IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SURVEY PAPER ON CREATING A SECURE COMMUNICATION SYSTEM USING HYBRID CRYPTOGRAPHIC TECHNIQUES

[1]Atharva Tarate, [2]Sakshi Jadhav, [3]Shreyas Jadhav, [4]Anuj Vidhate, [5]Priti Yadav
[1-4]Student, [5]Guide
[1]Department of Information Technology
[1]Sinhgad Institute of Technology & Science, Pune, Maharashtra, India

***Abstract:*** In today's digital landscape, the surge in cyber-attacks poses a growing concern, particularly for the younger demographic. Safeguarding data has become imperative, leading to the widespread use of encryption—a practice rooted in history to prevent unauthorized access to handwritten communications. The secure transmission of messages from sender to receiver is a pressing challenge for global internet users due to the prevalence of attacks, threats, and, notably, data privacy breaches. Cryptographic techniques offer a robust solution to these challenges. This report delves into the evaluation of various cryptographic methods aimed at fortifying internet communication. In the field of cryptography, the conversion of plaintext data into ciphertext, its transmission over the internet, and subsequent decryption to reveal the original information form the essence of securing data. The primary objective of this paper is to assess the efficacy of diverse cryptographic methods in this context. To achieve optimal security for data, the paper advocates for the application of hybrid cryptography—a cryptographic paradigm that blends the strengths of both symmetric and asymmetric encryption. This synthesis aims to provide a secure and efficient method for data protection, addressing the inherent challenges associated with purely symmetric or asymmetric encryption techniques. The proposed hybrid cryptography algorithm leverages the Vigenere and Polybius Ciphers, contributing to the attainment of confidentiality, authentication, and comprehensive data protection.

***Keywords*** - Encryption, Decryption, Cryptography, Cipher, Ciphertext, Plaintext, Polybius Cipher, Vigenere Cipher.

## I. INTRODUCTION

In today's digital era, the increasing utilization of sensitive information during online conversations has heightened concerns about data security among Internet users. Employing cryptographic techniques to encrypt data, transmit it over the Internet, and subsequently decode it to reveal the original information is recognized as a crucial approach. The focal point of cryptography lies in ensuring secure information transmission, aiming to thwart eavesdroppers from comprehending messages while enabling intended recipients to receive them accurately. Cryptography employs various techniques to encode or mask data, restricting access to those capable of reverting the data to its original state. In contemporary computer systems, cryptography stands as a reliable and cost-effective foundation for safeguarding data privacy and confirming data integrity.

While standard encryption techniques such as AES (encryption) and RSA (signing) perform admirably on computers with sufficient memory and processing capacity, they face scalability challenges in embedded devices and sensor networks. To address these issues, lightweight cryptography techniques have emerged as viable solutions. Consequently, this paper proposes solutions for lightweight cryptography to overcome the limitations associated with traditional encryption methods. To contribute to the broader understanding

of classical cryptography, this report introduces a novel hybrid plaintext encryption method. This method involves encrypting the plaintext with the Vigenère cipher and subsequently using the ciphertext to re-encrypt the plaintext with the Polybius cipher.

The following section delves into a comprehensive literature review, providing an in-depth analysis of existing research and advancements in the field of hybrid cryptography. It explores the evolution of cryptographic techniques, highlighting key methodologies and their applications in securing communication systems.

## II. Literature Review

The author introduces a novel approach to achieving secure communication by combining two classical ciphers, addressing data privacy and security concerns for internet users. The paper [1] categorizes cryptography into symmetric key cryptography, explaining the Vigenère cipher—a polyalphabetic substitution cipher—and the Polybius cipher, which converts letters into numbers using a square table. The hybrid cryptographic system presented combines these ciphers, enhancing both security and complexity.

The discussion encompasses various cryptographic techniques and their limitations, emphasizing the role of cryptography in securing data and information exchange. Another paper [2] categorizes cryptographic techniques into symmetric and asymmetric cryptography, briefly covering symmetric techniques like the Caesar Cipher, Playfair, Monoalphabetic, Polyalphabetic, and the Deffie Hellman Key Exchange. These techniques, while having strengths, exhibit vulnerabilities susceptible to various attacks. The conclusion emphasizes the significance of cryptography in ensuring data security and integrity.

The author explores the significance of secure communication in remote access scenarios, especially in server-client architectures and peer-to-peer devices, highlighting potential risks associated with insecure transmission in paper [3]. The proposed hybrid security model combines cryptographic algorithms, including Diffie-Hellman Key Exchange, RSA, private key encryption, and SHA-1, addressing issues of confidentiality, authentication, and integrity simultaneously. Overall, the paper [3] provides a comprehensive overview of the need for secure communication in various network architectures.

The author explores the significance of enhancing the traditional Vigenere cipher, overcoming vulnerabilities associated with attacks like Kasiski and Friedman in the paper [4]. The enhanced Vigenere cipher utilizes multiple tables, making cryptanalysis, frequency analysis, pattern prediction, and brute force attacks significantly more challenging. The paper also references related work in the field, highlighting modifications to the Vigenere cipher.

The Author introduces a novel approach to cryptography by combining two well-known ciphers, Vigenere and Polybius, to create a hybrid encryption system. In today's interconnected world, ensuring data security is of paramount importance, and the paper emphasizes the significance of cryptography in achieving this. This paper [5] highlights the historical context of cryptography, referencing classical ciphers like the Caesar Cipher and Vigenere Cipher, and it points out their limitations, especially in the face of modern security threats. The authors propose a hybrid solution that capitalizes on the strengths of both ciphers, enhancing data security by introducing a higher level of complexity and making it more resistant to various forms of attacks, such as Kasiski and Friedman attacks. This innovative approach to encryption reflects the ongoing need for improved data privacy and security in the digital age.

Finally, a paper [6] discusses the importance of securing data during transmission over networks and introduces the concept of hybrid cryptography, combining RSA and AES. The overview of previous research related to knowledge sharing and intranets sets the context for the research, emphasizing the significance of encryption algorithms, specifically RSA and AES, in ensuring data security. The proposed hybrid cryptography system combines the strengths of RSA for security and AES for speed, ensuring secure and efficient data transmission.

The upcoming section delves into the methodologies employed in this study, outlining the systematic approach used to develop and evaluate the proposed hybrid cryptographic system.

## III. METHOLOGY

In the realm of secure communication, a hybrid approach leveraging both the Vigenère cipher and the Polybius Square Cipher has proven to be a robust strategy. This method introduces an additional layer of complexity, enhancing resistance against various cryptanalysis techniques.

In the encryption process, the Vigenère cipher is employed initially. A randomly chosen key initiates the transformation of the plaintext into ciphertext. This ciphertext then serves as the key for the subsequent Polybius Square Cipher process. The final ciphertext, generated through these sequential steps, presents a formidable challenge for potential attackers employing cryptanalysis techniques.

For decryption, the recipient reverses the process, unraveling the message from the sender. To demonstrate the efficacy of this hybrid cryptographic approach, a Python program is developed, showcasing its practical implementation. Various cryptanalysis methods are subsequently applied to the ciphertext to evaluate its resilience.

Encryption Procedure:

Phase 1 (Vigenère Cipher):

1. Original Message: AMERICA VIRUS

2. Key: DELHI

3. Encrypted Output: DQPYQFEYCQUYD

Phase 2 (Polybius Cipher):

4. Text: DQPYQFEYCQUYD

5. Final Encrypted Output:411453451412514531145445 41

The resulting ciphertext is presented in a numerical format, offering an added level of security compared to the original alphabetical format. Even the output from the Vigenère cipher appears as a distributed, jumbled sequence of alphabets, further securing the message.

Decryption Procedure:

Phase 1 (Polybius Cipher):

1. Ciphered Message: 41

2. Decrypted Output: D

Phase 2 (Vigenère Cipher):

3. Text: D

4. Key: DELHI

5. Original Message: A

Decoding involves reversing the process through the Polybius Cipher and then the Vigenère Cipher. This intricate procedure adds a layer of complexity, deterring potential intruders and ensuring the integrity of secure communications. The hybrid cryptographic process finds practical applications in military, police systems, and any scenario demanding secure message transmission.

In conclusion, the implementation of this Encryption and Decryption process using a Hybrid cipher, seamlessly integrating the Polybius and Vigenère cipher systems, has been demonstrated through a Python program.

In its encryption process, the method employs both Vigenere Cipher and Polybius Square Cipher.

## IV. CHALLENGES

1) Vulnerabilities in the implementation: The cryptography used in a chat application may be strong, but if the implementation of the cryptography is flawed, it can lead to security vulnerabilities that can be exploited by attackers.
2) Weak passwords: Weak passwords can compromise the security of chat applications based on cryptography. If users choose weak passwords or reuse passwords across multiple accounts, their accounts can be compromised.
3) Social engineering attacks: Attackers can use social engineering techniques to trick users into revealing their login credentials or other sensitive information. For example, they may send phishing emails or messages that appear to be from the chat application's service provider.

## V. CONCLUSION

We analyze the performance of a few symmetric encryption techniques in this work. Double key exchange is the algorithm of choice. When the key size is changed, it is evident that the battery and time consumption alter significantly. The study could become broader in the future by incorporating strategies and schemes for handling various forms of data, such as image, sound, and video, and by developing a stronger encryption algorithm with quick speed and low energy usage.

## VI. REFERENCES

[1] Surendra, Mr KR, et al. "Design of Hybrid Cryptography System Based on Vigenere Cipher and Polybius Cipher."

[2] Mishra Annu."Analytical Study on Cryptographic Techniques and its Loopholes"

[3] Agrawal Arpit, and Gunjan Patankar."Design of Hybrid Cryptography Algorithm for Secure Communication" International Research Journal of Engineering and Technology (IRJET) 3.01 (2016):2395-0056.

[4] Soofi, Aized Asim, Irfan Riaz, and Umair Rasheed. "An enhanced vigenere cipher for data security"Int. J. Sci. Technol. Res 5.3 (2016): 141-145.

[5] Abhishek Mishra "Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher" - International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 2, Issue 5, May 2022

[6] Deepika, S. "Secure Data Transmission Using Hybrid Cryptography"(2021).

[7] Omolara, O.E.,I. Oludare, and S.E. Abdulahi. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication."Computer Engineering and Intelligent Systems 5.5 (2014):34-46.

[8] Kartha, Ranju S., and Varghese Paul. "Survey: Recent Modifications in Vigenere Cipher."IOSR J. Comput. Eng 16.2(2014):49-53.

[9] Arroyo, Jan Carlo T., Cristina E. Dumdumaya, and Allemar Jone P. Delima. "Polybius square in cryptography: a brief review of literature." International Journal 9.3 (2020)

[10] Vincent, PM Durai Raj. "RSA ENCRYPTION ALGORITHM -A SURVEY ON ITS

VARIOUS FORMS AND ITS SECURITY LEVEL.”International Journal of Pharmacy and Technology 8.2 (2016):12230-12240.