

Leveraging the Techniques of Vigenère Cipher and Modern Cryptographic Algorithms

Esther Careen Katema¹ and Fanny Chatola²

Student, DMI-St. John the Baptist University, Lilongwe, Malawi¹

Lecturer II, Head of Computer Science and Information Technology

DMI-St. John the Baptist University, Lilongwe, Malawi²

esthercareenkatema@gmail.com and fannychatolatmsic2022@gmail.com

Abstract: *The growing reliance on digital communication necessitates robust methods for secure data transmission. Hence this paper proposes a hybrid cryptography system integrating the Vigenère cipher with modern cryptographic techniques. The system aims to enhance security while maintaining computational efficiency. Functionalities of the system include key generation, encryption, decryption, and cryptographic analysis. The Vigenère cipher serves as the foundation for the system, providing a polyalphabetic substitution method. Additionally, modern cryptographic algorithms such as AES are integrated to strengthen security. Algorithms and methodologies employed include: Vigenère Cipher which utilizes a keyword to shift characters by different amounts, creating a polyalphabetic substitution; AES which Implements symmetric-key encryption with a block cipher, ensuring confidentiality and integrity of data; Cryptographic Analysis which employs statistical analysis and frequency distribution techniques to assess the strength of the encryption and identify potential vulnerabilities etc. By combining classical and modern cryptographic techniques, the hybrid system aims to provide robust security while addressing the limitations of individual methods*

Keywords: Vigenère Cipher, cryptography, AES cipher, LSB technique, Steganography