IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A MESSAGE ENCRYPTION TECHNIQUE COMBINING CAESAR CIPHER WITH ATBASH CIPHER

[1]S. Susheela Marry, [2*] Dr. K. Rajendran

[1] M.Phil. Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India.

[2*] Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India.

ABSTRACT:

Recent days, encryption techniques are the important thing to secure our personal communications and messages. Encryption techniques are promptly increased by the increasing usage of communication networks and evaluation of the internet. Sharing an information from one end to another end over an unsecured channel opens a door for hacking or attacking the information. In order to reduce this and to provide better security, encryption techniques are playing a vital role. Caesar cipher is one among the ancient and a simple encryption technique, which is also known as substitution cipher that means a cipher which substitutes one alphabet to another. But this method is too easy to break the letters. Atbash cipher is one of the monoalphabetic cipher, here the encryption is done by using the Hebrew alphabet, that is it will be encrypted by mapping every alphabet to its reverse order. In this paper, we implement a new encryption technique that will combine Caesar Cipher with Atbash Cipher (CCAC) in order to provide more security than the original Caesar cipher and Atbash Cipher and resist hackers.

1.0 INTRODUCTION

The study or practice of converting plain texts or messages into an unintelligible disguised form so that only the intended recipients can remove the hidden form or disguise and read the original message and the intermediates doesn't identify is known as cryptography. Cryptography is one of the mathematical techniques used to protect messages, data, and images from hackers and it helps us to increase the security of the transmissions or data transfers. The message we received was in plain text, while the one that was hidden is known as encrypted text or cipher text. Although both the plain text and the encryption text are written using alphabets, they are not the same alphabets. Sometimes letters or messages are written by using some special characters, such as punctuation, numbers, and blanks, or any other special characters that are acceptable to both the sender and the recipient. If we take this action, we can lessen the likelihood of theft or hacking.

Enciphering also known as encryption, is the process of turning plaintext or the original communication into ciphertext, which cannot be read by anyone else. Deciphering, also known as decryption, is the process of turning ciphertext back into plaintext. The transformation from plaintext into ciphertext is a function or it is a map from the set $\mathcal{M}$ the set of all possible plaintext message units to the set $\mathcal{C}$ of all possible ciphertext message units ($g: \mathcal{M} \to \mathcal{C}$). We know that this function g is $1-1$, meaning that for each ciphertext message unit, there is exactly one plaintext message unit to be used in the encryption process. The reverse process, or the process of transforming the ciphertext into plaintext, is the decoding process, which is the map g^{-1} ($\because\ g^{-1}: \mathcal{C} \to \mathcal{M}$).

A key is the variable amount or parameter in cryptography that allows us to convert plain text message units into cipher text message units and vice versa. The length of the key has a role in determining how challenging it is to decrypt the text from the original message. Both the sender and the receiver must use the same key for encryption and decryption in symmetric key cryptography, it is also known as private key cryptography, and in asymmetric key cryptography, that is in a public key cryptography (Two different keys are used one private key and one public key for the process of encryption and decryption) The term "public key cryptosystem" also refers to the "trap door function" or "one-way function," which is easy to compute one way but it is too difficult to compute the other way.

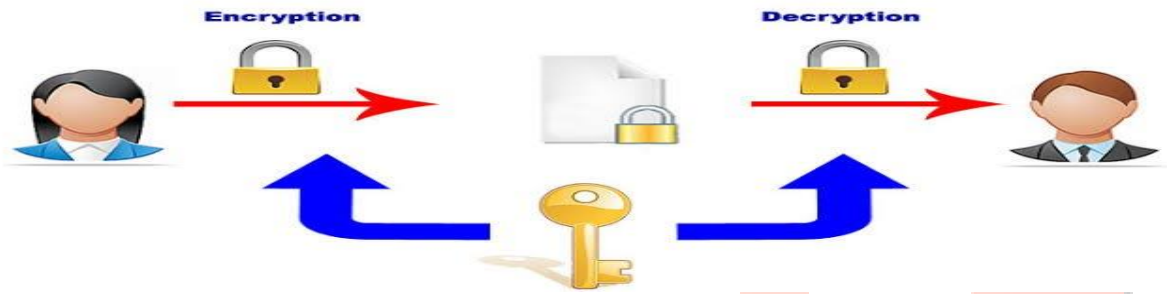

Figure1. Cryptosystem

In cryptography Caesar Cipher is the symmetric key cryptography that means both the sender and receiver should use the same key for both encryption as well as decryption in Caesar cipher the length of the key is three which is made by shifting the alphabets in their positions by three positions to right. It is too easy to break once the intermediates know the technique or using frequency analysis which means the hackers or intermediates can easily find out the original message with the help of most occurring letters in the given format, and Atbash cipher is an cryptography technique which is same as Hebrew alphabets that means, in order to perform the encryption the alphabets can be written in the form of reverse order and then the message units are converted in Atbash technique we does not need any key to encrypt or decrypt which just replacement of the swiping from the reverse order so this method is also too easy to break once the person know the technique. In order to reduce this and give more security we have proposed the new technique that combines Caesar cipher with Atbash cipher.

A new technique has been proposed in this paper is to combine the Caesar cipher with the Atbash cipher to strengthen the security and produce a new and simple approach. The new approach uses only one private common key for both the sender and receiver. The new approach is made by first the sender should encrypt the given message using Caesar Cipher and the encrypted message or the ciphered text can be converted with the help of Atbash cipher and then the output was sent to the receiver over an unsecured channel and the receiver should use the reverse process of this then he can able to read the original message, it will be difficult to break the message unit unless the intermediates should know this approach. The rest of this paper is defined as follows: an introduction to Caesar Cipher is presented in Section 2. And the Atbash cipher was introduced in Section 3.

Section 4 explains the new proposed approach, Section 5 the implementation example will be given. Security analysis will be given in Section 6. Finally, the conclusion and future works are given in Section 7.

2. Caesar Cipher

Caesar cipher is the method used by Julius Caesar in ancient times to communicate messages from one person to another person. Caesar cipher is also known as substitution cipher that means every character can substitute with another character or this can be simply changing a list or can be based on some rules. These methods are not secure anymore but they used this in ancient times to communicate some information secretly in kingdoms, military forces, etc. In Caesar cipher the message units in the plain texts are just replaced by some other message units with some fixed position for example if we use the shift by 1 means; in an alphabet A can be replaced by B, B can be replaced by C, and so on. By shift 2 means; A can be replaced by C, B can be D, and so on.

In Caesar cipher, Caser used to shift 3 positions of the alphabets to encrypt the message that means in an alphabet A can be replaced by D, B can be replaced by E, and so on which is shown in below Table 1. In the first row we have the numerical equivalent values of original message units. The second row we have the original message units, the third row has their equivalent cipher text message units (three positions shifted).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table1. Caesar Cipher technique

In other words, mathematically we can define using modular arithmetic if we have alphabets A to Z with labeling their numerical equivalent values from 0-25. Let $m \in \{0, 1, 2, \dots 25\}$ where m stands for the message unit of the original message. Let us define a function g from $\{0, 1, 2, \dots 25\}$to itself, then we have $g(m) = m + 3 \ (mod\ 26)$ for encryption and $g(m) = m - 3 \ (mod\ 26)$ for decryption, here length of the key be 3.

Example:

1. To perform encryption and decryption for the message “LION IS THE KING” using Caesar cipher.

Encryption (sender): The encryption is can be done by shift 3 positions to right to the alphabets then the shifted message units are $L \to O, I \to L, O \to R, N \to Q, I \to L, S \to V, T \to W, H \to K, E \to H, K \to N,\ I \to L, N \to Q, G \to J$. Hence the cipher text be,

Encrypt (LION IS THE KING) = OLRQ LV WKH NLQJ. **Decryption (receiver):** The decryption is done by shifting 3 positions left to the alphabets then message units of the cipher text are $O \to L, L \to I, R \to O, Q \to N, L \to I, V \to S, W \to T, K \to H, H \to E, N \to K,\ L \to I, Q \to N, J \to G,$ Decrypt (OLRQ LV WKH NLQJ) = LION IS THE KING.

2. To perform encryption and decryption for the message “KING” using Caesar cipher by modular arithmetic.

The encryption is done by first write the original message units into their numerical equivalent value and then using the formula $g(m) = m + 3 \ (mod\ 26)$that is

$$K \to 10 \Rightarrow 10 + 3 = 13\ (mod\ 26) = 13 \to N, I \to 8 \Rightarrow 8 + 3 = 11 (mod\ 26) = 11 \to L,$$

$N \to 13 \Rightarrow 13+3 = 16(mod\ 26) = 16 \to Q, G \to 6 \Rightarrow 6+3 = 9(mod\ 26) = 9 \to J.$

Hence the cipher text of "KING" be "NLQJ" and the decryption is done by first write the numerical equivalent values of cipher text message units and then use the formula $g(m) = m - 3\ \ (mod\ 26)$that is $N \to 13 \Rightarrow 13 - 3 = 10\ (mod\ 26) = 10 \to K, L \to 11 \Rightarrow 11 - 3 = 8(mod\ 26) = 8 \to I,\ Q \to 16 \Rightarrow 16 - 3 = 13(mod\ 26) = 13 \to N, J \to 9 \Rightarrow 9 - 3 = 6(mod\ 26) = 6 \to G.$

Hence the original message of "NLQJ" is "KING".

Weakness of Caesar Cipher technique

- It is very easy and simple method which can be easily broke up
- It is easy to predict by others, because there are only 26 alphabets we used and the length of the key size is also small.
- Using brute force attack or frequency analysis the hackers can predict the cipher text message units also.

3. Atbash Cipher

Atbash cipher is also a substitution cipher which is also known as monoalphabetic substitution cipher which was used based on the Hebrew alphabet. Atbash cipher is also a simple and too easy method to perform encryption and decryption of original message. In this cipher we cannot use any key for encryption or decryption, the encryption is the process done by simply reverse order of the alphabets i.e., A replaced by the last letter Z, B replaced by the second last letter Y, and so on. Which shown in the below table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Table2. Atbash Cipher Technique

The decryption is also made by the use of the above Table2. Since in Atbash Cipher we didn't use any key so it has no security, it is too easy to break even though they didn't know the algorithm or the procedure. But this method was also used in ancient times to communicate and share information secretly from military forces.

Example: Encrypt the message "ROSE IS A CODE" using Atbash Cipher.

The given plain text message units are replaced with cipher text message units using table 2, that is $R \to I, O \to L, S \to H, E \to V, I \to R, S \to H, A \to Z, C \to X, O \to L, D \to W, E \to V$,hence Encrypt(ROSE IS A CODE) = ILHV RH Z XLWV. Similarly, the decryption process is also done by using the reverse procedure.

4. The proposed cryptosystem

The proposed approach of Caesar Cipher with Atbash Cipher (CCAC) has been introduced in this section. This modification, which is a simple and effective method for encrypting our messages, provides better security and makes the system more efficient than the original Caesar cipher technique and also it reduces the time consumption. Since the key length is the same as Caesar cipher technique (Shifting alphabets). Suppose the sender (User A) wants to send a message to the receiver (User B) over an insecure channel:

Firstly, they should agree on Caesar Cipher and share the key parameter commonly $k = 3$, then each party need to know the encryption and decryption procedure of Caesar Cipher and Atbash Cipher, that is they should know both table 1 and table 2. The proposed approach (CCAC) is done as follows; for User A (The sender): First the sender should convert the given message units into a cipher text message units with the help of Caesar Cipher that is using Table.1 and the output ciphertext message units are now consider as the original plain

text units and now convert it into another ciphertext with the help of Atbash Cipher that is using Table 2 then this ciphertext will send to User B over an insecure channel, since the ciphertext is of the unreadable form, if the hackers tries to break this ciphertext using Caesar Cipher or Atbash Cipher means they may get some different message. Hence the security process under this approach is higher than the original Caesar Cipher and Atbash Cipher. Decryption is the reverse process of the encryption firstly the receiver should consider the cipher text message units as original plain text message units then he can convert the message units into a ciphertext message units with the help of Atbash Cipher and the output ciphertext now converted into a message unit with the help of Caesar Cipher hence User B (the receiver) can able to read the original message.

The new approach CCAC is done with the help of the following Table3 in that the first row defines the original message units i.e., alphabets, the second row defines the ciphertext message units of given alphabets when we perform Caesar Cipher and the third row defines the cipher text message units of given alphabets using Atbash Cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Table3. The proposed technique (CCAC)

First with the help of first row and second row we can convert the given message units into an cipher text message units then this cipher text message units are to be considered as original alphabets and then convert it into another cipher text message units with the help of first and third rows, the reverse process is also true that means, if first we perform Caesar Cipher then with that output we perform Atbash Cipher is same as first we perform Atbash Cipher then with that output we perform Caesar Cipher.

5. Implementation Example

Assume that User A wants to send a message "KING IS THE PASSWORD" to User B using CCAC technique. Since both the users should know the procedure of CCAC technique, i.e., they should know Table 3.

Encryption - User A (The sender): Encryption is done by the following three steps.

Step1: First the sender convert the given message units "KING IS THE PASSWORD" into a cipher text message units with the help of Caesar Cipher that is with the help of first and second row of Table3.0 i.e., $K \to N, I \to L, N \to Q, G \to J, I \to L, S \to V, T \to W, H \to K, E \to H, P \to S, A \to D,\ S \to V\ , S \to V\ , W \to Z\ , O \to R\ , R \to U\ , D \to G.$

"KING IS THE PASSWORD" → "NLQJ LV WKH SDVVZRUG"

Step2: The resultant ciphertext message units "NLQJ LV WKH SDVVZRUG" is now convert into another cipher text with the help of Atbash Cipher that is with the help of first row and third row of Table3.0 i.e.,$N \to M, L \to O, Q \to J, J \to Q,\ L \to O, V \to E\ , W \to D, K \to P, H \to S, S \to H, D \to W,\ V \to E\ , V \to E\ , Z \to A\ , R \to I\ , U \to F\ , G \to T.$

"NLQJ LV WKH SDVVZRUG" → "MOJQ OE DPS HWEEAIFT"

Step3: Then the final ciphertext "MOJQ OE DPS HWEEAIFT" will send to User B over an insecure channel.

Decryption - User B (The receiver): Decryption is the reverse process of encryption which done by the following three steps.

Step1: Firstly the receiver should convert the ciphertext message units "MOJQ OE DPS HWEEAIFT" into another cipher text message units with the help of Atbash Cipher that is with the help of third row and first row of Table 3.0.ie., $M \to N, O \to L,\ J \to Q,\ Q \to J,\ O \to L,\ E \to V\ ,\ D \to W, P \to K,\ S \to H, H \to S,\ W \to D,$ $E \to V\ , E \to V\ , A \to Z\ , I \to R\ , F \to U\ , T \to G.$

"MOJQ OE DPS HWEEAIFT" → "NLQJ LV WKH SDVVZRUG"

Step2: The resultant ciphertext units "NLQJ LV WKH SDVVZRUG" is now converted into a message units with the help of Caesar Cipher that is with the help of second row and first row of Table 3.0.i.e., $N \to K, L \to I, Q \to N, J \to G,\ L \to I,\ V \to S, W \to T, K \to H, H \to E, S \to P, D \to A,\ V \to S\ , V \to S\ , Z \to W\ , R \to O\ , U \to R\ , G \to D.$

"NLQJ LV WKH SDVVZRUG" → "KING IS THE PASSWORD"

Step3: Hence User B (the receiver) can able to read the original message as "KING IS THE PASSWORD".

6. Security analysis

Since the proposed technique CCAC has high security than the original Caesar Cipher or Atbash Cipher. Suppose an intermediate has your final ciphertext message units "MOJQ OE DPS HWEEAIFT" which was encrypted and send by the User A to User B over an insecure channel, the intendent people try to break the cipher text message units with the help of Caesar Cipher means he get the output as "MOJQ OE DPS HWEEAIFT" → "JLGN LB AMP ETBBXFCQ" and using Atbash Cipher means "MOJQ OE DPS HWEEAIFT" → "NLQJ LV WKH SDVVZRUG" in both the cases the hacker will get some other message, he didn't crack the original message units so the security analysis under this technique is higher than the original Caesar Cipher and Atbash Cipher techniques.

7. Conclusion

Nowadays information security is one of the most important issues, Caesar Cipher and Atbash Cipher are two simple message encryption techniques which were used in ancient times to communicate information secretly between kingdoms and military forces, etc. A new approach cryptosystem (CCAC) has been proposed in this paper which combines Caesar Cipher with Atbash Cipher in order to increase the security of our information than the original Caesar Cipher and Atbash Cipher techniques. The proposed approach is more efficient and resists against different breakup techniques, some of them are discussed in Section 6. The proposed approach can be used effectively in wireless applications; it is also a simple and fast encryption/decryption technique with better security. In this paper, we applied the new approach to message encryption, decryption. In the future, this approach will be modified and to be used for image encryption, decryption.

8. REFERENCES

- Diffie, W., Hellman, M., New directions in Cryptography, IEEE Trans. Inf. Theory 22 (6), 644 – 654, 1976.
- Joseph H. Silverman, An Introduction to the Theory of Elliptic Curve, University of Wyoming, 2014.
- Kenneth H. Rosen, Elementary Number Theory and its Applications, Addison- Wesley Publishing Company. Sydney, 1986.
- Mohan. P, Rajendran. K, Rajesh. A, An Encryption Technique using a Complete graph with a Self-invertible matrix, Journal of Algebraic statistics, Volume 13. No 3, (2022), https://publishoa.com/index.php/journal/article/view/816, pp.1821-1826.
- Mohan P, Rajendran K, Rajesh A. A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix, Indian Journal of Science and Technology, 15(44) (2022), pp.2351-2355.
- Mohan P, Rajendran K, Rajesh A. An encryption Technique using the adjacency matrices of certain graphs with a self-invertible key matrix, E3S Web of Conf, Volume 376, 01108(2023) https://doi.org/10.1051/e3sconf/202337601108
- Mohan P, Rajendran K, Rajesh A. Enhancing Computational Performance of Minimal Spanning Tree of Certain Graphs Based Enciphering Technique Using Self-Invertible Key Matrix, Journal of Aeronautical Materials(1005-5053), Vol 43, Issue-01(2023), pp 359-371, https://www.hkclxb.cn/article/view/2023/359.html.
- Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer, 2014.