DEPARTMENT OF APEX INSTITUTE OF TECHNOLOGY

PROJECT PROPOSAL

1. Project Title: -

High Security Encryption using AES and Visual Cryptography.

2. Project Scope: -

The objective of the project is to create a secure encryption system by combining the Advanced Encryption Standard (AES) with Visual Cryptography (the VC). Developing a strong AES encryption algorithm and safe key management procedures is required for implementation. Visual cryptography algorithms will be explored and used to visually encode an AES key, hence improving security. User data will have an extra degree of security thanks to the combination of VC and AES. Users will be able to select between AES-only and combined AES and VC encryption using the project's user-friendly interface for entering and managing encrypted communications. The encryption process will be reversed by a decryption module, and keys and shares are going to be handled by a secure key management system. Comprehensive documentation will be provided, and the system will go through extensive security research and performance improvement.

3. Requirements: -

- Hardware Requirements:

1.Server Infrastructure:
Deploy a secure server infrastructure to host the encryption system.
Ensure the server meets the recommended specifications for the chosen programming language and cryptographic libraries.

2.HSM (Hardware Security Module) :
Consider integrating a Hardware Security Module for added protection of cryptographic keys.
HSMs provide a secure environment for key generation, storage, and cryptographic operations.

3.Random Number Generator:
Ensure access to a reliable hardware random number generator for generating secure cryptographic keys.

4.High-Resolution Display :
For Visual Cryptography, a high-resolution display may be beneficial to enhance the quality of visual shares.

- Software Requirements:

1.Programming Language:

Choose a programming language suitable for cryptographic implementations, such as Python or Java.

2.Cryptography Libraries:

Select and integrate well-established cryptography libraries, such as PyCryptodome for Python or Bouncy Castle for Java, to implement AES encryption.

3.Visual Cryptography Library:

Integrate a Visual Cryptography library that supports the chosen visual cryptography algorithm.

4.User Interface Framework:

Use a suitable user interface framework for creating an intuitive and interactive interface. Examples include Tkinter for Python, JavaFX for Java, or web-based frameworks for online applications.

5.Version Control System:

Employ a version control system like Git to manage and track changes in the source code.

6.Secure Key Management System:

Implement a secure key management system to handle the storage, retrieval, and exchange of cryptographic keys. This may involve encryption of keys at rest and during transmission.

STUDENTS DETAILS:

Name	UID	Signature
PENTAKOTA SRIPRANEETH	21BCS3523	
MENDA MANMADHA RAO	21BCS3544	

APPROVAL AND AUTHORITY TO PROCEED

We approve the project as described above, and authorize the team to proceed.

Name	Title	Signature (With Date)
PRABJOT SINGH	HIGH SECURITY ENCRYPTION USING AES AND VISUAL CRYPTOGRAPHY	