @C$-*< <* X O W*W3*PM*OR.X *Q-DU* Y,W$*P<<$E XU$W.$R$U @P$ W $UTE .*UO @$W$ *P *R R U,*E$ <HU,PW.$<, XW.M*@U< XRR ,UWZ @O O $ Q I* I$XR,QY@<X*OE,QH@UP*W@,QMQ$XWU*O@C$ W.U$*W<<Z@HWO #TRU@,U@ W @C$.,<W *I$<*H$ W#@H$Q E,X Q W$U$- MP*@QW*@QU*-@,<@O QET$ AE$R WH, U$<< $QW@ *OE, PPXQ@ E* W @ , Q<M$Y*EX*W$Z,XQ-$-RU,PW O#MU$R ,U W *Q#XQH,U$<$$Q-YO, RP$QW <@ P P$-@*W$O#M W.$P@ <<@,Q,D L$EW@Y $@ <W.$-@<P*QWO@QI,HW.$D*Q-@W.@-$, X W W,.$Q<XU$U$I@,Q*O<$EXU@W#MI,-<R$$-TP*@QW*@QY@I@O*QE$T*Q-$ A $ EXW$Z@W.RU $E@<,QMW.@<,U -$ U@ <EO*<<@H @$-TXQ* XW.,U@C$ --@< E O,<XU$@<<WU@EWO#RU,.@D@W$-M"

The intending recipient and also intruders will receive the code

"*WW$QW@, QWU,,R<T,R$U*W@,QQU, QEO*-@<XQ-$UZ*#M@ QW$ OE,QH@U P< D*Q@W< <WU,QI.,O-*WI U@-E,,U-@Q*W$<AHCM$A$ EW$*<#QE. U, @C$-*< <* X O W*W3*PM*OR.X *Q-DU* Y,W$*P<<$E XU$W.$R$U @P$W$UTE .*UO @$W$ *P *R R U,*E$<HU,PW.$<,XW.M*@U<XRR,UWZ@OO$QI*I$XR,QY@<X*OE,QH@UP*W@,QM Q$XWU*O@C$ W.U$*W<<Z@HWO #TRU@,U@ W@C$.,<W *I$<*H$ W#@H$Q E,X Q W$U$- MP*@QW*@QU*-@,<@O QET$ AE$RWH, U$<< $QW@ *OE, PPXQ@ E* W @ , Q<M$Y*EX*W$Z,XQ-$-RU,PWO#MU$R,UW*Q#XQH,U$<$$Q-YO, RP$QW <@ P P$-@*W$O#MW.$P@<<@,Q,DL$EW@Y$@<W.$-@<P*QWO@QI,HW.$D*Q-@W.@-$, X W W,.$Q<XUUI@,Q*O<$EXU@W#MI,-<R$$-TP*@QW*@QY@I@O*QE$T*Q-$ A $ EXW$Z@W.RU $E@<,QMW.@<,U -$U@<EO*<<@H @$-TXQ* XW.,U@C$ --@< E O,<XU$@<<WU@EWO#RU,.@D@W$-M"

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 and, the frequency analysis will lead them to the wrong analysis.

The table below gives the analysis of the cipher text above, using **277** letters of 620 characters and special characters with **93** words.

Table 4: Frequency of English Letters after Encryption

Letters	Frequency	(%)	Letters	Frequency	(%)
E	4	1.4	M	11	4.0
A	18	6.5	H	10	3.6
R	16	5.8	G	0	0.0
I	8	2.9	B	0	0.0
O	20	7.2	F	0	0.0
T	6	2.2	Y	0	0.0
N	0	0.0	W	46	16.6
S	0	0.0	K	0	0.0
L	0	0.0	V	0	0.0
C	3	1.1	X	39	14.1
U	31	11.2	Z	5	1.8
D	4	1.4	J	4	1.4
P	13	4.7	Q	39	14.1

5. CONCLUSION AND FUTURE WORK

This work gives an insight on how to make more security in the Caesar cipher and it gives out more complex outcomes, modulo 40 was used in the proposed work in order to accommodate special characters and expand the key length from 25 possible key combinations in the classical Ceaser to 39 possible key combination, presenting a high level of security for potential attackers while maintaining simplicity for the intended recipient. And also, in terms of security analysis, the classical Ceaser cipher can easily be detected using security analysis, but in this proposed modified Caesar cipher, the Table 4 shows that, the security analysis is not effective, there by the data is secured when security analysis is performed. The improved Caesar cipher achieves a great defense against unauthorized access to the information. This increased security makes it a formidable challenge for attackers attempting to decipher the information received. The encryption's modification act as a layer, ensuring a higher level of confidentiality. The recipient experiences a simple decryption process thereby minimizing decryption length, 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 very important. 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.

Table 4 gives the frequency analysis of the letters after encryption which when compared to Table 1 the results indicate a disparity and with such, the aim of this work is being achieved indicating that, the attackers of the data will be misled to get the wrong information, while the intended recipient will get exactly the original message. The recommendation for the future work will be in a way that computer software will be developed that can process all input plaintext into the cipher text with time saving mechanism.

6. Acknowledgements

I would like to appreciate all the contributors from which this work was developed especially authors that were been referenced and all other related authors. May you find ease in your endeavors.

References.

[1] Hassan, A., Garko, A., Sani, S., Abdullahi, U and Sahalu, S. Combined techniques of hill cipher and transposition cipher, Journal of Mathematics Letters. **1**(822) pp 1-8. 2023 DOI:10.31586/jml.2023.822.2023

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

[3] Kasturia, P and Maheswa, K. Critical analysis of various cryptographic algorithms. Journal of Ultra Computer & Information Technology. 8(1), pp 5-9. 2017.

[4] Alhassan, M. J; Hassan, A; Sani, S. and Alhassan, Y. 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. A Modifying of hill cipher algorithm with 3 substitution ceaser cipher. Proceedings International Conference of Science and Engineering, Indonesia.**1**: 157-163.2017

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

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

[8] Badamasi, B. L., Sani, S., Ahmad, S. T and Hassan, A. 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. 2023. ISSN: 2456-2165. **8**(10). Pp 1-6

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

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

[11] Kashish G and Supriya K. Modified Ceaser cipher for a better security enhancement. International Journal of Computer Application.**73**:26-31. 2013

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

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

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

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

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

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

[18] Samuel Morse (1791-1872) https://www3.nd.edu/~busiforc/handouts/cryptography/

letterfrequencies.html

[19] Lubis, Fahrul & Simbolon, Hasanal & Batubara, Toras & Sembiring, Rahmat Widia. Combination of Caesar cipher modification with transposition cipher. Advances in Science, Technology and Engineering Systems Journal. 2017

[20] Savla, Dhairya & Rautela, P. Design and improvement of Caesar cipher. International Journal for Research in Applied Science and Engineering Technology. 11. 1190-1194. 10.22214/ijraset.2023.54819. 2023

[21] Asoronye, Gaylord & Goodluck, Ituru & Emereonye, Goodluck & Onyibe, Christian & Agha, Ibiam. An Efficient implementation for the cryptanalysis of caesar's cipher. 5. 101-109. 2019

[22] Verma, Priya & Gaba, Gurjot & Monga, Himanshu. Modified Caesar cipher using rectangular method for enhanced security. Journal of Communications Technology, 2016