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.

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].

DOI: 10.48175/IJARSCT-10591