International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 13 Issue 5, May-2024, Impact Factor: 8.375

Strengthening Data Security with a Series of Caesar Cipher Revisions

Nimay Seth[1], Pooja Jadon[2], Khushbu Sharma[3]

[1]Jayshree Periwal International School Jaipur, Rajasthan, India
[2]Jayshree Periwal Global School Jaipur, Rajasthan, India
[3]Vivekananda Global University Jaipur, Rajasthan, India

ABSTRACT

Since there is now more data being transmitted than ever before in today's environment, information security has become essential. The skill of turning a plain text message into one that cannot be read is known as cryptography. In information security systems, encryption methods are crucial. Encryption is regarded as one of the most effective methods for sending data securely over a communication network. A large number of ciphers have been created to secure data. This work aims to create a novel modified hybrid method of plaintext encryption in order to add to the body of knowledge in the field of classical cryptography. While using vast key areas with a large number of rounds and various complex procedures may increase security, it also slows down operations. Therefore, a modified Vigenere Cipher that boasts of confusion and diffusion that classical ciphers cannot match is proposed in this study. In addition to adding alphabets, numbers, and symbols, the Caesar and Vigenere ciphers were also enlarged upon, which resulted in a total confusion and diffusion within the modified cipher created.

INTRODUCTION

As computer technology advances quickly, more and more data files are being sent over the internet. Consequently, safe transmission of confidential information over open channels has gained widespread attention in research and academic domains.

An Introduction to Cryptology

Greek terms "Kryptos" (which means hidden) and "logos," which means "study," are combined to form the word cryptology. As old as writing itself, cryptology [1] has been employed for thousands of years mainly to secure diplomatic and military communications.

The field of cryptography:

Writing covertly such that the intended recipients are unable to understand the original message is known as cryptography [2]. It changes the data into a format that is so incomprehensible that unauthorized or unintentional users are unable to decipher the original meaning of the message and perceive it as worthless. The primary requirement for any transformation is that it must be reversible, allowing the intended user to obtain the original data by using the original key and procedure. This is the conventional application of cryptography; nevertheless, in the contemporary era, its range has expanded.

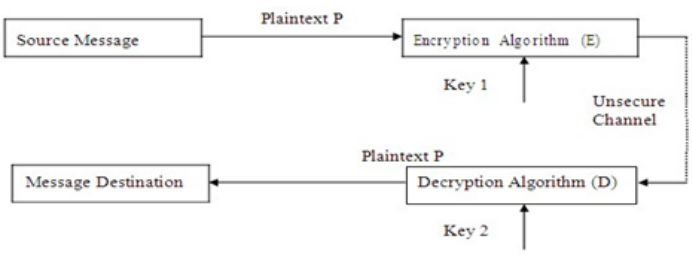

Fig. 1.1 Cryptography Systems

An Overview of Cryptography Terminology
The following definitions of several fundamental terms related to cryptography [3] are necessary because they will be used frequently in this thesis.

Text or Message The data that needs to be transmitted via the insecure channel is called the message, or plaintext P. Symbols are arranged in a group or order within the message.

Text cipher the encrypted data, or "Cipher text," is what will be transmitted over an unreliable channel for information transfer. Even if an adversary manages to decipher the Cipher text C, he should not be able to understand the Plaintext P.

The key is the secret key that will be sent from sender to recipient in order to encrypt the plaintext. Before any real communication happens, this key needs to be sent and received over a secure channel by the sender and the recipient. While distinct keys are used for encryption [4] and decryption, as is the case with asymmetric key cryptography, the same key is utilized to decrypt the cipher text back into plain text.

The use of encryption often known as EK (P): P x K → C, is an algorithm or function that uses the secret key K to transform plaintext into cipher text.

Decoding the inverse function of the encryption function, decryption, or DK (P): C x K → P, transforms the Convert the encrypted text into plaintext using secret key K.

Asymmetric key cryptography differs from symmetric key cryptography in that the encryption key (Ke) and decryption key (Kd) are distinct. The unsecure transmission routes that transfer messages from sender to recipient and cannot be made safe are the reason why cryptography is necessary.

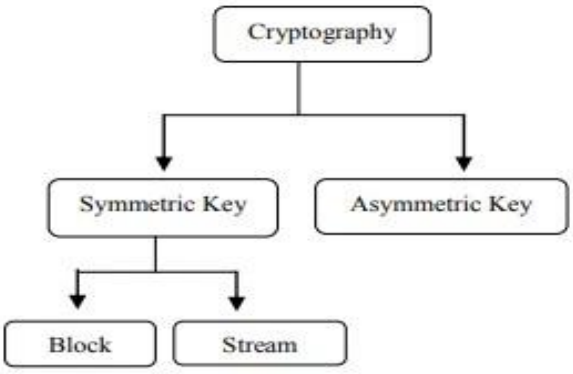

Fig.1.1.2Cryptographyclassification

Cryptanalysis
The subject area known as "cryptanalysis" focuses on methods for confirming and proving the security of cryptographic systems and algorithms. Evaluating the security claims made by cryptographic systems is the aim of cryptanalysis techniques. To demonstrate that the claimed security level is not met because of flaws in the cryptography system, cryptanalysts attempt to create an attack.

The quantity of information that an attacker has access to can be used to categorize attacks:
Text cipher: Just Attack All that the attacker may access is the encrypted text. Attack with a known-text here, the attacker has access to the plaintext as well as the pertinent cipher text. This technique can be employed by an attacker who has restricted access to the encryption equipment. Particular-Plain Textual Abuse An attacker selects a plaintext and uses the appropriate key to generate the corresponding cipher text. This is only applicable if the attacker has access to an encryption [7] equipment and is able to encrypt a desired message with it. This type of attack aims to find the secret key or algorithm for any given encrypted material.

Chosen-Cipher text Attack
After selecting a text to cipher, the attacker generates the corresponding plaintext by using the relevant key. The attacker must be able to fully control the decryption device in order to decrypt any message they want. Only then is this possible. Another goal of this type of attack is to figure out the secret key or technique for any given encrypted text [8].

The three major goals of such attacks are to either recover a secret key or recover plaintext without getting a key or identify the encryption/decryption method.

The Research's Objective

The main objective of this work is to create a modified hybrid of the Caesar and Vigenere ciphers[17] that can stop unwanted access to or alteration of sensitive data by adding a significant level of confusion and diffusion into the cipher—something that classical ciphers are unable to do. The goal of this work is to implement a modified Vigenere[18] Cipher with a 95% confusion and diffusion rate. "A small portion of the security required for "perfect" secrecy is provided by cryptography."

LITERATURE REVIEW

Literature overview:

Ajit Singh, Aarti Nandal[20], and Swati Malik (2019) presented an automated cipher key change after each encryption phase, resulting in a new method of implementing the Vigenere algorithm[21].

A variant of the Vigenere cipher using random numbers, punctuation, and mathematical symbols was proposed by C. Bhardwaj (2018) [22]. The suggested approach substituted mathematical symbols, punctuations, and numbers for characters in the key to increase the difficulty of brute force attacks.

An alpha-qwerty cipher was presented by Khalid (2023) as an expansion of the Vigenère[23] encryption. Instead of using the standard 26 alphabets, the Vigenère square table was expanded and modified by the system to include 92 characters. The Vigenère cipher is a technique for encrypting alphabetic text by singing a sequence of various Caesar ciphers based on the letters of a keyword, according to Md. Khalid[24], I. R., Neeta, W., & Vaibhav, M. (2022). This type of poly alphabetic substitution is straightforward-A. Kester (2012)[25] Plaintext is changed into cipher text through encryption, and cipher text is changed back into plaintext through decryption, and vice versa. Additionally, it is divided into two fundamental types: symmetric and asymmetric. José Xexéo and Flavio de Mello. 2018[48] The creation of public key cryptography is the second, more significant discovery that altered the entireMuhammad Osama, Bryan M. Li, Sicong Huang, Ivan Zhang, Aidan N. Gomez, and Lukasz Kaiser. (2018) [49] An extremely thorough history of cryptography the thorough chronicle of covert communication spanning antiquity to the internet. Stefan K¨olbl. and Ralph Ankele (2018) [50] The study illustrates how the performance of the Vigenère encryption and frequency analysis attack are affected by changing the key length.

METHODOLOGY

Proposed System Structure

Although professionals have put in place a number of instruments to convert data via encryption technology in order to stop unauthorized parties from accessing or changing private or official information, hackers and invaders continue to operate with impunity.

Therefore, in order to communicate more securely, it is necessary to
i) Enhance public-key cryptography system in communication technology on data encoding and decoding.
ii) Improve secure communication technology on data encryption and decryption
iii) Provide sufficient security to document or data confidentiality and secrecy
iv) Offer more workable solutions for maintaining the confidentiality of documents or data
v) Provide affordable, effective, and safe systems to safeguard the enormous amounts of data communicated and stored by electronic data-processing systems, the growth in electronic fund transfers, instant email, point-of-sale terminals, and home banking

Problem statement

"To stop unwanted access to or alteration of private data by adding a significant degree of confusion and dispersion to the cipher that traditional ciphers cannot match."

Significance of Work

Changing the cipher so that, in contrast to the standard Caesar and Vigenere Cipher, which could be cracked using letter frequencies, the plaintext cannot be ascertained by counting the frequency of the letters or symbols generated at the end of the day. In order to strategically promote the expansion of secure communication in the future, it is necessary to immediately implement various approaches for securing communication over non-secure communications channels as well as open and close innovation conceptions.

Vigenere Cryptosystem

The Vigenere cipher is a 26 by 26 matrix poly alphabetic substitution cipher. The Caesar cipher moves. It is composed of a set of Caesar cipher mono alphabetic substitution rules with shifts ranging from 0 to 25.

The encryption and decryption process of the vigenere cipher

can also be represented mathematically as:

$Ci = E\ (Pi + Ki)\ mod26$ ---------- (1)

$Pi = D(Ci + Ki) mod26$ ----------(2)

Where C represents the cipher text,

P represents the plaintext character,

K represents the key

E is the encryption function, while D is the decryption function.

If for example, we have a plaintext: "SECURITY IS ESSENTIAL", and a keyword: "TRUE". The Vigenere cipher encryption is done by aligning the keyword below the plaintext.

Plaintext: SECURITY IS ESSENTIAL----------(1)

Keyword: TRUETRUETRUETRUETRU----------(2)

The resultant cipher text from the above text becomes: "LVWYKZNCBJYWLVHXBRF".

Calculating the index of coincidence of the cipher text using the formula:

$$I.C = \frac{\sum_{i=A}^{i=Z} \bar{fi}(fi-1)}{N(N-1)}$$

$$I.C = \frac{\sum_{i=A}^{i=Z} fi(fi}{N(N-}$$

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

Table Vigenere Square (Fig. 3.1)

Proposed Algorithm:

In proposed technique we eliminate this problem by introducing different numeric value for space in each table. The encryption and decryption process by proposed approach is given below:

Formula for encryption by proposed method is:

$$Ci=Pi+Ki(modm)$$

In proposed approach h we have length of alphabet 27, sovaluem will be 27.

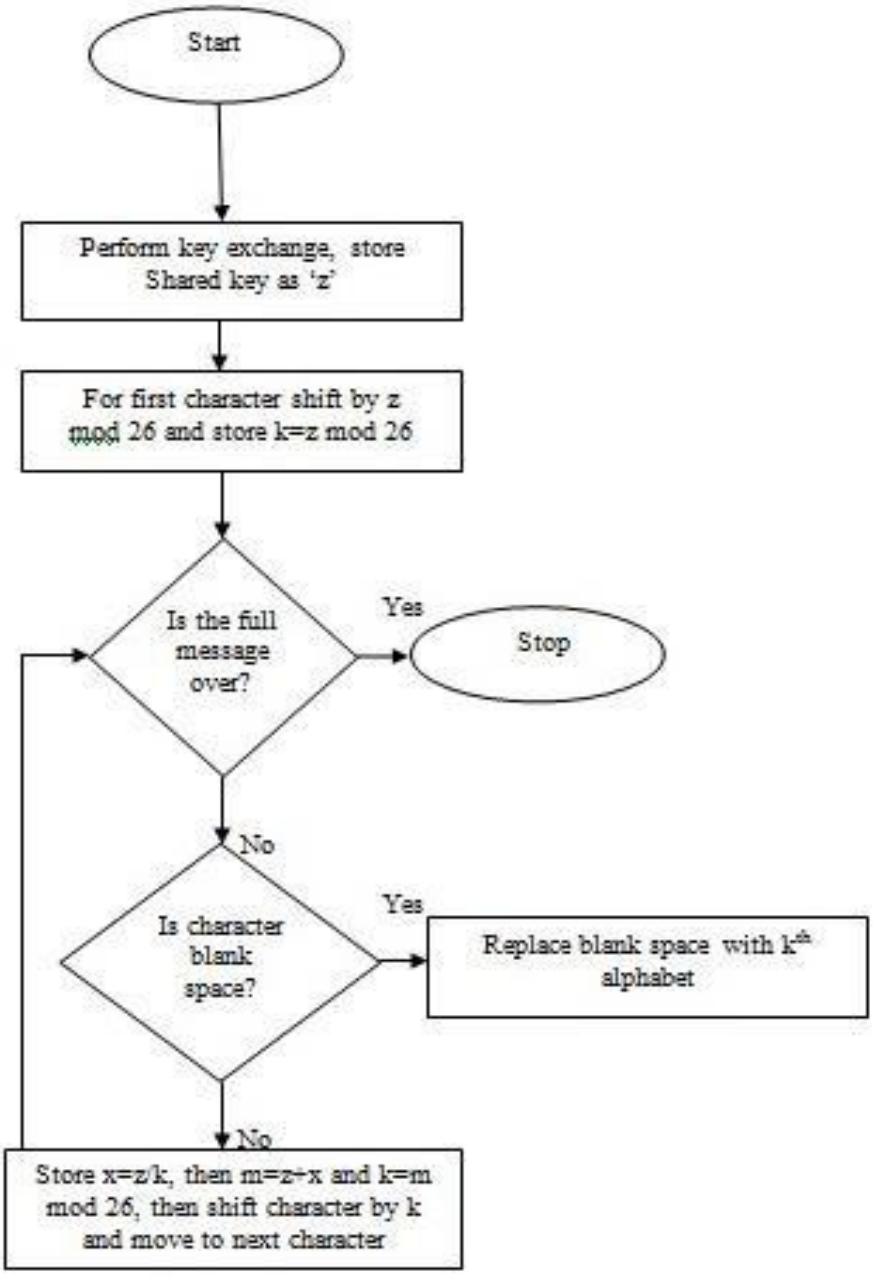

Fig.3.4 Proposed Approach

Fig.3.4 Proposed Approach

Encryption:

Mathematically we can express encryption process by proposed algorithm as:

$C1 = P1 + K1 \pmod{27}[T1],$

$C2 = P2 + K2 \pmod{27}[T2],$

------ ,

$C8 = P8 + K8 \pmod{27}[T8],$

$C9 = P9 + K9 \pmod{27}[T1],$

------,

$C16 = P16 + K16 \pmod{27}[T8],$

$C17 = P17 + K17 \pmod{27}[T1],$

Where, T in above mathematical relation represents table no.

Decryption:

The suggested method's decryption procedure functions similarly to encryption, but in the opposite way. The decryption formula using the suggested method is:

$Pi \pmod{m} = Ci - Ki$

the steps involved in the decryption process are:

i. In accordance with table 3.1, the numerical values of the first cipher text character and the key character will be deducted.

ii. The resultant value from the previous step will be calculated modulo 27. The first plain text character will be the one that corresponds to the modulo value that has been calculated.

iii. The procedure outlined in the preceding phases will continue through the eighth table. Following that, the following cipher character—character 9 in the cipher text and key—will follow the same procedure, using a value from table 3.1 and so forth.

Mathematically we can express decryption process by proposed algorithm as: P1 =

C1-K1 (mod 27) ..... [T1]

P2 = C2-K2 (mod 27) ..... [T2]

P8 = C8-K8 (mod 27) ..... [T8]

P9 = C9-K9 (mod 27) ..... [T1]

P16= C16- K16 (mod 27) ..... .[T8]

P17= C17- K17 (mod 27) ..... .[T1]

PROPOSED TECHNIQUE TABLE

T.No.	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	26
1	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	&	A
2	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
3	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E
4	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G
5	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I
6	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K
7	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K	L	M
8	P	Q	R	S	T	U	V	W	X	Y	Z	&	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

TABLE 3.4.2

IVEXPERIMENTAL RESULTS

Traditional Vigenere Cipher Caesar

Table 4.1 showing encryption time

TABLE 4.1

ENCRYPTION TIME

Cipher Ceasar Encryption

S. No.	PlainText	Key	Cipher Text	cipher ceaser
1	red cookies	5	wjifhttpnjx	0.000618423
2	orange	2	qtcpig	0.000550311
3	pineapple	7	wpulhwwsl	0.000416109
4	mango	4	qerks	0.000414857
5	apple	9	jyyun	0.000534017
6	pasta	8	xiabi	0.000564255
7	white sauce pasta	3	zklwhdvdxfhdsdvwd	0.000495078
8	honey chilli potato	6	nutkeginorrogvuzgzu	0.000545371

|Table 4.2 showing decryption time

TABLE 4.2

DECRYPTION TIME

Cipher Ceasar Decryption				
S. No.	Cipher Text	Key	PlainText	cipher ceaser
1	wjifhttpnjx	5	redacookies	0.00039315
2	qtcpig	2	orange	0.000334553
3	wpulhwwsl	7	pineapple	0.000409832
4	qerks	4	mango	0.000447336
5	jyyun	9	apple	0.000465054
6	xiabi	8	pasta	0.000337282
7	zklwhdvdxfhdsdvwd	3	whiteasauceapasta	0.000517255
8	nutkeginorrogvuzgzu	6	honeyachilliapotato	0.000568424

Modified Vigenere Cipher Caesar

Table 4.2 showing modified encryption Time

TABLE 4.2

MODIFIED ENCRYPTION TIME

Modified Cipher Ceaser Encryption				
S. No.	PlainText	Key	Cipher Text	Modified cipher ceaser
1	red cookies	game	WBKX&DN&NBZ	0.000739354
2	orange	fruit	SEPOQZ	0.000622084
3	pineapple	spikes	FUQHWWULL	0.000793666
4	mango	yellow	IBTKT	0.000614525
5	apple	circle	BUAGG	0.000888754
6	pasta	saucy	FYGOP	0.000696273
7	white sauce pasta	white	QLLE&KMULDV&OIJ&G	0.000766341
8	honey chilli potato	sweet	YGMBHGLXLAYXVIUWVUN	0.000787856

Table 4.2 showing modified decryption Time

TABLE 4.2

MODIFIED DECRYPTION TIME

Decryption				
S. No.	Cipher Text	Key	PlainText	Modified cipher ceaser
1	WBKX&DN&NBZ	game	RED COOKIES	0.000410718
2	SEPOQZ	fruit	ORANGE	0.000392413
3	FUQHWWULL	spikes	PINEAPPLE	0.000526309
4	IBTKT	yellow	MANGO	0.000422878
5	BUAGG	circle	APPLE	0.000545976
6	FYGOP	saucy	PASTA	0.00054923
7	QLLE&KMULDV&OIJ&G	white	WHITE SAUCE PASTA	0.000442938
8	YGMBHGLXLAYXVIUWVUN	sweet	HONEY CHILLI POTATO	0.000772577

Comparison Graph

a. Encryption

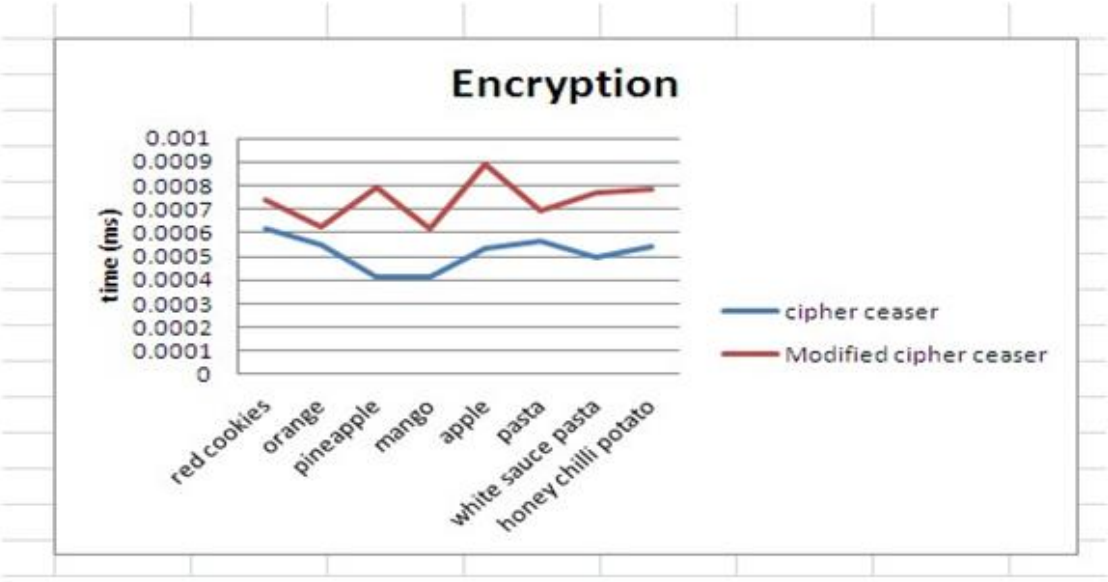

Fig. 4.3 Comparison Graph of Encryption

b. Decryption

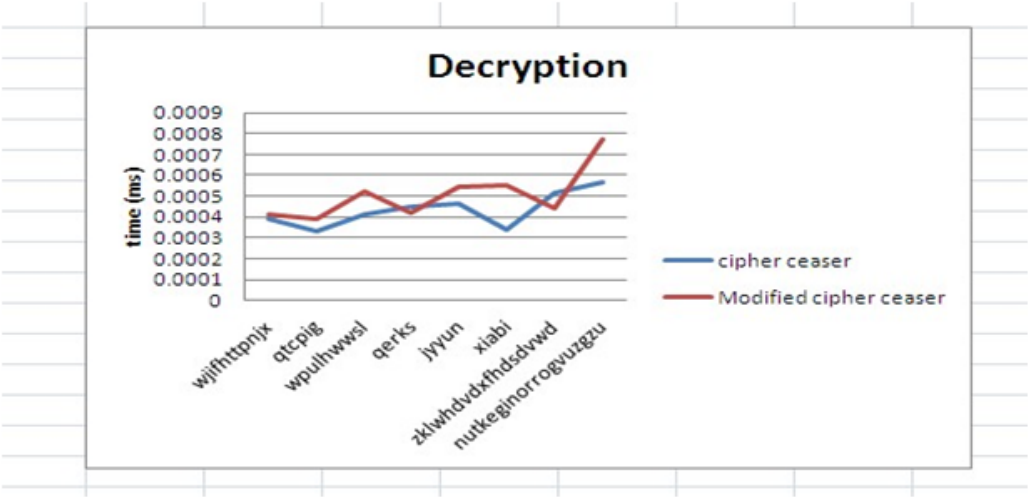

Fig. 4.3 Comparison Graph of Decryption

CONCLUSION

This thesis primarily examines the design and analysis of synchronous stream ciphers, a significant subclass of symmetric key cryptography. Because of their advantages over other encryption techniques in terms of efficiency and speed, symmetric key algorithms are still widely used. Despite the fact that the stream competition has garnered the attention of the research community in recent years, stream ciphers still lack a standard. This thesis has attempted to identify the situations in which stream ciphers, particularly synchronous stream ciphers (which are frequently employed because of their security properties), can be helpful even when a regular block cipher that can also be utilized as a stream cipher is present.

FUTURE SCOPE

The most common type of encrypted data is cryptography. The Vigenere encryption is regarded as the weakest because of its several drawbacks. We have suggested an improved Vigenere cipher that is substantially more secure against Kasiski and Friedman is in order to get over the cipher's limitations. Frequency analysis, analysis, pattern prediction, and brute force assault on the suggested encryption with many tables made it extremely challenging.

REFERENCES

[1]. Stjepan Picek, Annelie Heuser, and Sylvain Guilley “Template attack vs bayes classifier.Technical”, report, Cryptology ePrint Archive, Report 2017/531, 2017.
[2]. Sengupta N, Holmes J, “Designing of cryptography based security system for cloud computing”, International conference on cloud and ubiquitous computing and emerging technologies (CUBE), IEEE-2017.
[3]. Al-Ahwal, A. and Farid, S., “The effect of varying key length on a Vigenère cipher”, IOSR J. Comput. Eng., 17, 2, pp. 2278–661, 2017.
[4]. T. Gunasundari and K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science and Mobile Applications, ISSN, pp. 2321-8363, 2014.
[5]. S. Garg, S. Khera, and A. Aggarwal, “Extended Vigenere cipher with stream cipher. Int. J. Eng. Sci. Comput., 6, 5, 5176–5180 in 2016.
[6]. R. Martin Albrecht and Gregor Leander,”An all-in-one approach to differential cryptanalysis for small block ciphers”, In International Conference on Selected Areas in Cryptography, pages 1–15. Springer, 2012.
[7]. P. Wang, et al., "Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code", Optics Communications, vol. 332, pp. 36-41, 2014.
[8]. S. Burman, et al., "LFSR based stream ciphers are vulnerable to power attacks”, in Progress in Cryptology INDOCRYPT 2007, ed: springer, pp. 384-392 in 2017.

[9]. StjepanPicek, Ioannis PetrosSamiotis, Jaehun Kim, Annelie Heuser, Shivam Bhasin, and Axel Legay, “On the performance of convolution neural networks for side-channel analysis”, In International Conference on Security, Privacy, and Applied Cryptography Engineering, pages 157–176. Springer, 2018.
[10]. Massoud Sokouti, L.M.K., B. Sokout, and S.Pashazadeh, “FPGA implementation of improved version of the Vigenere cipher. Indian J. Sci. Technol., 3, 4, 459–462 in 2018.
[11]. O. Omolara, et al., "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication", Computer Engineering and Intelligent Systems, vol. 5, pp. 34-46, 2014.
[12]. F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipher by Stream
[13]. Cipher", International Journal of Computer Applications, vol. 100, pp. 1-4, 2014. [13] http://searchsecurity.techtarget.com/definition/cipher.pdf
[14]. http://searchsecurity.techtarget.com/definition/cryptanalysis.pdf
[15]. W.Stallings, “Cryptography and Network Security 4/E., Pearson Education India in 2014. [16] G. Singh Supriya “Modified vigenere encryption algorithm and its hybrid implementation
[16]. with Base64 and AES”, In 6th International conference on advanced computing, networking and security (ADCONS). IEEE in 2017.
[17]. K.Senthil, K. Prasanthi, and R. Rajaram. "A modernavatar of Julius Caesar and Vigenerecipher."Computational Intelligence and Computing Research (ICCIC), IEEE International Conference on.IEEE, 2013.
[18]. P. I. Wilson and M. Garcia, "A Modified Version of the Vigenère Algorithm", IJCSNS, vol. 6, p. 140, 2016.
[19]. Q.-A. Kester, "A cryptosystem based on Vigenère cipher with varying key", International Journal of Plain Text R Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, pp. pp: 108-113, 2018.
[20]. Ajit Singh, Aarti Nandal, and Swati Malik,"Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security",International Journal of Advanced Research in Computer Science and Software Engineering in 2012.
[21]. Gerhana, Y. A., Insanudin, E., Syarifudin, U., and Zulmi, M. R. “Design of digital image application using vigenere cipher algorithm”, 4th Int. Conf. Cyber IT Serv.Manag. CITSM 1–5, 2016.
[22]. C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols”, Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278-0661, 2012.
[23]. Quist-Aphetsi Kester,”A Hybrid Cryptosystem Based On Vigenere Cipher and Columnar Transposition Cipher”, International Journal of Advanced Technology and Engineering Research (IJATER) Vol. 3 Issue 1 pp141-147. July 2013.
[24]. M. Khalid, N. Wadhwa, and V. Malhotra, “Alpha-qwerty cipher,” International Journal of Advanced Computing, vol. 3, no 3, pp 107-118, May 2012.
[25]. Q. A. Kester, “A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher”, International Journal of Advanced Technology and Engineering Research, vol. 3, no. 1, pp. 141-147, Jan. 2017.
[26]. Q. A. Kester, “A cryptosystem based on Vigenère cipher with varying key,” International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, no. 10, pp. 108-113, Dec. 2016.
[27]. Kashish Goyal and Supriya Kinger,"Modified CaesarCipher for Better Security Enhancement",International Journal of Computer Applications (0975��8887) Volume2013.
[28]. C. Bhardwaj 2012, Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols. Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 4, Issue 2 (Sep.-Oct. 2016), PP 35-38 Available at: www.iosrjournals.org
[29]. A. Razzaq, et al., "Strong Key Machanism Generated by LFSR based Vigenère Cipher", presented at the 13 International Arab Conferences on Information Technology, 2013.