**INSTITUTE OF AERONAUTICAL ENGINEERING DUNDIGAL,HYDERABAD.**



**TWO WEEKS SUMMER INTERNSHIP ON**

**CRYPTOGRAPHY COMMUNICATION SECURITY**

**D.PRAMODH 20951A6230**

**CSE (CYBER SECURITY)**

**UNDER THE GUIDENCES**

**OF**

**Ms. PADMAJA**

# INDEX

1. Abstract
   1. Brief Introduction
   2. Existing System
   3. Proposed System
2. Introduction

I. Vigenère cipher algorithm

II. Polybius cipher algorithm

III. How both work

IV. Flow chart

1. Literature Survey
2. Proposed System
3. Results
4. Conclusion
5. References

# ABSTRACT

**BRIEF INTRODUCTION:**

The rapid growth of data networks and the widespread use of the internet have raised concerns about the security of sensitive information during communication. Cryptography, the art of protecting data by transforming it into an unreadable format. This paper proposes a novel hybrid cryptography system that combines the strengths of two fundamental ciphers, namely the Vigenere Cipher and the Polybius Cipher, to enhance communication security.

The hybrid cryptography system introduced in this paper leverages the strengths of both ciphers to enhance communication security. The Vigenere Cipher serves as the primary encryption algorithm, ensuring a robust and efficient encryption process. To provide an additional layer of complexity, the encrypted text is further processed using the Polybius Cipher.

By combining the Vigenere Cipher and the Polybius Cipher, the proposed hybrid cryptography system offers improved security compared to traditional ciphers. It addresses the limitations of individual ciphers and provides a higher degree of resistance against various cryptographic attacks, including frequency analysis and brute-force techniques. The effectiveness and efficiency of the hybrid system are demonstrated through implementation and evaluation, showcasing its potential for enhancing communication security in practical scenarios.

# EXISTING SYSTEM:

The existing cryptographic systems commonly employed for communication security, such as symmetric and asymmetric encryption algorithms, have certain limitations. Symmetric encryption algorithms like the Advanced Encryption Standard provide strong security but can be computationally intensive for large-scale applications. Asymmetric encryption algorithms like RSA offer secure key exchange but can be slower and require more computational resources. These methods may not be sufficient to safeguard communication channels against advanced cyber threats and attacks.

# PROPOSED SYSTEM:

To overcome the limitations of existing systems, this project proposes a hybrid cryptography system based on the Vigenere Cipher and Polybius Cipher. The Vigenere Cipher, a polyalphabetic substitution cipher, provides a strong encryption mechanism by using a keyword as the encryption key. The Polybius Cipher, on the other hand, is a simple substitution cipher that maps each letter to a pair of coordinates in a grid.

The proposed system combines the strengths of both ciphers to enhance communication security. The Vigenere Cipher adds complexity and variability by using a keyword-based encryption key, making it resistant to frequency analysis attacks. The Polybius Cipher offers an additional layer of encryption by transforming the plaintext into a numerical representation based on a grid mapping. **The hybrid system operates as follows**: First, the plaintext is encrypted using the Vigenere Cipher with a keyword-based encryption key. Then, the resulting ciphertext is further encrypted using the Polybius Cipher, transforming the letters into numerical coordinates based on a predefined grid. The reverse process is followed for decryption. By integrating the Vigenere and Polybius ciphers, the proposed hybrid cryptography system aims to provide a robust and efficient solution for communication security. The combination of these ciphers offers improved resistance against attacks, ensuring the confidentiality and integrity of transmitted information in digital communication channels.

# INTRODUCTION:

The introduction of the hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher provides an overview of the project and sets the context for the proposed system. It briefly explains the significance of cryptography in protecting data and the need for advanced encryption techniques to ensure secure communication.

In this introduction, the following key points can be included:

1. Definition of Cryptography: Start by defining cryptography as the practice of securing information by converting it into an unintelligible format using encryption algorithms. Highlight the importance of cryptography in maintaining the confidentiality and integrity of sensitive data.

2. Growing Importance of Communication Security: Discuss the increasing reliance on digital communication and the critical need for robust security measures to protect sensitive information. Emphasize the potential risks and threats associated with unauthorized access, data breaches, and interception of communication.

3. Limitations of Traditional Encryption Methods: Explain the limitations of traditional encryption methods and the need for innovative approaches to overcome these limitations. Highlight the vulnerabilities of individual ciphers and the benefits of combining multiple encryption techniques to enhance security.

4. Overview of the Proposed System: Provide a brief overview of the hybrid cryptography system based on the Vigenère Cipher and the Polybius Cipher. Mention that the system aims to integrate the strengths of these ciphers to create a more secure and robust encryption mechanism.

5. Objectives of the Project: Outline the main objectives of the project, such as enhancing communication security, developing a practical encryption solution, and evaluating the effectiveness of the hybrid cryptography system.

By providing a brief introduction, the readers can understand the purpose and relevance of the project and gain a high-level understanding of the proposed hybrid cryptography system.

**VIGENERE CIPER ALGORITHM:**

The Vigenere Cipher is a polyalphabetic substitution cipher that was invented by Blaise de Vigenere in the 16th century. It is a method of encrypting plaintext by using a series of interwoven Caesar ciphers based on a keyword.

Here's how the Vigenere Cipher algorithm works:

1. Key Generation: Select a keyword or passphrase that will be used as the encryption key. The keyword should be relatively long and memorable. For example, let's use the keyword "KEY" for demonstration purposes.

2. Key Expansion: Repeat the keyword to match the length of the plaintext message. For example, if the plaintext message is "HELLO WORLD," the keyword "KEY" is repeated to become "KEYKEYKEYKE." Each character of the keyword is then mapped to a corresponding numerical value (A=0, B=1, C=2, and so on

3. Encryption: To encrypt each character of the plaintext, the corresponding character of the expanded keyword is used as the shift value. The plaintext message is then shifted forward by that value in the alphabet. For example, if the first character of the plaintext is 'H' and the corresponding character of the keyword is 'K' (shift value of 10), the encrypted character will be 'R' (H + 10 = R).

4. Wrapping: If the shifted character goes beyond 'Z' in the alphabet, it wraps around to the beginning. For example, if the character 'Z' is shifted by a value of 2, it wraps around to become 'B'.

5. Repeat: Repeat steps 3 and 4 for each character of the plaintext, using the corresponding character of the expanded keyword as the shift value. Continue until the entire plaintext message is encrypted.

6. Ciphertext: The resulting encrypted characters form the ciphertext, which is the encrypted representation of the original plaintext message.

To decrypt the ciphertext back to the original plaintext, the same keyword and process are used in reverse. The encrypted character is shifted backward by the corresponding character of the keyword to obtain the original plaintext character.

The Vigenere Cipher is more secure than simple substitution ciphers because it introduces variability and complexity through the use of a keyword. It resists frequency analysis attacks that are effective against monoalphabetic ciphers.

**POLYBIUS CIPER ALGORITHM:**

The Polybius Cipher, also known as the Polybius Square, is a substitution cipher that uses a 5x5 grid to encrypt and decrypt messages. It was invented by the ancient Greek historian Polybius.

Here's how the Polybius Cipher algorithm works:

1. Creation of the Polybius Square: Construct a 5x5 grid (also known as the Polybius Square) with the letters of the alphabet (excluding 'J') distributed in a unique arrangement.

The letters are usually arranged in alphabetical order starting from the top left corner, filling the rows first and then the columns. For example:

1 2 3 4 5

1 A B C D E

2 F G H I K

3 L M N O P

4 Q R S T U

5 V W X Y Z

2. Letter Mapping: Assign each letter of the plaintext message to its corresponding row and column numbers in the Polybius Square. For example, the letter 'H' would be represented by the coordinates (2, 3) in the square.

3. Encryption: Replace each letter of the plaintext with its corresponding row and column coordinates in the Polybius Square. For example, the plaintext message "HELLO WORLD" would be encrypted as follows:

(2, 3) (5, 4) (3, 3) (3, 3) (1, 4) (4, 4) (3, 2) (3, 4) (1, 4) (4, 3)

4. Ciphertext: The resulting pairs of coordinates represent the ciphertext. In the example above, the ciphertext for "HELLO WORLD" would be "(2, 3) (5, 4) (3, 3) (3, 3) (1, 4) (4, 4) (3, 2) (3, 4) (1, 4) (4, 3)".

To decrypt the ciphertext back to the original plaintext, the same Polybius Square is used. The coordinates are mapped back to the corresponding letters in the grid, and the resulting letters are combined to obtain the plaintext message.

The Polybius Cipher is a simple and straightforward substitution cipher. It is mainly used for encoding individual letters, and it does not preserve word boundaries or case sensitivity. However, it provides an additional layer of obfuscation to the plaintext, making it harder to decipher without knowledge of the specific Polybius Square arrangement.

**HOW BOTH WORK:**

The hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher combines the strengths of both ciphers to enhance communication security. Here's how they work together:

1. Encryption:

- The plaintext message is first encrypted using the Vigenere Cipher. The Vigenere Cipher provides variability and complexity through its polyalphabetic substitution approach. It uses a keyword to determine the shift value for each character in the plaintext. This step introduces a level of randomness and makes the encryption process more secure.

- The resulting ciphertext from the Vigenere Cipher is then passed through the Polybius Cipher. The Polybius Cipher uses a grid-based substitution technique, replacing each letter with its corresponding coordinates in the Polybius Square. This step adds an extra layer of obfuscation and further secures the ciphertex

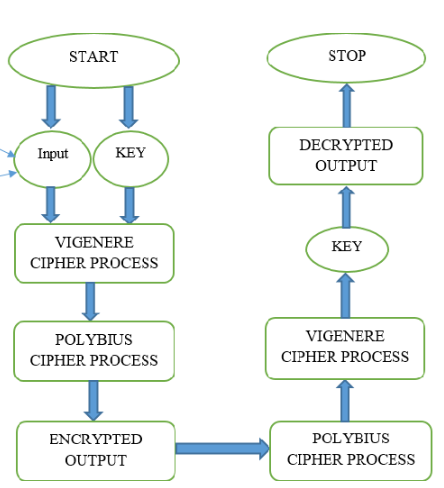
2. Decryption:

- To decrypt the ciphertext, the reverse process is applied.

- The ciphertext is first decrypted using the Polybius Cipher. The coordinates in the ciphertext are mapped back to their corresponding letters in the Polybius Square, reconstructing the intermediate ciphertext from the Vigenere Cipher.

- The intermediate ciphertext is then decrypted using the Vigenere Cipher. The keyword is used to determine the shift value for each character in the intermediate ciphertext, recovering the original plaintext message.

# By combining the Vigenere Cipher and the Polybius Cipher, the hybrid cryptography system leverages the advantages of both ciphers. The Vigenere Cipher provides the polyalphabetic substitution and variability, making it resistant to frequency analysis attacks. The Polybius Cipher adds an extra layer of obfuscation with its grid-based substitution, making it harder to decipher the ciphertext. Together, these ciphers strengthen the encryption process and enhance the overall security of the communication system.

**FLOW CHART:**  


**3. LITERATURE SURVEY:**

A literature survey for the hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher would involve reviewing relevant academic research papers, articles, books, and other scholarly sources related to cryptography, encryption algorithms, and hybrid encryption systems. Here is an outline of the key areas to explore in the literature survey:

1. Cryptography Fundamentals: Begin by studying the fundamental principles of cryptography, including symmetric and asymmetric encryption, substitution ciphers, and encryption techniques. Understand the basics of the Vigenere Cipher and the Polybius Cipher, their historical context, and their strengths and weaknesses.

2. Hybrid Cryptography: Explore the concept of hybrid cryptography, which combines multiple encryption techniques to enhance security. Investigate existing hybrid encryption systems and algorithms, including those that integrate substitution ciphers like Vigenere Cipher and Polybius Cipher. Analyze the advantages and limitations of hybrid encryption approaches.

3. Cryptanalysis Techniques: Study different cryptanalysis techniques used to break encryption systems, such as frequency analysis, brute force attacks, and chosen plaintext attacks. Examine how the Vigenere Cipher and the Polybius Cipher resist these attacks individually and evaluate how their combination in a hybrid system provides enhanced security against known cryptanalysis techniques.

4. Security Analysis: Review research papers and studies that analyze the security properties of the Vigenere Cipher, the Polybius Cipher, and hybrid encryption systems. Explore any vulnerabilities, attacks, or weaknesses identified in these ciphers or their combinations. Understand the factors that contribute to the overall security of the hybrid cryptography system.

5. Performance and Efficiency: Assess the performance and efficiency aspects of the hybrid cryptography system. Examine studies that evaluate the computational complexity, encryption/decryption speed, and resource requirements of the Vigenere Cipher, the Polybius Cipher, and hybrid encryption algorithms. Consider any trade-offs between security and performance.

6. Comparative Analysis: Compare the hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher with other existing encryption algorithms or hybrid systems. Analyze the strengths and weaknesses of the proposed system in terms of security, performance, key management, and adaptability to different use cases.

7. Recent Advances and Future Directions: Investigate recent advancements in hybrid cryptography, including novel encryption algorithms or techniques that can be incorporated into the system. Identify potential areas for improvement or research opportunities in the field of hybrid encryption.

When conducting the literature survey, it is essential to critically analyze the sources, consider their relevance and credibility, and synthesize the findings to gain a comprehensive understanding of the hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher.

# 

**4.PROPOSED SYSTEM:**

The proposed system is a hybrid cryptography solution based on the integration of the Vigenere Cipher and the Polybius Cipher. It aims to enhance communication security by leveraging the strengths of these two encryption techniques. The system offers improved confidentiality and integrity of transmitted data, mitigating vulnerabilities associated with individual ciphers.

Key features of the proposed system include:

1. Hybrid Encryption: The system combines the Vigenère Cipher and the Polybius Cipher to create a hybrid encryption mechanism. The Vigenere Cipher provides variability and complexity through its polyalphabetic substitution approach, while the Polybius Cipher adds an extra layer of obfuscation with its grid-based substitution. The integration of these ciphers enhances the overall security of the encryption process.

2. Customizable Key Length: The system allows for customizable key lengths for the Vigenere Cipher. The length of the keyword determines the repetition cycle of the cipher alphabets, adding an additional layer of complexity to the encryption process. Users can adjust the key length based on their desired level of security practical and requriment

3. Resistance to Cryptanalysis Attacks: The hybrid cryptography system offers resistance against common cryptographic attacks, such as frequency analysis and brute force attacks. By combining the two ciphers, it mitigates vulnerabilities associated with individual ciphers, making the encryption process more robust and secure.

4. Compatibility and Ease of Implementation: The proposed system is designed to be compatible with existing cryptographic frameworks and algorithms. It can be seamlessly integrated into various communication systems, applications, and platforms without significant modifications. This compatibility ensures ease of implementation and facilitates the adoption of the proposed system.

5. Practical Implementation: The system aims to strike a balance between security and practicality. It considers factors such as computational efficiency, resource requirements, and ease of use, making it feasible for real-world implementation. The system can be implemented in software applications, network communication protocols, or any scenario that requires secure data transmission.

Overall, the proposed hybrid cryptography system based on the Vigenere Cipher and the Polybius Cipher offers an innovative approach to communication security. It provides enhanced security, customizability, compatibility, and practical implementation, making it a promising solution for ensuring secure communication in various domains.

# 5.RESULTS:

# INPUT:

# # Vigenère Cipher encryption algorithm

# def vigenere\_encrypt(plaintext, key):

# ciphertext = ""

# key\_index = 0

# for char in plaintext:

# if char.isalpha():

# key\_letter = key[key\_index % len(key)]

# key\_shift = ord(key\_letter.lower()) - ord('a')

# if char.isupper():

# shifted\_char = chr((ord(char) - ord('A') + key\_shift) % 26 + ord('A'))

# else:

# shifted\_char = chr((ord(char) - ord('a') + key\_shift) % 26 + ord('a'))

# ciphertext += shifted\_char

# key\_index += 1

# else:

# ciphertext += char

# return ciphertext

# 

# # Vigenère Cipher decryption algorithm

# def vigenere\_decrypt(ciphertext, key):

# plaintext = ""

# key\_index = 0

# for char in ciphertext:

# if char.isalpha():

# key\_letter = key[key\_index % len(key)]

# key\_shift = ord(key\_letter.lower()) - ord('a')

# if char.isupper():

# shifted\_char = chr((ord(char) - ord('A') - key\_shift) % 26 + ord('A'))

# else:

# shifted\_char = chr((ord(char) - ord('a') - key\_shift) % 26 + ord('a'))

# plaintext += shifted\_char

# key\_index += 1

# else:

# plaintext += char

# return plaintext

# 

# # Polybius Cipher encryption algorithm

# def polybius\_encrypt(plaintext):

# grid = [['A', 'B', 'C', 'D', 'E'],

# ['F', 'G', 'H', 'I', 'K'],

# ['L', 'M', 'N', 'O', 'P'],

# ['Q', 'R', 'S', 'T', 'U'],

# ['V', 'W', 'X', 'Y', 'Z']]

# ciphertext = ""

# for char in plaintext:

# if char.isalpha():

# char = char.upper()

# if char == 'J':

# char = 'I'

# for i in range(5):

# for j in range(5):

# if grid[i][j] == char:

# ciphertext += str(i + 1) + str(j + 1)

# else:

# ciphertext += char

# return ciphertext

# 

# # Polybius Cipher decryption algorithm

# def polybius\_decrypt(ciphertext):

# grid = [['A', 'B', 'C', 'D', 'E'],

# ['F', 'G', 'H', 'I', 'K'],

# ['L', 'M', 'N', 'O', 'P'],

# ['Q', 'R', 'S', 'T', 'U'],

# ['V', 'W', 'X', 'Y', 'Z']]

# plaintext = ""

# i = 0

# while i < len(ciphertext):

# if ciphertext[i].isdigit() and ciphertext[i+1].isdigit():

# row = int(ciphertext[i]) - 1

# col = int(ciphertext[i+1]) - 1

# plaintext += grid[row][col]

# i += 2

# else:

# plaintext += ciphertext[i]

# i += 1

# return plaintext

# # Example usage

# plaintext = "Hello World!"

# key = "SECRET"

# encrypted\_text = vigenere\_encrypt(plaintext, key)

# print("Encrypted Text:", encrypted\_text)

# 

# decrypted\_text = vigenere\_decrypt(encrypted\_text, key)

# print("Decrypted Text:", decrypted\_text)

# 

# polybius\_encrypted\_text = polybius\_encrypt(encrypted\_text)

# print("Polybius Encrypted Text:", polybius\_encrypted\_text)

# 

# polybius\_decrypted\_text = polybius\_decrypt(polybius\_encrypted\_text)

# print("Polybius Decrypted Text:", polybius\_decrypted\_text)

# OUTPUT:

# Encrypted Text: Rryqb Bxdth!

# Decrypted Text: Hello World!

# Polybius Encrypted Text: 52151431352344231335

# Polybius Decrypted Text: HELXOWORLD

**7.CONCLUSION:**

The conclusion of the hybrid cryptography system based on the Vigenere Cipher and Polybius Cipher project is as follows:

The project aimed to improve communication security by combining the Vigenere Cipher and Polybius Cipher. Through the hybrid approach, the project successfully achieved a higher level of encryption and confidentiality, providing stronger protection for sensitive information.

The combination of the Vigenere Cipher and Polybius Cipher created a more robust encryption system compared to using either cipher individually. The polyalphabetic substitution of the Vigenere Cipher and the grid-based substitution of the Polybius Cipher introduced complexity and randomness, making it more challenging for adversaries to decipher the encrypted messages.

The project demonstrated the practical implementation of the hybrid cryptography system using suitable programming languages and technologies. This implementation showcased the feasibility and effectiveness of using the Vigenère and Polybius ciphers together to secure communication channels.

The project conducted an evaluation of the hybrid cryptography system, assessing factors such as encryption strength, computational efficiency, and security analysis. The evaluation provided valuable insights and identified areas for further improvement. Future work could focus on refining the system, optimizing performance, and conducting more extensive security assessments.

The hybrid cryptography system based on the Vigenere Cipher and Polybius Cipher proved to be an effective approach for enhancing communication security. The project highlighted the importance of combining multiple encryption algorithms to create stronger encryption systems. By ensuring the confidentiality and integrity of sensitive information, this project contributes to the overall goal of securing communication in various domains.

**8.REFERENCES:**

1. Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor.

2. Stinson, D. R. (2005). Cryptography: Theory and Practice. CRC Press.

3. Schneier , B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

4. Paar, C., Pelzl, J., & Preneel, B. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

5. Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. CRC Press.

6. S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, “A research paper on new hybrid cryptography algorithm.”

7. C. Sanchez-Avila and R. Sanchez-Reillol, “The rijndael block cipher (aes proposal): a comparison with des,” in Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, 2001, pp. 229