IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

Survey on Vigenère Cipher and Polybius Cipher for Cryptographic Encryption and Decryption

Mr. Shrikant Shinde, Satish Rathod, Yogesh Shelke, Akash Ghotale
Department of Computer Engineering
Sinhgad Institute of Technology and Science, Narhe, Pune

Abstract: *In this competitive world, securing data or information has become a challenge for the modern electronic communication system, making it the most valuable asset. Numerous techniques, including cryptography and steganography, are employed to ensure data/information security. This paper introduces the application of hybrid cryptography, combining AES and RSA, to enhance security. Hybrid cryptography in this paper involves encrypting the symmetric key used for message encryption, thereby ensuring better security. Additionally, a digital signature is created by encrypting the hash value of the message. This digital signature is utilized at the receiving end for integrity checking. To form a complete message, the encrypted message, encrypted symmetric key, and encrypted digest are combined. Further enhancing security, the complete message is then secured using the steganography method, specifically LSB (Least Significant Bit). By leveraging hybrid cryptography, the algorithm provides robust security, while steganography strengthens it further. An essential feature of this algorithm is message integrity checking. Successful simulations have been conducted, supporting the feasibility of this approach.*

Keywords: Cryptography, Hybrid cryptography, Algorithm,AES, RSA, Steganography, LSB.

I. INTRODUCTION

Data and information security is a formidable challenge in the modern electronic communication system nowadays. To ensure information security, three essential security goals must be followed, commonly referred to as the CIA triad: confidentiality, integrity, and availability [1]. These goals apply to data, information, and computing services.
The primary objectives of information security are as follows:

- Confidentiality: Concealing information from unauthorized entities.
- Integrity: Protecting information from unauthorized or illegal changes.
- Availability: Making information accessible to authorized entities [2].

Some techniques are required for the application of security goals. The two most dominant techniques used todayare cryptography and steganography [2][16]. Two Greekwords‘ Kryptos’ meaning ‘secret’ and ‘Graphein’ meaning ‘writing’ derive the word ‘Cryptography’. So Cryptography means ‘secret writing’, a science of transforming a message into anunintelligible form [3]. The unencrypted message iscalled ‘plain text’ and after encryption, it is converted into anunintelligible form which is called ‘cipher text’[4]. The ciphertext is then sent over an insecure channel with the presence ofa third party called adversary or intruder and at the receivingend after decrypting the cipher text again the plain text is found.
Cryptography introduces three different types of streams:
i) Symmetric-key (Shared secret key) Cryptography
ii) Asymmetric-key (Public-key) Cryptography
iii) Hashing

II.RELEVANCE

Hybrid cryptography is an effective approach to enhancing the security of sensitive data and information in the modern electronic communication system. By combining multiple encryption techniques, such as the Vigenère cipher and the Polybius cipher, hybrid cryptography offers increased complexity and robustness in protecting confidential information. The Vigenère cipher is a polyalphabetic substitution cipher that uses a series of interwoven Caesar ciphers based on a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

keyword. It introduces a variable key length, making it resistant to frequency analysis and providing a higher level of encryption. By incorporating the Vigenère cipher into hybrid cryptography, the confidentiality of the data is strengthened, as it adds an additional layer of complexity to the encryption process.On the other hand, the Polybius cipher is a transposition cipher that replaces letters with pairs of coordinates on a grid. This cipher provides a means of obscuring the original message and offers a different form of encryption compared to substitution ciphers like the Vigenère cipher. By integrating the Polybius cipher into hybrid cryptography, the encryption technique becomes more diverse, increasing the overall security of the communication system. The relevance of using hybrid cryptography with the Vigenère cipher and the Polybius cipher lies in their complementary strengths. While the Vigenère cipher provides strong encryption against frequency analysis and improves confidentiality, the Polybius cipher contributes to the complexity and obfuscation of the encrypted message. By combining these two ciphers within the hybrid cryptography framework, a more robust and resilient encryption solution is achieved, offering a higher level of data and information security in the modern electronic communication system.

III.MOTIVATION

The motivation behind utilizing hybrid cryptography with the Vigenère cipher and Polybius cipher stems from the increasing need for stronger data and information security in the modern electronic communication system. With the proliferation of digital communication and the rising threat of cyber-attacks, it has become crucial to develop encryption techniques that can effectively safeguard sensitive information. The Vigenère cipher and Polybius cipher are both historical encryption methods known for their individual strengths in encryption. The Vigenère cipher, with its variable key length and resistance to frequency analysis, provides a higher level of confidentiality. The Polybius cipher, with its transposition technique and grid-based encryption, adds complexity and obfuscation to the encrypted message.

IV. LITERATURE SURVEY

This paper [5] the security for web keeping money, account passwords, messages accounts secret word, etc requires content protection in mechanized media. It shows the security besides; pressure for the information with the move encryption standard. The age of key has been done with the assistance of the Polybius square. The extension in number of rounds it will require increasingly computational speculation and will end up irksome for the software engineer to break the system Caesar cipher, otherwise called the shift cipher, is one of the least complex and most generally known old style encryption systems. It is a kind of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the letters in order. For example, with a shift of 3, A would be replaced by D, B would become E, etc. The encryption step performed by a Caesar cipher is regularly joined as a component of progressively complex plans, for example, the Vigenère cipher, and still has present day application in the ROT13 framework. Similarly, as with all single letters in order substitution ciphers, the Caesar cipher is effortlessly broken and in present day practice offers basically no correspondence security.[6] In cryptography, a transposition cipher is a process of encryption by which the positions held by units of plaintext are shifted by a customary framework or example, so that the ciphertext comprises a stage of the plaintext. That is, the request for the units is changed toward the finish of the shifting process. Mathematically, a bijective function is utilized on the characters' positions to encode and an inverse function to decrypt. The letters themselves are kept unaltered, which suggests that the impact is just on their positions just, making their request inside the message mixed by a few all around characterized scheme. Numerous transposition ciphers are done as per a geometric design.[7][8] In [9] changed variant of vigenere algorithm was proposed in which dispersion is given by adding an arbitrary piece to every byte before the message is scrambled utilizing Vigenère. This strategy falls flat kasiski assault to discover the length of key on the grounds that the cushioning of message with irregular bits. The fundamental downside of this system is that the size of the scrambled message will be expanded by around 56In [10] another method for executing Vigenère algorithm was presented via naturally changing the cipher key after every encryption step. In this technique progressive keys were utilized that were reliant on the underlying key an incentive during the encryption process. In [11] adjustment of Vigenère cipher by irregular numbers, punctuations and scientific images was introduced. In proposed technique numbers, punctuations furthermore, scientific images were utilized for key instead of characters to make it increasingly hard for animal power

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

assault. It was inferred that if irregular numbers are utilized for key what's more, to spread the range then just skilled people can recognize the message recognize the message. Another algorithm [12] by combining Vigenère substitution cipher with Stream cipher was proposed in which repeated bits of plaintext consistently encrypted with the diverse segment of the catchphrase or binary key. The letters in odd location were encoded with stream cipher and the letters in even location with Vigenère cipher. It was inferred that proposed algorithm conceals the connection between cipher content and plain content that makes cryptanalysis much troublesome. Tianfu [13] address that internet is one of the most unsafe communication medium due to huge connection and public network. Information protection is one the of essential requirement. At present various security algorithms are proposed to achieve security during communication. All of them have certain good point and certain bad point. To improve the strength of encryption algorithm they proposed a hybrid model. Proposed model is combination of AES and DES. Both algorithms are symmetric key technique and itself they are very much capable for encryption. Integration of AES and DES would give a strong level of security at encryption end. A significant improvement in results has been observed with proposed solution. Jakimoski et al. [14] analysed and evaluated the most important security techniques for data protection that are already accepted from the cloud computing providers. They classified them in four sections according to the security mechanisms that they provide: authentication, confidentiality, access control and authorization. They conclude that if all recommended measures are taken into account providing authentication, confidentiality, access control and authorization, then the cloud computing can be trusted in data protection. They focused on the security issues that should be taken into account in depth in order to have proper data security in the cloud. They recommended important security measures relating to data protection in the cloud that must be taken into account.

V. FUTURE SCOPE

The future scope for hybrid cryptography with the Vigenère cipher and Polybius cipher includes:

1. Cryptanalysis and Security Enhancements: Analysing strengths and weaknesses to improve security measures.
2. Algorithm Optimization: Optimizing performance and efficiency of the hybrid cryptography system.
3. Integration with Modern Cryptographic Techniques: Combining with contemporary cryptographic techniques for enhanced security.
4. Adaptation to Emerging Technologies: Tailoring the system to address security challenges posed by new technologies.
5. Application in Specific Domains: Customizing implementations for industries like finance, healthcare, government, and defense.
6. Standardization and Adoption: Promoting widespread adoption and establishing security standards.

Overall, the future scope involves further research, innovation, and collaboration to address evolving security challenges and ensure robust data security in electronic communication.

VI. CONCLUSION

In conclusion, hybrid cryptography incorporating the Vigenère cipher and Polybius cipher presents a promising avenue for strengthening data security in the modern electronic communication system. By combining these historical encryption methods, we can leverage their unique strengths to enhance confidentiality, complexity, and obfuscation in encrypted communication. The future scope for hybrid cryptography with the Vigenère cipher and Polybius cipher is expansive. It includes cryptanalysis and security enhancements to address potential vulnerabilities and attacks. Algorithm optimization can improve performance and efficiency, while integration with modern cryptographic techniques offers flexibility and advanced security features.

Adapting the hybrid cryptography system to emerging technologies ensures its relevance and effectiveness in the face of evolving threats. Moreover, exploring domain-specific applications enables tailored implementations for industries where secure communication is critical. Efforts towards standardization and widespread adoption will drive the acceptance and seamless integration of hybrid cryptography in various electronic communication platforms, fostering a more secure digital environment.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

Overall, the future of hybrid cryptography with the Vigenère cipher and Polybius cipher holds great promise for advancing data security, protecting sensitive information, and ensuring secure communication channels in the ever-evolving landscape of electronic communication.

REFERENCES

[1] Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryptograph 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] Puneet Kumar, Shashi B. Rana, Development of modified AES algorithmfor data security, Optik - International Journal for Light and ElectronOptics, Volume 127, Issue 4, 2016.
[4] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AESproposal): a comparison with DES," in Security Technology, 2001 IEEE35th International Carnahan Conference on, 2001, pp. 229-234.
[5] Q.-A. Kester, "A cryptosystem based on Vigen`ere cipher with varyingkey," International Journal of Advanced Research in Computer EngineeringTechnology (IJARCET), vol. 1, pp. pp: 108-113, 2012.
[6] C. Bhardwaj, "Modification of Vigen`ere Cipher by Random Numbers,
Punctuations Mathematical Symbols," Journal of Computer Engineering(IOSRJCE) ISSN, pp. 2278-0661, 201215
[7] F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipherby Stream Cipher," International Journal of Computer Applications, vol.100, pp. 1-4, 2014
[8] Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing."
International Journal of Grid and Distributed Computing 9.1(2016): 49-56.
[9] M. Abror, "Pengertian dan Aspek-AspekKeamanan Komputer," 2018. [Daring]. Tersediapada: https://www.ayoksinau.com/pengertiandan-aspek- aspek-keamanan-komputer-lengkap/. [Diakses: 01-Okt-2018].