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: 7.53
Volume 4, Issue 3, November 2024

Leveraging the Techniques of Vigenère Cipher and Modern Cryptographic Algorithms

Esther Careen Katema[1] and Fanny Chatola[2]
Student, DMI-St. John the Baptist University, Lilongwe, Malawi[1]
Lecturer II, Head of Computer Science and Information Technology
DMI-St. John the Baptist University, Lilongwe, Malawi[2]
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

I. INTRODUCTION

Cryptography plays a pivotal role in securing digital communications, ensuring confidentiality, integrity, and authenticity of data. In recent years, the surge in cyber threats necessitates the development of robust cryptographic techniques. One such approach is hybrid cryptography, which combines the strengths of multiple encryption methods of multiple encryption methods to mitigate the vulnerabilities of individual algorithms. This study focuses on the integration of the Vigenère cipher, a classical encryption technique, into modern cryptographic systems to enhance security. The Vigenère cipher, invented by Blaise de Vigenère in the 16th century, is a polyalphabetic substitution cipher characterized by its use of a keyword and multiple Caesar ciphers to encrypt plaintext. Despite its simplicity, the Vigenère cipher offers a level of security superior to mono-alphabetic ciphers due to its key variability. However, it is vulnerable to frequency analysis and Kasiski examination, limiting its effectiveness in modern cryptographic contexts. The resurgence of interest in classical cryptography techniques, couples with advancements in computational power and cryptanalysis, has inspired researchers to explore the potential of integrating historical ciphers like the Vigenère cipher into contemporary cryptographic frameworks. By leveraging the strengths of classical and modern encryption methods, hybrid cryptographic systems can provide enhanced security against sophisticated attacks while preserving computational efficiency.

II. OBJECTIVES

The first objective is to implement secure encryption and decryption of text and images. This involves designing a robust cryptography system that incorporates the Vigenère cipher alongside contemporary encryption algorithms, AES and LSB. The second algorithm is to develop a user friendly chatroom which involves demonstrating the practical applicability of the cryptography approach in real-world scenarios, through the implementation of a user-friendly

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: 7.53
Volume 4, Issue 3, November 2024

chatroom where users can easily send and receive messages. Users can also send private messages on the same platform to specific intended audiences.

The third objective is to provide educational cryptography FAQs. This involves the design and implementation of a module that displays FAQs about cryptography, providing clear and concise answers to help users understand the principles and importance of cryptographic techniques. And lastly this system aims to ensure data security and integrity through the implementation of techniques that maintain the integrity and confidentiality of all data within the system, including message integrity and secure key management.

III. EXISTING SYSTEM

There are so many cryptographic systems that use various algorithms to encrypt various forms of data, images etc. There are systems that encrypt the texts/words/strings being exchanged between two parties. Other system encrypt messages imbedded in audios. And lastly, some systems encrypt messages hidden in images and videos. All these systems have many things in common like the use of AES, DES, RSA, hash functions, Caesar cipher etc. to carry out encryption and decryption. This leaves room for this project to focus on using other techniques like the Vigenère cipher to carry out encryption and decryption of text and images.

IV. PROPOSED SYSTEM

As humans are constantly advancing in a digital world, secure digital communication is still under threat. Due to this, there arises a need for innovative solutions that can stand the test of time and adversaries alike. Imagine a system that combines the elegance of a classical cipher with the robustness of modern cryptographic technologies, offering a formidable defense against prying eyes and malicious attacks. This is precisely the vision behind the proposed development of a hybrid cryptography system based on the vulnerable Vigenère cipher. By harnessing the simplicity and historical significance of the Vigenère cipher and augmenting it with the sophistication of contemporary encryption methods, the system aims to create a paradigm-shifting system solution that redefines the landscape of data security. this hybrid system propels cryptography into the future, offering a potent arsenal for safeguarding sensitive information in an increasingly interconnected world.

V. METHODOLODY

Agile methodology, particularly Scrum, is used in the application's development. Scrum's iterative approach involves dividing the development process into "sprints" and gathering user feedback to continuously refine the application. This flexibility allows the team to adjust priorities, ensuring adaptability to changes. Agile development prioritizes collaboration, ongoing delivery, and feedback responsiveness, resulting in a more user-focused and efficient development process.

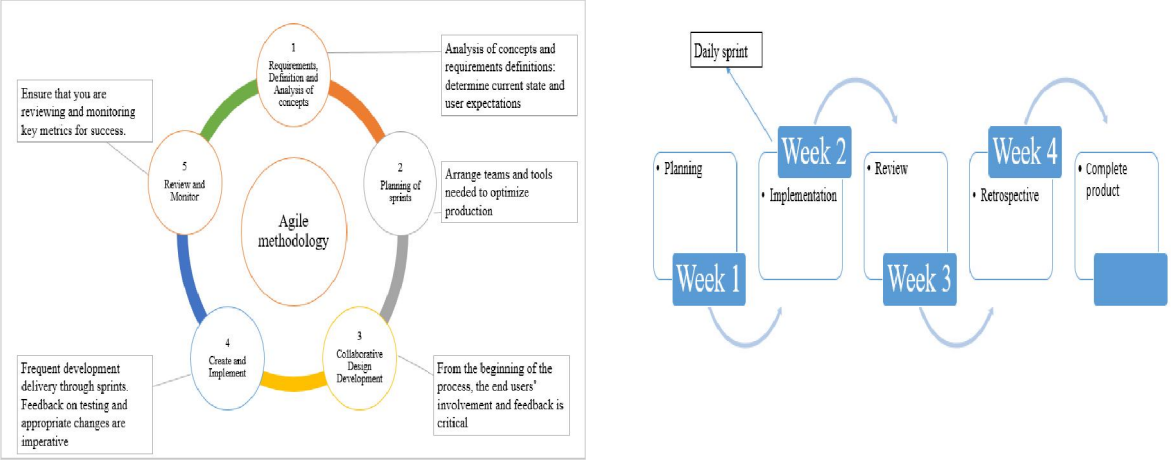


Figure 1: Agile, scrum methodology

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: 7.53
Volume 4, Issue 3, November 2024

VI. SYSTEM IMPLEMENTATION

System Architecture

A system architecture diagram is a blueprint that illustrates the structural components and organization of an application. It depicts the physical structure, intended usage, and purpose of the application from the perspective of developers, rather than end-users. To manage complexity and promote modular development, developers subdivide the system into layers based on functionality or access pathways, such as a home page or a contact form. This layering simplifies debugging and maintenance. System architecture also encompasses data flow between modules, defines integration points with external systems, and ensures compliance with industry standards and best practices.

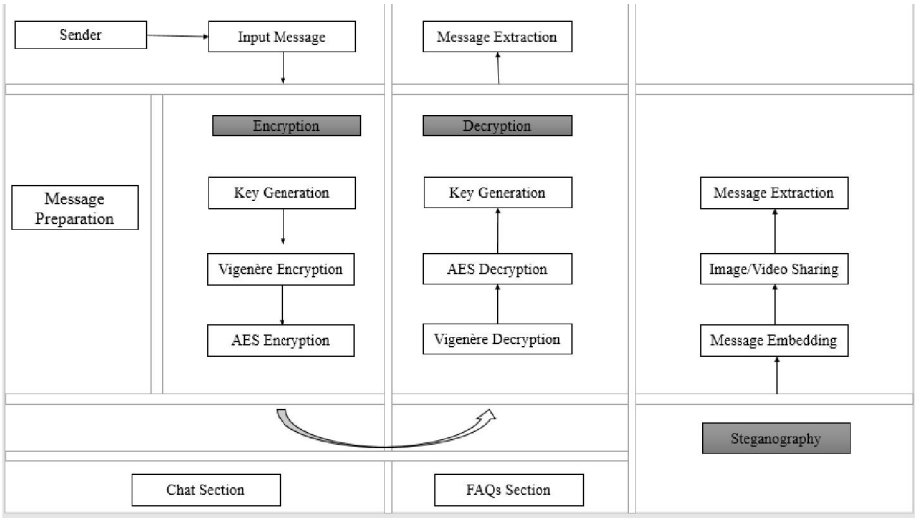


Figure 2: System architecture

Use Case Diagram

A Use Case Diagram outlines how users interact with a system to achieve specific goals. It shows the system's boundaries, user roles (actors), and how they interact with the system's functions. Use Case Diagrams help design and develop systems by capturing all possible user scenarios, ensuring that the system meets user needs. They also clarify the roles and responsibilities of different system components.

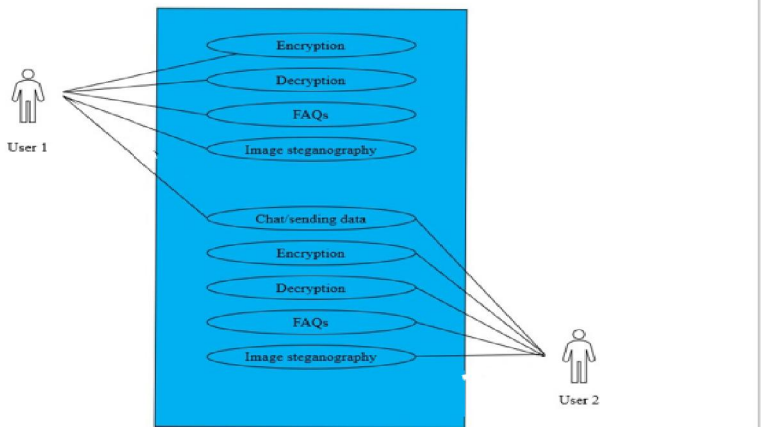


Figure 3: Use case diagram

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: 7.53
Volume 4, Issue 3, November 2024

Data Flow Diagram

A DFD is a visual representation of an information system's key processes and how they handle data. It outlines the system's general structure and is often used as a starting point for deeper analysis. DFDs can help in understanding data processing, identifying bottlenecks, and pinpointing areas where processes can be improved. They show the data entering the system, the steps it goes through, where it's stored, and the final output. This visual representation makes it easier to see how data is handled and processed within the system.

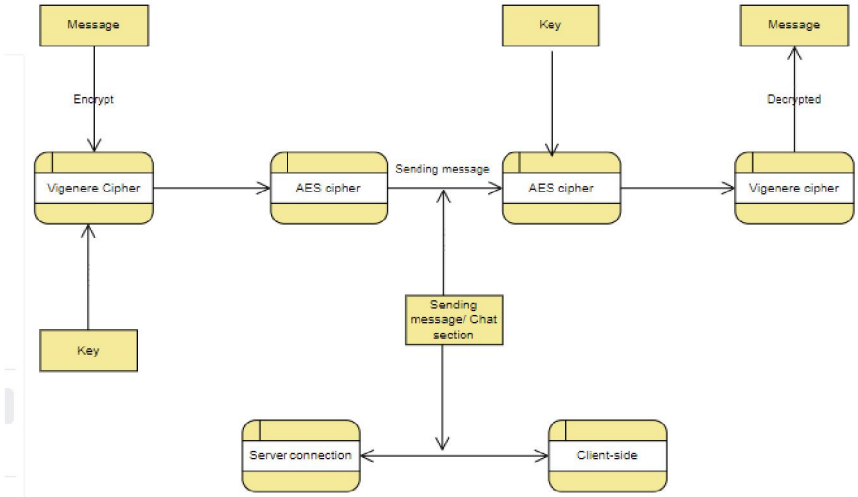


Figure 4: DFD diagram

VII. SYSTEM IMPLEMENTATION

Module Description

The module description offers a detailed analysis of a particular module in a software system or app. It's a comprehensive guide that explains the module's purpose, what it does, and its role in the system's overall design. By providing a clear understanding of each module, the module description helps developers understand the system as a whole, work together effectively, and maintain it over time. Each of the following system's module has its own set of tasks and interacts with other modules in a way that keeps the system running smoothly and as a whole.

- Message encryption: This module involves converting the plain text of the first user into cipher text. The user enters the data and a pre-defined key for the Vigenère cipher to turn it into cipher text. For the AES encryption, the user uses their own secret key to encrypt the message, which can also be used for decryption. This module ensures that sensitive information is securely encrypted, making it inaccessible to unauthorized users. The encryption process must be efficient and robust, providing strong security without significantly impacting system performance.
- Message decryption: This module involves converting encrypted/cipher text back into plain text. The second user enters the cipher text and the predefined key for Vigenère or the user's key for AES to decrypt the ciphered text. The decryption process must be reliable and user-friendly, allowing authorized users to easily retrieve the original message while maintaining the confidentiality and integrity of the data.
- Chat section**:** This is a section that allows users on the system to send and receive messages to and from other users. It has been implemented in such a way that users can send public and private messages to each other. The private messages are accessed using the "/private + username" technique that enable users to send messages to other users of their choice on a platform harboring many users. These private messages are only seen by the sender and intended receivers. Otherwise, the public messages are for all users connected to the server.

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: 7.53
Volume 4, Issue 3, November 2024

- FAQs section: This is a module which displays the frequently asked questions about cryptography in general and not specific to this system. It is very essential as it provides more and descriptive information about cryptography that can be easily understood by users new to the concept.
- Image steganography**:** Image steganography is a type of encryption where messages can be hidden in images using various techniques like the traditional LSB. Similar in this module, users are able to encrypt or embed secret messages in images. This module makes use of the spread spectrum technique. This is a technique in steganography where bits of the message are spread or scattered across the image without changing its appearance or shape. The images are then shared among users to transmit these secret messages. The receiver inputs the image with the message in order to extract it and display it on the message box.

System Screenshot

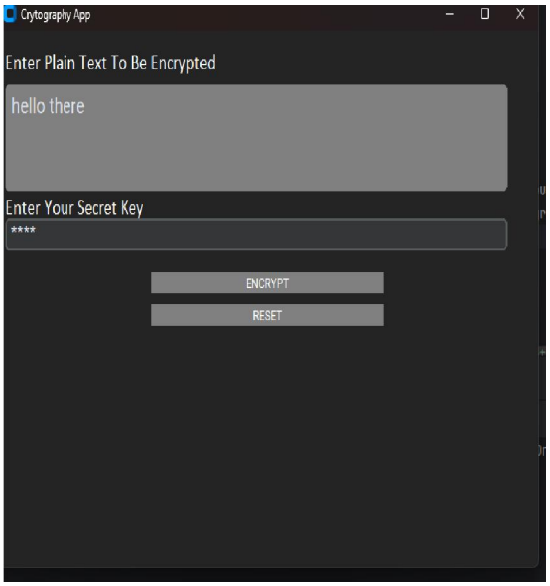
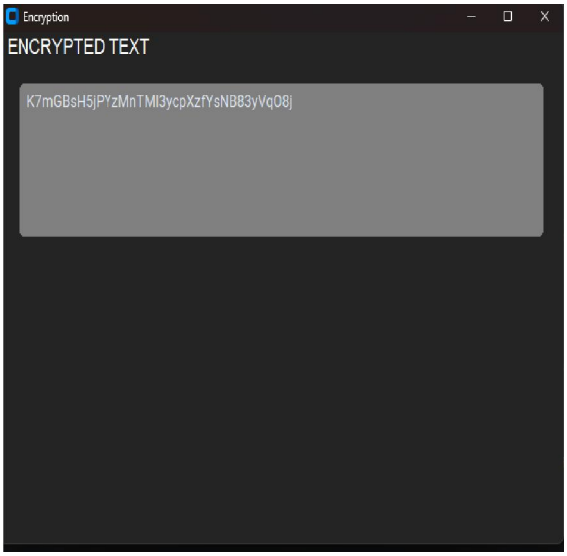


Figure 5: text encryption



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: 7.53
Volume 4, Issue 3, November 2024

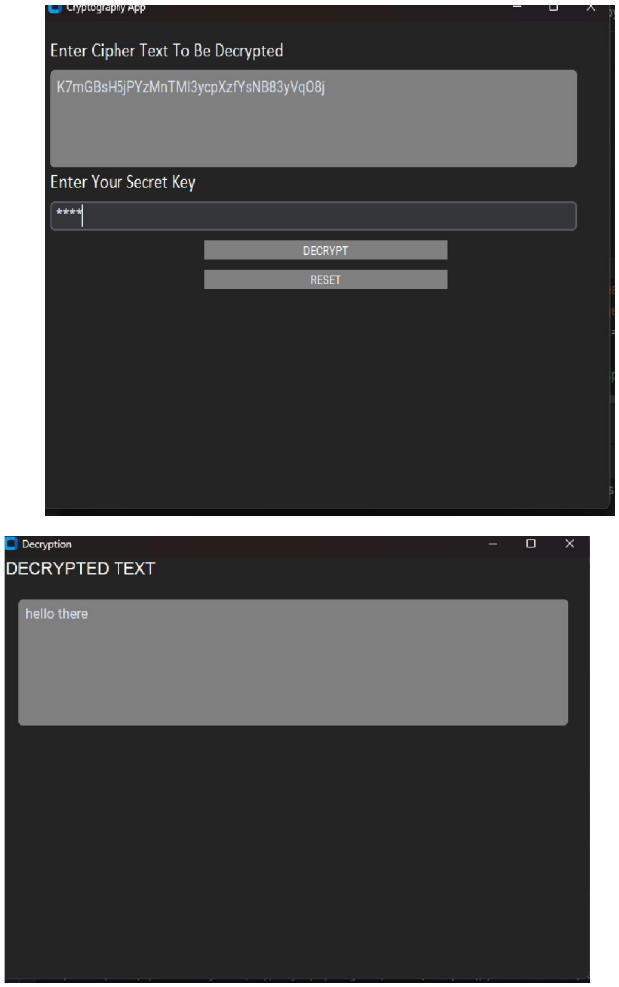


Figure 6: text decryption

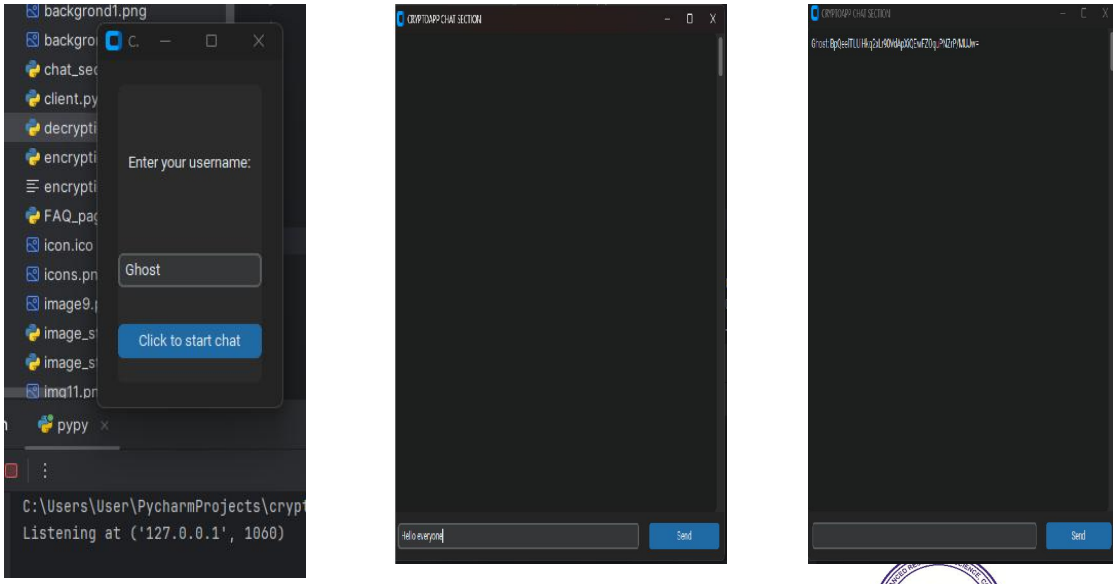


Figure 7: user chat section

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: 7.53
Volume 4, Issue 3, November 2024

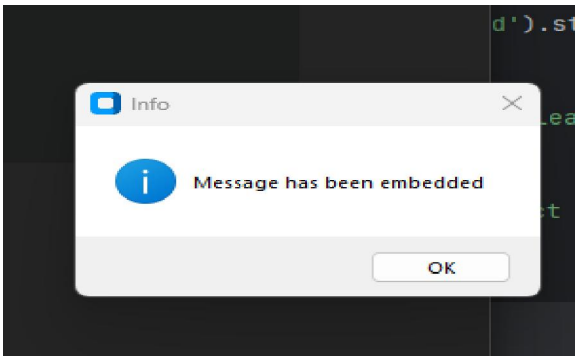


Figure 8: message embedding

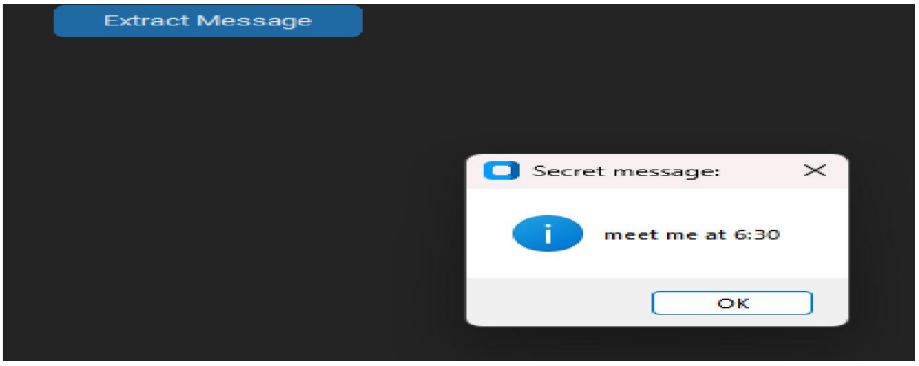


Figure 9: message extraction

VIII. RESULTS

After carrying out various test like unit test, integration test and system test, the system satisfies them and gives out the desired outputs. The system is able to provide encrypted cipher text of the plain text to the user. The system is able to provide decrypted plain text of the cipher text to the user. The system is able to display the FAQs and their corresponding answers. The system is able to correctly and smoothly embed and extract messages to and from images using the LSB technique. The chat section encrypts the message before sending and only displays the encrypted message on the sender's end and displays decrypted text on the receiver's end.

IX. DISCUSSION

This application showcases a high possibility of integrating the strengths and weaknesses of different cryptography algorithms to come up with a system that has combined strength. Vigenère cipher is thought to be weak and old, but by combining it with strong algorithms, it becomes just as strong. Though this is the case, additional research should be considered as security of systems still faces constant threats in this new digital age

X. CONCLUSION

In conclusion, the project has achieved its objectives, delivering a functional application for encrypting text using Vigenère cipher with a twist of modern cryptographic algorithms, AES. The project has been successfully completed with all deliverables meeting the requirements. This project's documentation has presented a comprehensive overview of the application. The objective of the project was to design and develop an application that will help people encrypt and send messages through a secure communication channel. Throughout the documentation, we have discussed various aspects of the project, including system analysis, specifications, design, implementation, and future enhancements. The project has been of great help for me in gaining valuable information on software development. It has given me a great satisfaction in having designed an application that has importance in the real world. The project's

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: 7.53
Volume 4, Issue 3, November 2024

success opens doors for future improvements, advancements, and potential collaborations to further enhance the application's capabilities and reach a wider audience in need of secure and proper transfer encrypted messages.

ACKNOWLEDGEMENT

Firstly, all praise goes to God for life and the ability to carry out my project work and this journal articles. All things work because of him. Secondly, I would like to thank my family for their unwavering support. I would like to thank the DMI – St. John the Baptist University Malawi, specifically DMI-SJBU Lilongwe campus for providing me the opportunity to do my project and journal article, in partial fulfilment of the computer science degree curriculum. I also sincerely thank Ms. Fanny Chatola for her support in making this paper possible as well guiding throughout my entire project. Another vote of thanks goes to the Mr. Mtende Mkandawire, Head of Computer Science and Information Technology for their kind help during my project work. Lastly, I would like to thank my friends and classmates who gave me a helping hand throughout the two phases of my project work.

REFERENCES

[1]. Kangmouse, M., Handoko, B., Rizqy, A (2023). *File Cryptography Optimization Based On Vigenère Cipher and AES.* Journal of Applied Intelligent System.

[2]. Soofi A.A., Riaz, I., Rasheed, U (2016). *An Enhanced Vigenère Cipher for Data Security.* International Journal of Scientific & Technology Research (IJSTR).

[3]. Pandey, S., Baniya, P., Nand, P (2020). *CryptStego: Powerful Blend of Cryptography for Securing Communications.* Emerging trends and applications in artificial intelligence. Springer Nature Switzerland.

[4]. Christopher, C., Gunawan, A., Sheila Prima (2022). *Encrypted Short Message Service Design Using Combination of Modified Advanced Encryption Standard (AES) And Vigenère Cipher Algorithm*. Engineering, Mathematics and Computer Science (EMACS) journal.

[5]. Olaniyan, A., Aliyu, A (2016). *Vigenère Cipher: Trends, Reviews and Possible Modifications.* International Journal of Computer Applications.

[6]. Li, C., Ma, J., Jun, T., Mayo, J., & Shene. C.K, (2015). *Vigvisual: A Visualization Tool for the Vigenère Cipher*. ACM Conference on Innovation and Technology in Computer Science Michigan Technological University.

[7]. Kushwah, R., Rajpurohit, R., Jonathan, P., & Kumar, G. (2022). *Web Application Based Text Encryption*. Fourteenth international conference on contemporary computing.

[8]. Gjergji, M., & Lamagna, E.A. (2021). *Web-Based Toolkit for Exploring Cryptography*. Journal of computing sciences in colleges.

[9]. Picela, S., & Jakobovic, D. (2020). *Evolutionary Computing and Machine Learning in Cryptography*. University of Zagreb.

[10]. Slayton, R. (2020). *Democratizing Cryptography: The Work of Whitefield Diffle and Martin Hellman.* Cornell University