Project 1 Design Document

General Architecture

The program was designed so that the agents could establish a reliable connection between them and the server to allow the secret agents to communicate. To establish a reliable connection, sockets were opened on both hosts that implement TCP.

The Server

The server is always listening on an available socket for any secret agents who wants to reach out. If a handshake is made successfully, a connection will be established and a new thread/process will be started independently from the program. It is important to note that the process is not a daemon, so the process ends if the program ends.

In this process, it listens for any codes entered by the agent, where it will then go to verify the agent by checking the codes and asking questions. Things to note:

* Each question is assigned to an answer in a map
* Each agent code is assigned to an agent named in a map
* Agent characters are predefined to cross-check them with the code by just checking if the relevant information in the maps

The Client

The client is very simple, whenever a secret agent wants to make contact, all it needs to do is request a connection by creating a handshake, thereafter the agent can send messages back and forth.

General Communication

TCP is built on top of the network, and physical layers. So, information sent through TCP cannot be sent in its plain form. The text messages sent from and to the agents are encoded into bytes as they are sent, and decoded as they are pulled from the buffer. The buffer is a location in memory where data received by a program are held until they can be processed.

The program is designed to receive up to 1024 bytes, no overflows (flow issues) are expected as messages are short. But bytes themselves are meaningless on either receiving end, so they must be decoded in a specific format which the program can allow the user to understand, which is UTF-8. This is done anytime-either side receives packets from each other.

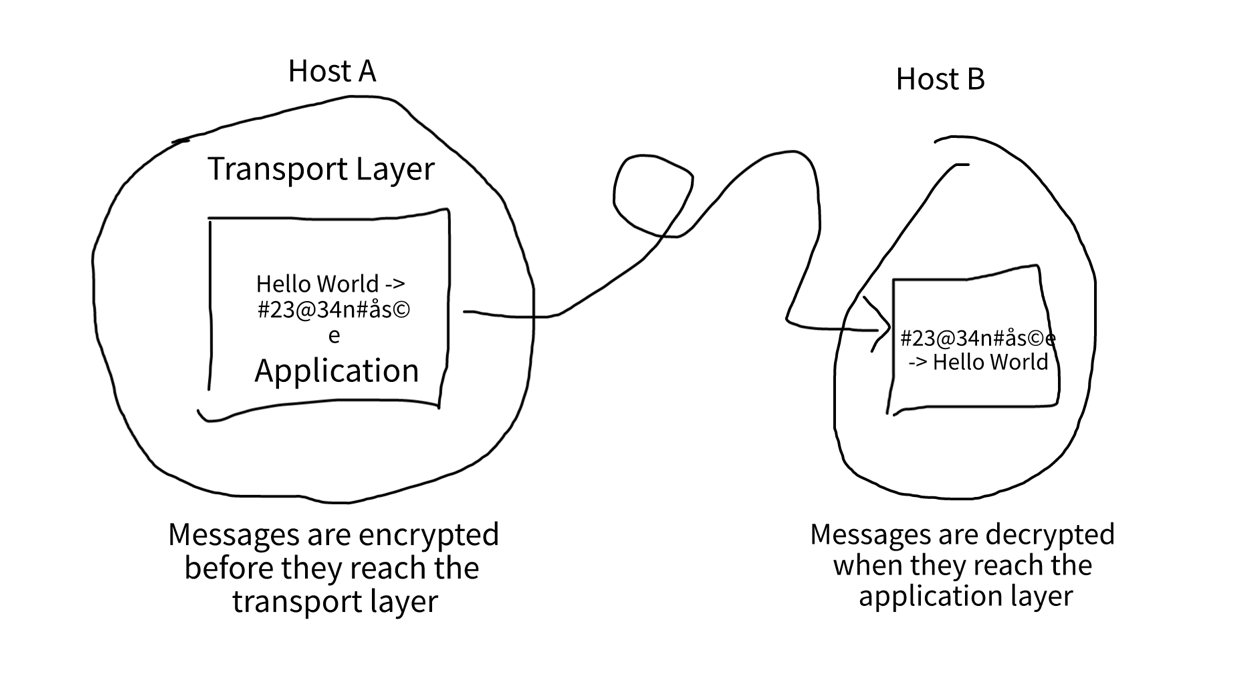
Improvements

1. Security

Secret agents must remain secret, and if the messages between them and the server are intercepted the integrity of the system and national security are compromised. Security can be improved in the following ways

* 1. Encryption (Application Layer)

If encryption is not available on the transport layer, the super-secret application developers can implement it themselves. Each outgoing message can be encrypted using a hashing algorithm, and decoded by the same algorithm when received. The key can be a common denominator between the two, such as weather or office lunch for the day.



* 1. Encryption (Transport Layer)

Just in case if the organization faces any budget cuts, transport layer security can be implemented. This is where cryptography is applied on the transport layer as messages leave the application layer