TITLE: Encryption and Decryption System for Secure File Protection.

NAME: Benjamin Makwangwala

ABSTRACT

This study presents the design and implementation of a software system capable of encrypting and decrypting multiple file formats—specifically documents, text files, MP3s, MP4s, and images. In today's digital age, the security of personal and confidential data is of utmost importance. Unauthorized access, data theft, and cyber-attacks threaten information stored on digital devices. This project addresses these challenges by developing a simple, user-friendly file encryption and decryption tool for PCs. The methodology involves using cryptographic algorithms to transform readable files into encrypted formats and restore them back when needed. The system was tested on various file types to evaluate its performance, effectiveness, and reliability. Results show that the system efficiently encrypts and decrypts files without data loss, ensuring confidentiality and protection. This tool is useful for individuals, organizations, and institutions needing a secure method of storing and transferring files. Future improvements could include cross-platform support and integration of advanced encryption standards.

KEYWORDS

Encryption, Decryption, Data Security, File Protection, Cryptography, Information Privacy

INTRODUCTION

In an increasingly digital world, the need for protecting sensitive data is more urgent than ever. Files such as documents, images, audio, and video are frequently transmitted and stored on personal and organizational systems. Without adequate protection, this data can be intercepted, modified, or misused. Encryption and decryption are essential mechanisms in data security. Encryption transforms readable information into a coded format, while decryption restores it to its original form. This project aims to build a system that encrypts and decrypts common file types—text, MP3, MP4, images, and documents—on a PC environment. The tool is intended to offer simple and reliable protection to digital files, especially for non-technical users. The motivation

behind this project stems from growing concerns over data privacy and the lack of accessible security tools for everyday users.

LITERATURE REVIEW

A wide body of research has focused on encryption algorithms and their application in data security. Traditional techniques such as the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and RSA have been studied and implemented in various security systems. Researchers like Schneier (1996) emphasized the importance of strong encryption in digital communication, while Stallings (2005) explored cryptographic principles in real-world applications. More recent works address the usability of encryption tools and their integration into user-friendly platforms. Studies also reveal gaps in availability of simple encryption systems for common users, especially those not in enterprise environments. This project builds upon existing encryption research, focusing on practical file protection rather than complex network security.

METHODOLOGY

The project was developed using a combination of Python and third-party cryptographic libraries. The system follows a modular design, with two main components: the encryption module and the decryption module.

1. File Input Handling – The system allows users to select files in various formats (.txt, .docx, .mp3, .mp4, .jpg, .png, etc.).

2. Encryption Algorithm – The AES algorithm was implemented due to its strong security and performance. It uses a symmetric key provided by the user to encrypt the data.

3. Decryption Algorithm – Files encrypted by the system can be restored using the correct key. Any mismatched key results in failure, ensuring data integrity.

4. User Interface – A graphical interface was created for ease of use, allowing users to encrypt or decrypt files with just a few clicks.

Testing was carried out using sample files in all supported formats to ensure successful encryption and decryption without corruption.

RESULTS

The system was tested on five categories of files: .txt, .docx, .mp3, .mp4, and .jpg/.png. Encryption times varied slightly based on file size, but all files were processed within acceptable time limits. Decryption consistently restored files without data loss. No compatibility issues were found during testing on Windows-based PCs. Table 1 shows average processing time for each file type.

Table 1: Average Processing Time per File Type

File Type	Encryption Time	Decryption Time

| File Type | Average Size | Encryption Time | Decryption Time | |----------|-------------|----------------|----------------| | .txt | 50KB | 0.2 seconds | 0.2 seconds | | .docx | 120KB | 0.5 seconds | 0.4 seconds | | .mp3 | 3MB | 1.4 seconds | 1.3 seconds | | .mp4 | 20MB | 4.5 seconds | 4.3 seconds | | .jpg | 500KB | 0.6 seconds | 0.5 seconds |

DISCUSSION

The results indicate that the encryption and decryption system functions reliably across various file types. The use of AES ensures robust protection, while the user interface allows accessibility to non-experts. Compared to prior research and tools focused on text encryption alone, this system expands usability by including multimedia files. Challenges faced included managing large video files and ensuring compatibility with multiple file formats, which were resolved through optimized buffer handling and format detection. The system does not currently support cloud storage encryption, which presents an area for future work.

CONCLUSION

This project successfully developed an Encryption and Decryption System that secures a wide range of file formats on PCs. It provides an easy-to-use tool for protecting sensitive files from unauthorized access. The system was tested thoroughly and achieved reliable performance across all supported file types. It contributes to data privacy efforts by offering a practical solution for everyday users. Future upgrades could include support for mobile platforms, cloud integration, and the use of biometric authentication.

REFERENCES

Schneier, B. (1996). Applied Cryptography. John Wiley & Sons.

Stallings, W. (2005). Cryptography and Network Security. Pearson Education.

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor.

National Institute of Standards and Technology (NIST). (2001). Advanced Encryption Standard (AES). [FIPS Publication 197].

Paar, C., & Pelzl, J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.