Low Level Document (LLD)

Hybrid techniques for data Encryption

Version number: 1.0

Last date of revision: 03 March 2023

Sudhanshu Meshram

**DECLARATION**

We declare that this written submission represents us ideas is our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources.

We also declare that we have adhered to all principles of academic honesty

and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when

needed.

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Reviewer** | **Approver** | **Comments** |
| 0.1 | 25-02-23 | Sudhanshu Mehsram | Saurabh Moon |  |  |
| 0.2 | 27-02-23 | Sudhanshu  Meshram | Saurabh moon |  |  |
| 0.3 | 28-02-23 | Saurabh Moon | SudhanhsuMeshram |  |  |
| 0.4 | 1-02-23 | Sudhanhsu Meshram | Sudhanshu Meshram |  |  |
| 1.0 | 2-02-23 | Digambar Rarthod | Sudhanhsu  Meshram |  | n |

Table of Contents

1. Introduction ………………………………………………………………………………….6

1.1 Scope of the document…………………………………………………………………6

1.2 Intended Audience………………………………………………………………………6

1.3 System Overview………………………………………………………………………..7

1. Project Briefing……………………………………………………………………………….
2. Problem Statement…………………………………………………………………………..
3. Problem Solution……………………………………………………………………………..
4. Objective of Project…………………………………………………………………………..
5. Scope of Project………………………………………………………………………………
6. Block Diagram…………………………………………………………………………………
7. Requirements Gathering…………………………………………………………………….
8. Analysis……………………………………………………………………………………….
9. Final Screenshot of Project Output…………………………………………………………
10. **Introduction:**

**1.1 Scope of the Document**

* This section will cover details regarding scope of the document
* Low level design document will be at component level i.e., for website portal there will be one LLD

**1.2 Intended Audience**

* The intended audience for a discussion on hybrid techniques for data encryption would be individuals with a basic understanding of cryptography and computer science. This could include students studying computer science or information security, professionals working in cyber security or data privacy, or anyone interested in understanding how data is kept secure in the digital age.

**1.3 System Overview**

* This section will capture overview of system application i.e for what system is being developed
* Who are the stake holders of system?
* What are other external Systems through which this will be interacting.

1. **Project Briefing:**

The system, is for data protection of users while sending to someone known but if someone else interest in stealing your data will be not able to know what was the data actually. For this , the project will focus on exploring and implementing hybrid techniques for data encryption. Hybrid encryption refers to combination of symmetric and asymmetric encryption techniques to achieve the balance between security and performance. The goal of this project is to develop a comprehensive understanding of hybrid encryption techniques , their strength and weakness, and to implement a prototype that demonstrates the effectiveness of approach in practice. In hybrid encryption the message is encrypted by using symmetric encryption algorithm with a randomly generated key. The key is then encrypted using asymmetric encryption algorithm with the public key of the recipient. The encrypted message and the encrypted key are then sent to recipient. The recipient uses their private key to decrypt the symmetric key to decrypt the message . In this way we are going to secure our data from the attackers as even if they access it , they didn’t know what type of key we have used this makes it difficult to understand the message for others rather than receiver who has the key to access the data provided by us to him.

1. **Problem Statement:**

Now a days we are working with online data transfer more and more this data travels through radio active waves need to be can be accessed by anyone in the medium so providing security for confidentiality of data we are using encryption and decryption of data contents.

1. **Problem Solution:**

In the project what we do is as following:-

1. Generate a symmetric encryption key : A symmetric key is generated to encrypt the data . This key is randomly generated and is used to encrypt the data.
2. Encrypt data using symmetric encryption : The data is encrypted using the symmetric encryption key generated in step 1.

Symmetric algorithms are fast and efficient , which makes them suitable for bulk data encryption.

1. Encrypt the symmetric key using the asymmetric encryption : Asymmetric encryption algorithms are used to encrypt the symmetric key. The recipient's public key is used for encryption, and the encrypted symmetric key is sent along with the encrypted data.
2. Send the encrypted data and encrypted symmetric key: The encrypted data and the encrypted symmetric key are sent to the recipient.
3. Decrypt the symmetric key using asymmetric encryption: The recipient uses their private key to decrypt the encrypted symmetric key.
4. Decrypt the data using the symmetric key: The recipient uses the decrypt symmetric key to decrypt the encrypted data.
5. **Objective of the Project:**

Objective of this project is to Understand, Choose, Implement, Test, Document, Evaluate and Ensure the data security aspects of Encryption and decryption.

1. **Scope of Project:**

Best example of this project processing is we use whats app daily which uses end to end encryption of our data.

1. **Block Diagram:**

Plain text

Symmetric key

Symmetric Cipher

Asymmetric Cipher

Encrypt

Encrypt

Encrypted Symmetric key

Encrypted data

Encrypted Data

1. **Requirements Gathering:**

* Window 10 Operating system
* Visual studio software
* 1 individual members for the research part
* Project integration idea from IEEE website

1. **Analysis:**

Hybrid techniques for data encryption are widely used in modern communication systems and secure applications. This technique combines the advantages of both symmetric and asymmetric encryption algorithms to provide a secure and efficient method of encrypting data.

Here are some key advantages and disadvantages of using hybrid encryption :-

Advantages :-

Strong security: Hybrid encryption provides strong security for data transmission by using symmetric encryption to encrypt the data and asymmetric encryption to encrypt the symmetric key used to encrypt the data. This provides a double layer of security that is difficult to break.

Efficiency: Symmetric encryption is faster and more efficient than asymmetric encryption, making hybrid encryption more efficient than using only asymmetric encryption.

Scalability: Hybrid encryption is scalable for use in different types of communication systems and applications, as it can accommodate varying levels of security requirements.

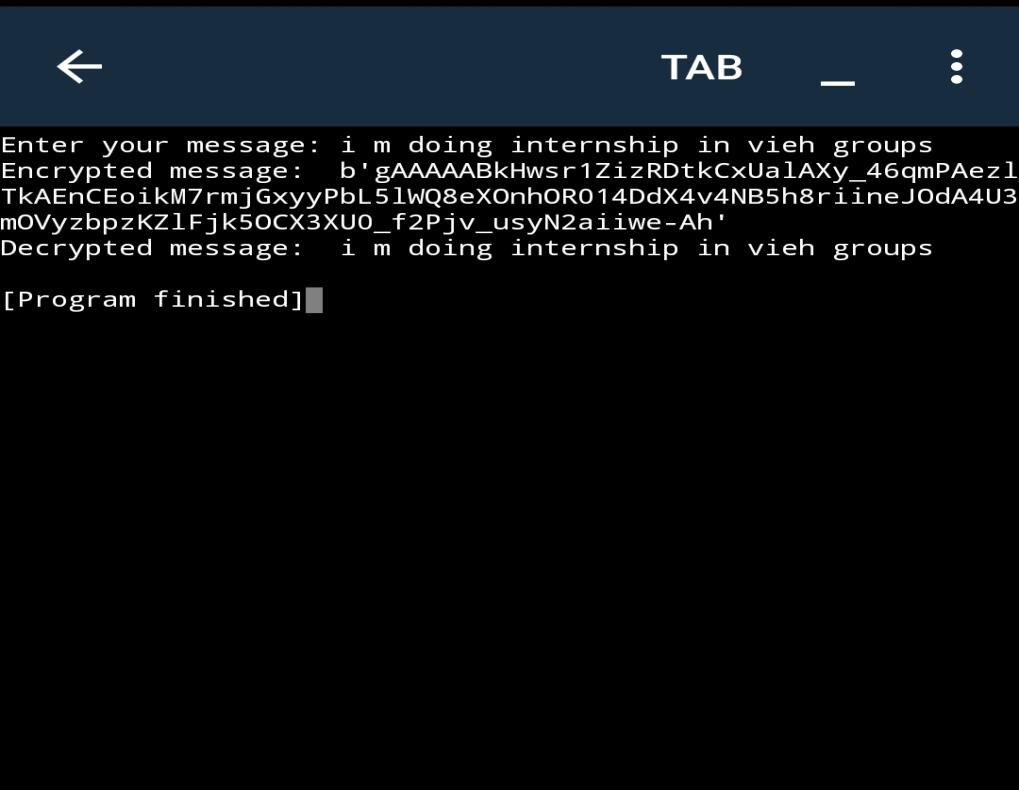
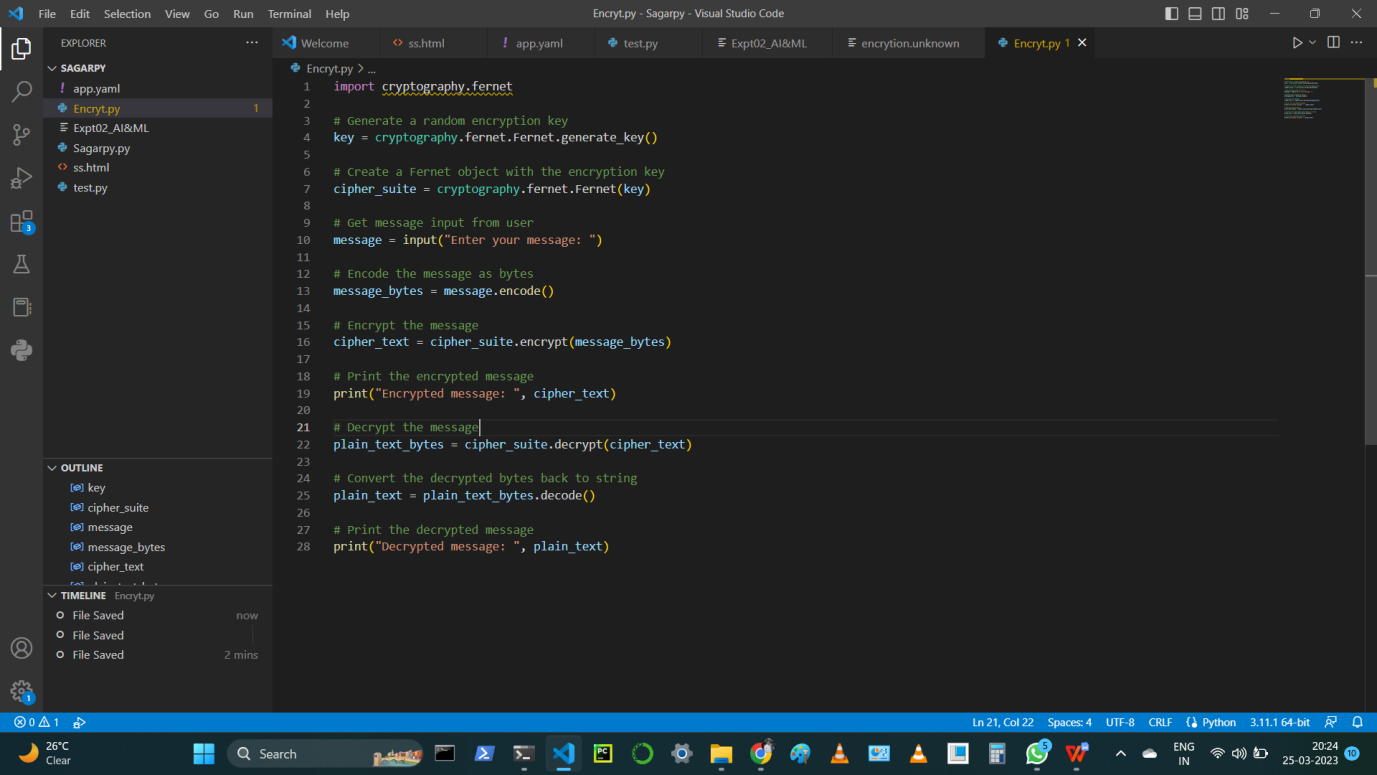
Disadvantages :-

Key management: Hybrid encryption requires managing both symmetric and asymmetric keys, which can be complex and time-consuming.

Implementation complexity: Implementing hybrid encryption requires knowledge of both symmetric and asymmetric encryption algorithms, which can be complex and require specialized expertise.

Vulnerable to side-channel attacks: Hybrid encryption can be vulnerable to side-channel attacks that exploit weaknesses in the implementation of the algorithm or the key management system.

1. **Final Screenshot of Project Output**

****