­

**Faculty Name:** RAJESH R

**Subject:** Cryptography and Network Security Lab (BCSE309P)

**Project Title:** Implementing cryptographic techniques in a cloud platform for storage and transit

**Team Members:**

1. Yamasani Purushotham Reddy 21BCE5289
2. Vagadia Anand Kantilal 21BCE1212
3. Akili Harsha Vardhan 21BCE5353

**Abstract:**

Aims to implement cryptographic techniques in a cloud platform for secure storage and transit of data. By surveying various research papers and studies, this project will address the problem of data security in cloud environments and propose effective solutions. The motivation behind this project is to ensure the confidentiality, integrity, and availability of data stored and transmitted in the cloud. Challenges include that need to be overcome, such as selecting the appropriate cryptographic algorithms, managing encryption keys, and ensuring efficient data transfer. Aims is to develop a robust and scalable system that leverages cryptography to protect data in the cloud.

**Problem Statement:**

The problem addressed is the lack of adequate data security in cloud environments, which can lead to unauthorized access, data breaches, and loss of data integrity.

**Motivation:**

The motivation behind this project is to enhance the security of data stored and transmitted in the cloud, ensuring that sensitive information remains confidential and protected from unauthorized access. By implementing cryptographic techniques, the project aims to provide a secure and reliable cloud storage and transit platform.

**Challenges:**

Selection of Cryptographic Algorithms: Choosing the most suitable cryptographic algorithms for data encryption and decryption in the cloud is a challenge. Will evaluate different algorithms and select the ones that provide the highest level of security and efficiency.

Key Management: Managing encryption keys securely is crucial for the success of the project. Needs to ensure that encryption keys are properly generated, stored, and distributed to authorized users while preventing unauthorized access.

Efficient Data Transfer: Ensuring efficient and fast data transfer in the cloud while maintaining data security is a challenge. Will explore techniques to optimize data transfer speed without compromising the security of the transmitted data.

**Methodologies:**

Hybrid Cryptography: Utilizing a combination of symmetric and asymmetric cryptographic algorithms, such as AES and RSA, to achieve a balance between security and efficiency in data storage and transit.

Data Integrity Verification: Employing hash functions, such as SHA-256, to generate hash values for data before and after encryption to ensure data integrity during storage and transit in the cloud.

By successfully addressing these challenges, this project will contribute to a more secure cloud storage and transit environment.

**Literature survey:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.no** | **Title** | **Author** | **Methodology** | **Advantages** |
| **1.** | The research article "Security in Cloud Computing Using Cryptographic Algorithms" was published in the International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, in September 2014 | Shakeeba S. Khan and Sakshi S. Deshmukh, | The article analyses different security issues in cloud computing and explores the adoption of cryptographic algorithms to enhance cloud security. It provides a comprehensive review of various types of clouds, characteristics of cloud computing, and security challenges specific to cloud environments. Additionally, the article delves into the detailed workings of different cryptographic algorithms used in cloud security, including symmetric-key and asymmetric-key algorithms. | The article offers valuable insights into cloud security challenges and the role of cryptographic algorithms in addressing these concerns. It provides a thorough analysis of different types of clouds, characteristics of cloud computing, and various security issues specific to cloud environments, making it a comprehensive resource for understanding and enhancing cloud security measures |
| **2.** | Study and Comparison of Cryptographic Methods for Cloud Security" by Ashwini Bangar & Swapnil Shinde | Uma Somani, Prasad Rewagad, Kalpana parsi, and Dr. A. Padmapriya | The paper presents a comprehensive study and comparison of various cryptographic algorithms and hybrid systems for enhancing cloud security. It discusses the application of encryption, hash functions, and asymmetric key systems such as RSA and Diffie Hellman for data security in cloud computing | The proposed systems provide a high and efficient level of security, offering methods for secure file selection, hash function application, key exchange, digital signature authentication, and encryption using algorithms like RSA, DES, and AES. These techniques aim to ensure confidentiality, integrity, and availability of data in the cloud environment. |
| **3.** | The NIST definition of cloud computing | P. Mell, and T. Grance | Cryptography Implementation: Addressing security concerns in cloud computing through cryptographic solutions.  Shared Ownership: Exploring shared ownership as a potential solution in cloud security.  Cryptography Usage: Utilizing cryptography for proofs of irretrievability, homomorphic encryption, private information retrieval, broadcast encryption, and more.  Third-Party Box Work: Suggesting a third-party box as a gateway between client and cloud for enhanced security. | Confidentiality: Ensuring data confidentiality through cryptographic techniques.  Data Control: Addressing issues related to data control in cloud computing.  Secure Data Sharing: Implementing trusted data sharing mechanisms over untrusted cloud storage providers.  Improved Security: Enhancing security through collaborative approaches between crypto algorithms and security policies. |
| **4.** | An Enhancement of Data Security in Cloud Computing with an Implementation of a Two-Level Cryptographic Technique, using AES and ECC Algorithm | Dickson Kodzo Mawuli Hodowu, Dennis Redeemer Korda, Dr. Edward Danso Ansong | Techniques: Two-level cryptographic technique - symmetric (AES) and asymmetric (ECC) cryptographic techniques.  Implementation: AES for data at rest and ECC for data in transit.  Key Processes: AES encryption involves Byte Substitution, Shift Rows, Mix Column, Inverse Byte Substitution, and Inverse Mix Column.  ECC Features: Efficient encryption keys, digital signatures, smaller key sizes compared to RSA. | Enhanced Data Security: Ensures secure data transfer in cloud computing.  Improved Speed: ECC's smaller key sizes enhance cryptographic operations' speed.  Increased Trust: Enhances user trust in cloud services due to improved data security measures. |
| **5.** | Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques | G K Patra, Nilotpal Chakraborty | Introduction of Cloud Computing: Proposes using cloud computing to provide high performance computing (HPC) services to a wider audience.  Security Concerns: Addresses security issues in cloud computing, especially in the context of HPC services.  Cryptographic Techniques: Focuses on fully homomorphic encryption and functional encryption to secure cloud infrastructure for scientific computations.  Research Work: Conducts surveys on encryption schemes, analyses Gentry's scheme, and explores variants for efficient processing.  Implementation: Discusses ongoing work on devising schemes based on Learning with Errors (LWE) for noise control in encryption/decryption processes. | Cost-Effective Computing: Cloud computing offers a shared pool of resources, reducing the overhead costs of maintaining HPC infrastructure.  Accessibility: Provides HPC services to organizations of all sizes, including those with limited budgets.  Efficiency: Enables users to submit jobs through a web-based interface, streamlining the computation process.  Security Enhancement: Implementation of cryptographic techniques enhances the security of cloud infrastructure, ensuring data protection and privacy. |
| **6.** | Research Work on Encryption Schemes and Cloud Computing Advantages | Dr.Dlip Kumar | Conducts surveys on encryption schemes. Analyzes Gentry's scheme and explores variants for efficient processing. Ongoing work on devising schemes based on Learning with Errors (LWE) for noise control in encryption/decryption processes. | Cost-Effective Computing: Reduces overhead costs of maintaining HPC infrastructure.  Accessibility: Provides HPC services to organizations of all sizes, including those with limited budgets.  Efficiency: Streamlines the computation process by enabling users to submit jobs through a web-based interface.  Security Enhancement: Enhances the security of cloud infrastructure through cryptographic techniques, ensuring data protection and privacy. |
| **7.** | A Survey on Data Encryption Techniques in Cloud Computing, Asian Journal of Information Technology | S. Balasubramaniam, V. Kavitha | The study surveyed encryption techniques such as AES, DES, RSA, Blowfish, and homomorphic encryption, comparing their features and limitations for cloud security. | Dynamic selection of encryption algorithms Efficient encryption and verification scheme for data storage security Fully homomorphic encryption for computing arbitrary functions of encrypted data Hierarchical attribute-based encryption model for data sharing in cloud servers |
| **8.** | A novel DNA sequence dictionary method for secure data in DNA using spiral approach and framework of DNA cryptography | Shipra Zhen and Dr. Massive Flutter | Approach: DNA cryptography using a novel DNA sequence dictionary method and a spiral approach.  Techniques: Encryption algorithms and DNA assortment procedures for data security.  Focus: Secure data storage and transmission using DNA-based techniques. | Approach: DNA cryptography using a novel DNA sequence dictionary method and a spiral approach.  Techniques: Encryption algorithms and DNA assortment procedures for data security.  Focus: Secure data storage and transmission using DNA-based techniques. |
| **9.** | Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography) | Waseem Akram | Research Methodology: Based on secondary data collected from online sources, research papers, and Google Search Engine. | Enhanced Security: Advanced and enhanced algorithms and encryption techniques ensure secure storage and exchange of cloud data.  Data Protection: Cryptography techniques provide reliable security and protection of sensitive data, including cloud data protection through encryption and cryptographic key management.  Efficient Encryption: Use of DES and RSA algorithms for encryption and decryption processes to increase security in cloud storage. |
| **10.** | Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm | Sana Belguith, Abderrazak Jemai, and Rabah Attia | The methodology involves proposing a new lightweight encryption algorithm that combines symmetric and asymmetric cryptographic techniques to enhance data security in cloud computing | The advantages of this approach include efficient security, rapid performance, and the preservation of user access rights to data in a secured and authorized manner. The document also presents a comparison of various cryptographic algorithms and evaluates the proposed lightweight algorithm, demonstrating its faster processing time compared to state-of-the-art cryptographic algorithms |
| **11.** | A Survey on Data Encryption Techniques in Cloud Computing, Asian Journal of Information Technology. | R. Gupta, M. Singh | Surveyed encryption techniques (AES, DES, RSA, Blowfish, homomorphic encryption) for cloud security. | Enhanced data security through dynamic encryption algorithm selection. Robust encryption and verification scheme for secure data storage. Fully homomorphic encryption enables computation of arbitrary functions on encrypted data. Implementation of hierarchical attribute-based encryption model for secure data sharing in cloud servers |
| **12.** | Secure File Storage on Cloud using Hybrid Cryptography | Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam | The system utilizes a hybrid cryptography approach combining algorithms like 3DES, RC6, and AES with LSB steganography. Files are divided, encrypted using different algorithms simultaneously, and key information is securely stored in an image using LSB technique. Registration of users is required for accessing services, and decryption involves retrieving keys from the steganographic image created during registration. | Enhanced security through the combination of multiple cryptographic algorithms. Efficient data integrity, high security, low delay, authentication, and confidentiality. Better protection of customer data on a single cloud server. |
| **13.** | An improved attribute-based encryption technique towards the data security in cloud computing | Suyel Namasudra | Utilizes attribute-based encryption (ABE), distributed hash table (DHT) network, and identity-based timed-release encryption (IDTRE). Data encrypted based on user attributes, with ciphertext shares distributed in DHT network. IDTRE algorithm used to encrypt decryption key for secure data access. Access control model implemented for resource and knowledge sharing in cloud computing. | Enhanced data security in cloud computing environments. Fine-grained data access control for improved security. Resists various attacks in the cloud environment. Efficient data sharing and access control mechanisms. Performance analysis shows proficiency over existing schemes. |
| **14.** | Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques | G K Patra and Nilotpal Chakraborty | The paper discusses the challenges of security in cloud computing for high performance scientific computations. It explores the use of cryptographic techniques like fully homomorphic encryption and functional encryption to enhance cloud security. The authors propose schemes to secure model outputs and control access to shared data in scientific and engineering applications. | The research aims to enable the provision of high-performance computing services through cloud infrastructure, reducing costs and maintenance overhead. By implementing cryptographic techniques, the paper addresses security threats in cloud computing, ensuring data confidentiality and access control. |
| **15.** | A Hybrid Cryptographic Technique for Secured Authentication in Cloud Computing | Juber Mirza and Meena Sharma | Proposed a hybrid cryptographic technique for secure data storage and retrieval in cloud computing. Focused on server security and user trust by using a combination of cryptographic algorithms. Implemented a trust management technique to enhance trust between service providers and users. Utilized a secure and efficient encryption and decryption process for data protection. | Efficient encryption and decryption times compared to traditional cryptographic techniques. Reduced memory consumption for both encryption and decryption processes. Enhanced security and trust management for data preservation and access in cloud environments. |

**Encryption algorithm:**

The cryptographic encryption module serves as a crucial component in our cloud-based security system, facilitating the secure encryption of sensitive data. Key features and functionalities include:

Multiple Encryption Algorithms: The module supports various encryption algorithms, including AES in CBC mode, ChaCha20Poly1305, AES-GCM, and AES-CCM. Each algorithm offers unique strengths in terms of security and performance, allowing for flexibility in encryption strategies.

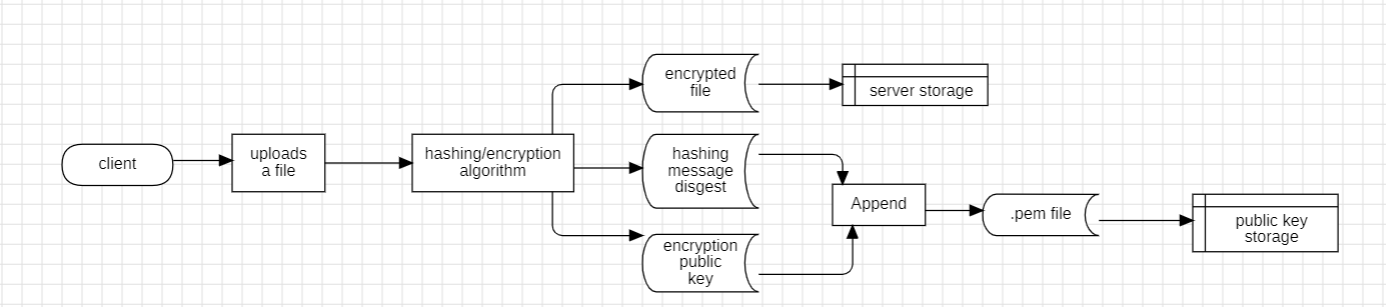
Key Management: Encryption keys are generated dynamically for each encryption session. Key rotation is implemented to enhance security by periodically changing encryption keys. The module also incorporates the use of asymmetric encryption for securely sharing and storing encryption keys.

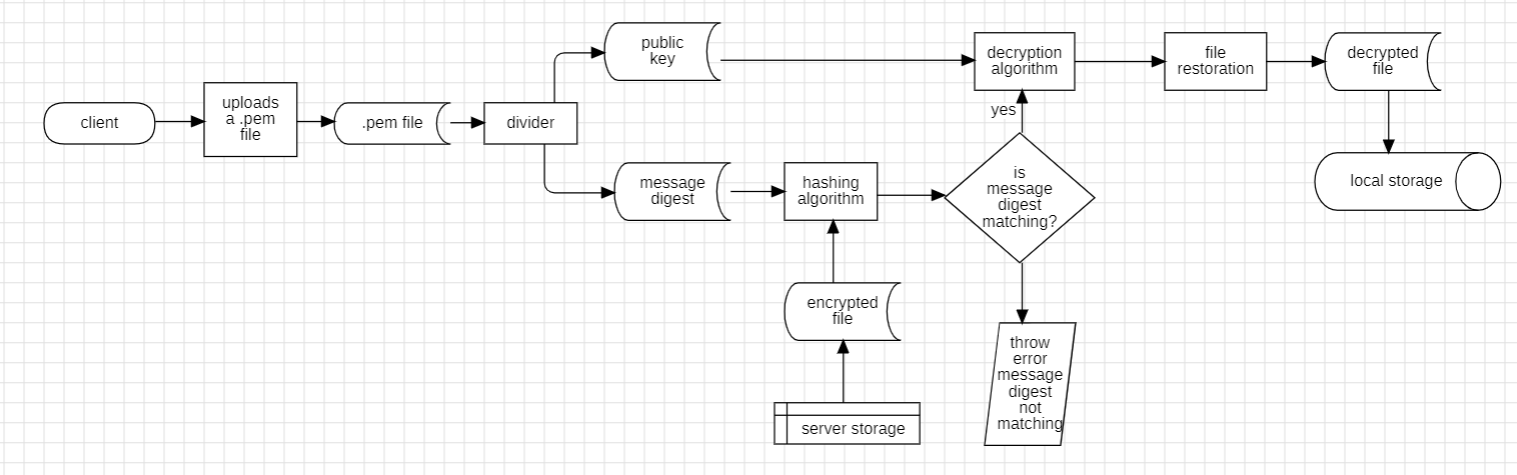
File Encryption: Files uploaded to the system are encrypted using the selected encryption algorithm and the corresponding encryption key. The encrypted files are stored securely in the cloud, ensuring confidentiality and data integrity.

Secure Key Storage: Encryption keys are securely stored and managed to prevent unauthorized access. The module utilizes cryptographic techniques to encrypt and protect encryption keys, mitigating the risk of key compromise.

Integration with Flask Application: The encryption module seamlessly integrates with our Flask-based web application, allowing users to upload files for encryption and decryption. The module provides robust encryption services through a user-friendly interface, enhancing the overall security of the system.

**Architecture of the application:**

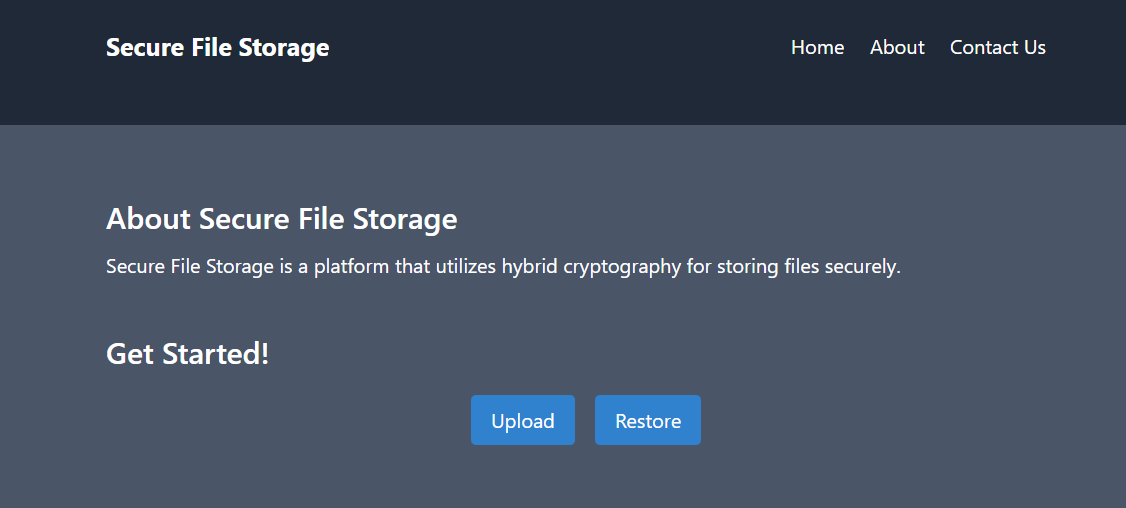
**Encryption:**

**Decryption:**

**Using the flask app:**

**Encryption:**

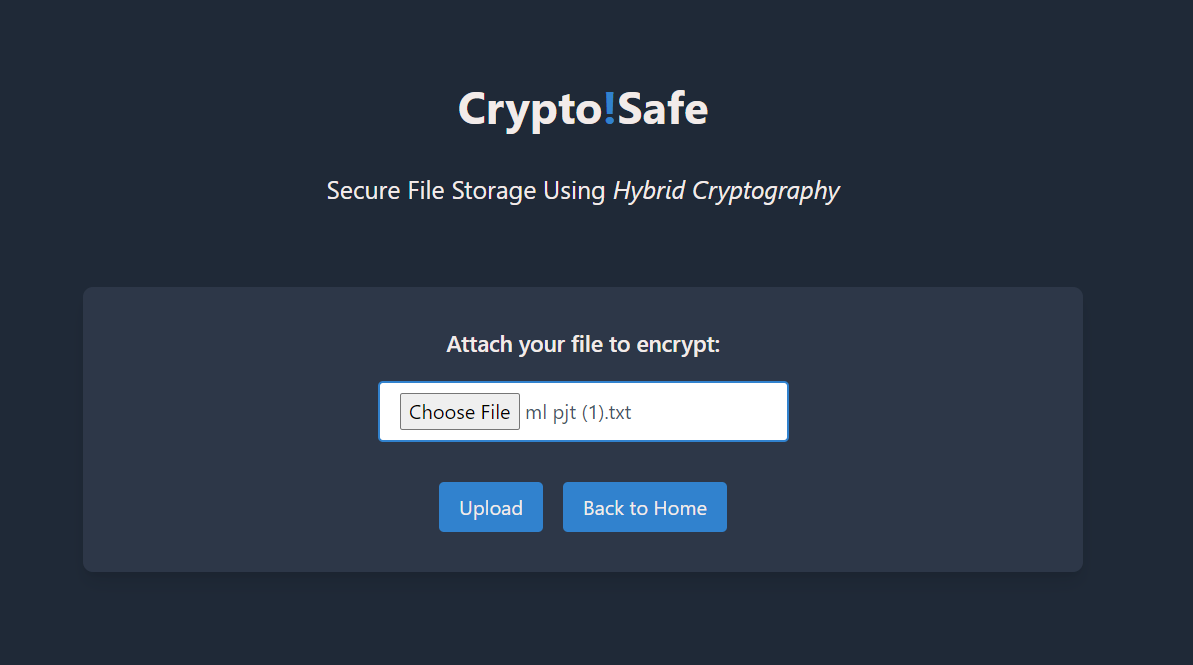
1. Accessing the Application:

Open your web browser and navigate to the URL where the application is hosted.  


1. Uploading Files:

Click on the "Upload" button to initiate the file upload process.

Select the file(s) you wish to encrypt from your local system and confirm the selection.



1. Initiating Encryption:

Once the file(s) are uploaded successfully, the encryption process will automatically begin.

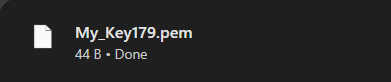
The application will divide large files into smaller chapters for efficient processing during encryption.



1. Downloading Encrypted Files:

After encryption is completed, you will be provided with options to download the encrypted files.

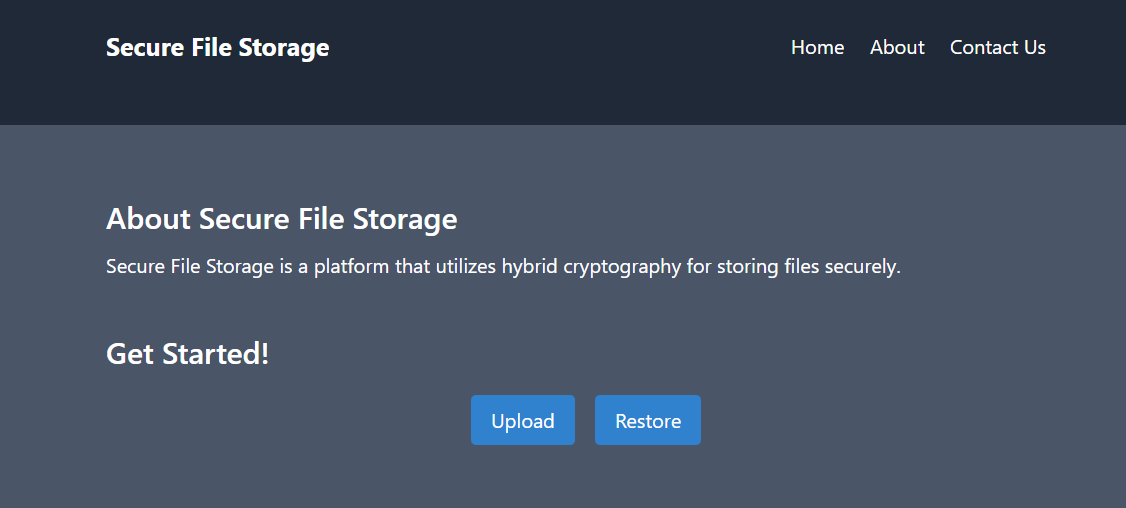
Click on the download link(s) to save the encrypted files to your local system securely.

****

**Decryption:**

1. Accessing the Application:

Open your web browser and navigate to the URL where the application is hosted.



1. Uploading Encrypted Files and Keys:

Click on the "Upload" button to initiate the file upload process.

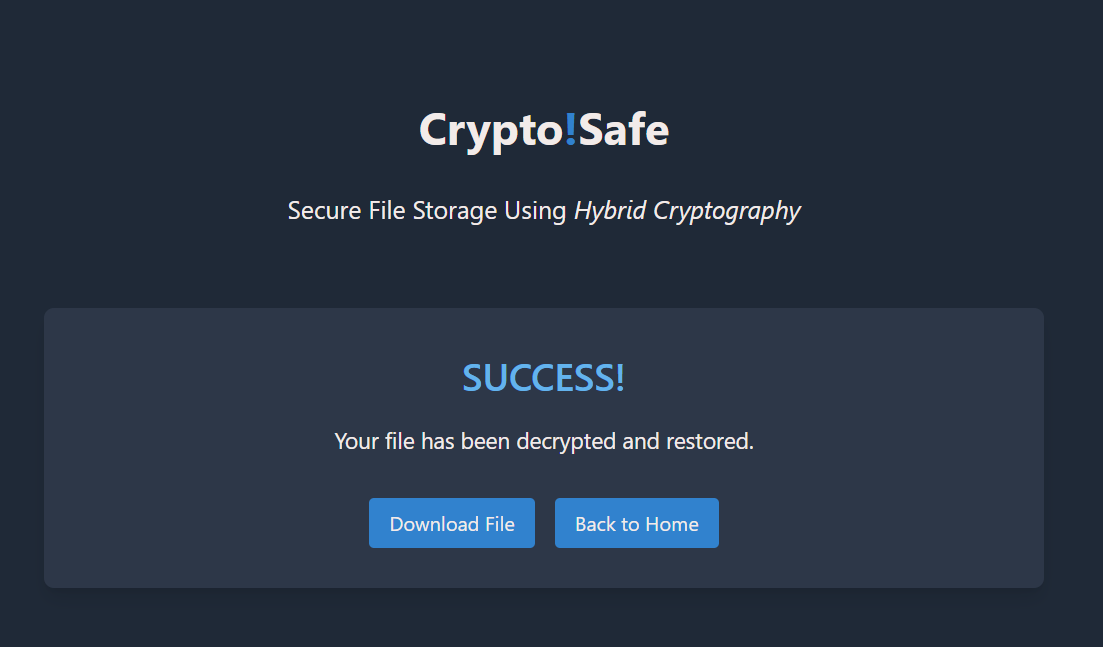
Select the encrypted keys necessary for decryption from your local system.



1. Initiating Decryption:

Once the keys are uploaded successfully, the decryption process will automatically begin.

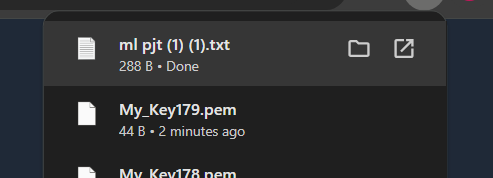
The application will retrieve the encrypted keys and decrypt them to access the decryption keys.



1. Restoring Decrypted Files:

After decryption is completed, you will be provided with options to download the decrypted files.

Click on the download link(s) to retrieve the decrypted files securely to your local system.



**Conclusion:**

In conclusion, the file encryption and decryption project presented here offers a comprehensive solution for securing sensitive data. By leveraging advanced cryptographic algorithms such as AES, ChaCha20-Poly1305, and RSA, along with secure key management techniques, the project ensures robust protection against unauthorized access.