# PROBLEM STATEMENT 05:

## Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction

**Category:** Cryptography

**Participants:** 5th-8th Semester Students

## Objective:

To develop an interactive simulation of cryptographic techniques using C code and mbedTLS/OpenSSL, enabling users to understand and experiment with different aspects of cryptography, including encryption, decryption, key generation, and cryptographic algorithms.

## Background:

Cryptography is essential for securing communication in the digital world, involving techniques like encryption and decryption to protect data. Understanding these concepts is crucial for students, developers, and professionals in the field of computer security.

## Key Challenges:

1. **Algorithm Implementation**: Accurately implementing various cryptographic algorithms (e.g., RSA, AES, DES, SHA) using mbedTLS/OpenSSL libraries and usage of C language.
2. **Interactive Encryption/Decryption**: Allowing users to input text or data, select an encryption method, view the encrypted result, and then decrypt it back to the original text or data.
3. **Key Generation and Management**: Simulating the process of cryptographic key generation, exchange, and management.
4. **User-Friendly Visualization**: can be command line or user interface based, depending on the student interest/skill. The application must be capable of taking user input.
5. **Security Concepts Education**: Providing educational content or interactive tutorials on fundamental security concepts like public/private keys, symmetric/asymmetric encryption, key derivation function, digital signatures, and hash functions etc.
6. **User Interaction**: Offering interactive elements for users to experiment with different algorithms, key sizes, and encryption parameters.

## Deliverables:

1. **Cryptography Engine**: A C based backend that handles the implementation of cryptographic algorithms and processes.

2. **Interactive User interface**: Can be command line or UI based and must demonstrate the challenges described above.
3. **Documentation**: Comprehensive documentation detailing the implemented cryptographic algorithms, usage guide, and technical details.

## Constraints:

1. **Simplicity vs. Depth**: Balancing the need for a simple and intuitive user interface with the desire to offer in-depth exploration of complex cryptographic concepts.
2. **Accuracy and Reliability**: Ensuring the cryptographic algorithms are accurately implemented and reliably demonstrate their intended behavior.
3. **Educational Value**: Designing the simulation to be educational for users with varying levels of prior knowledge in cryptography.

## Expected Outcomes:

The successful completion of this project will result in an interactive tool that serves as an educational resource for understanding and experimenting with cryptography. It will be particularly valuable for students and professionals in the field of cybersecurity, providing a hands-on experience with cryptographic concepts and techniques. The tool will facilitate a deeper understanding of how cryptography secures digital communication and data.