tcg crest
Inventing Harmonious Future

Institute for Advancing Intelligence, TCG CREST
(TCG Centres for Research and Education in Science and Technology)

Design and Analysis of Algorithms

PhD Coursework, Semester-II, Session: 2023-24

Project-I

Maximum Marks: 5 Submission Deadline: **2023-Mar-20**

Title: **Secure Communication Protocol Implementation with Hash Table in C**

Requirements:

1. Write code in C programming language.
2. Implement a hash table data structure Using open addressing .
3. Develop code to facilitate secure communication between two parties (P1 and P2).
4. Design a two-person protocol where P1 sends encrypted hash table queries (add/delete/search) to P2, and P2 returns the query result in encrypted form.
5. At the beginning of the communication session, P1 and P2 must agree on a shared secret key using a key agreement protocol.

Assignment Details:

Implement a hash table data structure in C. The hash table should support operations such as adding, deleting, and searching for key-value pairs. Develop functions or methods to encrypt and decrypt data using AES algorithms from *openssl* library Design the communication protocol:

- P1 and P2 should establish a secure communication channel.
- P1 generates hash table queries (add/delete/search), encrypts them using the agreed-upon secret key, and sends them to P2.
- P2 receives the encrypted queries, decrypts them using the shared secret key, and performs the requested operations on the hash table.
- P2 encrypts the query result and sends it back to P1.
- P1 decrypts the response and processes the result accordingly.

Implement a key agreement protocol (e.g., Diffie-Hellman key exchange) to allow P1 and P2 to agree on a shared secret key securely at the beginning of the communication session. Submission Guidelines:

Write well-commented C code for implementing the hash table, encryption/decryption functions, and the communication protocol. Include a brief explanation of the implemented algorithms and protocols. Submit the source code files along with a README file containing instructions for compiling and running the code. Clearly document any external libraries or dependencies used in the implementation. Note: Ensure that the code is efficient, secure, and follows best practices for C programming and cryptographic techniques. Test the implementation thoroughly to validate its correctness and security properties.

[1]

[1] This project is for Crypto students only. For AI/ML students, the project will be updated soon.