An Enhanced Secure System Based On Vigenere Cipher And Polybius Cipher

Amit Kanojia[1] Saqlin Khan[2] Vaibhav Ghewadekar[3] Arfat Bagban[4] Sonali Karthik[5]
[1,4]Student [5]Faculty
[1,2,3,4,5]Department of Information Technology
[1,2,3]Theem College Of Engineering, India

Abstract— In the ever-expanding arena of cryptography, the project introduces a unique cryptographic system founded on the synergistic combination of the Vigenère cipher and the Polybius cipher for encryption, BASE64, URI, HEX, and ROT13 for encoding. Drawing from the strengths of these classical encryption techniques, the system presents a fresh perspective on enhancing information security. The Vigenère cipher, renowned for its resistance to frequency analysis, introduces a polyalphabetic substitution approach. By utilizing a keyword-driven cyclic shift, the Vigenère cipher adds complexity to plaintext transformation, rendering simple monoalphabetic substitutions inadequate for decryption. Complementing this, the Polybius cipher employs a matrix-based substitution, converting individual letters into coordinates on a grid. This grid representation obscures the linguistic patterns inherent in the original message. The fusion of the Vigenère and Polybius ciphers capitalizes on their merits, resulting in a more robust encryption mechanism. This hybrid approach blends the Vigenère cipher's polyalphabetic complexity with the Polybius cipher's coordinate-based substitution, thereby introducing dual layers of encryption. This added complexity challenges traditional cryptanalysis methods and contributes to the system's strength against attacks. However, the implementation of such a cryptographic system necessitates a balanced consideration of its merits and limitations. Factors like key management, susceptibility to known attacks, and adaptability to modern security paradigms require careful evaluation. Keywords— *HEX, ROT13, URI, BASE64.*

I. INTRODUCTION

An Enhanced Secure System based on the Vigenère Cipher and Polybius Cipher represents a fusion of historical cryptography techniques, offering a unique approach to data security. The Vigenère Cipher, known for its polyalphabetic substitution method, employs a keyword to apply variable shifts to plaintext characters. Simultaneously, the Polybius Cipher, a transposition cipher, replaces characters with grid coordinates. By combining these ciphers, a dual-layered encryption system emerges, delivering heightened protection against traditional cryptanalysis techniques like frequency analysis. This innovative approach also offers the advantage of customizable keys, allowing users to employ complex, non-dictionary phrases as encryption keys. Regularly changing these keys further enhances security. The decryption 2 process reverses the encryption, first unraveling the Polybius Cipher and then the Vigenère Cipher using the correct key. Cryptography ensures the integrity of data using hashing algorithms and message digests. By providing codes and digital keys to ensure that what is received is genuine and from the intended sender, the receiver is assured that the data received has not been tampered with during transmission While this system provides an intriguing blend of classical and modern cryptography, it should be viewed as a building block within a broader security framework rather than a standalone solution for today's sophisticated security challenges. In our digital world, sending private information online is risky. Hackers and unauthorized people could steal or read our messages. We need a way to make sure our messages are secret and safe while they travel through the internet. This is where cryptography comes in, fi— finding the best and easiest way to use cryptography to protect our messages without making things too complicated, this project aims to solve this problem by exploring simple and effective ways to use it. To make Encryption and decryption security to a particular website by using Vigenère cipher and Polybius Cipher. The scope of an enhanced secure system based on the Vigenère Cipher and Polybius Cipher is multifaceted and offers opportunities for exploration in both educational and research domains from an educational perspective, this topic serves as a valuable tool for cryptography enthusiasts, students, and educators alike. It provides a platform to delve into the historical significance of these classical ciphers, shedding light on their origins, historical usage, and relevance in modern contexts. Moreover, it offers insights into encryption and decryption techniques, encouraging experimentation with key generation, encryption processes, and decryption algorithms.

The enhanced secure system amalgamating the Vigenère Cipher and Polybius Cipher represents a convergence of classical and modern cryptography techniques. With the Vigenère Cipher's polyalphabetic substitution and the Polybius Cipher's grid-based transposition, the system offers a dual-layered encryption method that augments data security. Utilizing customizable keys and variable shifts, it provides resilience against traditional cryptanalysis methods like frequency analysis. Moreover, the system's capacity for employing non-dictionary phrases as encryption keys enhances its cryptographic strength, especially when combined with regular key rotation practices. In practical terms, this system finds application in securing online communication channels, especially for websites handling sensitive user data. It ensures the confidentiality and integrity of transmitted information by encrypting it during transmission and enabling data integrity verification through hashing algorithms and digital signatures. Furthermore, from an educational standpoint, it serves as a valuable tool for cryptography enthusiasts and students, offering insights into historical ciphers' significance and their adaptation to modern security needs. Continued exploration and research into this fusion of classical and modern cryptographs Furthermore, the system's adaptability and versatility extend beyond traditional encryption techniques.

II. Literature Survey

Vigenère published a type of polyalphabetic cipher called an autokey cipher – because its key is based on the original plaintext – before the court of Henry III of France. The cipher now 5 known as the Vigenère cipher, however, is that originally described by Giovan Battista Bellas in his 1553 book La cirri del Sig. Giovan Battista Bellas. He built upon the tabula recta of Tritheism but added a repeating "countersign" (a key) to switch cipher alphabets to every letter. Whereas Alberti and Tritheism used a fixed pattern of substitutions, Bellas's scheme meant the pattern of substitutions could be easily changed, simply by selecting a new key. Keys were typically single words or short phrases, known to both parties in advance, or transmitted "out of band" along with the message. The Vigenère cipher is simple enough to be a field cipher if it is used in conjunction with cipher disks.[1]

The Polybius square, also known as the Polybius checkerboard, is a device invented by the ancient Greeks Cleoxenus and Democleitus and made famous by the historian and scholar Polybius. The device is used for fractionating plaintext characters so that they can be represented by a smaller set of symbols, which is useful for telegraphy, steganography, and cryptography. The device was originally used for fire signaling allowing for the coded transmission of any message, not just a finite number of predetermined options as was the convention before This alphabet, and this latter form of the Polybius square, is used when implementing the square in other Western European languages such as English, Spanish, French, German, Italian, Portuguese, and Dutch. Each letter is then represented by its coordinates in the grid. The figures from one to five can be indicated by knots in a string, stitches on a quilt, contiguous letters before a wider space, or many other ways The Polybius square is also used as a basic cipher called the Polybius cipher. This cipher is quite insecure by modern standards, as it is a substitution cipher with characters being substituted for pairs of 6 digits, which is easily broken through frequencyanalysis.[2]

The particular set of 64 characters chosen to represent the 64-digit values for the base varies between implementations. The general strategy is to choose 64 characters that are common to most encodings and that are also printable. This combination leaves the data unlikely to be modified in transit through information systems, such as email, that were traditionally not 8-bit clean for example, MIME's Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations share this property but differ in the symbols chosen for the last two values; an example is UTF-7. The earliest instances of this type of encoding were created for dial-up communication between systems running the same OS, for example, uuencode for UNIX and Bin Hex for the TRS-80 (later adapted for the Macintosh), and could therefore make more assumptions about what characters were safe to use. For instance, uuencode uses uppercase letters, digits, and many punctuation characters, but no lowercase.[3]

III. System Architecture

Encoding and decoding is the method by which information is converted into secret code that hides the information's true meaning. Encryption and Encoding are the terms commonly interchanged and used incorrectly. There is a lot of difference between these two terms and it is very vital to know the differences.

A. System Architecture

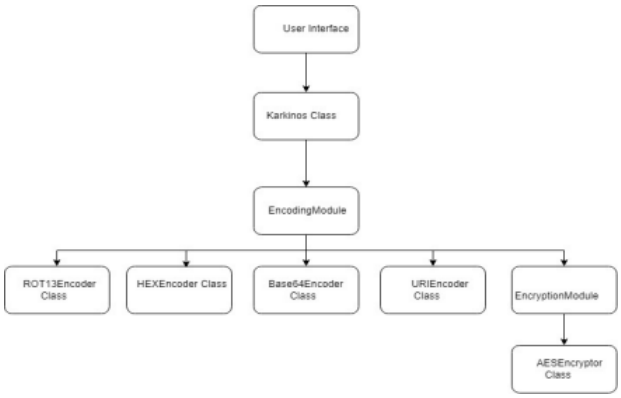

Fig 1. System Architecture of Enhance Secure System Based on Vigenere Cipher and Polybius Cipher

B. Proposed system

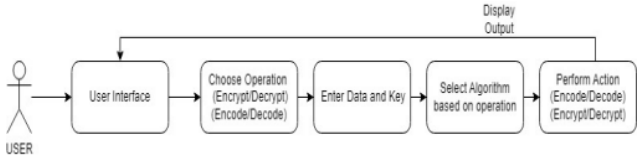

Fig 1. Proposed System of Secure System

IV. System flow

The system flow is the structure and behavior of the system and gives a proper view of the system. Designing the software for the Encryption and Decryption of images, Plain text encoding and decoding, and Plain Encryption and Decryption are done here.

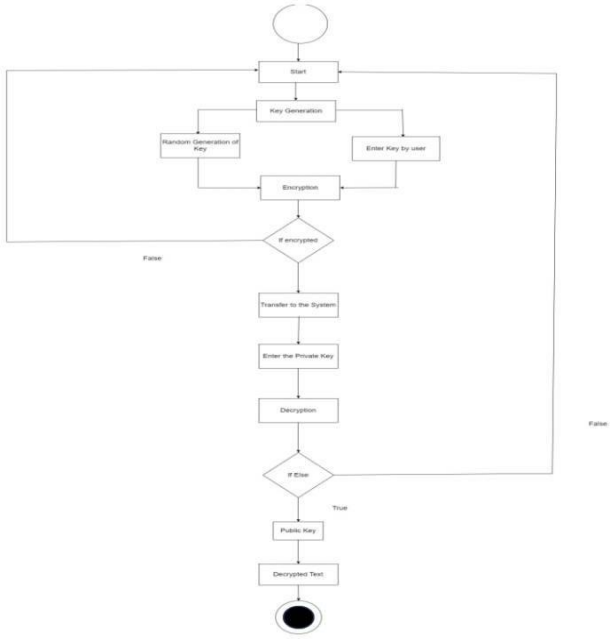

Fig 2. System Flow of Enhanced secure system based on Vigenère cipher and Polybius cipher

A System diagram is a structure that shows the generation of the key from an option having a random generation of key or an enter a key by the user which is used for the encryption of data after the encryption we transfer the data to the system after that we have to enter the private key for decryption of data if any error occurs then If Else condition occurs the whole process will repeat once again to get the successful decryption of data.

C. Working

In a cryptographic system, the encryption and decryption process begins with the user inputting plaintext data to be secured. Utilizing a combination of cryptographic techniques, including the Vigenère cipher, Polybius cipher, steganography, Base64 encoding, hexadecimal encoding, and URI encoding, our system ensures robust encryption and decryption procedures.

Firstly, the plaintext undergoes encryption using the Vigenère cipher, employing a user-defined keyword for added security. This process generates an intermediate ciphertext, which is then further encrypted using the Polybius cipher. The Polybius cipher replaces characters with their respective coordinates in a grid, providing an additional layer of encryption to the data. To enhance confidentiality, the Polybius encrypted text is concealed within an innocuous image file using steganography techniques. This step ensures that the encrypted data remains hidden from unauthorized access, adding an extra layer of security to the transmission process.

Following encryption, the steganography-modified image containing the ciphertext is encoded using Base64 encoding for secure transmission across different systems and protocols. This encoding method ensures that the encrypted data is represented in a format that is compatible and easily transferable, maintaining the integrity of the information during transmission.

On the decryption end, the process is reversed to retrieve the original plaintext. The encoded image data is decoded using Base64 encoding to recover the steganography-modified image. The ciphertext embedded within the image is then extracted using steganography extraction techniques.

Algorithms Employed: Multiple algorithms are used to run the project which is based on the cryptography of data the algorithms are:

Vigenère Cipher: The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It uses a keyword and a table of alphabets shifted one position to the right.

Polybius Cipher: The Polybius cipher, also known as the Polybius square, is a substitution cipher that encodes pairs of letters into a grid of numbers.

V. RESULT

Secure system integrating these two ciphers, the resulting cryptographic system can offer improved resistance to various cryptanalysis techniques, including frequency analysis and known- -plaintext attacks. However, it's crucial to use sufficiently long and random keys in the Vigenère cipher to ensure its effectiveness the security of any cryptographic system, including one based on the Polybius and Vigenère ciphers, depends on the implementation and management of key exchange and storage, as well as the overall protocol's robustness.

Fig 3. Graphical User Interface

Fig 3 displays the GUI. It contains of down arrow button which shows the new web page for encoding/decoding and Encrypt
/Decrypt page.

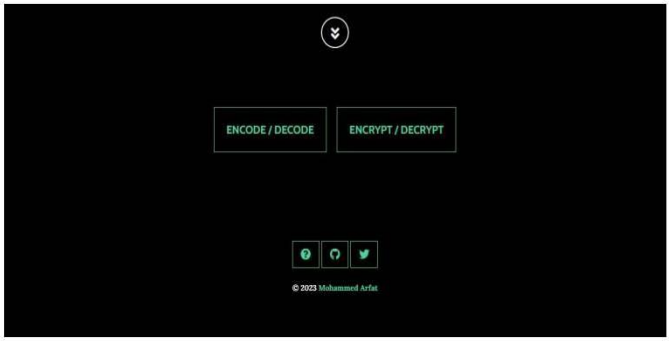

Fig 3. Result for the dashboard of Secure System

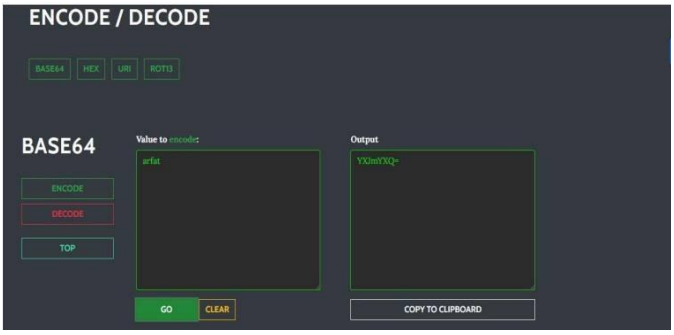

Fig 4. Result for Encode and Decode

Fig 4 describes the result of encoding and decoding the word “Arfat”. Itconsists of input with different algorithms of raw data.

VI. CONCLUSION

URI encoding, Base64 encoding, hexadecimal encoding, steganography, and the Vigenère cipher are just a few of the cryptographic approaches that are integrated into an upgraded safe system. Combining various cryptographic techniques results in a strong, multi-layered security strategy for sensitive data. Through encryption, the system maintains confidentiality by integrating the Vigenère and Polybius ciphers. By introducing the idea of a keyword for encryption, the Vigenère cipher strengthens the plaintext's defense against attacks using frequency analysis. The Polybius cipher further operates the ciphertext by replacing characters with their coordinates in a grid, adding an extra layer of protection. Steganography also adds a layer of secrecy by enabling encrypted messages to be hidden within other media.

\

VII. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of this project An Enhanced Secure System Based on Vigenère Cipher and Polybius Cipher. First and foremost, we extend our deepest appreciation to our project supervisor Prof. Sonali Karthik whose guidance, support, and invaluable insights have been instrumental throughout the entire duration of this project. Their expertise and encouragement have been indispensable in steering us in the right direction and overcoming various challenges along the way. We are also immensely grateful to the entire team involved in the project, whose dedication, collaboration, and hard work have been vital in bringing this vision to fruition. Each team member's unique skills and contributions have played a crucial role in the development, implementation, and testing phases of the project.

Secure system integrating these two ciphers, the resulting cryptographic system can offer improved resistance to various cryptanalysis techniques, including frequency analysis and known- -plaintext attacks. However, it's crucial to use sufficiently long and random keys in the Vigenère cipher to ensure its effectiveness the security of any cryptographic system, including one based on the Polybius and Vigenère ciphers, depends on the implementation and management of key exchange and storage, as well as the overall protocol's robustness.

REFERENCES

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

[2] Chen and J. S. Rosenthal, “Decrypting classical cipher text using Markov chain Monte Carlo," Statistics and Computing, vol. 22, no. 2, pp.397–413, 2012

[3] S.D. Nasution, G. L. Genting, M. Shahrazad, and R. Rahim, “Data security using Vigenère cipher and Goldbach codes algorithm,” Int. J. Eng. Res. Techno, vol. 6, no. 1, pp. 360–363, 2017.

[4] P. U. Siahaan, “Protection of important data and information using Grunfeld cipher,” 2018.

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

[6] J. Chen and J. S. Rosenthal, “Decrypting classical cipher text using Markov chain Monte Carlo,” Statistics and Computing, vol. 22, no. 2, pp. 397–413, 2012.