**ABSTRACT**

**Hybrid cryptography is a combination of two or more cryptographic techniques to achieve a greater level of security. It is used to protect sensitive data while also ensuring the data is accessible to the intended recipients.**

**Secure file storage using hybrid cryptography is a method of processing data by combining public key cryptography and symmetric key cryptography. This ensures that the data is both secure and accessible, make it an ideal choice for many applications.**

**CHAPTER 1**

* 1. Feasibility Study

A feasibility study to secure file storage using hybrid cryptography would involve several key steps:

Identify the goals of the file storage system: What data needs to be stored, who needs access to it, and what level of security is required? This will help determine the appropriate encryption and key management strategies.

* + 1. Economical Feasibility

An economic feasibility study to secure file storage using hybrid cryptography would involve analyzing the costs and benefits of implementing the system. Here are some key steps:

1. Identify the costs of implementing the system: This includes hardware, software, and personnel costs. Hardware costs may include servers, storage devices, and encryption accelerators. Software costs may include licenses for encryption software and key management systems. Personnel costs may include salaries for IT staff to manage and maintain the system.

2. Estimate the benefits of the system: This includes the value of the data being protected, such as intellectual property or sensitive customer information. The study should estimate the potential losses from data breaches and compare them to the costs of implementing the system.

* + 1. Technical Feasibility

A technical feasibility study to secure file storage using hybrid cryptography would involve analyzing the technical requirements and capabilities of the proposed system. Here are some key steps:

1. Identify the technical requirements of the system: This includes the type and amount of data to be stored, the number of users who need access, and the performance requirements for encryption and decryption.

2. Evaluate the encryption algorithms to be used: Hybrid cryptography combines symmetric and asymmetric encryption. The feasibility study should evaluate the strengths and weaknesses of the chosen algorithms, such as AES for symmetric encryption and RSA for asymmetric encryption. This includes analyzing the key lengths, block sizes, and other parameters of the algorithms.

3. Determine the key management strategy: The study should consider how keys will be generated, stored, and distributed to authorized users. This may involve a public key infrastructure (PKI) or other key management systems.

* 1. System Requirement
     1. Hardware Requirements
* Servers: The file storage system will require one or more servers to store the encrypted files and manage user access.
* Storage Devices: The encrypted files will need to be stored on one or more storage devices, such as hard disk drives (HDD) or solid-state drives (SSDs).
* Encryption accelerators: Hybrid cryptography can be computationally intensive, especially for large files or large numbers of users. Encryption accelerators, such as dedicated hardware or FPGA (field-programmable gate array) devices, can help offload some of the processing overhead from the servers and improve performance.
* Network infrastructure: The file storage system will require a network infrastructure to allow users to access the encrypted files securely. The network should be fast, reliable, and secure, with appropriate security protocols such as SSL/TLS.
  + 1. So