Deliverable

- This exercise should be completed in groups. Please form groups of up to five members.
- Randomly selected groups will present their implementations and results during the exercise session. Be prepared for discussion and questions.
- Keep a record of challenges encountered during the task, and reflect on the lessons learned from this exercise.

Exercise 1.1 - Virtual Machine Setup

This section decribes the configuration of the virtual machine environment.

1. Use either `VirtualBox` (free) or `VMware Workstation` (proprietary, but has a free Player version).
2. Select an operating system (you are free to use your favored os). We recommend using either `Ubuntu Server LTS` or `Debian`, since they are lightweight.
3. Set up the virtual machine with at least:
   - CPU: 1-2 cores
   - RAM: 2GB or more
   - Storage: At least 10GB
4. Ensure the virtual machine boots correctly and you can log in to the system.
5. Install tools you will need: `sudo apt install -y build-essential cmake git`

To enable SSH access to the virtual machine from your host system, you need to configure a NAT port forwarding rule.

1. Go to the network settings of your virtual machine.
2. Ensure that the network adapter is set to `NAT`.
3. Add a new rule with the following settings:
   - Protocol: TCP, Host IP: (leave empty), Host Port: 2222
   - Guest IP: (leave empty), Guest Port: 22
4. Save and start the virtual machine.
5. Try connecting via ssh:
   - `ssh -l username -p 2222 127.0.0.1`

Exercise 1.2 - Basic Protocol Implementation

The task involves creating a minimal client-server implementation of TLS (Transport Layer Security). Specifically, only the sending and receiving of the *ClientHello* and *ServerHello* messages need to be implemented. No cryptographic functionality is required.

Detailed descriptions of the *ClientHello* and *ServerHello* messages can be found in RFC 8446, sections 4.1.2 and 4.1.3 respectively. The objective of this minimal implementation is to gain a fundamental understanding of network protocol implementations and the TLS handshake process. You will also learn how to read technical specifications.

To simplify your task, we have created templates for the client and the server. You need to extend these files and add the missing code fragments. Two files are available: server_template.c and client_template.c