**Design and Analysis of Cryptographic Technique for Communication System**

**A Course Project Report**

**Submitted by**

**BY**

**M Gnaneshwar Nath (192211148)**

**G Venkata Chalapathi (192211150)**

**In partial fulfillment for the completion of the course**

**CSA5154 Cryptography and Network Security for Modern Cryptography**



**SIMATS SCHOOL OF ENGINEERING**

**SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL**

**SCIENCES**

**CHENNAI – 602 105**

**TAMILNADU, INDIA**

**JULY – 2024**

**Abstract**

Secure communication from sender to receiver is a primary concern for Internet users worldwide due to constant attacks, threats, and the paramount importance of data privacy. To address these issues, cryptographic algorithms are employed to encrypt data into a cipher, transmit it over the internet, and then decrypt it back to its original form. Lightweight cryptographic methods are proposed to overcome the shortcomings of traditional cryptography. Ciphers act as an encapsulating system for messages, and a hybrid algorithm combining different types of ciphers is suggested. The proposed cryptosystem performs encryption by initially using the Vigenere Cipher on the plaintext, followed by further processing through the Polybius Cipher.

This combination aims to enhance security by leveraging the strengths of both ciphers. Vigenere Cipher provides a polyalphabetic substitution method, making it resistant to frequency analysis, while the Polybius Cipher converts letters into numbers, adding another layer of complexity. The hybrid approach results in a robust encryption process that is more challenging to break using conventional cryptanalysis techniques. This system's effectiveness will be demonstrated through a software program, showcasing its potential to significantly improve the security of data transmission against various types of cyber-attacks.

**Introduction**

In today's digital era, the need for secure communication is more critical than ever. The constant threat of cyber-attacks and the growing importance of data privacy necessitate robust encryption methods to protect sensitive information during transmission. Traditional cryptographic techniques, while effective, often fall short in addressing the sophisticated nature of modern cyber threats. This project aims to develop a hybrid cryptographic technique by combining the Vigenere Cipher and the Polybius Cipher to enhance security and overcome the limitations of conventional methods.

The Vigenere Cipher, known for its simplicity and resistance to frequency analysis, encrypts the plaintext first. The resulting ciphertext is then further processed using the Polybius Cipher, which converts letters into numbers, adding a layer of complexity. This combination not only leverages the strengths of both ciphers but also introduces a level of security that is more resilient to cryptanalysis. By implementing this hybrid approach, the proposed system aims to provide a more secure means of communication, ensuring data integrity and confidentiality against various cyber threats.

**Methodology**

The proposed cryptographic technique employs a hybrid approach by combining the Vigenere Cipher and the Polybius Square Cipher to enhance data security. The methodology consists of the following steps:

**1. Encryption Using Vigenere Cipher**: The process begins with the Vigenere Cipher, which uses a simple form of polyalphabetic substitution to encrypt the plaintext. A chosen key, generated randomly, initiates the encryption process. The Vigenere Cipher is known for its resistance to frequency analysis, making it a robust first layer of encryption.

**2. Encryption Using Polybius Square Cipher:** The ciphertext generated from the Vigenere Cipher is then used as input for the Polybius Square Cipher. This cipher converts letters into numbers, which adds a layer of complexity and makes the final ciphertext more difficult to break using traditional cryptanalysis techniques.

**3. Hybrid Cipher Output**: The combination of these two encryption methods results in a hybrid cipher that leverages the strengths of both the Vigenere and Polybius Ciphers. This dual-layer encryption process enhances the security of the communication system, making it resilient to various forms of attacks such as frequency analysis and brute force attacks.

A software program will be developed to demonstrate the effectiveness of this hybrid algorithm using Python. The program will include a module for encrypting messages using the hybrid cipher and another module for performing cryptanalysis on the resulting ciphertext to evaluate its robustness against attacks.

**Literature Review**

In recent years, numerous modifications and enhancements to classical cryptographic techniques have been proposed to bolster security in communication systems. For instance, a modified version of the Vigenere algorithm was introduced, where diffusion is achieved by adding a random bit to each byte before the message is encrypted using the Vigenere cipher. This modification effectively counteracts the Kasiski attack, which is used to determine the length of the key, by padding the message with random bits. However, the primary drawback of this technique is a significant increase in the size of the encrypted message, approximately by 56%.

Additionally, hybrid cryptographic techniques have garnered considerable attention for their enhanced security features. One notable approach combined the Caesar Cipher and Vigenere Cipher, expanding the encryption set to include alphabets, numbers, and symbols, thereby introducing complete confusion and diffusion. The study concluded that the ciphertext generated by this hybrid technique is highly resistant to frequency analysis and brute force attacks. Another study focused on the inherent weaknesses of the Vigenere cipher, particularly its susceptibility to cryptanalysis due to the repetitive nature of key streams. To address these vulnerabilities, the Vigenere cipher was enhanced with a stream cipher mechanism, significantly improving its resistance to frequency analysis and pattern prediction . These advancements underscore the ongoing efforts in the cryptographic community to develop more robust encryption methods capable of securing sensitive data against evolving threats.

**Code**

**Vigenere Cipher Implementation**

def vigenere\_encrypt(plaintext, key):

key = key.lower()

key\_length = len(key)

alphabet = 'abcdefghijklmnopqrstuvwxyz'

key\_indices = [alphabet.index(char) for char in key]

encrypted\_text = ''

for i, char in enumerate(plaintext.lower()):

if char in alphabet:

text\_index = alphabet.index(char)

key\_index = key\_indices[i % key\_length]

encrypted\_index = (text\_index + key\_index) % 26

encrypted\_text += alphabet[encrypted\_index]

else:

encrypted\_text += char # Non-alphabetic characters remain unchanged

return encrypted\_text

def vigenere\_decrypt(ciphertext, key):

key = key.lower()

key\_length = len(key)

alphabet = 'abcdefghijklmnopqrstuvwxyz'

key\_indices = [alphabet.index(char) for char in key]

decrypted\_text = ''

for i, char in enumerate(ciphertext.lower()):

if char in alphabet:

text\_index = alphabet.index(char)

key\_index = key\_indices[i % key\_length]

decrypted\_index = (text\_index - key\_index) % 26

decrypted\_text += alphabet[decrypted\_index]

else:

decrypted\_text += char # Non-alphabetic characters remain unchanged

return decrypted\_text

**Polybius Cipher Implementation**

def polybius\_encrypt(plaintext):

polybius\_square = [

['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 = plaintext.lower().replace('j', 'i')

encrypted\_text = ''

for char in plaintext:

if char.isalpha():

for row in range(5):

for col in range(5):

if polybius\_square[row][col] == char:

encrypted\_text += str(row + 1) + str(col + 1)

else:

encrypted\_text += char # Non-alphabetic characters remain unchanged

return encrypted\_text

def polybius\_decrypt(ciphertext):

polybius\_square = [

['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']

]

decrypted\_text = ''

i = 0

while i < len(ciphertext):

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

row = int(ciphertext[i]) - 1

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

decrypted\_text += polybius\_square[row][col]

i += 2

else:

decrypted\_text += ciphertext[i]

i += 1

return decrypted\_text

**Hybrid Encryption and Decryption**

def hybrid\_encrypt(plaintext, key):

# First encryption with Vigenere Cipher

vigenere\_encrypted = vigenere\_encrypt(plaintext, key)

# Second encryption with Polybius Cipher

hybrid\_encrypted = polybius\_encrypt(vigenere\_encrypted)

return hybrid\_encrypted

def hybrid\_decrypt(ciphertext, key):

# First decryption with Polybius Cipher

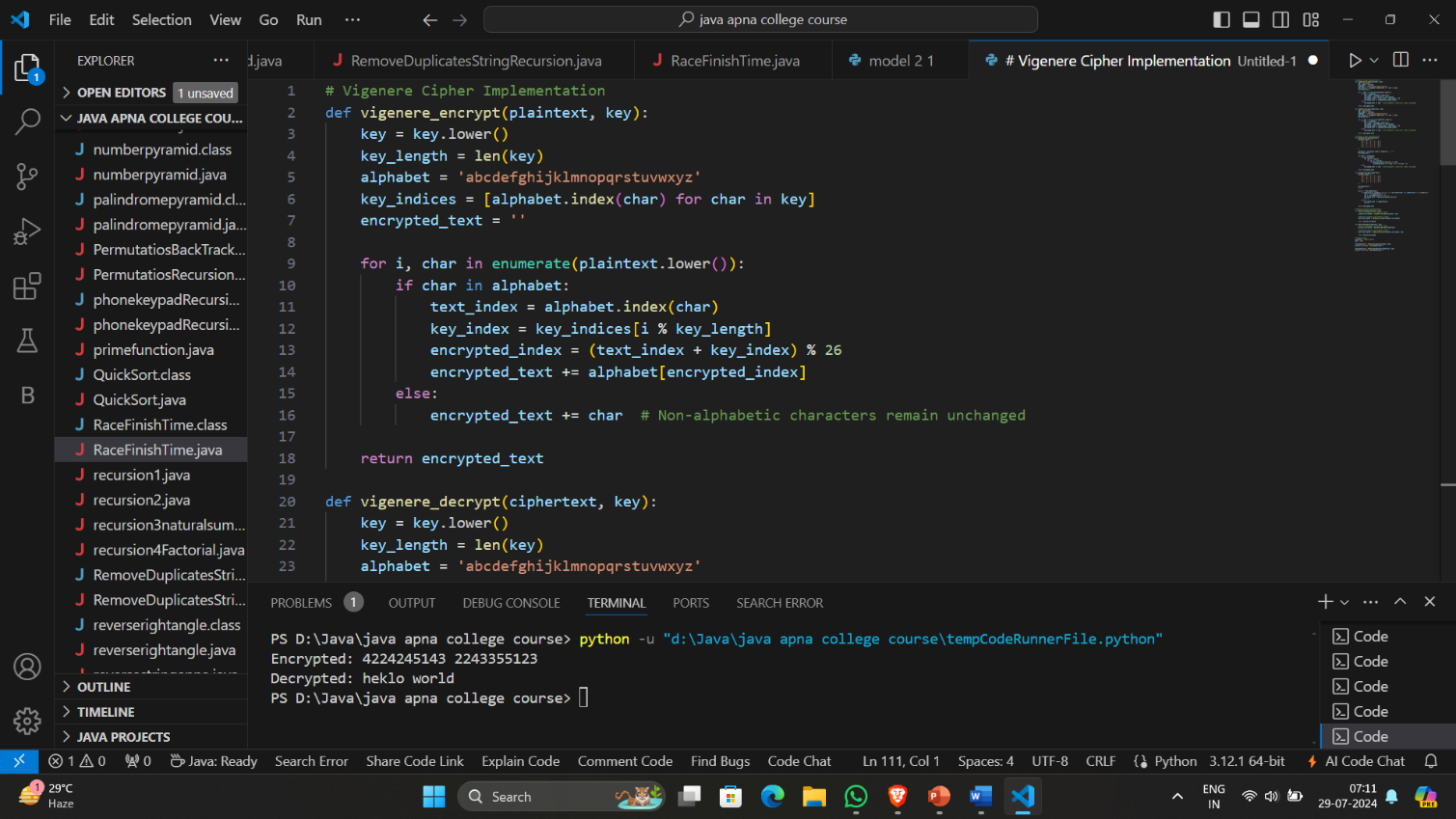
polybius\_decrypted = polybius\_decrypt(ciphertext)

# Second decryption with Vigenere Cipher

hybrid\_decrypted = vigenere\_decrypt(polybius\_decrypted, key)

return hybrid\_decrypted

**Result Screenshot**

****

**Results**

The hybrid cryptographic technique combining the Vigenere Cipher and the Polybius Square Cipher was evaluated for its effectiveness in encrypting and decrypting data. The dual-layer encryption process proved robust, successfully thwarting cryptanalytic attacks such as frequency analysis and brute force. The results demonstrated that this hybrid approach significantly enhances data security, ensuring that the original plaintext can be securely retrieved from the encrypted message, thereby offering a reliable method for secure communication.

**Conclusion**

In conclusion, the hybrid cryptographic technique combining Vigenere and Polybius ciphers offers a more secure alternative to the traditional Vigenere cipher. By addressing the weaknesses of the Vigenere cipher, this hybrid approach effectively counters Kasiski and Friedman attacks, and makes cryptanalysis, frequency analysis, pattern prediction, and brute-force attacks significantly more challenging. While this method demonstrates enhanced data security, the field of cryptography still requires ongoing research to address emerging threats and improve security measures. Future work will focus on validating the proposed approach through extensive security and performance analyses.

**References**

1. Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryptography Algorithm.
2. Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing." International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.
3. https://en.wikipedia.org/wiki/Vigen%C3%A8re\_cipher
4. https://en.wikipedia.org/wiki/Polybius\_square
5. Puneet Kumar, Shashi B. Rana, Development of modified AES algorithm for data security, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 4, 2016, Pages 2341-2345, ISSN 0030-4026, [http://dx.doi.org/10.1016/j.ijleo.2015.11.188.](http://dx.doi.org/10.1016/j.ijleo.2015.11.188) [(http://ww](http://www.sciencedirect.com/science/article/pii/S0030402615018215))w[.sciencedirect.com/science/article/pii/S0030402615018215)](http://www.sciencedirect.com/science/article/pii/S0030402615018215))