International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security Enhancement Using Caesar Cipher

Manepalli Dharani Pujitha

Student, Rajam, Vijayanagaram, 532127, India

ABSTRACT

Cryptography is the facility and glance of secure communication techniques and used for converting the original messages into unreadable form. cipher is classified into classical and modern cipher Caesar cipher is a technique of encrypting messages into unreadable form to protect it from dissentients. Caesar cipher comes under symmetric techniques which contains a secret key for converting the message. The challenges faced by Caesar cipher are that it is easy to hack, provide less security and by looking at patterns. The entire message can be decrypted. To provide more security using techniques like affine cipher, Vigenere cipher, three-pass protocol, columnar cipher all these are used to create an encrypted text which is very hard to decode. Caesar cipher can be encrypted by using all ASCII and extended ASCII characters including alphabets. This will provide an enriched side of Caesar cipher which can defeat all the threats endured by the Caesar cipher.

Keywords: Caesar Cipher, Vigenere cipher, Encryption, Shift Cipher, Columnar cipher, plaintext, ciphertext, Affine Cipher, Decryption.

Main text

INTRODUCTION:

Now-a-days internet is incredibly important, a world without the internet was impossible to imagine. The fashionable epoch is intimidated by digital technology - messages, calls, mails, and online stores. Because of this, there will be a high requirement of the internet. The data may be personal or private; all it requires is security. By using encryption algorithm at sender side and decryption algorithm at receiver side might increase security. The technique and research of keeping information secure by changing it into an unreadable or unintelligent form that fortuitous receivers cannot understand is called cryptography. Cryptography or cryptology is the word derived from Greek krypton that means hidden, secret. Akdeniz said the definition of cryptography as “Cryptography is the knowledge and learning of hidden script” that data will be hidden by encrypting it. To avoid the information from revealing through different techniques like recording of the messages or eavesdropping. Cryptography covers mainly four objects i.e,

1) Confidentiality: Confidentiality means preventing unauthorized access and to protect the data from unauthorized access and disclosure, including protecting personal privacy information.
2) Integrity: Data integrity ensures that the received data is the actual valid data that no unauthorized persons are modified, and has not been tampered or manipulated.
3) Non-repudiation: Affirmation that the data of the sender will be verified by the receiver with the proof provided by the sender earlier, or after quash having processed the information.
4) Authentication: Authentication is used by a client when the client needs to know that the server is the system it claims to be. In the authentication process, the user or computer has to prove its identity to the server or client. Usually, authentication by a server needs the use of a username and password.
5) Access control: Access control identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens.

Encryption is a method of inducing the data from intelligent form to unintelligent form. Decryption is a method of inducing data from unintelligent form to intelligent form. Plain text is the original message and Ciphertext is the output of an encrypted message. Encryption techniques are two types they are substitution technique and transposition technique.

In substitution technique, plain text is replaced by some other letters or numbers or any symbols. Examples: Caesar cipher, hill cipher, monoalphabetic cipher, polyalphabetic cipher. Transposition technique is a cryptography technique that converts the message into unreadable form by performing permutations on the message. Cryptography is classified into 2 types: symmetric key cryptography and asymmetric key cryptography. In symmetric technique a secret key is used at both ends. By using a single key the sender will encrypt the plaintext using the encryption technique. By using the same single key the receiver will decrypt the plaintext by using a decryption algorithm. Symmetric techniques are further divided into stream cipher and block cipher.

1) Stream Cipher: It encrypts the message into unreadable form taking 1byte of plain text at a time.

2) Block Cipher: It encrypts the message into unreadable form by taking plain text as a block at a time.

In asymmetric key cryptography uses two different keys one is private key and another one is public key. Public key is generated by the sender for sending messages. That can be shared to all the users. The receiver will decrypt the plaintext by using his generated his own private key.

Illustrations

LITERATURE SURVEY:

In paper [1] Sravani, Jayanti Proposed an algorithm on modified caesar cipher.[1] [2] The author explains about the encryption techniques for secure cryptosystems to maintain Confidentiality in transmission, storage, usage of information and rigorous in the procedure of Cryptanalysis. [6]At present, it is very necessary to exchange data using the open network that is the internet. The main advantage of the technology is that banking and e-commerce transactions are taking place digitally.

[8] Due to huge growth in technology, security has become more Priore. The unauthorized relay of data in the defense system is extremely anguish and causes damage. [9]Because of numerous reasons mankind has to communicate in a secure manner .Providing security based on modular arithmetic plays a major important role in cryptography from classical crypto systems to modern asymmetric systems.

[10] Asoronye, Gaylord O., Goodluck I authors says about Organizations will have confidential data such as financial forecasts, earnings, customer lists, product roadmaps, staff and customer contacts, and strategic corporate data that is used for internal usage on a classified manner; data sniffing or outright theft of these classified data could lead to the violation of organizations privacy thereby limiting the organizations competitive advantage over her rivals. [11]Naji, M. says A wide proportion of mechanized data such as voices, pictures and video are traded from point to point on different frameworks like web, versatile frameworks, remote distinguishing satellites and others. It is crucial to shield huge data from an unapproved catch or modifying on the open framework.

[12] In some cases if we neglect security someone is eavesdropping upon us but in such situations. confidentiality becomes necessary and we want to secure the information from outsiders. In all above cases to provide security we use cryptography. Cryptography [3][2][4] is a technique for the studying of secure communication without interference from outside elements and used for converting the original messages into unreadable form. [13] Siahaan, Andysah Putera Utama authors proposed a work on three pass protocol in modern cryptography in which there is no need of exchanging keys from both ends and implements using the Caesar cipher technique.

[14] Rao, P. Srinivasa, and D. Nagaraju told the word Cryptography is derived from Greek. It is a combination of two words 'Kryptos' and 'Graphy' which mean 'Secret' and 'Writing' respectively. Cryptography is the study and practice of secret and hidden writing and its techniques. [15] Jain, Atish, Ronak Dedhia, and Abhijit Patil talk about Confidentiality, Integrity, Non-repudiation and Authentication. They provide some policies for secure communication. The Classical ciphers work on letters and digits are to be modified for security enhancement. To enhance the security several various ciphers are developed. The algorithms used are Caesar cipher, affine cipher and uses unicode characters. In this paper classical ciphers are combined with Caesar ciphers. In paper [5] Wulandari, Septi Yana author emphasis will be placed on classical cryptography. Earlier, in cryptology there were a huge number of terms that had to be studied. In some classical cryptography can be used to hide messages as a Caesar cipher and affine cipher.

In paper [7] Santos, António, and Renato Vasconcelos Júnior show that a small change for Caesar cipher will give some improvement in the method's safety. Intending to complete socialization, but as time passed humans began to disperse and the need to disclose with humans evolved into writing and sending messages. For safer communication encryption methods are adapted. In this paper the author uses modified Caesar cipher for greater security. The suggested method enhances the security to an advanced extent due to the fact that intending to decrypt the ciphertext one should have access to keys in the algorithm.The Unicode characters used will increases the possibilities of key combinations making it difficult for cryptanalysis by brute force attack that adds to the security enhancement.

METHODOLOGY:

Caesar cipher:

The Caesar cipher is ancient and well known in the evaluation of cryptography. That produces ciphertext by exchanging the characteristic of plaintext into exactly one character in the ciphertext. This method is called the single cipher alphabet. The main idea of the algorithm is to shifting towards all the characteristics in the plaintext with the same shift value

VIGENERE CIPHER:

Vigenere cipher is a symmetric algorithm in which the single key is used for both encryption and decryption. The security for key and key distribution is necessary as if the key is known automatically the plain text and cipher text can be known.

The vigenere cipher uses various Caesar cipher techniques for encryption based on some letters of keywords. In this shifting mechanism is applied. It will shift the characters of plain text by various amounts using the vigenere table. The table defined in this method is used to implement various algorithms.

It is the foremost popular ciphers within the past and it also resisted the frequency analysis test of the letters that may crack many ciphers techniques like Caesar cipher. The Vigenere cipher consists of the many Caesar ciphers with different shift values.

Encryption formula for above process:

C= (P+K) mod 26.

Decryption formula for above process:

P= (C-K) mod 26.

The Vienere cipher will use the repeated words as key-streams may cause the repetition of patterns in the cipher texts the identical as the length of the keyword used. in line with this table, the plaintext CALLMEATNINE will be replaced by ciphertext CTELOOAMGIPO using Key ATTACKATTACK. If the length of the key is a smaller amount than the plaintext then the key is going to be used repeatedly until the extent of the key becomes capable of plain text.

[12]

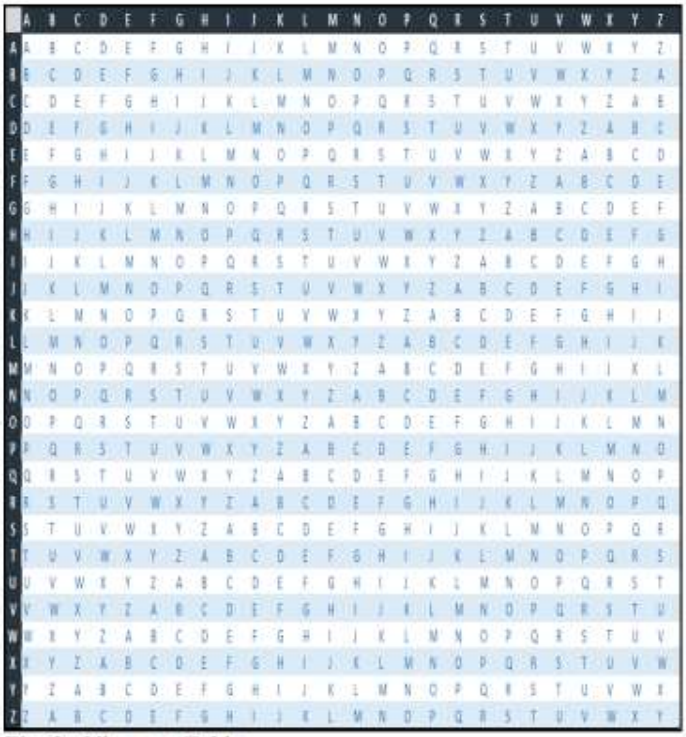

Fig. 2. Vigenere Table

Three-pass protocol:

Three-pass protocol allows one party to send messages securely to a second party without exchanging the encrypted key. The process is called Three-pass protocol as it exchanges three times to verify the sender and receiver of the initial protocol. This technique is implemented using XOR operation. The basic concept of this technique is that each party has the private encryption or a private decryption key. Both of them use the key for encrypting the message first and then to decrypting the message. The protocol works based on communicative cipher or LIFO method.Communicative means the order of encrypting and decrypting process is interchangeable (Encryption A - Encryption B - Decryption A - Decryption B).

This technique's purpose is to make the process secure to send the message using various algorithms and there is no need to know the key by both the parties.

The purpose of this study is to make the process of security for the message to be sent using different algorithms and both parties do not need to know the key to each party. In the process of encoding results are obtained in the form of ciphertext.

[13]

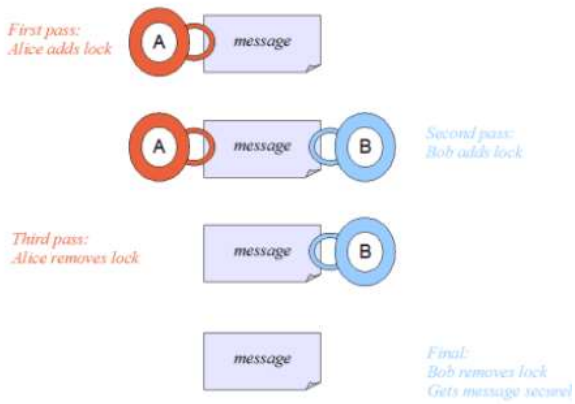

Fig. 1 : The Three-Pass Protocol scheme

Caesar Cipher:

C = $Cipher\ text$

P = $Plain\ text$

i=index of letter

Encryption: C i≡ (Pi + ki)m$od\ n$

Decryption: Pi ≡ (C i−k i)m$od\ n$

n = $number\ of\ characters$ (26 $alphabets$)

k = key

Affine Cipher:

Encryption: C i≡($a * P$i + b)$mod\ n$

Decryption: Pi ≡ (a −1 $* C$i − b)m$od\ n$

$where\ n$ = $number\ of\ characters$ (26 $alphabets$)

a = $first\ key$ (*greatest common divisor*(a, n) = 1 $for\ inverse\ of\ a$)

b = $second\ key$

a −1 = $inverse\ of\ a$ ($a * a$ −1 ≡ 1(mod 26))

Columnar Cipher:

A columnar cipher changes the letters or words in the given message to get the ciphertext. So, encrypted text is attained by using swapping on the given message. To decrypt the message the key used is the reciprocal of the encryption key. In this technique the message is wrote in stable length rows(n*n), now the columns will be modified based on the secret key generated, and the message is encrypted one column after another column. In case the matrix is not completed or spaces are filled by adding(padded) the null or some other character to the matrix to be filled.

Example:

Message: Thief attack our house (z is used for padding).

Key:41325

Step 1: Each letter in the message will be written column by column(n*n).

1 2 3 4 5

t h i e f

a t t a c

k o u r h

o u s e z

Step 2: In this step the message will be rearranged in the columns depending on the key.

4 1 3 2 5

e t i h f

a a t t c

r k u o h

e o s u z

Step 3: Arranged matrix will be written column by column to get ciphertext.

Encrypted text: earetakoitushtoufchz.

By dividing the length of ciphertext by the key length the receiver has to divide the column lengths. now write the cipher text in columns one more time and reorder the columns by amending the keyword to get the original message.

Caesar and Affine Cipher:

The cesarean section and affine cipher in hiding messages by converting the message into ASCII code first. Examples of transforming the messages into ASCII code, as given below in table 2.

[5]

Tabel 2. Message transformation to code ASCII.

Character	Unicode (Heksadesimal)	ANSI ASCII (Decimal)	Description
SP	20	32	Spacing
!	21	33	exclamation mark (exclamation)
“	22	34	Double quotes
#	23	35	Hash tag (kres)
A	41	65	Latin capital letter A
B	42	66	Latin capital letter B
C	43	67	Latin capital letter C

The combination of cesarean cipher and affine cipher might be worked out by doing encryption and decryption in an order using both ciphers techniques. So that the ciphertext 1 is obtained when the message is encrypted with a cesarean cipher. Ciphertext 1 is located as a plaintext is again encrypted with an affine cipher inorder to produce ciphertext 2. In the decryption process, ciphertext 2 is decrypted first so that it becomes a plaintext which adduces to the ciphertext 1 and that ciphertext is again decrypted to get the original plaintext.

The Caesar cipher is part of a classical cipher called shift transformation. In cesarean cipher the plaintext(p) is encrypted to produce ciphertext(c) by utilizing the key can be expressed as follow:

$C = (P + k) \bmod 256, 0 \leq P \leq 255$

Where k is the no. of ASCII code shifts required. For decryption of cesarean cipher can be finished by transforming ciphertext (C) to produce a plaintext (P) can be expressed as follow:

$P = (C - k) \bmod 256, 0 \leq P \leq 255$

Affine cipher is an extension of Caesar cipher. In affine cipher to produce encrypted text plaintext (P) is transformed into ciphertext (C) that can be expressed as the follow:

$$C \equiv ((a \times P) + b) \pmod{256} \qquad 0 \leq P \leq 255$$

Where a, b are integers

b= number of desired alphabet shifts.

a= relatively prime with 256 or (a,256) in inverse [1,10].

Depending upon the relationship between ciphertext (C) and plaintext (P), then to get the plaintext (P) is the reciprocal of ciphertext (C). Plaintext (P) can be expressed as follow:

$$P \equiv (\bar{a}\,(C - b)) \pmod{256} \qquad 0 \leq C \leq 255$$

Where $\bar{a}$ = inverse of a (mod 26).

$\bar{a}$ can be find using congruence $\bar{a} \equiv a\ \emptyset(256)-1 \pmod{256}$. Or$(a, m) = 1$, an integer solution x of $ax \equiv 1\ (mod\ m)$ is called an inverse of a modulo m."

RESULT & DISCUSSION:

Application of Caesar and Affine Cipher:

A combination of Affine cipher and Caesar cipher encryption is more difficult to solve due to only encoding using a Caesar cipher will be easy to decode by utilizing the brute force approach and the most frequent presentation of letter frequencies. Every time Caesar ciphers do not have to be combined with affine ciphers or vice versa for secure communication. Affine cipher and Caesar cipher may be separately joined with other methods for better and secure communication.

The use of changing into the ASCII code will influence the modulo calculation. In the case of changing into alphabetical numbers, it is sufficient to use modulo 26 as the number of the alphabet was 26. But the ASCII code is 256 with extra space, so the modulo used is modulo 256.

Three-Pass Protocol Implementation:

Now to prove the Three-Pass Protocol algorithm works on Caesar Cipher. By taking an example with the plaintext "REMEMBER THE PRIVATE PASSWORD" and the shift value is 5. The encryption process takes twice as long. First, the sender must encrypt the message. Later when the message arrives at the receiver, they must encrypt the message for the second time. As shown in the Table 1

[13]

Table 1 : The first round of encryption

ENCRYPTION 1								
PT	R	E	M	E	M	B	E	R
CT	W	J	R	J	R	G	J	W
PT	T	H	E					
CT	Y	M	J					
PT	P	R	I	V	A	T	E	
CT	U	W	N	A	F	Y	J	
PT	P	A	S	S	W	O	R	D
CT	U	F	X	X	B	T	W	I

In Table 1 plaintext will be encrypted using Caesar Cipher. The final encrypted ciphertext is "WJRJRGJW YMJ UWNAFYJ UFXXBTWI".

[13]

Table 2 : The last round of encryption

ENCRYPTION 2								
PT	W	J	R	J	R	G	J	W
CT	A	N	V	N	V	K	N	A
PT	Y	M	J					
CT	C	Q	N					
PT	U	W	N	A	F	Y	J	
CT	Y	A	R	E	J	C	N	
PT	U	F	X	X	B	T	W	I
CT	Y	J	B	B	F	X	A	M

Table 2 shown about the second round of the encryption using shift value 4. The ciphertext would be "ANVNVKNA CQN YAREJCN YJBBFXAM". It is the final set of the encryption process.

[13]

Table 3 : The first round of decryption

DECRYPTION 1								
PT	A	N	V	N	V	K	N	A
CT	V	I	Q	I	Q	F	I	V
PT	C	Q	N					
CT	X	L	I					
PT	Y	A	R	E	J	C	N	
CT	T	V	M	Z	E	X	I	
PT	Y	J	B	B	F	X	A	M
CT	T	E	W	W	A	S	V	H

Table 3 shows the decryption. It will produce the ciphertext format since the text is not readable. This ciphertext has to be sent to the receiver once again to make it fully readable. In Table 4 we can see the last decryption of all processes.

[13]

Table 4 : The last round of decryption

DECRYPTION 1								
PT	V	I	Q	I	Q	F	I	V
CT	R	E	M	E	M	B	E	R
PT	X	L	I					
CT	T	H	E					
PT	T	V	M	Z	E	X	I	
CT	P	R	I	V	A	T	E	
PT	T	E	W	W	A	S	V	H
CT	P	A	S	S	W	O	R	D

CONCLUSION:

From the above methods enhance the security to a greater extent. The methods used in the paper can overwhelm all the infirmity and challenges of Caesar cipher. On carrying out cryptanalysis it is unattainable to decode the ciphertext by persistent analyzation. Security presumed by these methods can be improved later by utilizing it with various encryption techniques or by utilizing asymmetric key rather than symmetric key. The combination of affine cipher and Caesar cipher is done because affine cipher has advantages that can cover the shortcomings of Caesar cipher so that the code formed is more difficult to solve and harder to break.

References

[1]. Sravani, Jayanti. "A Study on some modified Classical Ciphers for Secure Crypto-System." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.6 (2021): 5316-5319.

[2]. Maihankali, Munura, and Esther Chinwe Eze. "Symmetric Cryptography for Confidential Communications: Implemented by Enhancing the Caesar Cipher." International Journal of Computing and Engineering 2.1 (2021).

[3]. Thakkar, Binita, and Blessy Thankachan. "A Multilevel Approach of Transposition Ciphers for Data Security over Cloud." GIS Sci. J 8.5 (2021): 1732-1738.

[4]. Noman Abed, Hazim, Zainab Mohammed Ali, and Ahmed Luay Ahmed. "A Robust Encryption Technique Using Enhanced Vigenre Cipher." International Journal of Nonlinear Analysis and Applications 12.2 (2021): 447-454.

[5]. Wulandari, Septi Yana. "Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message." Proceeding International Conference on Science and Engineering. Vol. 3. 2020.

[6]. Ortzow, Kyle. "Original Code for Encrypting and Decrypting Caesar Ciphers." Available at SSRN 3694155 (2020).

[7]. Santos, António, and Renato Vasconcelos Júnior. "Improving Caesar Cipher for greater security".

[8]. Arroyo, Jan Carlo T., and Allemar Jhone P. Delima. "A Hybrid Caesar-Polybius Cipher with XOR Operation for Enhanced Cryptography."

International Journal 9.3 (2020).

[9]. Madushani, A. P., and P. G. R. S. Ranasinghe. "A symmetric and a transposition cipher using the Euler's totient function." Ceylon Journal of Science 48.4 (2019): 327-330.

[10]. Asoronye, Gaylord O., Goodluck I. Emereonye, and Ibiam A. Agha. "An Efficient Implementation for the Cryptanalysis of Caesar's Cipher." The Melting Pot 5.2 (2019).

[11]. Naji, M., et al. "Implantation of Caesar and Hill Cipher on Database for Better Security." Eur. J. Technol. Eng 18 (2019): 24.

[12]. Gautam, Deepanshu, et al. "An enhanced Cipher technique using Vigenere and modified Caesar cipher." 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2018.

[13]. Siahaan, Andysah Putera Utama. "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography." (2017).

[14]. Rao, P. Srinivasa, and D. Nagaraju. "Enhanced Caesar Cipher algorithm with variable length key and increased cipher complexity."

[15]. Jain, Atish, Ronak Dedhia, and Abhijit Patil. "Enhancing the security of caesar cipher substitution method using a randomized approach for more secure communication." arXiv preprint arXiv:1512.05483 (2015).