**Assignment 02**

**CS3002**

**Information Security**

**Submitted by:** Umar Waseem, Muhammad Huzaifa

**Roll number:** 20i-0762, 20i-2473

**Date:** 27th October 2023

**Table of Contents**

[**Introduction** 2](#_Toc149319265)

[**Implementation** 2](#_Toc149319266)

[**Challenges Faced** 2](#_Toc149319267)

[**Rationale** 3](#_Toc149319268)

[**References** 3](#_Toc149319269)

[**Appendix** 3](#_Toc149319270)

# 

# **Introduction**

As digital communication becomes increasingly prevalent, the need for robust security mechanisms to protect the integrity and confidentiality of data has never been more critical. This report presents the implementation of a protocol inspired by SSL/TLS, a cornerstone of secure communication on the internet, which incorporates encryption, hashing, and key exchange techniques.

This report will provide an overview of the key components of the implemented protocol, outlining the encryption and decryption processes, the role of hashing algorithms in data integrity verification, and the mechanism for secure key exchange. We will also discuss the various cryptographic libraries and tools utilized to implement these functions, ensuring a comprehensive understanding of the technology stack.

The primary objectives of this assignment were to develop a functional security protocol capable of encrypting and decrypting data, verifying data integrity through hashing, and securely exchanging keys between client and server. As such, we will delve into the technical aspects of these objectives, addressing both the theoretical concepts and the practical implementation.

# **Implementation**

# **Challenges Faced**

# **Rationale**

# **References**

# **Appendix**