Model of Cryptography System by using Vigenere Cipher and Polybius Cipher

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

Abstract: *Cryptography, derived from a Greek word, is the art of safeguarding information by transforming it into an intricate and unreadable format. It encompasses both mathematics and computer science. The exponential growth of the Internet has raised awareness about concerns related to privacy and uncertainty. Despite security being a significant concern over the internet, numerous applications have been developed and designed without considering the fundamental objectives of data security, namely confidentiality, authentication, and protection. As our daily activities increasingly rely on data networks, understanding these security issues and challenges becomes crucial. Cryptography is necessary to prevent unauthorized access to data by undesirable users or individuals. This paper presents a novel hybrid security cipher that combines two vital ciphers: the Polybius Cipher and the Vigenère Cipher. This hybrid encryption cipher offers enhanced security compared to traditional ciphers.*

Keywords: Encryption, Cryptography, Polybius Ciphers, Vigenere Ciphers

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 computing," 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 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.

[5] 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.

[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.

[7] M. B. Pramanik, "Implementation of cryptography technique using columnar transposition," International Journal of Computer Applications, vol. 975, p. 8887, 2014.

[8] C. Sanchez-Avila and R. Sanchez-Reillol, "The rijndael block cipher (aes proposal): a comparison with des," in Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, 2001, pp. 229–234.

[9] Q.-A. Kester, "A cryptosystem based on vigen`ere cipher with varying key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 10, pp. 108–113, 2012.

[10] C. Bhardwaj, "Modification of Vigenère cipher by random numbers, punctuations & mathematical symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.

[11] F. M. S. Ali and F. H. Sarhan, "Enhancing security of Vigenère cipher by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.

[12] P. Gutmann, Cryptographic security architecture: design and verification. Springer Science & Business Media, 2003.

[13] A. P. U. Siahaan, "Protection of important data and information using gronsfeld cipher," 2018.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-10595

259

ISSN
2581-9429
IJARSCT

[14] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigen`ere cipher and goldbach codes algorithm," Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.

[15] M. Maity, "A modified version of polybius cipher using magic square and western music notes," International Journal For Technological Research In Engineering, ISSN, pp. 2347–4718, 2014.