iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56920

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

A Survey: Cryptography Techniques for Communication System

Prof. Ms. S.P.Vanjari[1], Vaishnavi Bhangale[2], Deepti Singh[3], Nitin Andhale[4], Amruta Dalavi[5]
Department of Information Technology Smt. Kashibai Navale college of Engineering, Vadgaon (SPPU- Pune)

Abstract: ***Sensitive data is being used more and more in online communication these days. Therefore, internet consumers' top concern is data security. The best course of action is to utilize a cryptography technique that encrypts data, translates it over the internet, and then decrypts it back to the original data. The process of securely transmitting data is the focus of the field of cryptography. The intention is to prevent eavesdroppers from comprehending a message while enabling the intended recipients to receive it correctly. A collection of methods known as cryptography are used to jumble or hide data so that only a person skilled in data restoration may access it in its original format. Cryptography offers modern computer systems a robust and cost-effective foundation for maintaining data secrecy and confirming data indignity. While our traditional cryptography techniques, like RSA signature and AES encryption, function well on computers with respectable amounts of RAM and computing capacity, they are not well suited to the realm of embedded systems and sensor networks. As a result, techniques for lightweight cryptography are put forth to address numerous issues with traditional cryptography. This work develops a new hybrid method of plaintext encryption with the goal of adding to the body of knowledge in the field of classical cryptography. For an additional degree of protection, the cryptosystem employs three distinct numerical and alphabetical keys in cipher. Super Cipher is the name given for the new proposed cipher.***

Keywords: cryptography, encryption, keys, algorithm, cipher

I. INTRODUCTION

Information security involves a set of measures, procedures, and strategies designed to prevent and monitor unauthorized access, troubleshooting, disclosure, disruption, and modification of computer network resources. Strengthening the privacy, integrity, and reliability of data requires continuous efforts to enhance existing methods against persistent attempts to compromise them and to develop new, resilient approaches that can withstand various types of attacks. Historically, encryption has proven to be one of the most reliable strategies for securing information. This method dates back to ancient times, such as the Romans, who employed similar techniques to safeguard their valuable information and documents. Cryptography is the practice of devising codes, whether written or generated, to maintain the confidentiality of information. It involves transforming data into an unreadable format for unauthorized users, enabling secure transmission without the risk of unauthorized decoding and compromise of the data. Information security relies on cryptography at various levels, ensuring that information remains unreadable without the appropriate decryption key. Cryptography is the practice of safeguarding information and communication by employing codes, ensuring that only intended recipients can comprehend and process the data. This process serves to thwart unauthorized access to sensitive information. The term "crypt" in cryptography signifies "hidden," while the suffix "graphy" refers to "writing."

A. Components of a Cryptosystem

``Cryptosystems are built upon several essential components:

1) *Plaintext:* Original, unencrypted data that needs to be securely transmitted or stored. It can be a file, a message, or any kind of data.
2) *Encryption Algorithm:* This is the algorithm turning plaintext into ciphertext. RSA, DES (Data Encryption Standard), and AES (Advanced Encryption Standard) are few examples of common encryption algorithms being used
3) *Key*: The key serves as the secret parameter for encryption and decryption. Thus, establishing the method that is used for encryption and decryption. This section discusses the distinctions between public and private keys in asymmetric and symmetric cryptography.

a) *Public Key:* It is used for encryption in asymmetric cryptography and openly shared.
b) *Private Key:* It is kept confidential and used for decoding in asymmetric cryptography or for both encryption and decryption in symmetric cryptography.

4) *Ciphertext*: Ciphertext represents the encrypted form of plaintext, appearing as seemingly random data and requiring the decryption key for comprehension.
5) *Decryption Algorithm:* Mathematical procedure that reverses the encryption, turning ciphertext back into plaintext. The decryption key is used in the algorithm
6) *Key Management:* This section explores the critical aspects of key management, including creation, distribution, storage, and rotation. A robust key management system is imperative for ensuring the overall security of the cryptosystem.

B. Purpose

In today's digital environment, cyberattacks happen often. Attacks are more likely to occur on any social networking site, web application, etc. Studying and analyzing attacks is typically crucial in order to create a system that is resistant to attacks and solves big problems. Here are a few examples of attacks.

C. Cryptographic Attacks

An attacker's primary goal is to crack a cryptosystem and extract the plaintext from the ciphertext. Since the technique is now public knowledge, the attacker just needs to discover the secret decryption key to retrieve the plaintext. He therefore puts in his best effort to discover the cryptosystem's secret key. The attacked system is regarded as broken or compromised once the attacker is able to determine the key. The following categories apply to attacks on cryptosystems based on the methods used:

1) *Ciphertext Only Attacks (COA):* Ciphertext Only Attacks involve an attacker having access to a set of ciphertexts without corresponding plaintext. Success in COA is defined by the attacker determining the corresponding plaintext or, in some cases, deducing the encryption key. It is noteworthy that contemporary cryptosystems are designed with safeguards to mitigate the risks associated with ciphertext-only attacks.
2) *Known Plaintext Attack (KPA):* With this technique, certain portions of the ciphertext are known to the attacker as plaintext. Using this knowledge, the challenge is to decrypt the remaining ciphertext. This could be accomplished via finding the key or in another way. Block ciphers are most effectively attacked via linear cryptanalysis.
3) *Chosen Plaintext Attack (CPA):* The attacker uses this method with an encrypted version of the text of his choice. He can therefore choose the pair of ciphertext and plaintext. This makes it easier for him to figure out the encryption key. Differential cryptanalysis used against hash functions and block ciphers is an example of this type of attack. RSA, a well-known public key cryptosystem, is susceptible to chosen-plaintext assaults.
4) *Dictionary Attack:* There are numerous variations of this approach, all of which entail creating a "dictionary." The most basic form of this attack involves the attacker compiling a dictionary of all the plaintexts and ciphertexts that he has learned over time. When an attacker receives the ciphertext in the future, he consults the dictionary to determine the matching plaintext. Attack by Brute Force (BFA) − With this technique, the attacker tries every key that could be used in order to figure out the key. Two eight = 256 keys are possible if the key has eight bits. Knowing the algorithm and the ciphertext, the attacker tries to decrypt using each of the 256 keys one at a time. If the key is long, the attack would take a very long time to finish.
5) *Man in Middle Attack (MIM):* The majority of public key cryptosystems, which need key exchange prior to communication, are the targets of this attack. o Host A asks host B's public key in order to connect with them. o The request is intercepted by an attacker, who then sends his public key in its place. o As such, the attacker can read whatever that host A sends to host B. o After reading the data with his public key, the attacker re-encrypts it and sends it to B in order to keep up communication. o To make it appear as though B is taking it from A, the attacker sends his public key as A's public key.
6) *Side Channel Attack (SCA):* This kind of attack doesn't target any specific kind of algorithm or cryptosystem. Rather, its purpose is to take advantage of a flaw in the cryptosystem's physical implementation.
7) *Timing Attacks:* They take advantage of the fact that different processor calculations compute at varying speeds. It is possible to determine the specific computation the processor is performing by measuring these timings. An elongated encryption time, for instance, suggests that the secret key is lengthy.
8) *Power Analysis Attacks:* With the exception of using power usage to determine the type of underlying computations, these attacks are comparable to timing attacks.
9) *Fault analysis Attacks:* These attacks introduce mistakes into the cryptosystem, and the attacker looks for valuable information in the output that results

II. RELATED WORK

A literature survey consists of different learning techniques research data as follows:

1) Anuja proposed a fashion in which security is crucial with text as the main concern. This paper provides security in textbook field only but rearmost exploration said that there's an attack possible in crucial fields also. To avoid this attack a secure approach is important in crucial field also. To avoid this problem a new approach is used i.e. One Time Pad cipher. In proposed cipher, the key is secured by a one time pad cipher. In the encryption part, communication is translated by using One Time Pad Cipher, in which an arbitrary key is generated, this key is XOR with the communication and the crucial length is equal to the communication length. After communication is translated by first key, transposition cipher is applied under certain order also adds some logical bits, now use alternate key by One Time Pad Cipher for encryption and again apply transposition cipher, which gives further secure cipher textbook and vice-versa process applied in decryption part.
2) Quist-Aphetsi Kester proposed a method that employs Vigenere square and key in its encryption process but the successive keys used will be dependent on the initial key value during the encryption process. That is the key varies as it is used in the encryption process. The first step key will be different from the second step key but the second step key will be as a result of a function that operated on the first step and so forth. The algorithm ultimately makes it possible for encryption and decryption of the text and also makes the Vigenere cryptosystem more difficult against frequency attack. This is as a result of varying keys employed for each encryption process. A software program was written to demonstrate the effectiveness of the algorithm using java programming language and cryptanalysis performed on the ciphertext.
3) A technique was presented by O.E. Omolara that employs the Caesar and Vigenere ciphers for both encryption and decryption, but with some modifications to the original cipher. A random integer key and a lettered key are both generated. On the lettered key, a Caesar Cipher was performed using the shift value of the numbered key. The plain text that has to be encrypted is presently being processed using the Vigenere cypher, and the key created during the first Caesar cypher operation is being replaced with the new key. The key was changed to prevent a simple frequency analysis, particularly in short texts. The procedure culminates in the conversion of the result to its Binary value in the ASCII Table after the binary of the first letter of the generated cypher text is XORed with the binary of the numbered key, the result is then encrypted with the next cypher text, and so on. The final result of the ciphertext is a cipher text that is composed of letters, numbers, and symbols.
4) Saloni Garg suggested combining the stream cipher with vigenere cipher to boost security. She also suggested adding all lowercase, numeric, and special symbols to the cipher to expand its flexibility and enable encryption of any type of data rather than only uppercase letters. Bit by bit encryption, or adding a bit from plaintext to a bit in the keystream, is how stream ciphers work
5) Aized suggested assigning a distinct numerical value to each alphabet in each table.The plaintext is defined by the Vigenere technique as a string of alphabets with no spaces between them. By placing spaces between the words and forcing the recipient to guess where to position the spaces in the ciphertext, it can make it difficult for them to understand the message.The suggested method solves this issue by adding numerous numerical numbers for the table's space.
6) Senthil et al. used rigorous mathematical techniques that make use of a prime factor, its primitive roots, and their generator to provide some novel enhancements to the vigenere and Caesar cipher approach. Both cipher systems involve non-uniform shifts and substitutions that adhere to a specific scientific procedure.
7) Chhavi Gupta demonstrated a method where the sender has two keys, Key1 and Key2, along with a plaintext message. While Key2's value might vary from 0 to 93, Key1's size is the same as that of plaintext.Understanding the complete process requires going over each step of the plan one by one.

TABLE I. SUMMARY OF RELATED WORK / GAP ANALYSIS\

Title	Author	Year/Journal name	Summary
An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher	Deepanshu Gautam, Dr. Munish Mehta	IEEE-2018	This paper combines the Vigenere cypher with the stream cypher. It encrypt any data and is not limited to upper case characters.
Design of Hybrid	Shivam	IEEE-2020	In this paper, two ciphers are

Cryptography System based onVigenere Cipher and Polybius Cipher	Vatshayan, Raza Abbas Haidri		combined to provide secure communication and that security algorithm can be combined with different applications
An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication	Srikanta Patnaik	ScienceDirect-2019	In this paper, secure communication is established using a combination of Vigenere and caesar cipher. There is only one key for the encryption and decryption techniques
A Study On Cryptographic Techniques	Anjali Krishna, Dr. L. C. Manikandan	IJSRCSEIT-2020	In this paper, we came to know about all the ciphers and comparison between them and we can select which cipher we need to use
"ASCII conversion based two key V4S scheme for encryption and decryption—A four step approach."	Gupta, Chhavi, and Prateek Thakral.	IEEE-2017	In this paper, we explored different techniques where various encryption and decryption algorithms were used for ASCII conversion based on two keys.

III. OBSERVATIONS AND FINDING

As per the observation of the research topic finding of following things,

A. Methodology

Specific problems addressed in this project includes:

I. Sophisticated Cyber Threats: Cyber threats, ranging from sophisticated malware to targeted attacks, have outpaced traditional security measures. The project aims to develop cryptographic techniques capable of thwarting advanced threats, ensuring the confidentiality of sensitive information.

II. Data Tampering and Manipulation: The integrity of transmitted data is crucial for maintaining the trustworthiness of communication systems. The project addresses the problem of preventing unauthorized tampering or manipulation of data during transit.

III. Quantum Computing Vulnerabilities: As quantum computing capabilities progress, the cryptographic algorithms currently in use may become susceptible. The project recognizes the need to explore and implement post-quantum cryptographic techniques to future-proof communication systems.

IV. Key Exchange Security: Secure key exchange is fundamental to cryptographic protocols, especially in asymmetric key systems.

V. The project focuses on addressing the 11 challenge of securely establishing and managing cryptographic keys to prevent unauthorized access and decryption.

VI. Regulatory Compliance and User Trust: With the increasing stringency of data protection regulations, organizations must adhere to compliance standards. The project acknowledges the need to implement cryptographic measures that not only meet regulatory requirements but also maintain and enhance user trust in communication systems.

The strategy utilizes a combination of Caesar cipher, Rail- fence Cipher and Vigenere cipher in its encryption process. The ciphertext will originally be worked on exercising Caesar cipher. Further it's reused with the posterior ciphertext also turns into a key for the Rail- fence Cipher process and also on the Vigenere Cipher at the end. The key is used to work on the communication which is the plaintext to produce the last ciphertext. This process will wind up making the last ciphertext precipitously hard to be broken exercising being cryptanalysis processes.

Decryption will be done by the receiver in rear order for reclamation of a communication from the sender. A product program will be composed to parade the viability of the computation exercising python coding and different cryptanalysis fashion will be performed on the ciphertext.

I. Caesar cipher: It's a type of substitution cipher that was used by Julius Caesar to protect sensitive information. The basic idea behind the Caesar cipher is to shift the letters of the alphabet by a fixed number of positions.

Encryption $En(x) = (x + n) \bmod 26$

Decryption $Dn(x) = (x – n) \bmod 26$

II. Vigenere cipher: The Vigenere Cipher is a method for encrypting alphabetic text, employing a basic form of polyalphabetic substitution. Encryption involves utilizing the Vigenère square or table, comprising 26 rows of alphabets. Each row represents the alphabet shifted cyclically to the left compared to the previous one, corresponding to the 26 possible Caesar Ciphers. In the encryption process, the cipher employs distinct alphabets from various rows, determined by a repeating keyword.

III. Rail- fence Cipher: The rail fence cipher, also referred to as the zigzag cipher, is a straightforward and historical transposition cipher utilized in both encryption and decryption of messages. The term "rail fence" is derived from the zigzag pattern in which the letters are written, resembling the rails of a fence. Following the completion of writing each alphabet, the rows are combined to generate the cipher-text.

Comparison

1) Key Mechanism

a) Caesar Cipher: Uses a single numeric key to shift letters in the alphabet.

b) Vigenère Cipher: It uses a keyword that determines the shift value for each letter.

c) Rail-Fence Cipher: Uses the number of rails as the key to determine the pattern of writing.

2) Security:

a) Caesar Cipher: Relatively insecure due to its limited key space (only 25 possible keys).

b) Vigenère Cipher: More secure than Caesar cipher but vulnerable to frequency analysis if the keyword is short or easily guessable.

c) Rail-Fence Cipher: Generally considered less secure, especially for small numbers of rails, and can be susceptible to pattern recognition.

3) Flexibility:

a) Caesar Cipher: Simple and easy to implement but lacks flexibility in terms of key variations.

b) Vigenère Cipher: More flexible than Caesar cipher due to the variable-length keyword, making it resistant to simple frequency analysis.

c) Rail-Fence Cipher: Limited flexibility; the security depends on the number of rails, which is a fixed parameter.

4) Algorithm Complexity:

a) Caesar Cipher: Simplest, involving only a single shift operation.

b) Vigenère Cipher: More complex due to the use of a variable-length key and the need to iterate through the key for encryption.

c) Rail-Fence Cipher: Simple, involving rearranging characters in a pattern determined by the number of rails.

5) Use Cases:

a) Caesar Cipher: Suitable for educational purposes or situations where low-security requirements are acceptable.

b) Vigenère Cipher: Historically used for more secure communication, especially when a strong, non-repeating keyword is employed.

c) Rail-Fence Cipher: Often used for simple, fun applications rather than serious cryptographic needs.

6) Cryptanalysis:

a) Caesar Cipher: Vulnerable to brute-force attacks due to the limited key space.

b) Vigenère Cipher: Resistant to simple frequency analysis but can be broken with more advanced methods like Kasiski examination.

c) Rail-Fence Cipher: Vulnerable to attacks like frequency analysis, especially for a small number of rails.

B. Key issues and challenges

1) *Bandwidth Limitations:* Communication channels have a limited capacity, which might lead to dropped signals, slower data transfer rates, or delays.
2) *Security Concerns:* Information confidentiality, integrity, and authenticity can be difficult to ensure. Unauthorized access, data tampering, and eavesdropping are among the threats.
3) *Privacy Concerns:* It can be difficult to strike a balance between the necessity of communication and the preservation of personal privacy, particularly in the age of digital communication.
4) *Ethical Issues:* Ensuring ethical communication practices, avoiding misinformation, and addressing issues of bias and manipulation are critical considerations.
5) *Accessibility:* Ensuring that communication systems are accessible to all, including individuals with disabilities, is an important aspect of inclusive communication.
6) *Dynamic Nature of Communication:* Communication is dynamic and constantly evolving. Adapting to changes in communication patterns and technologies requires flexibility and proactive measures.
7) *Regulatory Compliance:* Adhering to legal and regulatory requirements, such as data protection laws and communication standards, can be complex and demanding.
8) *Reliability and Redundancy:* Ensuring the reliability of communication systems is crucial. Redundancy measures are needed to address failures or disruptions, such as backup systems and alternative communication channels.
9) *Noise and Interference:*

a) Physical Noise: Disturbances that affect the transmission of the message, such as background sounds, poor signal quality, or interference.
b) Semantic Noise: Differences in interpretation of symbols, language, or meaning that can lead to misunderstandings.

10) *Technological Advancements*

Rapid advancements in communication technologies require constant adaptation. Keeping up with the latest technologies and ensuring compatibility can be challenging.

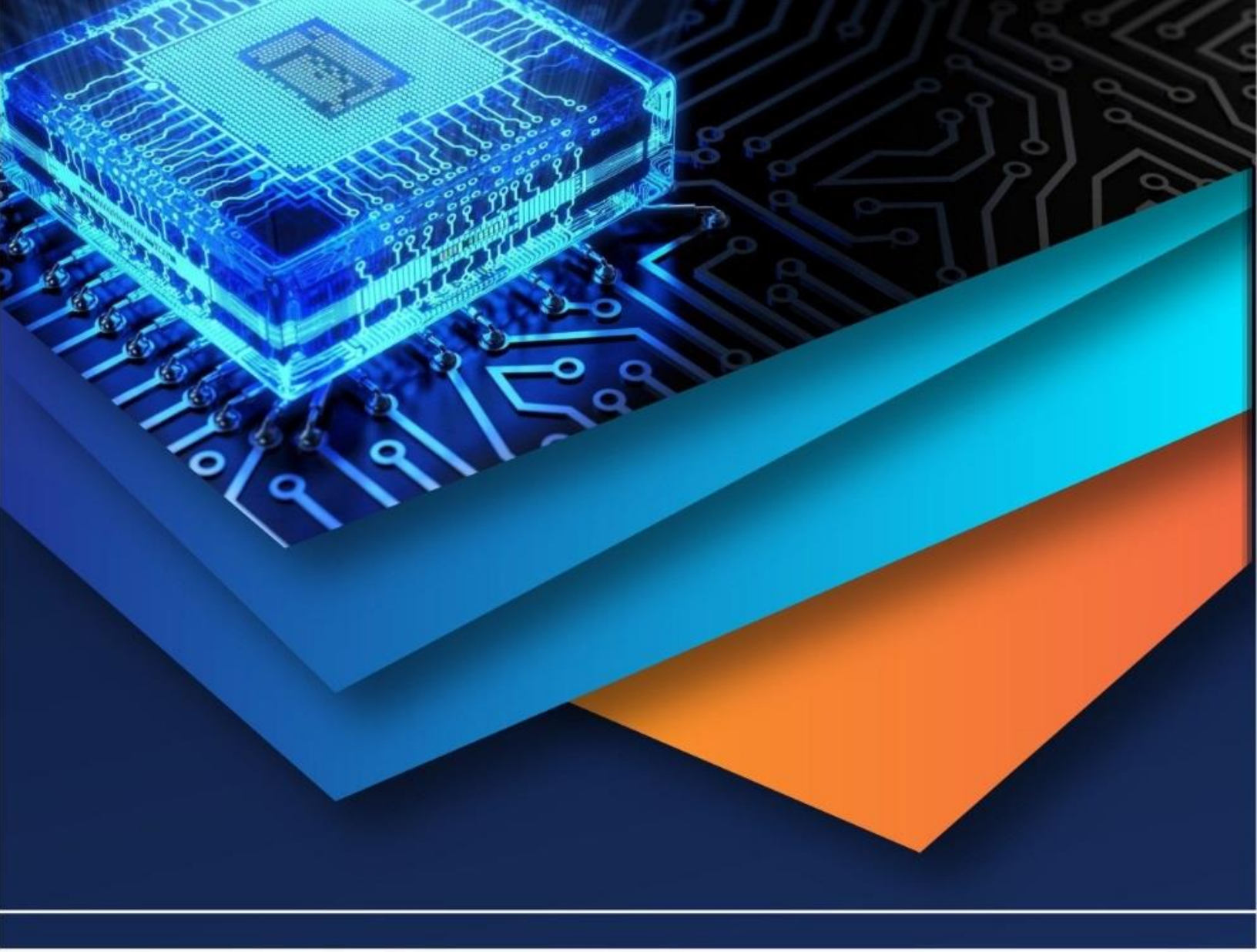
IV. CONCLUSION AND FUTURE WORK

The method most frequently used to secure data is cryptography. To sum up, super ciphers—a method of combining many cryptographic algorithms—provide a practical way to improve encryption system security. Super ciphers enable strong encryption, safe key exchange, integrity verification, and resistance against a variety of assaults by combining the advantages of several cyphers and methodologies. Super ciphers can greatly improve data confidentiality and integrity when used in distributed networks, file transfer protocols, and secure messaging systems. To obtain a high level of security in super ciphers, it is imperative to make sure that each component is carefully designed, implemented, and analyzed. approaches in cryptography that are thought to be the least complicated and most susceptible due to various obstacles. In order to overcome the limitations of the standard cipher, we suggested an improved version that uses three separate keys and is much more resistant to attacks by Kasiski and Friedman. Because many tables are used for encryption, cryptanalysis, frequency analysis, pattern recognition, and brute attack on the suggested technique are likewise considerably more challenging. The algorithm that creates the updated hybrid cyphers with additional keys now has a high percentage of Diffusion and Confusion, making them extremely strong and challenging to crack. Despite the abundance of cryptographic techniques available, this field still needs careful consideration from the academic community in order to increase data security. In the future our point is to give approval of the proposed approach by performing security and performance analysis.

REFERENCES

[1] Anuja Priyam.” Extended Vigenère using double Transposition Cipher with One Time Pad Cipher.” Intl J Engg Sci Adv Research 2015 June; 1(2):62-65.
[2] Quist-Aphetsi Kester, “A cryptosystem based on Vigenère cipher with varying key.” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012.
[3] O.E. Omolara. “Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication.” Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.5, 2014.
[4] Garg, Saloni, Sonam Khera, Archana Aggarwal, and P. G. Scholar. "Extended Vigenere Cipher with Stream Cipher." International Journal of Engineering Science and Computing (IJESC) 6, no. 5 (2016).
[5] Aized Amin Soofi, Irfan Riaz, and Umair Rasheed. "An Enhanced Vigenere Cipher for Data Security." International Journal of Scientific & Technology Research 5, no. 03 (2016).
[6] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-3. IEEE, 2013.

[7] Sanjeev Kumar Mandal, "A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme." (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (4) 2016, 2096- 2099.
[8] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.
[9] F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.
[10] A. P. U. Siahaan, "Protection of important data and information using gronsfeld cipher," 2018.
[11] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigenere cipher and goldbach codes algorithm," Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.
[12] M. Maity, "A modified version of polybius cipher using magic square and western music notes," International Journal For Technological Research In Engineering, ISSN, pp. 2347–4718, 2014.
[13] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Peformance Analysis of Data Encryption Algorithms", IEEE Delhi Technological University India, 2011.
[14] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-3. IEEE, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY