IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Cryptographic Technique For Communication System

Dr. Suresh L

Rishabh Raj Rohit Kumar Prashant Sahu Jha Rahul

RajeevStudents,Information Science Engineering
Rns Institute Of
Technology
Bangalore,India

Abstract—Cryptography, derived from Greek, is the art of protecting data by transforming it into an obfuscated and unreadable format. This field blends mathematics and computer science. The internet’s rapid expansion has increased public awareness of information security issues. Online security is very important, yet many apps are created without taking the three main goals of data security into account: secrecy, authentication, and integrity. As our daily activities become increasingly reliant on data networks, the importance of understanding these security issues and challenges will also rise. To prevent unauthorized access to data, cryptography is essential.

This paper introduces a novel hybrid security cipher by merg- ing the three most crucial ciphers: Gronsfeld, Polybius,Vigenѐre, and steganography. This hybrid encryption cipher offers signifi- cantly enhanced security compared to classic ciphers.

I. INTRODUCTION

In today’s technologically driven world, the internet reigns supreme as the preferred channel for information exchange, with emails and chats becoming ubiquitous communication tools. This ubiquitous connectivity offers unparalleled con- venience, speed, and accuracy in data exchange. However, a sinister side lurks beneath the surface: the inherent vul- nerability of data transmitted over the internet. Personal and sensitive information can be compromised or hacked through various means, posing a significant threat to privacy and security. Therefore, prioritizing data security throughout the transmission process becomes critical.

In this context, cryptography emerges as a vital tool, playing a pivotal role in safeguarding data within open networks. This ancient and secure method extends beyond mere data confidentiality, encompassing a broader the spectrum of ob- jectives known as the CIA triad: Confidentiality, Integrity, andAuthentication.

Confidentiality: This fundamental idea makes sure that transmitted data may only be accessed and retrieved by authorized users who possess the proper key. Cryptography serves as a barrier, keeping private information hidden from prying eyes by Securing clear text communications into an unintelligible format known as ciphertext.

Integrity: This crucial aspect ensures that transmitted data remains unaltered during its journey. Cryptographic hashing algorithms act as vigilant watchdogs, detecting any unau- thorized modifications and guaranteeing the authenticity and validity of information.

Authentication: This vital process verifies the sender’s identity in online interactions, fostering trust and preventing fraudulent activities. Digital signatures, a powerful tool within cryptography, empower the recipient to confirm the sender’s identity and assure that messages haven’t been tampered with in transit.

There are a couple of primary types of

cryptography, each with special advantages and disadvantages: 1. Symmetric Key Encryption: This approach is straightforward and effective because it only requires a single key for encryption and decryption. The safe dispersal and administration of this shared key, however, present a significant difficulty since any key compromise compromises security of all encrypted data. 2. Asymmetric Key Encryption: The public and the private key that are mathematically connected are use in this strategy. While private key is kept a closely-guarded secret and is known only to the intended recipient, the public key is easily available. This method increases security but adds computing complexity because it involves intricate mathematical compu- tations.

II. BACKGROUND AND LITERATURE SURVEY

In today's technology landscape, there is an indisputable preference for using the internet as the major medium for global information transmission. Email and chat platforms are just two examples of the many communication channels that make data transportation across the Internet quick, easy, and precise. However, a significant issue arises with regard to the security risks associated with transmitting confidential data.

The planning phase of a survey is crucial before its execu- tion. A fundamental component of this planning is the liter- ature review, which serves as a starting point for developing project ideas into concepts and, ultimately, theories.

Security assumes a critical role in securing public networks, and cryptography stands as an indispensable tool in this realm. Dating back to ancient times, cryptography serves as a robust method for protecting information in public networks. Its objectives encompass more than just confidentiality; cryp- tography addresses data integrity, authentication, and non-repudiation.

As a systematic technique, cryptography conceals informa- tion during communication, ensuring that only the intended recipient can access the data. The rising need for safeguarded data transmission channels has grown significantly as technol-ogy progresses.

Encryption, a systematic procedure, transforms plain text messages into ciphertext. This procedure involves an encryp- tion algorithm as well as a key to convert the plain text into an encrypted form. At the sender's end in a cryptographic system, encryption precedes message transmission to the receiver.

Contrarily, decryption reverses the encryption process by converting encrypted ciphertext back into plaintext.This action occurs at the receiver's end and necessitates a deciphering algorithm and a cryptographic key. Cryptography can be clas- sified into two key categories: Asymmetric Key and Symmetric Key Encryption, based on the key's role in converting originaltext into encrypted text.

Symmetric key encryption employs a sole key for both encrypting and decrypting, offering simplicity and potency, yet the distribution of this key presents a notable challenge. Conversely, asymmetric key encryption involves mathemati- cally related keys—the Public Key and the Private Key. While the public key is available to all, data encrypted using a user's public key can only be decrypted by their specific private key, whether they are the sender or the receiver.

III. THEORIES

PCs may become unreliable when connected to global networks, particularly the internet [2]. Many websites which are frequently visited are infected with viruses, malware, or similar threats that can also compromise personal data stored on a computer. To avoid data replication, theft, visualization, detection, and intrusion, maintaining security is crucial. The essence of PC security lies in ensuring the safety and protec- tion of data within the computer system

PC security encompasses various aspects, including:

1) **Privacy:** Information confidentiality is involved. The main goal is to keep critical information out of the hands of unauthorized people. To prevent this, encryption technology can be used, giving access to the actual data only to the data owner.

2) **Confidentiality:** It entails a set of rule and agreements that limit access or can impose restrictions on specific type of information. When required to provide evidence of someone's wrongdoing, the data custodian decides whether to disclose the requested information or maintain client confidentiality.

3) **Non-repudiation:** It describes the capacity to guarantee that the people engaged in a conversation

or agreement cannot dispute the legitimacy of their signature on the document or the transfer of the message that they have started. To deny is to disown. Over the time, attempts have been made to render repudiation unfeasible under specific conditions. Sending a letter through registered mail, for instance, guarantees that the recipient cannot dispute receiving it. Comparably, witnesses are frequently required to sign legal documents in order to avoid signature withholds. Given that only one individual can establish a digital signature, it was also used on the Internet to prevent future denials of supplying a signature in addition to confirming that a communication or document has received an electronic signature from the intended recipient.

4) **Integrity:** Data integrity refers to the reliability and accuracy of data throughout its lifecycle. It ensures that data remains valid and free from manipulation or corruption.

5) **Authentication:** It is a security measure designed to establish the validity and identity of transmission, message, or originator, or to verify a person's authorization to access specific categories of information. Authentication is performed to verify the credentials of a user attempting to log in before granting access to the system. It is critical process for infor- mation protection.

6) **Availability:** It ensure that the systems, applications, and the data is accessible to users when they require them. The most frequent attack that can affects availability is a denial of service, where an attacker disrupts access to data, systems, devices, or other network resources. In an internal vehicle network, a denial of service could lead to an Electronic Control Unit (ECU) being unable to gain access to the necessary data, rendering it non operational or even endangering the system. To avoid availability issues, redundancy paths, failover procedures, and intrusion prevention systems that can monitor network traffic patterns and detect abnormalities should be included in the design phase.

IV. METHODOLOGY AND IMPLEMENTATION

Conduct Research on Drug Databases and Their Effects:

Begin the process by delving into comprehensive research regarding various drugs and their effects. Utilize a range of medical databases, resources, and explore drug-related news articles and reports while maintaining anonymity.

Create a User Interface: Develop a user-friendly interface (UI) for the application using Java. Prioritize a simple and intuitive design that enables users to report drug use anony- mously with ease.

Design the Database: Construct a database system intendedto store collected data from the application. This databaseshould encompass essential details such as drug type, quantityused, and any associated side effects experienced by the user.Establish a Reporting System: Formulate a secure and encrypted reporting system that facilitates anonymous usersubmissions. Ensure the system collects only necessary data for efficient functionality.

Test and Launch the App: Thoroughly test the application to validate proper functioning of all features. Upon confirmation of smooth operations, proceed with the app's launch, making it accessible to users. Maintain vigilance by consistently monitoring the app for potential issues.

Steps:

1. Initiate Project Creation: Kickstart a new project within the Flutter framework, carefully selecting suitable UI compo- nents tailored for the app's purpose.
2. Craft User Interface Design: Strategically design the app's interface, prioritizing user-friendliness for seamless anony- mous drug reporting.
3. Develop the Backend: Create the backend infrastructure of the app to efficiently store user data and securely deliver it to relevant authorities.
4. Implement Security Measures: Embed encryption and robust user authentication features to fortify security and prevent unauthorized access to sensitive information.
5. Thoroughly Test the App: Conduct extensive testing procedures to verify the app's functionality and the accuracyof reported data.
6. Deploy the App: Launch the app on the designated platform for user access after successful testing and validation.
7. Monitor and Sustain: Continuously monitor the app's performance and conduct routine maintenance to ensure its security and relevance through updates and improvements.

The implementation of drug reporting applications using Java can be done in the following steps:

1) Create a New Project: Create a new project in Flutterand name it appropriately.

2) Design the UI: Design the user interface and

layout for the application. Make sure that all the necessary elements are included such as a text field for entering the drug name, a dropdown for selecting the type of drug, a form for submitting the report, and a submit button.[5] The authentication and authorization part can be implemented using Firebase Authen- tication. Firebase Authentication is an authentication service provided by Google that allows users to sign in using their email address or phone number. Firebase Authentication also provides various methods of authentication such as OAuth, SMS, and social media providers. The user can be authenti- cated and authorized using Firebase Authentication.

3) Add Data Validation: Add validation to the form fields such as checking for valid drug names and types.

4) Connect to the API: Connect the application to the backend API to submit the drug report.

5) Implement the API: Implement the API to handle the drug report requests.

6) Test the application: Test the application to make sure everything is working as expected.

7) Implement two-factor Authentication: Two-factor authen- tication is a security measure that requires a user to provide two pieces of evidence to gain access to an account. This can be achieved by using a mobile phone number or email address for authentication.

8) Encrypt data: Encrypt the data that is being transferred between the client and the server.

9) Use a Secure Connection: Use a secure SSL connection for all communication between the client and the server.

10) Implement a Privacy Policy: Implement a privacy policy which clearly outlines how user data is used, stored, and shared.

V. Deploy the Application: Deploy the application to the app store and play store.To make the drug reporting applicationmore secure and anonymous, the following measures can be taken.

VI. CONCLUSION

In conclusion, the examination of cryptographic methods such as the Polybius cipher and Vigenère cipher within com- munication systems reveals their significant implications and advantages. This survey paper thoroughly investigates these techniques, highlighting their unique attributes and applica- tions in establishing secure communication frameworks.

The Polybius cipher, recognized for its simplicity in sub- stituting letters with specific coordinates, presents a straight- forward yet effective encryption approach. Its process of converting alphabets into numerical coordinates contributes to enhancing data transmission security .

Conversely, the Vigenère cipher, employing a polyalpha- betic substitution method, enhances encryption by using a keyword or phrase to modify the cipher alphabet. Its intricacy and adaptability significantly bolster security, making it an adept choice for fortified communication systems.

This survey paper provides an extensive analysis of both cryptographic techniques, encompassing their respective mer- its, limitations, and practical implementations. These methods are observed to substantially fortify data security and confidentiality in diverse communication scenarios.

The simplicity of the Polybius cipher and the complexity of the Vigenère cipher cater to distinct security requisites across various communication contexts. Through this comprehensive exploration, the paper emphasizes the relevance of these techniques and their potential contributions to bolstering secure communication systems.

The Polybius cipher and Vigenère cipher serve as funda- mental elements in the cryptographic domain, offering diverse encryption methodologies crucial in safeguarding sensitive information across communication channels. As technology evolves, these foundational techniques persist as essential tools for ensuring data security in contemporary communicationsystems.

REFERENCES

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

[2] K. Jakimoski, “Security techniques for data protection in cloud comput- ing,” International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.

[3] 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.

[4] Development of a modified aes algorithm, P. Kumar and S. B. Rana, Optik, vol. 127, no. 4, pp. 2341– 2345, 2016.

[5] Procedia Computer Science, vol. 92, pp. 355–360, 2016, A. Saraswat,
C. Khatri, P. Thakral, P. Biswas, et al., ”An extended hybridization of vigenere and caesar cipher techniques for secure communication.”.

[6] J. Chen J. S. Rosenthal, ”Using Markov Chain Monte Carlo to Decrypt Classic Cipher Text,” Statistics and Computing, vol. 22, no. 2, pp. 397–413, 2012.

[7] In the International Journal of Advanced Research in Computer Engineering Technology (IJARCET), volume 1, issue 10, pages 108–113, 2012, Q.-A. Kester wrote about ”A cryptosystem based on vigenere cipher with varying key.”