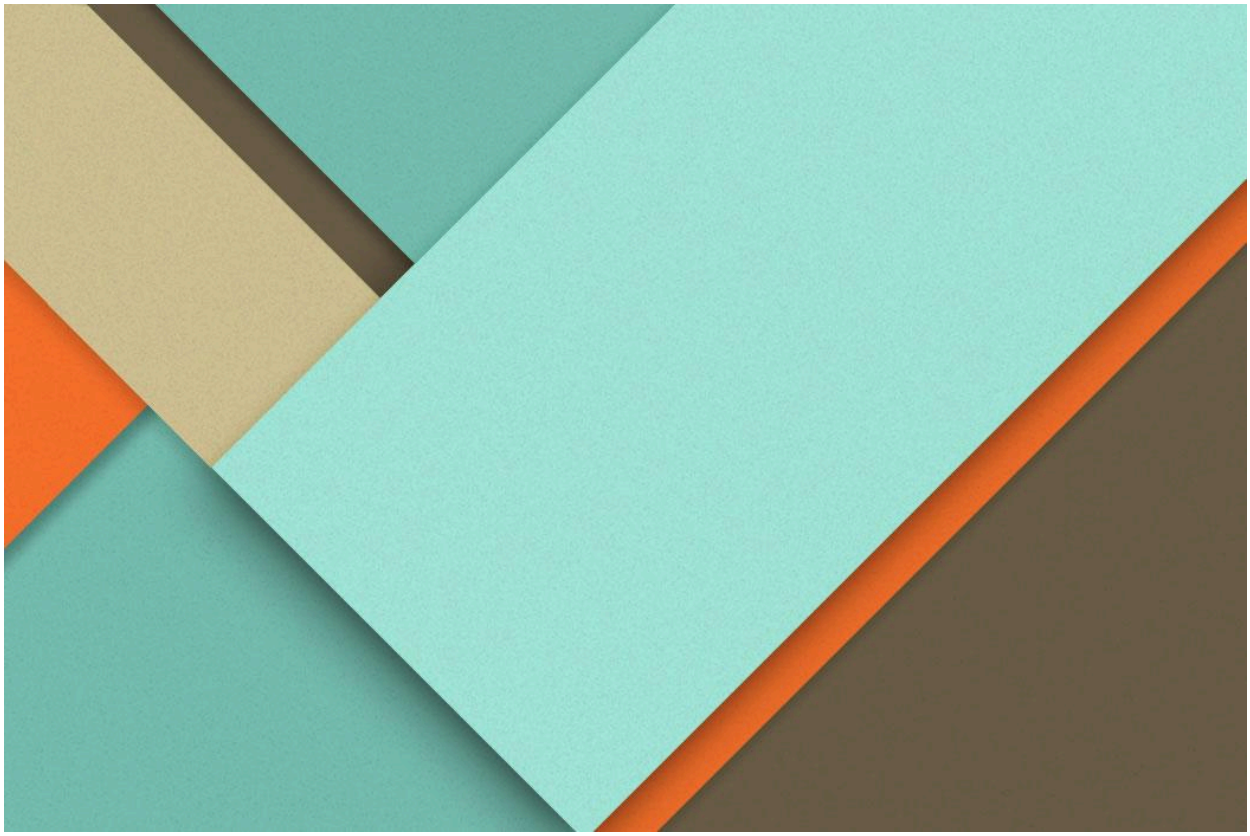

COSC340 - Assessment 4

Protocol

16.05.2024

—

Bart Stolarek
220178419

Introduction

The Secure Messaging Protocol is designed to enable secure communication between a client and a server for a messaging application. This document describes the protocol in detail, including the commands, responses, and security measures employed.

Protocol Overview

The protocol consists of a series of commands and responses exchanged between the client and server. Each command and response is represented as a string of ASCII characters followed by a line feed character (ASCII code 10). The communication is encrypted using symmetric encryption (Fernet) to ensure confidentiality. HMAC signatures are used to ensure message integrity and authentication. RSA key pairs are used for digital signatures to provide message authentication and non-repudiation.

Commands and Responses

REGISTER

Command: REGISTER <username> <password>

Description: Registers a new user account with the provided username and password.

Response: REGISTERED (successful registration) or an error message (e.g., username already exists).

LOGIN

Command: LOGIN <username> <password>

Description: Logs in a user with the provided username and password.

Response: <number_of_unread_messages> (successful login) or an error message (e.g., invalid username or password).

COMPOSE

Command: COMPOSE <recipient>

Description: Initiates the composition of a message to the specified recipient. The message content is sent in the subsequent line.

Response: MESSAGE SENT (successful message delivery) or an error message (e.g., recipient not found).

READ

Command: READ

Description: Retrieves the earliest unread message for the logged-in user.

Response: <sender> (username of the message sender) and <message> (the encrypted message content) on separate lines, or READ ERROR if there are no unread messages.

EXIT

Command: EXIT

Description: Logs out the user and terminates the connection.

Security Measures

Encryption

All communication between the client and server is encrypted using Fernet symmetric encryption. The encryption key is securely shared between the client and server during the initial setup.

Message Integrity and Authentication

Each message sent between the client and server is accompanied by an HMAC signature. The HMAC signature is calculated using a shared secret key and the message content. The receiving party verifies the HMAC signature to ensure the integrity and authenticity of the message.

Digital Signatures

RSA key pairs are used for digital signatures. The server holds the private key, and the public key is distributed to the clients. When a message is sent, the server signs the message using its private key. The client can verify the signature using the server's public key, ensuring message authentication and non-repudiation.

Password Security

User passwords are hashed using SHA-256 along with a randomly generated salt. The hashed passwords are stored on the server, and the plain-text passwords are never transmitted over the network.