Advanced Encryption Standard(AES) File Encryption and Decryption Tool

Mandar Angchekar
386916341

Paras Suri 5643363582

Research and Analysis: Mandar Angchekar focused on the research aspects related to AES cryptography and its application in file security and data transmission. Drawing insights from the paper "Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," Mandar explored the intricacies of AES in enhancing data security and protecting against data breaches. This research included a deep dive into cryptographic measures, security issue identification, and the analysis of file security systems. Additionally, Mandar reviewed the "AES Algorithm-Based File Transfer System" paper, which emphasized the use of AES in securing data during transmission. This research was pivotal in understanding AES's efficiency and robust security features, especially in comparison to other encryption algorithms.

Implementation: In the implementation phase, Mandar played a crucial role in developing the user interface of the AES encryption and decryption tool. Leveraging the insights gained from the research, he focused on ensuring the tool was user-friendly and accessible, particularly for users with limited technical expertise. Mandar's contribution was instrumental in integrating a command-line interface that simplified encryption tasks, making the tool more approachable for a broader audience. He also worked on the backend processes, ensuring the seamless integration of AES encryption and decryption functionalities within the Python script.

Research and Analysis: Paras Suri's research contributions were centered around enhancing computational efficiency and security in AES encryption. He analyzed the "Parallel Multiprocessing and Scheduling on the Heterogeneous Xeon+FPGA Platform" paper, which provided insights into optimizing performance in cryptographic processing. This research was crucial in understanding how to balance computational load efficiently, a concept that was later applied to the encryption tool's development. Additionally, Paras reviewed the "Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach" paper, focusing on dynamic key generation and S-box generation to bolster AES against sophisticated cyberattacks. This research guided the implementation of secure and dynamic key management in the tool.

Implementation: In the implementation phase, Paras Suri was instrumental in integrating the security enhancements and performance optimizations into the AES tool. He applied the concepts of dynamic key generation and efficient computational load balancing to ensure the tool was not only secure but also performed optimally. Paras's work in the project included developing the core encryption and decryption logic in Python, ensuring the tool adhered to the highest standards of data security. He also contributed to the testing and validation process, rigorously evaluating the tool across different file formats and sizes to guarantee its reliability and effectiveness.

***Abstract*—In the digital age, data security is a paramount concern, with encryption being a cornerstone in protecting sensitive information. The Advanced Encryption Standard (AES) is widely acknowledged for its robustness in securing data, yet its complexity often poses a barrier to widespread adoption. This project introduces an AES-based file encryption and decryption tool, designed to demystify cryptographic practices for non-expert users while maintaining high standards of security. Developed as part of the CIS 628 Introduction to Cryptography course at Syracuse University, this tool leverages Python and the Crypto.Cipher library to implement AES in Cipher Block Chaining (CBC) mode, coupled with a user-friendly command-line interface. The tool automates key generation and management, significantly reducing the risk of key mismanagement and making AES encryption more accessible. This report details the development process, highlighting the tool's novel approach to simplifying encryption, its contribution to the field of data security, and the challenges encountered during its creation. The result is a practical, efficient, and secure tool that bridges the gap between advanced cryptographic techniques and everyday data protection needs, promoting wider adoption of AES encryption in various user scenarios.**

I. Introduction

In an era where data security is paramount, the need for robust encryption tools has never been greater. With the increasing frequency of cyber threats and data breaches, protecting sensitive information has become a critical concern for individuals and organizations alike. The Advanced Encryption Standard (AES) has emerged as a leading encryption algorithm, widely recognized for its strength and efficiency in securing data. However, the technical complexity of implementing AES encryption has often been a barrier to its widespread adoption, particularly among users with limited technical expertise in cryptography.

This project, titled "Advanced Encryption Standard (AES) File Encryption and Decryption Tool," aims to address this gap by developing a user-friendly tool that simplifies the process of encrypting and decrypting files using AES. The primary objective is to make AES encryption more accessible and approachable for a broader audience, thereby enhancing the overall security of data management practices.

The project was undertaken as part of the coursework for CIS 628 Introduction to Cryptography at Syracuse University in the Fall of 2023. It represents a collaborative effort to integrate advanced cryptographic techniques with ease of use, ensuring that strong data protection is not just the domain of experts but is available to everyone.

In this report, we delve into the execution, significance, literature background, results, and challenges of the project. The report aims to provide a comprehensive overview of the project's development process, its contributions to the field of cryptography, and its potential impact on data security practices.

II. Execution

A. What the Project Does:

The project develops an Advanced Encryption Standard (AES) based tool for file encryption and decryption, aimed at enhancing the security of file encryption and decryption operations. This tool is designed to be accessible to users with varying levels of technical expertise, democratizing the use of advanced cryptographic practices. It allows users to securely encrypt files using AES and decrypt them using a uniquely generated key.

B. Solution Approach:

The implementation of the tool was achieved using Python, leveraging the Crypto.Cipher library for AES operations. The approach was methodical, focusing on both security and user accessibility. Key features of the implementation include:

- **AES in CBC Mode**: The tool employs Cipher Block Chaining (CBC) mode for AES encryption. CBC mode is chosen for its robustness against various cryptographic attacks and its ability to ensure data integrity.
- **Random Key Generation**: A critical aspect of AES encryption is the key used. The tool uses **Crypto.Random** to generate a 16-byte key, ensuring a high level of security. This random key generation is crucial for preventing predictable patterns in encryption, making it more resistant to brute-force attacks.
- **File Handling**: The tool handles the encryption and decryption of files efficiently. It reads the original file, performs the encryption or decryption operation, and then writes the output to a new file. This process includes saving the encrypted data and the encryption key in a secure manner, ensuring that the key is accessible for decryption but not easily compromised.
- **User Interface**: A significant focus was on developing a user-friendly command-line interface. This interface guides users through the encryption and decryption processes with clear instructions and feedback. It was designed to be intuitive, requiring minimal technical knowledge from the user.

C. How the Solution was Achieved:

The development process involved several key steps:

- **Writing the Python Script**: The core of the project was writing a script that integrates AES encryption and decryption functionalities. This script includes the **AESCipher** class, which encapsulates the encryption and decryption logic.
- **Interface Development**: A command-line interface was developed to interact with the tool. This interface uses simple prompts and clear instructions to guide the user through the process of encrypting or decrypting a file.

- **Testing and Validation**: Rigorous testing was conducted to ensure the tool's reliability and security. This included testing with various file types and sizes to ensure the tool's performance remained consistent and effective across different use cases.
- **Security Considerations**: Special attention was given to the security aspects, particularly in key generation and management, to ensure that the encryption provided by the tool is robust against common cryptographic attacks.

III. Significance

This section elucidates the significance of the AES File Encryption and Decryption Tool and its novel contributions to the existing body of knowledge in the realm of cybersecurity and cryptography.

A. Significance of the Work: The development of this tool has considerable implications in the field of data security. Its significance lies in the following areas:

1. Enhancing Data Security: By providing a user-friendly means to implement AES, the tool directly contributes to strengthening the security of sensitive information for a diverse user base, encompassing individuals and organizations alike.
2. Fostering Adoption of Encryption: The tool lowers the barrier to adopting encryption by making the process simpler and more accessible, which is crucial in an age where data breaches are increasingly common.
3. Empowering Users: It empowers users with limited technical knowledge to take proactive steps in protecting their data, contributing to a more security-conscious society.
4. Education and Awareness: This project also serves an educational purpose, potentially being used as a teaching aid to demonstrate encryption in practical, real-world scenarios.

B. Novelty of the Work: The innovative aspects of this tool that add to the existing body of knowledge are:

1. User-Friendly Interface: While AES is known for its security, it is also known for its complexity. This tool breaks down these barriers with a user interface that is approachable for non-experts, which is a significant departure from existing tools that often cater to a more technically savvy audience.
2. Automated Key Management: The tool automates the generation and management of encryption keys, a task that typically requires sophisticated understanding. This automation is key to preventing common errors in key management that can compromise security.
3. Integration of Security and Efficiency: The research that underpins the tool's development has led to an implementation that does not sacrifice computational efficiency for security, ensuring that the tool is practical for use with large files and in environments where resources are constrained.
4. Adaptability Across Platforms: The Python-based design provides cross-platform compatibility, making the tool versatile across different operating systems and user environments.
5. Educational Framework: By simplifying AES encryption and decryption, the tool also provides an educational framework for users to understand cryptographic principles in a hands-on manner, thus contributing to broader learning objectives in cybersecurity education.

In conclusion, the AES File Encryption and Decryption Tool presents a novel approach to data security by merging ease of use with advanced encryption standards. It stands out in the existing literature and market as a bridge between complex cryptographic algorithms and everyday data protection needs, promoting wider adoption and understanding of encryption as a fundamental aspect of digital security.

IV. Literature search

A. Related Works:

This In developing the "Advanced Encryption Standard (AES) File Encryption and Decryption Tool," a comprehensive literature search was conducted to understand the current state of AES-based security systems and identify areas for innovation. Four key research papers were instrumental in shaping the direction and development of this project:

1. **"Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based"**
    - **Overview**: This paper delves into enhancing data security through AES, addressing cryptographic measures to protect against data breaches. It outlines a framework for identifying security issues, analyzing file security, and studying AES cryptography.
    - **Relevance**: The research's focus on developing a user-friendly AES-based cryptographic system parallels our project's goal of simplifying encryption tasks. However, our project extends this concept by integrating a command-line interface, making it more accessible to users with varying technical backgrounds.
2. **"AES Algorithm-Based File Transfer System"**
    - **Overview**: This paper emphasizes the use of AES in securing data during transmission, highlighting AES's efficiency and robust security. It presents an AES-based file transfer system with a user interface

developed using HTML and CSS, and backend processes in Java.

- **Relevance**: While this research focuses on data transmission security, our project concentrates on file encryption and decryption at the user level. The comparison of AES with other encryption algorithms in this paper provided valuable insights into the superiority of AES, reinforcing our choice of encryption standard.

3. **"Parallel Multiprocessing and Scheduling on the Heterogeneous Xeon+FPGA Platform"**

    - **Overview**: This study explores the enhancement of heterogeneous computing through a dynamic, adaptive scheduler on a CPU-FPGA platform. It demonstrates significant performance improvements in computing efficiency.

    - **Relevance**: The concepts of efficiency and performance optimization were influential. Our project leverages these ideas in the context of cryptographic processing, ensuring that our tool remains efficient and responsive during encryption and decryption tasks.

4. **"Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach"**

    - **Overview**: This paper proposes enhancements to AES by integrating dynamic key generation and S-box generation, aiming to increase resistance to cryptographic attacks. It introduces complexity to the encryption process, adding layers of confusion and diffusion.

    - **Relevance**: The concept of dynamic key generation resonated with our project, as we implemented a secure random key generation mechanism. However, our approach maintains a balance between added security and maintaining user-friendliness, which is crucial for our target audience.

Differentiation from Existing Literature: Our project distinguishes itself from these studies by focusing on the amalgamation of robust AES encryption with a user-friendly interface, specifically targeting users with limited technical knowledge in cryptography. While the reviewed papers provide valuable insights into AES's security aspects and potential enhancements, our project uniquely addresses the challenge of making AES encryption accessible and practical for everyday use. This approach not only contributes to the field of cryptography by broadening the user base for AES encryption but also enhances overall data security practices by simplifying the encryption process for a wider audience.

cryptographic techniques accessible to non-experts. The development of a simple, intuitive user interface and the automation of key management are key differentiators that set this project apart from existing solutions.

V. Results

A. *Accomplishments:*

- **Development of AES Tool**: Successfully developed a fully functional AES encryption and decryption tool with a focus on user accessibility.

- **Effective Testing**: The tool was rigorously tested across various file formats and sizes, ensuring its reliability and effectiveness in real-world scenarios.

- **Balanced Security and Usability**: Achieved a balance between robust security features and user-friendliness, making the tool suitable for both technical and non-technical users.

B. *Impact of Result:*

The successful development and testing of this tool demonstrate that it is possible to create cryptographic tools that are both secure and accessible. This has implications for the wider adoption of encryption practices, potentially leading to enhanced data security across different user groups.

Acknowledgment

I would like to express my sincere gratitude to Professor Vir Phoha for his invaluable guidance and profound insights, which have significantly shaped this research. My appreciation also extends to TA Sajjad and Grader Jay Ganatra for their continuous support and constructive feedback throughout the development of this paper.

References

[1] F. J. D'souza and D. Panchal, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach," in Proceedings of the International Conference on Computing, Communication and Automation (ICCCA2017), 2017, pp. 647-652.,

[2] A. Rodríguez, A. Navarro, R. Asenjo, F. Corbera, R. Gran, D. Suárez, and J. Nunez-Yanez, "Parallel multiprocessing and scheduling on the heterogeneous Xeon+FPGA platform," in The Journal of Supercomputing, vol. 76, 2020, pp. 4645–4665.

[3] K. Muttaqin and J. Rahmadoni, "Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," in Journal of Applied Engineering and Technological Science, vol. 1, no. 2, 2020, pp. 113-123.

[4] M. Katiyar, A. Dixit, and Dr. P. Murali, "AES Algorithm-Based File Transfer System," in International Research Journal of Modernization in Engineering Technology and Science, vol. 04, no. 05, May 2022, pp. 446