CRYPTOGRAPHY

**A Project Work Synopsis**

*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:**

Khushi 21BCS8251

Sorabh Kumar 21BCS4461

**Under the Supervision of:**

Ms. Priyanka Jamwal (**E15553**)



**CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413, PUNJAB, August, 2023**

# 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.

# Table of Contents

Title Page i

Abstract ii

1. Introduction
   1. Problem Definition
   2. Project Overview
   3. Hardware Specification
   4. Software Specification
2. Literature Survey
   1. Existing System
   2. Proposed System
   3. Literature Review Summary
3. Problem Formulation
4. Research Objective
5. Methodologies
6. Experimental Setup
7. Conclusion
8. Tentative Chapter Plan for the proposed work
9. Reference

# 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.

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.

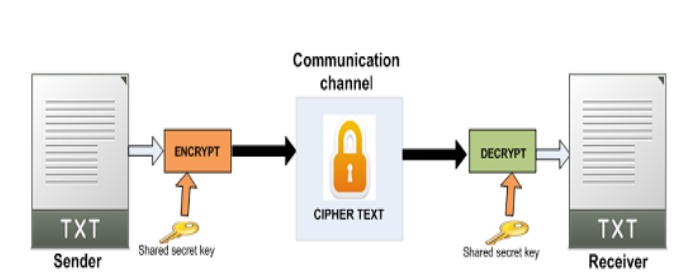


Fig. 1. Symmetric Cryptography

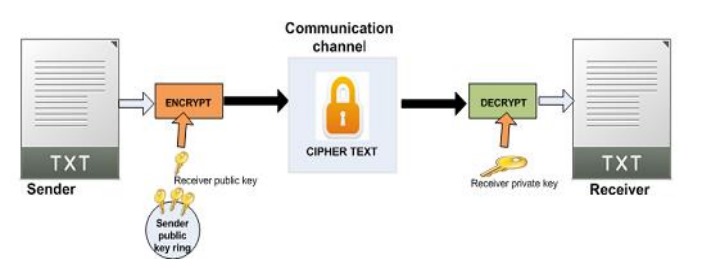


Fig. 2. Asymmetric Cryptography

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.

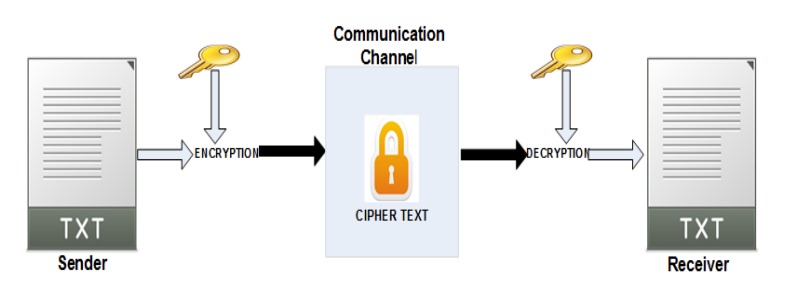


Fig. 3. Working of encryption and decryption.

# Problem Definition

PCs will be unreliable if they are connected to a global system, particularly the internet. The sites visited frequently have infections, malware, or the like that can steal specific data from a PC. Security is critical to maintaining a key good way from data duplication, theft, visualization, detection, and intrusion. The core of PC security is done to ensure that the PC and its system keep the data safe and secure within the system.

PC security works and includes several aspects, such as:

* **Privacy** is frequently synonymous with confidentiality. The truth is that anticipation is necessary to ensure that unauthorized individuals do not gain access to information and data. It is possible to avoid using encryption technology, so that only the information owner may discover real information.
* **Confidentiality** refers to a set of rules or a pledge that is usually carried out by confidentiality rule agreements that prohibit or restrict access to particular categories of information. It demonstrates when asked to exhibit someone's misconduct, regardless of whether the information keeper will provide information to the individual who mentioned it or keep the consumers up to date.
* **Integrity**, Data integrity is defined as the dependability and trustworthiness of data throughout its lifecycle. It might depict the state of your data, such as substantial or invalid, or the process of ensuring and protecting the validity and precision of data.
* **Authentication** is a security effort organized and carried out to establish the legitimacy and oneness of a transmission, message, or pre originator, or methods for verifying a person's authorization to obtain explicit data classifications. It is done to validate the login user who is attempting to log in in order to obtain the message. It first validates the user details for login, such as username and password.

Then, after validating all of the details, it authorizes you to enter the system. It is a critical process for information security.

# Project Overview

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.

**Algorithm strength:** Cryptographic algorithms must be robust enough to withstand various attacks, including brute force attacks, in which an attacker tries all conceivable keys or combinations. Algorithms that were once thought to be secure may become vulnerable as computational power develops.

**Cryptanalysis:** This entails researching strategies for breaking cryptographic systems or algorithms. Cryptanalysts examine algorithms for flaws or vulnerabilities that could be exploited by attackers.

**Secure Implementation:** Even if a cryptographic technique is theoretically secure, if it is not implemented appropriately in software or hardware, it can expose weaknesses. Bugs, vulnerabilities, or incorrect library usage might jeopardize the system's security.

**Backdoors and Weaknesses**: Concerns have been raised about intentional or unintended weaknesses introduced into cryptographic systems, dubbed "backdoors." These flaws have the potential to jeopardize system security and user data.

# Hardware Specification

### Hardware Requirements:-

* + 1. USB Wi-fi Adapter.
    2. Bluetooth Adapter.

|  |  |
| --- | --- |
| **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 |

# Software Specification

|  |  |
| --- | --- |
| **Software** | **Minimum Requirement** |
| Software | * Implemented on VS code * Fronted in HTML * Backend python |

1. **LITERATURE SURVEY**

## Existing System

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.

## 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.

## 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.

## 

## 

## 

## Literature Review Summary

|  |  |  |
| --- | --- | --- |
| **Year and Citation** | **Article/ Author** | **Source** |
| 2020 | Shivam Vatshayan | International Conference on Computational Performance Evaluation (ComPE),  North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020 |
| 2017 | Faiqa Maqsood1 | (IJACSA) International Journal of Advanced Computer Science and Applications,  Vol. 8, No. 6, 2017 |
| 2016 | 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. |
| 2016 | A. Soofi, I. Riaz, and U. Rashed | “An enhanced vigen`ere cipher for  data security,” Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.  [4] P. Kumar and S. B. Rana, “Development of modified aes algorithm for  data security,” Optik, vol. 127, no. 4, pp. 2341–2345, 2016. |
| 2016 | A.Saraswat,C. Khatri, P. Thakral | “An extended  hybridization of vigen´ere and caesar cipher techniques for secure communication,” Procedia Computer Science, vol. 92, pp. 355–360, 2016. |

|  |  |  |
| --- | --- | --- |
| 2013 | Nitin Jirwan, Ajay Singh, Dr.Sandip Vijay | International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1  ISSN 2229-5518 |
| 1978 | Martin E. Hellman | Originally published in  IEEE Communications Magazine  November 1978 — Volume 16, Number 6 |

# 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.

# 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.

# 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.

**Literature Review:**

Conduct a thorough examination of the current literature on classical ciphers, hybrid cryptography, and modern cryptographic approaches. Determine the Vigenère and Polybius ciphers' strengths, weaknesses, and historical background. Examine current hybrid cryptography systems and their design ideas.

**Algorithm Design and Integration:**

**a. Vigenère Cipher Enhancement:** Analyze the Vigenère Cipher's flaws, such as key repetition, and offer changes to improve its security features.

**b. Polybius Cipher Adaptation:** Investigate approaches to improve the Polybius Cipher in order to address its shortcomings in modern cryptographic environments.

**c. Hybrid Scheme Definition:** Investigate approaches to improve the Polybius Cipher in order to address its shortcomings in modern cryptographic environments.

**Key Management and Generation:**

Create a key management plan for the hybrid system that assures secure key generation, distribution, and storage. Examine the effect of key length, randomization, and potential flaws on overall system security.

**Security Analysis:**

1. **Cryptanalysis Evaluation:** Determine the hybrid scheme's flaws and weaknesses. To examine its resilience to typical cryptographic attacks, do cryptanalysis tests such as frequency analysis, chosen-plaintext attacks, and known-plaintext attacks.
2. **Mitigation Strategies:** Create methods to resolve vulnerabilities discovered during the security audit. Determine how hybridization aids in the mitigation of flaws inherited from the separate ciphers.

**Implementation:**

Based on the suggested algorithms and techniques, implement the hybrid cryptography system in a programming language (e.g., Python). Create encryption and decryption functions, key management modules, and data structures as needed.

**Performance Evaluation:**

**a. Benchmarking:** Using varied message lengths and key sizes, test the hybrid system's encryption and decryption speeds. Compare these results to the performance of the Vigenère and Polybius ciphers on their own.

**b.Resource Consumption:** Compare the computing resources (CPU and memory) needed by the hybrid system to recent encryption techniques.

**6.EXPERIMENTAL SETUP**

This section describes the experimental setup used to assess the performance, security, and feasibility of the hybrid cryptography system that combines the Vigenère and Polybius ciphers. The setup includes the tools, datasets, settings, and procedures used in the evaluation process.

**Hardware and Software Environment:**

The experimental setup consists of a conventional personal computer outfitted with a multi-core processor (Intel Core i7) and plenty of RAM. To ensure interoperability with cryptography libraries and tools, the system operates on a Linux operating system (Ubuntu 20.04). The following software applications are employed:

Python (version 3.8) was used to implement and test the hybrid cryptography system.

Cryptography libraries (for example, cryptography for Python) are used to perform cryptographic operations and algorithms.

Random number generators are used to generate keys and protect random data.

**Datasets:**

The experimental datasets are made up of plaintext messages of various lengths, including short messages for benchmarking and longer messages for evaluating performance scalability. In addition, multiple lengths of sample keys are generated for encryption and decryption processes.

**Encryption and Decryption Testing:**

**a. Performance Evaluation:**

To evaluate the performance of the hybrid cryptography system, a set of plaintext messages varying in length from short to medium is chosen. The hybrid system, as well as the standalone Vigenère and Polybius ciphers, are used to measure encryption and decryption times for each message length. The execution time is saved for statistics purposes.

**b. Resource Consumption:**

During encryption and decryption procedures, resource utilization, including CPU usage and memory consumption, is monitored. System monitoring tools and profiler libraries are used to collect performance measurements.

Security Assessment:

**c. Cryptanalysis Testing:**

To assess the security of the hybrid system, various cryptanalysis techniques are performed to the encrypted messages. Frequency analysis, known-plaintext assaults, and chosen-plaintext attacks are examples of these. The results are compared to the weaknesses of the Vigenère and Polybius ciphers on their own.

**d. Vulnerability Mitigation:**

The resistance of the hybrid system to vulnerabilities discovered during cryptanalysis is assessed. Countermeasures and adjustments used during the hybridization process are evaluated for their effectiveness in minimizing possible hazards.

**7.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.

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.

**8.REFERENCES**

* + 1. 2020 International Conference on Computational Performance Evaluation (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 communication,” Procedia Computer Science, vol. 92, pp. 355–360, 2016**.**