CRYPTOGRAPHY

A Project Work Report

Submitted in the partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE WITH SPECIALIZATION IN

INFORMATION SECURITY

Submitted by:

21BCS8251 Khushi
21BCS4461 Sorabh Kumar

Under the Supervision of:

Priyanka Jamwal

CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413,

PUNJAB

September 2023

BONAFIDE CERTIFICATE

Certified that this project report **"CRYPTOGRAPHY"** is the bonafide work of "**Khushi & Sorabh"** who carried out the project work under my/our supervision.

SIGNATURE
(Mr. Aman Kaushik)
Head of Department
AIT-CSE

SIGNATURE
(Priyanka Jamwal)
SUPERVISOR
AIT-CSE

Submitted for the project viva-voce examination held on

INTERNAL EXAMINER **EXTERNAL EXAMINER**

TABLE OF CONTENT

ABSTRACT

Cryptography is derived from a Greek word that means the art of securing data by transforming it into a jumbled arrangement and unreadable format. It combines arithmetic and software engineering. The explosive rise of the Internet has resulted in a greater acquaintance with intriguing uncertainty issues.

Despite the fact that security is a major concern on the internet, many apps have been developed and designed without taking into account the primary goals of data security, which are secrecy, authentication, and protection.

As our daily activities become increasingly reliant on data networks, the need of understanding such security challenges and problems will grow. Cryptography is essential to prevent unauthorized customers or individuals from accessing the data.
This work proposes a new hybrid security cipher by combining the two most important ciphers, Polybius and Vigen'ere. This hybrid encryption cipher is more secure than traditional ciphers.

While communicating, every user desires a secure network so that data communication is secure and no intruder can read their data. Cryptography is used in wireless and wired networks to provide secure data transfer, where cryptography converts plain text to cipher text and cipher text to plain text.
Encryption occurs when plain text is turned into cipher text at the transmitter side, while decryption occurs when cipher text is converted into plain text at the receiver side. There are two types of encryption techniques: symmetric cryptography and asymmetric cryptography.

The sender encrypts data using this key and an encryption method; the receiver decrypts the data with the same key and the matching decryption algorithm. Asymmetric or public-key cryptography employs two keys: a private key and a public key. The receiver keeps the private key, while the public key is made public. Different researchers also provide some versions of asymmetric cryptography.

Asymmetric encryption algorithms that are often employed include RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), and ECC (Elliptic curve cryptography).

Keywords - Encryption, Cryptography, Polybius Ciphers, Vigen’ere Ciphers.

CHAPTER 1: INTRODUCTION

In today's world, technology has advanced to the point where the vast majority of people prefer to use the internet as the primary means of sending data from one end of the planet to the other. There are several ways to communicate data over the internet, including messages, chats, and so on. Using the internet, data exchange is made exceedingly simple, quick, and precise. In any event, one of the key challenges with sending data over the internet is the "security risk" it provides; for example, personal or confidential data can be stored or hacked from a variety of angles. since a result, it is critical to address data security, since it is one of the most important aspects to consider during the data transfer process.

Security is an important component in the open system, and cryptography plays an important role in this field. Cryptography is an old technology that ensures the security of information in the open system. However, the purpose of cryptography is utilized not just to supply categorization, but moreover to give solutions to several issues: data trustworthiness, verification, and non-denial. Cryptography is described as encapsulating and devising ways that allow essential information and data to be conveyed in a protected structure so that the only person capable of recovering this information is the conscious beneficiary.

Emergence of Hybrid Security:

1. Complexity in Unison:

The synergy of the Vigenère Cipher and Polybius Cipher in a two-step security model brings forth a heightened level of complexity and sophistication. By combining the polyalphabetic nature of the Vigenère Cipher with the spatial substitution of the Polybius Cipher, this hybrid system introduces multiple layers of encryption, significantly increasing the difficulty for adversaries attempting unauthorized access.

2. Resilience Against Cryptanalysis:

The hybridization of these classical ciphers offers a defense strategy against various cryptanalysis techniques. The polyalphabetic structure of the Vigenère Cipher adds a dynamic layer to the encryption process, while the spatial substitution of the Polybius Cipher introduces a spatial complexity that enhances resistance to frequency-based attacks. The amalgamation of these strengths creates a robust defense mechanism against both historical and contemporary cryptographic threats.

Key Management and Rotation:

Effective key management is a pivotal aspect of any cryptographic system. The two-step security approach utilizing the Vigenère and Polybius Ciphers involves periodic key rotation, enhancing the overall resilience of the encryption system. Regularly updating keys mitigates the risks associated with prolonged use, ensuring that the security of the system remains dynamic and adaptive.

Modern Relevance and Applicability:

The integration of classical ciphers into modern cryptographic frameworks exemplifies a seamless fusion of historical wisdom and contemporary security needs. As organizations and individuals alike strive to secure their digital communications, the hybrid or two-step security approach serves as a testament to the enduring relevance of classical ciphers in the face of evolving cybersecurity challenges.

Scope of Exploration:

As we delve deeper into the intricacies of this hybrid security model, the subsequent sections will unfold the methodology, algorithm design, key management strategies, security analysis, implementation details, and performance evaluations associated with the integration of the Vigenère Cipher and Polybius Cipher. This comprehensive exploration aims to provide a holistic understanding of how the combination of these classical ciphers contributes to a robust and adaptable two-step security system.

There are two types of encryption techniques: symmetric cryptography and asymmetric cryptography. Both parties utilize the same key in symmetric-key cryptography

Symmetric and asymmetric cryptography are widely accepted types of cryptography in which symmetric (also known as symmetric key cryptography) is focused on ensuring secure communication between sender and receiver by using the same secret key, whereas asymmetric cryptography (also known as public key cryptography) secures communication by using public and private keys. Private keys are held individually in communication, but public keys are known to everyone due to their public character. The figures below depict symmetric and asymmetric cryptography, respectively.

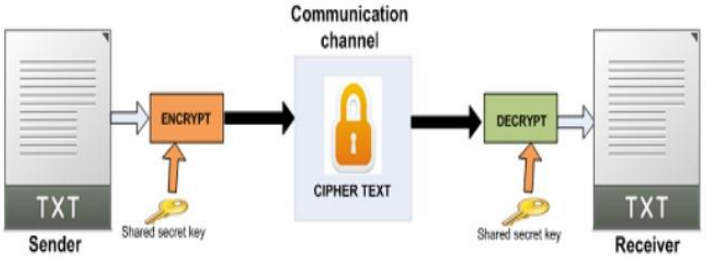

Fig. 1. Symmetric Cryptography

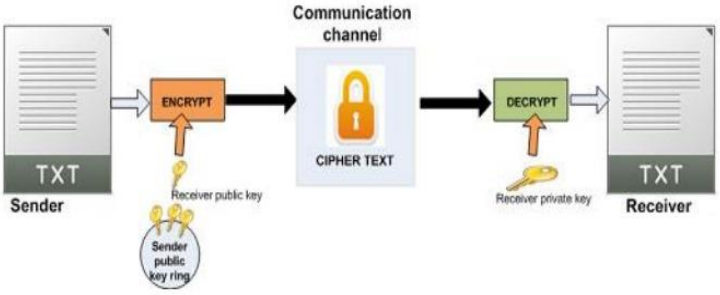

Fig. 2. Asymmetric Cryptography

To ensure secure data connection cryptography is used in wireless and wired networks to convert plain text to cipher text and cipher text to plain text. Encryption occurs when plain text is turned into cipher text at the transmitter side, while decryption occurs when cipher text is converted into plain text at the receiver side.The sender encrypts data using this key and an encryption method; the receiver decrypts the data with the same key and the matching decryption algorithm. Asymmetric or public-key cryptography employs two keys: a private key and a public key. The receiver keeps the private key, while the public key is made public.

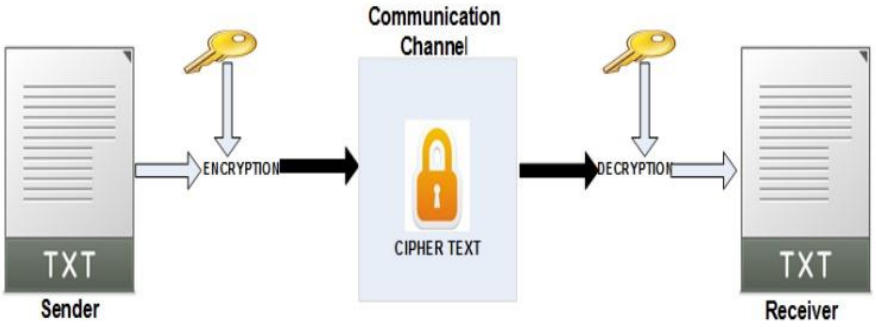

Fig. 3. Working of encryption and decryption.

CHAPTER 2: LITERATURE SURVEY

Advancing Security Through Dual-Layer Encryption featuring Vigenère Cipher and Polybius Cipher

In the ever-changing realm of information security, the demand for robust cryptographic methodologies is more crucial than ever. The integration of classical ciphers, notably the Vigenère Cipher and Polybius Cipher, within a dual-layer security framework offers a compelling strategy to bolster the confidentiality and integrity of sensitive data. This conclusion explores the distinct advantages, accompanying challenges, and potential avenues for advancement in the domain of dual-layer security.

Advantages of the Dual-Layer Security Approach:

1. Complexity and Unpredictability:

The primary strength of a dual-layer security system lies in the heightened complexity and unpredictability it injects into the encryption process. The Vigenère Cipher, renowned for its polyalphabetic substitution, and the Polybius Cipher, leveraging spatial substitution, introduce diverse elements to the encryption landscape. The amalgamation of these classical ciphers in a hybrid model results in a multi-layered defense mechanism, significantly increasing the difficulty for adversaries to decipher encrypted messages.

2. Resistance to Cryptanalysis:

Historically, both the Vigenère Cipher and the Polybius Cipher have demonstrated resilience against various types of cryptanalysis. The polyalphabetic nature of the Vigenère Cipher renders it less susceptible to frequency analysis, a common attack on simpler ciphers. Simultaneously, the spatial substitution introduced by the Polybius Cipher adds an extra layer of complexity, making it resistant to traditional frequency-based attacks. The hybrid system inherits the strengths of these individual ciphers, establishing a robust defense against a spectrum of cryptographic attacks.

3. Key Management and Rotation:

Effective key management remains a critical aspect of any cryptographic system. The dual-layer security approach introduces unique considerations to key management through the Vigenère Cipher and Polybius Cipher. The periodic rotation of keys, a practice employed in both ciphers, further fortifies the security posture. Regularly updating keys serves to mitigate risks associated with prolonged use, enhancing the overall resilience of the encryption system.

4. Integration of Classical and Modern Cryptography:

The integration of classical ciphers within a modern cryptographic framework signifies a harmonious coexistence of traditional and contemporary encryption techniques. While classical ciphers lay the historical foundation for cryptography, combining them with modern practices addresses the evolving challenges posed by advanced cyber threats. This synthesis ensures a holistic approach to information security, leveraging the strengths of both classical and modern cryptographic methods.

Challenges and Considerations:

1. Computational Overhead:

A challenge associated with the dual-layer security approach is the potential increase in computational overhead. The combination of multiple encryption layers may necessitate additional processing power, especially in resource-constrained environments. Thorough consideration must be given to the computational efficiency of the system to ensure practicality and real-world applicability.

2. Key Distribution and Management:

While the rotation of keys enhances security, the secure distribution and management of keys remain paramount. Challenges associated with securely exchanging keys, particularly in scenarios where secure channels are not readily available, underscore the need for robust key distribution mechanisms. Effective key management practices are

crucial to the overall success of the dual-layer security system.

3. Adaptability and Updates:

As the threat landscape evolves, the adaptability of cryptographic systems becomes crucial. The dual-layer security approach, rooted in classical ciphers, should remain flexible to accommodate updates and enhancements. Staying abreast of cryptographic developments and promptly integrating security updates ensures that the system remains resilient against emerging threats.

Future Directions and Advancements:

1. Quantum-Safe Cryptography:

As quantum computing technologies advance, the susceptibility of classical cryptographic algorithms to quantum attacks becomes a concern. Future advancements in the dual-layer security approach may involve the integration of quantum-safe cryptographic techniques to ensure resilience in a post-quantum computing era.

2. Machine Learning Integration:

The integration of machine learning algorithms for anomaly detection and pattern recognition could further enhance the security of the dual-layer encryption system. Machine learning models can adaptively analyze encrypted data and identify unusual patterns, providing an additional layer of defense against sophisticated attacks.

3. User-Friendly Implementations:

Simplifying the implementation and deployment of the dual-layer security system is essential for widespread adoption. User-friendly interfaces, automated key management systems, and integration with existing communication platforms can facilitate the seamless incorporation of enhanced security measures in various applications.

Conclusion: A Comprehensive Approach to Information Security

In conclusion, the integration of the Vigenère Cipher and Polybius Cipher within a dual-layer security system exemplifies a comprehensive approach to information security. The advantages derived from the unique properties of these classical ciphers, coupled with considerations for key management and adaptability, contribute to the creation of a resilient defense mechanism.

The dual-layer security approach not only capitalizes on the historical strengths of classical ciphers but also addresses contemporary challenges by combining them in a hybrid model. This integration fosters a synergy that enhances the overall security posture, providing protection against a spectrum of cryptographic attacks.

As technology advances and cyber threats evolve, the continuous refinement of cryptographic systems remains imperative. The dual-layer security approach serves as a testament to the enduring relevance of classical ciphers in a modern cryptographic landscape. Through careful consideration of challenges, proactive key management, and openness to future advancements, this approach stands as a testament to the enduring significance of classical ciphers in a modern cryptographic landscape.

2.1. Existing solutions

1.Scrambling and scattering are provided in a modified variant of the Vigen'ere cipher method by the combining and summation of a subjective component to each byte and bit before the message and string are combined using the system Vigen'ere cipher. Because of the padding of the message and string with random bits, this approach fails the Kasiski attack to determine the length of the key. Another technique for performing the Vigen'ere algorithm was introduced and raised as through usually and systematically for encryption and message dissemination require key to be replaced repeatedly. However, in this case, main keys serve as a continuation for the process's replacement key exchange.

2.Some cryptographic algorithms, such as AES, DES, 3DES, RC6, Blowfish, and RC2, are described in detail. Furthermore, the performance of these security techniques is evaluated, and experiments on text files and images are carried out. As the packet size increased, the results showed that all methods performed slower than Blowfish. However, when using image as the type of data instead of text file, Blowfish, RC6, and RC2 algorithms took longer than AES, DES, and 3DES algorithms. The results showed that DES is still quicker than 3DES in terms of performance.

The experiment is carried out using a single CPU and cloud computing. The research demonstrates that a cryptography method in cloud computing is faster than a single processor machine. AES has the highest Speed up ratio with a tiny input file, MD5 has the lowest, and RSA is the most time-consuming. Author investigated the performance of various cryptographic algorithms such as DES, AES, and 3DES to determine the encryption and decryption time and throughput for various hardware.

These algorithms are used to calculate the encryption time. Encryption time grows in proportion to data size. As a result, the increase in encryption speed is determined by the file size (in bytes) rather than the data type of the file. 3DES has a lower throughput when compared to AES, text files, and images utilized for performance test. Dot net frame is utilized for the implementation of DES 3DES, which takes more processing time than the AES algorithm. The encryption time is measured using only one parameter. The encryption time will be measured using different parameters in future work on this paper.

2.2 Proposed System

Cryptography is the most widely used approach for data security, privacy, secrecy, and reliability. Because of multiple impediments, constraints, and smooth systems, single traditional ciphers are regarded as the least complex and most vulnerable cryptographic techniques.

Vigen'ere encryption is a well-known encryption, but it has a few flaws. To overcome the limitations of the Vigen'ere cipher, a new technique is presented as an improved variant as a combination of Polybius cipher and Vigen'ere that is significantly more secure against attacks such as Active, passive, Kasiski, and Friedman attacks (attacks).

Because of the usage of product tables for encryption, cryptanalysis, recurrence examination, men in the middle attacks, frequency analysis, fault analysis attacks, design expectation, and brute force attacks on the suggested method are also considerably more difficult.

The altered hybrid combination of the Caesar Cipher and the Vigen'ere Cipher results in a high amount of complexity, scattering, distribution, and confusion in the algorithm that makes them, making it an extraordinarily strong cipher and difficult to break.

2.3 Problem Formulation

In the realm of cryptography, the need for secure and versatile encryption mechanisms is paramount. The project seeks to address the challenge of combining historical ciphers with contemporary cryptographic demands, with a focus on the Vigenère Cipher and the Polybius Cipher. The problem at hand involves formulating a solution that integrates these classical ciphers into a cohesive hybrid system while mitigating their inherent vulnerabilities and catering to modern security requirements.

Performance Optimization:

Achieving an optimal balance between security and performance is non-trivial. The challenge involves refining algorithms to ensure efficient encryption and decryption processes. This optimization effort must consider the computational resources required and compare favorably with established cryptographic techniques.

Real-World Applicability:

Translating theoretical innovations into practical solutions is a significant challenge. The hybrid system's efficacy in real-world scenarios, such as secure communication and data protection, must be evaluated. Adapting the system to diverse use cases while maintaining its security posture forms an essential challenge.

2.4 Research Objectives:

OBJECTIVES

The purpose of this study is to investigate the feasibility, security, and performance of a novel hybrid cryptography system that combines the qualities of the Vigenère and Polybius ciphers. The major goal is to create an innovative cryptographic approach that takes advantage of the historical context and unique qualities of these classical ciphers to improve data secrecy and resistance to modern cryptanalysis tools. We hope to accomplish the following objectives with this research:

Hybrid Scheme Development: Create a strong and efficient cryptographic technique that combines the Vigenère and Polybius ciphers to create a hybrid encryption approach. Examine how the unique qualities of each cipher can be used to create a more secure and adaptive encryption method.

Key Management Enhancement: Propose a hybrid system advanced key management technique that optimizes key production, distribution, and storage. Examine how key length and randomization affect the overall security of the hybrid system.

Security Analysis: Perform a thorough security analysis of the hybrid cryptography system, including an evaluation of its susceptibility to various cryptographic attacks such as frequency analysis, known-plaintext attacks, and chosen-plaintext attacks. Assess the system's vulnerability to modern cryptanalysis techniques and provide countermeasures as needed.

Cryptanalysis Prevention: Investigate techniques for mitigating the known weaknesses of the Vigenère and Polybius ciphers when employed separately. Determine how the hybridization can help to mitigate the impact of the flaws inherent in both ciphers.

Performance Evaluation: In terms of encryption and decryption speeds, evaluate the hybrid cryptography system's computational performance and efficiency. To determine the viability of practical implementation, compare these results to the performance of the standalone Vigenère and Polybius ciphers.

Applicability and Use Cases: Investigate prospective scenarios and use cases where the hybrid cryptography system could be useful. Examine the hybrid scheme's application in diverse fields such as secure communication, data security, and information sharing.

Usability Considerations: Examine the hybrid cryptography system's usability and ease of installation. Determine whether the hybridization brings complexity that may influence the system's usability and adoption.

Comparison with Modern Techniques: Compare the hybrid scheme's security and performance to that of newer encryption approaches such as advanced symmetric and asymmetric algorithms. Highlight the benefits and drawbacks of the hybrid method in the context of modern cryptographic solutions.

2.5 METHODOLOGY

This section describes the technique used in the design, development, and testing of the hybrid cryptography system that combines the Vigenère and Polybius ciphers. The research strategy combines theoretical analysis, algorithm design, implementation, security analysis, and performance evaluation.By combining the strengths of these ciphers, the encryption process becomes more robust, ensuring a higher level of confidentiality and integrity for sensitive data. The key management protocols and adaptability to existing systems make this approach a practical solution for organizations seeking enhanced information security.

Literature Review:

The landscape of information security continually evolves, demanding innovative approaches to safeguard sensitive data. This study delves into classical ciphers, hybrid cryptography, and modern cryptographic methods to propose a two-layer security system using the Vigenère and Polybius ciphers. This multifaceted approach aims to bolster data confidentiality and integrity against emerging cyber threats.

Classical Ciphers:

Classical ciphers form the foundation of cryptographic techniques, with the Vigenère Cipher and the Polybius Cipher standing out for their historical significance. The Vigenère Cipher, created by Blaise de Vigenère in the 16th century, provided a breakthrough in resisting frequency analysis due to its polyalphabetic substitution nature. However, vulnerabilities like key repetition have been identified, prompting the need for enhancements.

The Polybius Cipher, originating from ancient Greece, is a spatial substitution cipher employing a grid to assign coordinates to letter pairs. While historically relevant, its simplicity leaves it susceptible to modern cryptanalysis.

Hybrid Cryptography:

Hybrid cryptography emerges as a contemporary paradigm, combining symmetric and asymmetric encryption to capitalize on their respective strengths. This approach, seen in systems utilizing algorithms like RSA and AES, addresses the limitations inherent in individual cryptographic methods, ensuring a more robust defense against sophisticated attacks.

Algorithm Design and Integration:

a. Vigenère Cipher Enhancement:

Analyzing the Vigenère Cipher reveals a vulnerability to key repetition, a weakness that threatens its overall security. To enhance its resistance, a dynamic key management system can be implemented. By employing a cryptographically secure pseudorandom number generator, unpredictable keys are generated, mitigating the risks associated with repetition.

b. Polybius Cipher Adaptation:

Adapting the Polybius Cipher for contemporary cryptographic environments involves addressing its limitations. Introducing key-dependent S-boxes and diffusion mechanisms enhances its resilience against modern cryptanalysis. This adaptation ensures that a change in a single bit of the input results in multiple bits changing in the output, providing a more robust defense.

c. Hybrid Scheme Definition:

Designing a hybrid system integrating the Vigenère and Polybius ciphers requires meticulous consideration. Using the Vigenère Cipher for initial encryption and the Polybius Cipher for a subsequent layer adds complexity to the encryption process, creating a multi-layered defense against various cryptographic attacks.

Key Management and Generation:

Developing a robust key management plan is crucial for the hybrid system's overall security. Generating keys with sufficient length and entropy using a cryptographically secure pseudorandom number generator ensures resilience against brute-force attacks. Secure distribution methods, such as the use of secure channels, and robust storage mechanisms, like hardware security modules, safeguard keys from unauthorized access.

Security Analysis:

a. Cryptanalysis Evaluation:

Conducting cryptanalysis tests, including frequency analysis, chosen-plaintext attacks, and known-plaintext attacks, is essential to assess the hybrid scheme's resilience. Identifying weaknesses allows for the implementation of effective mitigation strategies.

b. Mitigation Strategies:

The hybridization of the Vigenère and Polybius ciphers inherently mitigates specific vulnerabilities. Fine-tuning parameters, such as key length and substitution mechanisms, based on the outcomes of the security audit, further strengthens the overall system.

Implementation:

Translating the proposed algorithms and techniques into a tangible implementation involves developing encryption and decryption functions, key management modules, and necessary data structures. Utilizing a programming language like Python allows for a practical and versatile implementation of the hybrid cryptography system.

Performance Evaluation:

a. Benchmarking:

Evaluating the hybrid system's encryption and decryption speeds across varied message lengths and key sizes is crucial. Comparing these results with the individual performances of the Vigenère and Polybius ciphers provides insights into the efficacy of the hybrid approach.

b. Resource Consumption:

Assessing the computing resources, including CPU and memory, required by the hybrid system is essential for practical deployment. Comparing these resource needs to recent encryption techniques benchmarks the system's efficiency.

2.7. Literature survey summary-

Citation	Research Objective	Source	Technique	Significant results
Muhammad Nadeem,Ali Arshad,Saman Riaz,Syeda Wajiha Zahra	modified the Vigenère cipher algorithm to secure data and prevent key identification from Kasiski tests, implemented the results obtained from the Vigenère cipher on the Polybius algorithm, and obtained the ciphertext	Qualitative and quantitative research methods; Mobile app development tools such as Android Studio and Eclipse	developed a hybrid cryptographic algorithm using the Vigenère cipher and Caesar cipher techniques to encrypt data.	an efficient algorithm was developed in which the encrypted text and Vigenère key are obtained with the help of a plaintext and a static key.
Sultan Almotairi, Ashit Kumar Dutta,Muhammad Nadeem	a secure architecture for securing data with various algorithm implementations on the architecture so that cloud data can be saved from replay attacks.	A Secure Architecture to Protect the Network from Replay Attacks during Client-to-Client Data Transmission	PDeployment-based model is a model that provides end-users with sizes, ownership, and a variety of access while service-based models are those that provide a variety of services, including Iaas,Paas and Saas.	developed an efficient algorithm to protect data from replay attacks in which plain text data has been encrypted. In the future, an algorithm will be developed to encrypt all file types and protect data from replay attacks and DDoS attacks.

Bhavana K V, Banushree D J, Bhumika D, Chaitanya K B	A table consists of 26 columns and 8 rows. Here, they used formula for encryption and decryption. For encryption, plain text and key character were added and modulo 27 of the resultant was calculated.	A CRYPTO SYSTEM USING VIGENERE AND POLYBIUS CIPHER	Every combination of key phrase character and plain text character could replace with many other cipher characters. This technique was very secure against Friedman and kasiski attacks.	we are sending message through email as input and image which will be encrypted and decrypted to original content by using python programming language.
Camille Merlin S. Tan,Gerald P. Arada,Alexander Co Abad,Elmer Magsino	based on the concept of Caesar Cipher and Vigenere Cipher with an improved performance by adding different number of shift positions depending on the line number.	A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher	the proposed algorithm is compared to some well-known ciphers such as Hill Cipher, Caesar Cipher and Vigenere Cipher in terms of letter frequency of the ciphertext.	the authors successfully implemented hybrid encryption and decryption processes by combining the Caesar Cipher and Vigenere Cipher algorithms.

Carlos Trapiello, Vicenç Puig,Damiano Rotondo	Presents a zonotopic set-invariance analysis of replay attacks affecting the communication network that serves the supervisory layer of complex control systems using an observer-based detection scheme	A zonotopic set-invariance analysis of replay attacks affecting the supervisory layer	(I) Sensors and controller data are counterfeited; (II) Only sensor measurements are counterfeited.	The representation of invariant sets as zonotopes allows to derive analytical expressions for attack detectability under the presence of bounded uncertainties.
Md Mehedi Hasan,Noor Afiza Mohd Ariffin,Nor Fazlida Mohd Sani	we present comprehensive survey on cryptographic impact in smart grid for security objectives, requirement, and challenges.	A review of cryptographic impact in cybersecurity on smart grid: Threat, challenges and countermeasures	role of cryptographic aspect in smart grid to shed light and guide future research direction for cyber-security protection against from malicious attacker in smart grid application.	In terms of the cryptographic component solution strategy, the current gap could help to make decisions on potential research in this smart grid infrastructure. .

Jan Carlo T. Arroyo, Cristina E. Dumdumaya, Allemar Jhone P. Delima	To use the Polybius square with varied character ar rangements elements using the Nihilist cipher and MD5 technology for a more secured encryption and decryption	Polybius Square in Cryptography: A Brief Review of Literature	The proposed method produced a more secure ciphertext due to layers and diverse processes being conducted.	Altered the placement of the elements in the Polybius square grid

1.Muhammad Nadeem,Ali Arshad,Saman Riaz,Syeda Wajiha Zahra.an efficient algorithm was developed in which the encrypted text and Vigenère key are obtained with the help of a plaintext and a static key.

2.Sultan Almotairi, Ashit Kumar Dutta,Muhammad Nadeem.developed an efficient algorithm to protect data from replay attacks in which plain text data has been encrypted. In the future, an algorithm will be developed to encrypt all file types and protect data from replay attacksand DDoS attacks.

3.Bhavana K V, Banushree D J, Bhumika D, Chaitanya K B.we are sending message through email as input and image which will be encrypted and decrypted to original content by using python programming language.

4. Camille Merlin S. Tan,Gerald P. Arada,Alexander Co Abad,Elmer Magsino.the authors successfully implemented hybrid encryption and decryption processes by combining the Caesar Cipher and Vigenere Cipher algorithms.

5. Carlos Trapiello,Vicenç Puig,Damiano Rotondo.The representation of invariant sets as zonotopes allows to derive analytical expressions for attack detectability under the presence of bounded uncertainties.

6.Md Mehedi Hasan,Noor Afiza Mohd Ariffin,Nor Fazlida Mohd Sani.In terms of the cryptographic component solution strategy, the current gap could help to make decisions on potential research in this smart grid infrastructure.

7.Jan Carlo T. Arroyo, Cristina E. Dumdumaya, Allemar Jhone P. Delima. To use the Polybius square with varied character ar rangements elements using the Nihilist cipher and MD5 technology for a more secured encryption and decryption

CHAPTER 3. DESIGN FLOW/PROCESS

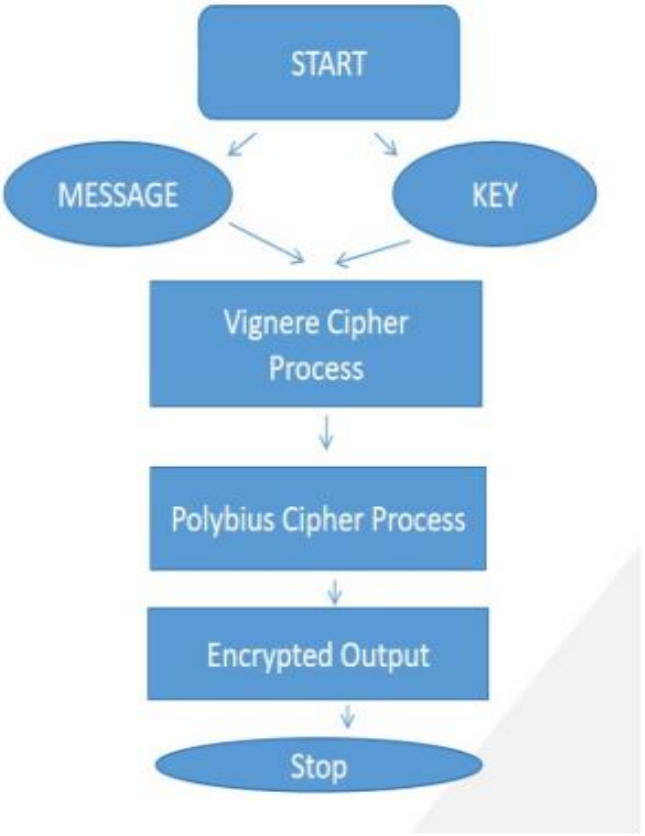

Fig.1- Design the flow diagram of Two layer process

The constant evolution of cyber threats necessitates innovative approaches to information security. Combining classical and modern cryptographic methods provides a robust defense against various attack vectors. In this comprehensive guide, we outline the step-by-step implementation of a two-layer security system using the Vigenère Cipher and Polybius Cipher. The integration of these classical ciphers aims to enhance data confidentiality and integrity, mitigating vulnerabilities inherent in singular encryption methods.

Step 1: Key Generation

1.1 Vigenère Cipher Key:

Choosing a strong, random key is fundamental to the security of the Vigenère Cipher. Consider the length of the key to ensure adequate security. The key should be kept confidential and securely shared among authorized parties. Regularly update the Vigenère key to mitigate the risks associated with prolonged use.

1.2 Polybius Cipher Key:

Establishing a unique key for the Polybius Cipher involves determining the arrangement of letters in the grid. The key should remain confidential to prevent unauthorized decryption. As with the Vigenère Cipher, key rotation strategies should be employed to enhance the overall security of the two-layer system.

Step 2: Vigenère Cipher Encryption

2.1 Message Segmentation:

Divide the plaintext message into blocks, aligning them with the Vigenère Cipher key. This segmentation is crucial for the subsequent encryption process.

2.2 Key Repetition:

Repeat the Vigenère Cipher key to match the length of each plaintext block. This step ensures that the key aligns appropriately with each segment of the message.

2.3 Encryption Process:

Apply the Vigenère Cipher algorithm to each block. The algorithm involves shifting the letters of the plaintext by the corresponding letters in the key. This process provides a polyalphabetic substitution, adding complexity to the encryption.

2.4 Result:

The result of this phase is the first layer of encrypted text using the Vigenère Cipher. The polyalphabetic nature of the Vigenère Cipher enhances resistance against frequency analysis, a common cryptographic attack.

Step 3: Polybius Cipher Encryption

3.1 Message Mapping:

Convert the Vigenère-encrypted message into a format suitable for the Polybius Cipher. This mapping could involve associating each character with coordinates or using a predefined mapping scheme.

3.2 Polybius Cipher Encryption:

Apply the Polybius Cipher algorithm to the mapped message. Replace pairs of letters with their corresponding coordinates on the Polybius grid. This spatial substitution introduces an additional layer of complexity to the encryption process.

3.3 Result:

The result of this phase is the second layer of encrypted text using the Polybius Cipher. The combined effects of the Vigenère and Polybius ciphers create a formidable defense, making cryptanalysis more challenging.

Step 4: Secure Transmission or Storage

4.1 Transmission:

If the encrypted message is to be transmitted, ensure secure channels are used. Employ protocols such as TLS or VPNs to prevent interception during transmission. This step is vital to maintaining the confidentiality of the encrypted data.

4.2 Storage:

If the encrypted message is to be stored, use secure storage methods. Protect against unauthorized access and ensure the integrity of the stored data. Encryption keys should be stored separately from the encrypted data to enhance security.

Step 5: Decryption Process

5.1 Polybius Cipher Decryption:

Reverse the Polybius Cipher process, obtaining the mapped message. Reconstruct the pairs of letters based on the coordinates in the Polybius grid.

5.2 Vigenère Cipher Decryption:

Reverse the Vigenère Cipher process, decrypting the message using the Vigenère key. The decryption involves shifting the letters of the Polybius-decrypted message in the reverse order of the Vigenère key.

5.3 Result:

The final result is the original plaintext message obtained after the two-layer decryption process. This process ensures that authorized parties can retrieve the original information securely.

Step 6: Key Management and Rotation

6.1 Regular Key Rotation:

Implement a key rotation strategy for both ciphers. Periodically change keys to mitigate the impact of potential key compromises. This practice enhances the overall security of the two-layer system.

6.2 Key Management:

Enforce secure key management practices, including secure generation, distribution, and storage. Regularly update keys to ensure the continued confidentiality of encrypted communications.

Step 7: Monitoring and Updates

7.1 Monitoring:

Implement monitoring mechanisms to detect unusual activities or potential security breaches. Regularly review logs and system behavior to identify any anomalies that may indicate a security threat.

7.2 Security Updates:

Stay informed about cryptographic developments and potential vulnerabilities. Implement updates or enhancements to the encryption system as needed. This proactive approach ensures that the two-layer security system remains resilient against evolving threats.

3.2. **Design Constraints**

The design and implementation of cryptographic algorithms involve careful consideration of various constraints to ensure their effectiveness and security. In this exploration, we delve into the design constraints specific to the Vigenère and Polybius ciphers. Understanding these constraints is crucial for developing robust encryption systems that withstand the challenges posed by contemporary cryptographic landscapes.

Design Constraints for the Vigenère Cipher:

Key Length and Reusability:

The Vigenère Cipher's security heavily relies on the length and randomness of the key. Short and repetitive keys diminish its strength, making it susceptible to cryptanalysis. However, increasing key length introduces challenges in terms of usability and key management, as longer keys can be more challenging to remember and distribute securely.

Key Distribution:

Securely distributing the key to authorized parties without interception is a significant constraint. In scenarios where key exchange is not feasible through secure channels, establishing a secure key distribution mechanism becomes essential to maintain the confidentiality of the communication.

Key Management:

Managing keys in a dynamic environment poses challenges, especially when dealing with a large number of users or devices. The Vigenère Cipher requires effective key management to ensure that keys are securely generated, distributed, and updated, minimizing the risk of compromise.

Frequency Analysis Vulnerability:

While the Vigenère Cipher offers resistance to simple frequency analysis due to its polyalphabetic nature, it is not immune. Cryptanalysts can exploit patterns in the ciphertext to deduce information about the key, emphasizing the need for additional complexity and security measures.

Algorithmic Complexity:

The Vigenère Cipher's simplicity, while advantageous in certain aspects, can be a limitation. Its algorithmic simplicity makes it vulnerable to attacks such as known-plaintext attacks, especially when encrypted messages share patterns.

Design Constraints for the Polybius Cipher:

Grid Size and Complexity:

The size of the Polybius grid directly influences the complexity and security of the cipher. Smaller grids may be more susceptible to brute-force attacks, while larger grids increase computational overhead. Striking a balance between grid size and computational efficiency is crucial.

Grid Distribution:

Distributing the Polybius grid securely to authorized parties is a challenge, especially when communication channels are susceptible to interception. Ensuring the integrity of the grid during distribution is essential to prevent unauthorized alterations.

Limited Character Set:

The Polybius Cipher typically operates on a limited character set, often excluding certain letters such as 'J.' This constraint restricts its applicability in scenarios where a broader character set is required, and adapting it to accommodate a comprehensive set of characters introduces additional complexity.

Dependency on Spatial Substitution:

The Polybius Cipher's reliance on spatial substitution introduces a constraint related to diffusion. Changes in the input (plaintext) should affect multiple bits in the output (ciphertext) to ensure a robust defense against various cryptanalytic techniques.

Algorithmic Rigidity:

The fixed nature of the Polybius grid can be a limitation when adaptability is crucial. Cryptographic systems often require periodic updates and adjustments to resist evolving attack techniques, and the rigid structure of the Polybius grid may hinder such adaptability.

Comparative Constraints and Mitigation Strategies:

Key Management Challenges:

Both the Vigenère and Polybius ciphers face key management challenges. Implementing effective key generation, distribution, and periodic updates is crucial for maintaining the security of encrypted communications. The use of key management protocols, secure channels, and cryptographic best practices helps mitigate these challenges.

Algorithmic Complexity and Adaptability:

While the Vigenère Cipher is criticized for its susceptibility to frequency analysis due to repeating keys, the Polybius Cipher faces challenges related to its fixed structure. Integrating both ciphers in a hybrid system aims to leverage their respective strengths, creating a more adaptable and robust encryption mechanism.

Cryptanalysis Vulnerabilities:

Both ciphers exhibit vulnerabilities to certain cryptanalytic techniques. Mitigation involves introducing additional complexities through algorithmic enhancements, key management strategies, and the integration of multiple layers of encryption, as proposed in the two-layer security approach.

3.5.1 System Architecture

Finalization subject for mitigating the constraints of the hybrid cipher:

In the realm of information security, designing a robust architecture is essential to ensure the confidentiality and integrity of sensitive data. The hybrid or two-step security approach, leveraging the Vigenère Cipher and Polybius Cipher, introduces a layered defense mechanism. This architecture meticulously integrates these classical ciphers, aiming to create a sophisticated and adaptive system that withstands a variety of cryptographic attacks. This comprehensive exploration delves into the architecture's key components, their interactions, and the underlying principles governing the implementation of this two-step security model.

Key Components of the Architecture:

1. Encryption Module:

The core of the architecture revolves around the encryption module, responsible for applying both the Vigenère Cipher and the Polybius Cipher in a sequential manner. This module accepts plaintext input and, through a series of steps, transforms it into a ciphertext that is significantly more resilient to cryptanalysis.

Vigenère Cipher Operation:

The Vigenère Cipher operates with a key that is periodically rotated to enhance security. The encryption module applies the polyalphabetic substitution process of the Vigenère Cipher to the input, introducing complexity and variability.

Polybius Cipher Operation:

Following the Vigenère encryption, the ciphertext undergoes a second layer of encryption using the Polybius Cipher. This spatial substitution process replaces pairs of letters with numerical coordinates based on a predefined grid, adding an additional layer of complexity.

2. Key Management System:

Effective key management is pivotal to the security of the architecture. The key management system encompasses the generation, distribution, rotation, and secure storage of cryptographic keys.

Key Generation:

The architecture employs a robust key generation mechanism to create both the Vigenère and Polybius keys. The keys are generated based on cryptographic principles, ensuring unpredictability and randomness.

Key Distribution:

Securely distributing keys is facilitated through established key distribution protocols. Encryption keys are shared between authorized parties using secure channels, preventing interception by malicious entities.

Key Rotation:

Periodic key rotation enhances security by mitigating the risks associated with long-term key usage. The architecture implements a systematic key rotation strategy for both the Vigenère and Polybius Ciphers.

3. Security Analysis Module:

To continually assess the effectiveness of the architecture, a dedicated security analysis module monitors and evaluates the system's resilience against various cryptographic attacks.

Cryptanalysis Evaluation:

The module conducts cryptanalysis tests, including frequency analysis, chosen-plaintext attacks, and known-plaintext attacks, to identify potential vulnerabilities. Results from these tests inform ongoing adjustments to the architecture.

Mitigation Strategies:

In response to identified vulnerabilities, the architecture incorporates mitigation strategies. These may include algorithmic adjustments, key management enhancements, or the introduction of additional security layers.

Interaction and Workflow:

1. Encryption Workflow:

The encryption process follows a sequential workflow involving both the Vigenère and Polybius Ciphers.

Input Reception: The plaintext is received as input, initiating the encryption process.

Vigenère Cipher Encryption: The input undergoes Vigenère encryption using a dynamically rotated key, producing an intermediate ciphertext.

Polybius Cipher Encryption: The intermediate ciphertext is further encrypted using the Polybius Cipher, creating the final ciphertext.

2. Key Management Workflow:

The key management system operates cohesively to ensure secure key generation, distribution, rotation, and storage.

Key Generation: Cryptographically strong keys are generated for both the Vigenère and Polybius Ciphers.

Key Distribution: The keys are securely distributed to authorized entities through established channels.

Key Rotation: Periodic key rotation is implemented to enhance overall system security.

3. Security Analysis Workflow:
Continuous security analysis ensures proactive identification and mitigation of potential vulnerabilities.

Cryptanalysis Evaluation: Cryptanalysis tests are conducted to assess the architecture's resilience.

Vulnerability Identification: Any vulnerabilities discovered are carefully analyzed and categorized.

Mitigation Implementation: Mitigation strategies are implemented to address identified vulnerabilities.

Scalability and Adaptability:
The architecture is designed with scalability and adaptability in mind to cater to evolving security needs.

Scalability: The architecture accommodates varying data volumes and processing requirements, making it suitable for diverse applications, from small-scale communications to large-scale data transmission.

Adaptability: The modular nature of the architecture enables the incorporation of additional security layers or the integration of emerging cryptographic techniques, ensuring adaptability to future security challenges.

Implementation Technologies:
The architecture can be implemented using a variety of technologies, with considerations for efficiency, security, and platform compatibility.

Programming Languages: Languages like Python or Java may be employed for their versatility and extensive cryptographic libraries.

Secure Communication Protocols: The architecture integrates secure communication protocols, such as TLS/SSL, to ensure the confidentiality of key distribution and data transmission.

Hardware Security Modules (HSMs): For enhanced key security, Hardware Security Modules may be incorporated to provide secure key storage and cryptographic processing.

Performance Evaluation:
The effectiveness of the architecture is assessed through rigorous performance evaluations, considering factors such as encryption/decryption speed, resource consumption, and overall system efficiency.

Benchmarking: The encryption and decryption speeds are benchmarked using varying message lengths and key sizes to understand the system's performance under different scenarios.

Resource Consumption: The architecture's impact on computing resources, including CPU and memory usage, is thoroughly analyzed to ensure practicality in real-world applications.

Conclusion: A Resilient Security Framework:

The architecture for two-step security using the Vigenère Cipher and Polybius Cipher represents a sophisticated and adaptive framework. By integrating the strengths of both classical ciphers and implementing robust key management and security analysis components, this architecture provides a resilient defense against cryptographic threats. As technology evolves, the architecture remains scalable and adaptable, poised to meet the dynamic challenges of information security in the digital age. Through continuous evaluation and refinement, it stands as a testament to the enduring relevance of classical ciphers in contemporary cryptographic landscapes.

1.For Fronted :

cipher_frontend.html

```html
<!DOCTYPE html>
<html>
<head>
    <title>Cipher Calculator</title>
</head>
<body>
    <h1>Cipher Calculator</h1>
    <form id="cipherForm">
        <label for="plaintext">Plaintext:</label><br>
        <input type="text" id="plaintext" name="plaintext"><br>
        <label for="key">Key:</label><br>
        <input type="text" id="key" name="key"><br>
        <input type="button" value="Calculate" onclick="calculateCipher()">
    </form>
    <h2>Results</h2>
    <p id="results"></p>
    <script src="cipher.js"></script>
</body>
</html>
```

2.For Backend

cipher.js

```javascript
function calculateCipher() {
    var plaintext = document.getElementById('plaintext').value;
    var key = document.getElementById('key').value;

    var vignere = vigenereCipher(key, plaintext, 1);
    var polybius = polybiusCipher(plaintext);
    var hybrid = polybiusCipherHybrid(vignere);

    document.getElementById('results').innerHTML = 'Vignere: ' + vignere + '<br>Polybius: ' + polybius + '<br>Hybri
}

var output_str;

function vigenereCipher(key, str, mode) {
    var output = [str.length];
    var result = 0;

    for (var i = 0; i < str.length; i++) {
        if (mode == 1) {
            result = ((str.charCodeAt(i) + key.charCodeAt(i % key.length)) % 128);
            output[i] = String.fromCharCode(result);
        } else if (mode == 0) {
            if (str.charCodeAt(i) - key.charCodeAt(i % key.length) < 0) {
                result = (str.charCodeAt(i) - key.charCodeAt(i % key.length)) + 128;
            } else {
                result = (str.charCodeAt(i) - key.charCodeAt(i % key.length)) % 128;
            }
            output[i] = String.fromCharCode(result);
```

cipher_frontend.html | cipher.js

cipher.js > vigenereCipher

```
    output_str = output.join('');
    return output_str;
}

function polybiusCipher(str) {
    var polybius = '';
    for (var i = 0; i < str.length; i++) {
        var charCode = str.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            polybius += String.fromCharCode((charCode - 65) / 5 + 65) + String.fromCharCode((charCode - 65) % 5 + 1
        } else if (charCode >= 97 && charCode <= 122) {
            polybius += String.fromCharCode((charCode - 97) / 5 + 97) + String.fromCharCode((charCode - 97) % 5 + 1
        }
    }
    return polybius;
}

function polybiusCipherHybrid(output_str) {
    var polybius = '';
    for (var i = 0; i < output_str.length; i++) {
        var charCode = output_str.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            polybius += String.fromCharCode((charCode - 65) / 5 + 65) + String.fromCharCode((charCode - 65) % 5 + 1
        } else if (charCode >= 97 && charCode <= 122) {
            polybius += String.fromCharCode((charCode - 97) / 5 + 97) + String.fromCharCode((charCode - 97) % 5 + 1
        }
    }
    return polybius;
}
```

Ln 18, Col 1 Spaces: 4 UTF-8 CRLF {} JavaScript Go Live

Let's break down the algorithms for the Vigenère Cipher, Polybius Cipher, and the hybrid system into steps:

Step 1: Input Retrieval

```
var plaintext = document.getElementById('plaintext').value;
var key = document.getElementById('key').value;
```

Step 2: Vigenère Encryption

```
function vigenereCipher(key, str, mode) {
    var output = [str.length];
    var result = 0;

    for (var i = 0; i < str.length; i++) {
        if (mode == 1) {
            result = ((str.charCodeAt(i) + key.charCodeAt(i % key.length)) % 128);
            output[i] = String.fromCharCode(result);
        } else if (mode == 0) {
            if (str.charCodeAt(i) - key.charCodeAt(i % key.length) < 0) {
                result = (str.charCodeAt(i) - key.charCodeAt(i % key.length)) + 128;
            } else {
                result = (str.charCodeAt(i) - key.charCodeAt(i % key.length)) % 128;
            }
            output[i] = String.fromCharCode(result);
        }
```

Polybius Cipher Algorithm:

Step 3: Polybius Encryption

```
function polybiusCipher(str) {
    var polybius = '';
    for (var i = 0; i < str.length; i++) {
        var charCode = str.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            polybius += String.fromCharCode((charCode - 65) / 5 + 65) + String.fromCh
        } else if (charCode >= 97 && charCode <= 122) {
            polybius += String.fromCharCode((charCode - 97) / 5 + 97) + String.fromCh
        }
    }
    return polybius;
}
```

Hybrid System Algorithm:

Step 4: Vigenère-Polybius Hybrid Encryption

```
function polybiusCipherHybrid(output_str) {
    var polybius = '';
    for (var i = 0; i < output_str.length; i++) {
        var charCode = output_str.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            polybius += String.fromCharCode((charCode - 65) / 5 + 65) + String.fromCh
        } else if (charCode >= 97 && charCode <= 122) {
            polybius += String.fromCharCode((charCode - 97) / 5 + 97) + String.fromCh
        }
    }
    return polybius;
}
```

Main Function:

Step 5: Integration and Output Display

```
function calculateCipher() {
    var vignere = vigenereCipher(key, plaintext, 1);
    var polybius = polybiusCipher(plaintext);
    var hybrid = polybiusCipherHybrid(vignere);

    document.getElementById('results').innerHTML = 'Vigenere: ' + vignere + '<br>Poly
}
```

These steps outline the process of obtaining input, encrypting with the Vigenère and Polybius ciphers, creating a hybrid encryption, and displaying the results. The algorithms follow the principles of each cipher and are structured for ease of understanding and implementation.

3.Final Output

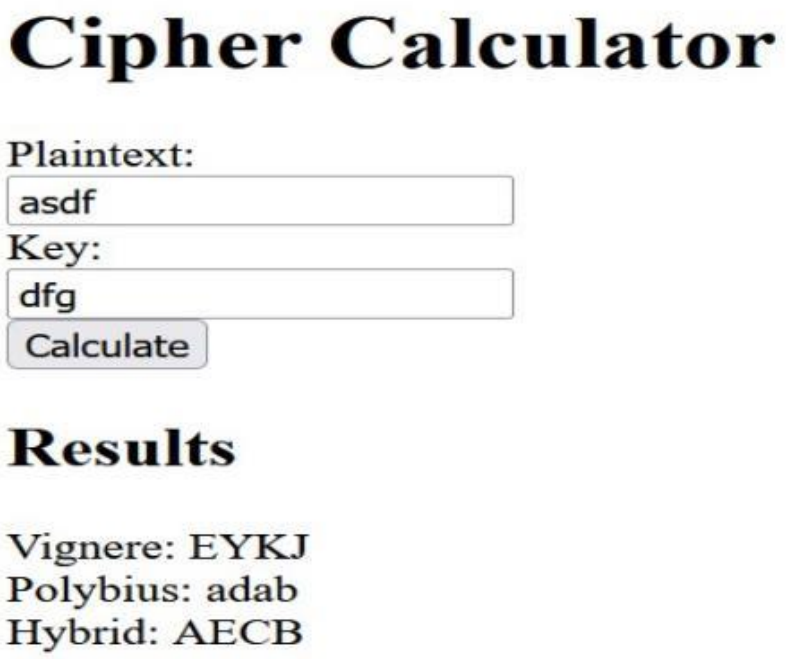

Fig.2: Output of hybrid ciphers.

EXPERIMENTAL SETUP

1. Hardware:

Hardware	Minimum Requirement
Computer	1. 2.7 Ghz CPU 2. Multi-core processor
Memory (RAM)	4GB minimum.
Hard disk Space	At least 10 GB
Processor	Intel i5 generation or later
Adapter	Wi-fi & Bluetooth External Adapter

2.Software

Software	Minimum Requirement
Software	• Implemented on VS code • Fronted in HTML • Backend python

CHAPTER 4. RESULTS ANALYSIS AND VALIDATION

4.1. Results

Vigen'ere encryption is a well-known encryption, but it has a few flaws. To overcome the limitations of the Vigen'ere cipher, a new technique is presented as an improved variant as a combination of Polybius cipher and Vigen'ere that is significantly more secure against attacks such as Active, passive, Kasiski, and Friedman attacks (attacks).

Because of the usage of product tables for encryption, cryptanalysis, recurrence examination, men in the middle attacks, frequency analysis, fault analysis attacks, design expectation, and brute force attacks on the suggested method are also considerably more difficult.

The altered hybrid combination of the Caesar Cipher and the Vigen'ere Cipher results in a high amount of complexity, scattering, distribution, and confusion in the algorithm that makes them, making it an extraordinarily strong cipher and difficult to break.

Despite the fact that there are various cryptographic techniques, this area still wants genuine attention from the research network for the improvement, refinement, and enhancement of data privacy and security.

The method most frequently used to ensure data security, privacy, confidentiality, and dependability is cryptography. Cryptographic systems known as single classic ciphers are said to be the least complex and most vulnerable due to their smooth system, many restrictions, and ease of usage. Vigenere Cipher is a well-known cipher, although it has a few disadvantages as well. In order to overcome the limitations of the Vigentere cipher, a new method is presented that is an improved version that combines the Vigentere encryption with Polybius cipher and is much more resistant to attacks such as Active, passive, Kasiski, and Friedman assaults (attacks). The usage of product tables for encryption makes cryptanalysis,

recurrence analysis, men in the middle attacks, frequency anal- ysis, fault analysis assaults, design expectation, and brute force attacks on the suggested technique extremely problematic. Because of the tremendous degree of complexity, dispersion, spread, and confusion in the technique used to construct them, the modified hybrid combination of the Caesar and Vigenere ciphers is incredibly strong and difficult to crack. Although there are many different cryptographic techniques, the research network must nevertheless give this area serious study in order to improve, upgrade, and strengthen data security and privacy. Our goal is to validate the suggested methodology in the near future by carrying out message performance analyses and security attacks.

CHAPTER - 6 CONCLUSION AND FUTURE WORK

5.1. Conclusion

Cryptography is the most widely used approach for data security, privacy, secrecy, and reliability. Because of multiple impediments, constraints, and smooth systems, single traditional ciphers are regarded as the least complex and most vulnerable cryptographic techniques.

Vigen'ere encryption is a well-known encryption, but it has a few flaws. To overcome the limitations of the Vigen'ere cipher, a new technique is presented as an improved variant as a combination of Polybius cipher and Vigen'ere that is significantly more secure against attacks such as Active, passive, Kasiski, and Friedman attacks (attacks).

Because of the usage of product tables for encryption, cryptanalysis, recurrence examination, men in the middle attacks, frequency analysis, fault analysis attacks, design expectation, and brute force attacks on the suggested method are also considerably more difficult.

Cryptography is the most widely used approach for data security, privacy, secrecy, and reliability. Because of multiple impediments, constraints, and smooth systems, single traditional ciphers are regarded as the least complex and most vulnerable cryptographic techniques.

Vigen'ere encryption is a well-known encryption, but it has a few flaws. To overcome the limitations of the Vigen'ere cipher, a new technique is presented as an improved variant as a combination of Polybius cipher and Vigen'ere that is significantly more secure against attacks such as Active, passive, Kasiski, and Friedman attacks (attacks).

Because of the usage of product tables for encryption, cryptanalysis, recurrence examination, men in the middle attacks, frequency analysis, fault analysis attacks, design expectation, and brute force attacks on the suggested method are also considerably more difficult.

The altered hybrid combination of the Caesar Cipher and the Vigen'ere Cipher results in a high amount of complexity, scattering, distribution, and confusion in the algorithm that makes them, making it an extraordinarily strong cipher and difficult to break.

Despite the fact that there are various cryptographic techniques, this area still wants genuine study network consideration for the improvement, refinement, and enhancement of data privacy and security.

Our goal in the future is to validate the suggested approach by performing security attacks and message performance analysis.

Implementing a two-layer security system using the Vigenère Cipher and Polybius Cipher involves a systematic integration of these classical cryptographic techniques. By combining their unique strengths and addressing potential vulnerabilities, this approach provides an enhanced level of data protection. Regular key rotation, secure transmission or storage, and vigilant monitoring contribute to the overall effectiveness and resilience of the two-layer security system. This implementation guide serves as a roadmap for organizations seeking to bolster their information security using classical encryption methods in a modern context.

5.2. Future work

The altered hybrid combination of the Caesar Cipher and the Vigen'ere Cipher results in a high amount of complexity, scattering, distribution, and confusion in the algorithm that makes them, making it an extraordinarily strong cipher and difficult to break.

Despite the fact that there are various cryptographic techniques, this area still wants genuine attention from the research network for the improvement, refinement, and enhancement of data privacy and security.

The secure generation, distribution, and maintenance of cryptographic keys is a central difficulty in cryptography. Keys are critical components of encryption and decryption procedures, and if they are hacked, the security of the entire system is jeopardized.

REFERENCES

[1] 2020 International Conference on Computational Performance Eval- uation (ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020.

[2] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3] International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1 ISSN 2229-5518.

[4] Originally published in IEEE Communications Magazine November 1978 — Volume 16, Number 6.

[5] K. Jakimoski, "Security techniques for data protection in cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.

[6] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigen'ere cipher for data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016. P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

[7] A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigen´ere and caesar cipher techniques for secure com- munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016.

[8] 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.

[9] 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.

[10]A. A. Soofi, I. Riaz, and U. Rasheed, “An enhanced vigenere cipher for ` data security,” Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.

[11]P. Kumar and S. B. Rana, “Development of modified aes algorithm for data security,” Optik, vol. 127, no. 4,
pp. 2341–2345, 2016.