Project Synopsis
Of

Cryptographic Website Development

CIPHER :"Unlocking Tomorrow, Securing Today: Your Cryptographic Gateway to a Safer Digital World Create Today."

Submitted to:

Submitted by:

Mohd Kalam Aslam Pinjar

SYNOPSIS

1.Title of the project :-

Cryptographic Website Development

2. Objective of the project :-

The objective of the Cryptographic Website Development project is to create a secure website that utilizes various cryptographic techniques for data encryption and decryption. The website will provide services such as encryption and decryption of sensitive information, steganography techniques for hiding information within other files, and user database handling for secure user authentication and authorization.

The Cryptographic Website project seeks to revolutionize online security by creating an immersive platform employing cutting-edge cryptographic techniques. The primary goals are to design an intuitive website interface and implement robust security measures using encryption, decryption, steganography, and a sophisticated user database management system. By amalgamating creativity with functionality, the project aspires to redefine the standards of secure online communication.

3. Project category:

The project falls under the category of web development and cryptography.

Cryptographic Website Development falls under the category of Web Development with a focus on implementing cryptographic protocols and techniques to enhance data security.

4.Language and software tools used:

Front End	:HTML5,CSS3,JAVASCRIPT,PHP
Operating System	:Windows/Linux
Back End	:Apache Server & MYSQL

The front-end of the project will be developed using HTML5, CSS3, and JavaScript for an interactive and responsive user interface. The back-end will be built using PHP for server-side scripting. The operating system used will be Windows. The project will be hosted on an Apache server and the data will be stored in a MySQL database.

5.Structure of the project:

5.1 Proposed System:

The proposed system is a web application that allows users to perform encryption, decryption, and steganography operations securely on the website. It provides a user-friendly interface and ensures the confidentiality and integrity of the data.

The proposed system aims to integrate state-of-the-art cryptographic methods into a website to ensure secure data transmission and storage

5.2 Module Description :-

a. Types of Encryption and Decryption: The website will support various encryption and decryption techniques such as symmetric key algorithms, asymmetric key algorithms, and hashing algorithms.

It is the Implementation of various encryption and decryption algorithms to safeguard sensitive data.

- Symmetric Encryption: Implementing algorithms like AES (Advanced Encryption Standard) to secure data with a single, shared key.
- Asymmetric Encryption: Utilizing RSA (Rivest–Shamir–Adleman) for secure key exchange and data encryption.
- Homomorphic Encryption: Exploring techniques that allow computation on encrypted data without decryption, preserving privacy during processing.

b. Steganography: The website will implement steganography techniques to hide sensitive information within digital media files to achieve covert communication and data protection.

It is Integration of steganographic techniques to hide information within digital media, enhancing covert communication.

- Image Steganography: Concealing information within image files, ensuring covert communication.

c. User Database Handling: The website will include a user database for authentication and management purposes, ensuring secure access to the cryptographic features.

It is the Creation of a secure database system for user management, authentication, and authorization.

- Secure Authentication: Implementing secure user authentication mechanisms, including password hashing and salting.
- Authorization Control: Defining user roles and access levels for enhanced security and data integrity.

6. Future scope of the project :-

- Post-Quantum Cryptography: Integrating algorithms resilient to quantum attacks for future-proof security.
- Blockchain Integration: Exploring the integration of blockchain for secure and transparent data transactions.
- Machine Learning for Anomaly Detection: Enhancing security by incorporating machine learning algorithms to detect abnormal user behavior
- Integration of additional encryption algorithms and steganography techniques.
- Implementation of two-factor authentication for enhanced security.
- Integration with cloud storage for secure file sharing.
- Development of a mobile application for on-the-go encryption and decryption.

7. Hardware Requirements:

Minimum RAM: 2GB

Hard Disk: 10GB

Processor: Dual-core or higher

Network: Internet connectivity for hosting and accessing the website.

8. Software Requirements:

- Operating System: Windows or Linux

- Editor: Visual Studio Code

- Server: Wamp

- Database: MYSQL