Encryption and Decryption of a file

A Mini Project Report Submitted in Partial Fulfillment for the Award of the Degree of Bachelor of Technology in Computer Science and Engineering

Dr. A. P. J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

Submitted by:

Tanu Keshari (2300100100443)

Supriya Verma (2300100100431)

Isha Sahu (2302840100103)

Shraddha Singh (2302840100216)

UNDER THE SUPERVISION OF

Mr.Dinesh Kumar Kushwaha

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNITED COLLEGE OF ENGINEERING AND RESEARCH, PRAYAGRAJ,

September,2024

CERTIFICATE

This is to certify that the project titled **"Encryption and Decryption of a file"** submitted by **Tanu Keshari (2300100100443)**, **Isha Sahu (2302840100103)** , **Shraddha Singh (2302840100216)** and **Supriya Verma (2300100100431)** in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science Engineering) submitted to Dr. A. P. J Abdul Kalam Technical University, Lucknow at United College of Engineering and Research, Prayagraj is an authentic record of their own work carried out during a period from **29th August,2024 to 11th September,2024** under the guidance of **Mr.Dinesh Kumar Kushwaha**, Assistant Professor Department of Computer Science Engineering. The Major Project Viva-Voce Examination has been held on _____.

Signature of the Guide:
Mr.Dinesh Kumar Kushwaha

Signature of Project Coordinator:
Dr.Rahul Kesharwani

Signature of the Head of Department:
Dr. Vijay Kumar Dwivedi

Place: Prayagraj
Dated:

CANDIDATE'S DECLARATION

We, hereby certify that the project entitled **"Encryption and Decryption of a file"** submitted by us in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science Engineering) submitted to **Dr. A. P. J. Abdul Kalam Technical University, Lucknow** at **United College of Engineering and Research, Prayagraj**, is an authentic record of our own work carried out during a period from **29th August,2024 to 11th September,2024** under the guidance of **Mr.Dinesh Kumar Kushwaha, Assistant Professor**, Department of Computer Science Engineering. The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

Signature of the Student
Tanu Keshari (2300100100443)

Signature of the Student
Supriya Verma (2300100100431)

Signature of the Student
Isha Sahu (2302840100103)

Signature of the Student
Shraddha Singh (2302840100216)

Place: Prayagraj
Dated:

ACKNOWLEDGEMENTS

We express our sincere gratitude to Dr. A. P. J Abdul Kalam Technical University, Lucknow for giving us the opportunity to work on the Summer Training Project during our final year of B.Tech. (CSE) is an important aspect in the field of engineering.

We would like to thank **Dr.Swapnil Srivastava, Principal and Dr. Vijay Kumar Dwivedi, Head of Department, CSE at United College of Engineering and Research, Prayagraj** for their kind support.

We also owe our sincerest gratitude towards **Mr.Dinesh Kumar Kushwaha** for her valuable advice and healthy criticism throughout our project which helped us immensely to complete our work successfully.

We would also like to thank everyone who has knowingly and unknowingly helped us throughout our work. Finally, a word of thanks for the authors of all those books and papers which we have consulted during our project work as well as for preparing the report.

ABSTRACT

The title of our project is “ENCRYPTION AND DECRYPTION of a file”. This project encypts and decrypts the textual files by using simple XORed encryption ,decryption algorithm.Our aim is to develop the file named ENCRYPTION AND DECRYPTION that encrypts and decrypts the textual files by using simple XORed algorithm. Encryption and Decryption is a strong text and file encryption software for personal and professional security . It protects privacy of our documents and sensitive files by encrypting them using simple XORed alogrithm to provide high protection against unauthorized data access. If you need to sensitive message over the internet, you should send it in the encrypted form. Encryption and decryption allows you easily encrpyt and decrypt your file

Contents

0.1 *Introduction*

The File Encryption and Decryption Project is designed to provide a secure way to protect sensitive data stored in files. With the increasing concern over data breaches and unauthorized access, it has become essential to ensure that personal and organizational data remains confidential.

This project aims to implement a system that can securely encrypt files to prevent unauthorized access and decrypt them for authorized users.

In today's digital age, the protection of sensitive information is more crucial than ever. As we increasingly rely on digital communication, the risk of unauthorized access to our data grows. Encryption and decryption techniques play a vital role in safeguarding this information, ensuring that only intended recipients can access and understand the data being transmitted

0.2 *Objective of the project*

The main objective of this project is to ensure secure storage and transmission of sensitive data by implementing encryption and decryption techniques for files. The project aims to:

- Protect Data Confidentiality – Prevent unauthorized access to sensitive information stored in files.
- Maintain Data Integrity – Ensure that the original content of the file is not altered during storage or transmission.
- Provide Secure File Transmission – Allow files to be shared over networks without risk of interception or misuse.
- Implement Cryptographic Algorithms – Apply suitable encryption algorithms (e.g., AES, RSA, DES) to convert readable data into an unreadable format and decrypt it back when required.
- User Authentication – Restrict access to encrypted files so that only authorized users can decrypt and view the contents.
- Practical Application – Demonstrate how cryptography can be used to secure personal, organizational, or confidential data.

0.3 *Module*

- File Selection : The user can select a file using JfileChooser
- Encryption/Decryption : The file's content is read into a byte
- array,and each byte is XORed with the provided key (which is taken from
- the user via a text field).
- File Overwrite : After encryption or decryption,the modified data
- is written back to the same file.
- GUI Element :
- A Jframe with a jbutton for starting th encryption and decryption process.
- A JtextField for entering the encryption key.

0.4 *Benefits*

- Data Confidentiality
- Data Integrity
- Secure Communication
- User Authentication
- Protection Against Data Theft
- Compliance with Security Standards
- Versatility
- Enhanced Trust and Reliability

0.5 *Hardware and Software Requirements*

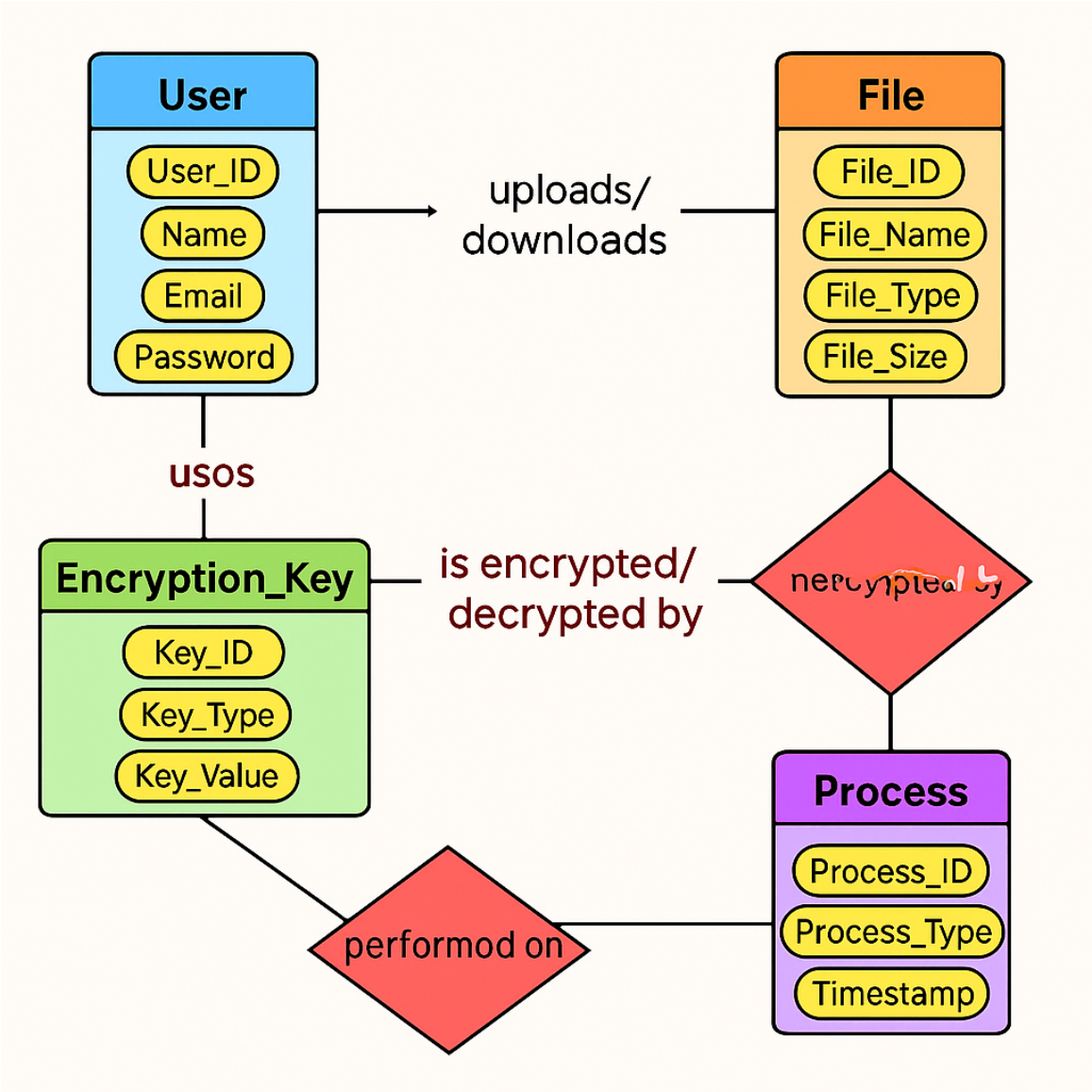
Hardware Requirement

- Processor:Intel i3 or AMD equivalent
- Linux or abovee or later
- RAM:At least 4GB
- Storage: 200MB Free space for JDK IDE

Software Requirement

- Operating System: Window7,
- mac0S10.14(Mojave)
- Developing tools:JDK 8 later,IDE

0.6 *ER Diagram*



0.7 *Conclusion*

The project on file encryption and decryption highlights the importance of securing sensitive data against unauthorized access, theft, and misuse. By applying cryptographic techniques, files can be transformed into an unreadable format during storage or transmission and later restored to their original form by authorized users. This ensures confidentiality, integrity, and security of information.

The implementation of encryption and decryption not only protects personal and organizational data but also builds trust in digital communication and storage systems. With growing cyber threats and data breaches, encryption has become a crucial security measure for individuals, businesses, and government organizations.

In conclusion, this project demonstrates that cryptography is an effective and reliable solution for safeguarding digital information, making it a key component of modern cybersecurity practices.

0.8 *Future scope*

- Integration of Advanced Algorithms
- Implementing stronger encryption standards like AES-256, RSA-4096, or Elliptic Curve Cryptography (ECC) to enhance security.
- Hybrid Cryptosystems
- Combining symmetric and asymmetric encryption for faster processing with stronger key management.
- Cloud-Based Encryption
- Extending the system to secure files stored and shared on cloud platforms such as Google Drive, Dropbox, or OneDrive.
- Multi-Factor Authentication (MFA)
- Adding authentication mechanisms like OTPs, biometrics, or smart cards before decrypting files.
- Automation and User-Friendly Interface
- Developing a GUI-based application that allows users to encrypt/decrypt files with simple clicks instead of command-line operations.
- Cross-Platform Support
- Expanding the system to work across multiple operating systems (Windows, Linux, macOS, Android).
- Performance Optimization
- Improving the speed and efficiency of encryption for large files without compromising security.
- Blockchain Integration
- Using blockchain for decentralized file storage and encrypted file sharing to ensure transparency and tamper-proof records.
- AI-Powered Threat Detection

- Integrating artificial intelligence to detect unauthorized decryption attempts and alert the user.
- Compliance and Legal Use Cases
- Enhancing the system to meet legal and industry standards (like GDPR, HIPAA, PCI-DSS) for secure data handling.