Problem Statement

Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction

Team : XO
Team Member 1: Matam Manaswini
Team Member 2: Shree Raksha B N
Team Member 3: Meghana B

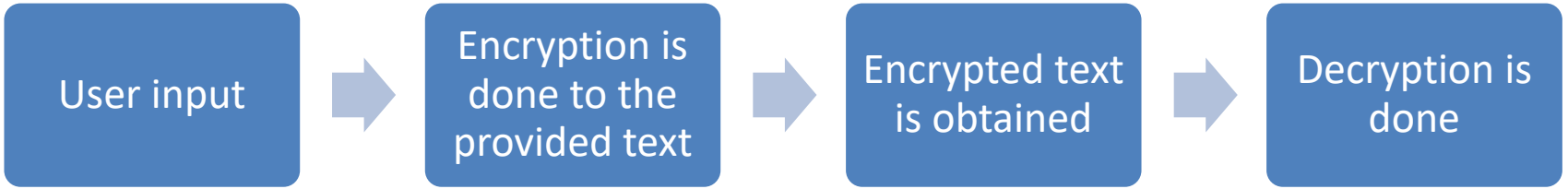
Unique Idea Brief (Solution)

- Develop an interactive simulation tool using mbedTLS/OpenSSL libraries in C.
- This tool allows users to experiment with encryption, decryption, and key generation, providing a practical learning experience. By engaging with these processes hands-on, users can gain a deeper understanding of cryptographic techniques.
- The tool is designed to make learning about cryptography accessible and engaging for students and professionals, enhancing their knowledge and skills in digital security. It offers an intuitive interface and detailed educational content to support users at various levels of expertise in cryptography.

Features Offered

- ❑ Cryptographic Algorithm Implementation
- ❑ Interactive Encryption/Decryption demo
- ❑ User-Friendly Interface
- ❑ Experimentation with different algorithms, key sizes, and encryption parameters.
- ❑ Live example on how encryption and decryption works in simple manner

Process flow

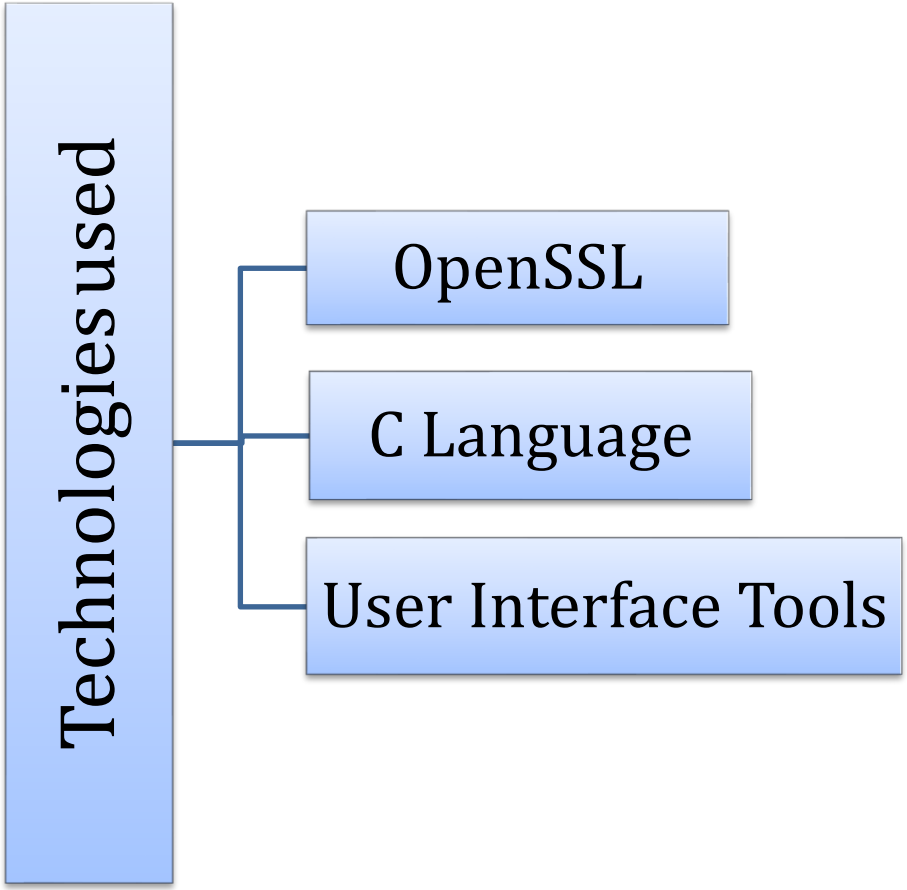


Architecture Diagram

- The Cryptography Engine handles all cryptographic operations using the OpenSSL libraries. It implements encryption, decryption, and key generation algorithms. This core component ensures the accuracy and reliability of cryptographic processes, providing a robust backend for secure data handling.

- The User Interface facilitating user interaction with the cryptographic engine. It allows users to input data, select algorithms, and view output. This component ensures the tool is user-friendly, making cryptographic concepts accessible through an intuitive interface.

- The Data Flow component illustrates the movement of data through encryption, decryption, and key management processes. It shows how user input is processed by the cryptography engine, encrypted or decrypted, and then presented back to the user. This flow ensures clarity in how data is handled securely within the tool.


Technologies used
OpenSSL
C Language
User Interface Tools

Team members and contribution:

- Matam Manaswini (Team Lead): Set milestones and managed team, helped in backend code development.
- Shree Raksha B N (Team member): Frontend website designing to show interactive live website for encryption and decryption.
- Meghana B (Team member): Backend code using OpenSSL with C language.

Conclusion

- The interactive simulation tool will serve as an educational resource, providing a hands-on experience with cryptographic techniques.

- It will be valuable for students and professionals in cybersecurity, facilitating a deeper understanding of how cryptography secures digital communication and data. The project aims to make learning cryptography accessible, engaging, and practical.