CS558 Tor Homework

Chenliang Wang
edwangd@bu.edu

Task1

Review Questions

1. Data is the content that a user/client/server wants to transfer, Metadata is the data needed to transfer the content. TLS and encrypted email have the chance to leak the identity/IP address of the sender and the receiver. If I am a revolution activist, then a censor will find out the people I contact and start surveillance even if they don't know the exact content.
2.

- Encryption: Rather than using a TLS connection, the Tor circuit will apply multiple layers of encryption and will be decrypted partially by each relay. Therefore it is hard to decrypt any data even if they know the private key of the server/user
- Anonymity: When sending to a proxy, the IP address of the destination still needs to be specified, therefore, a censor would still know the receiver of the message. However, with the Tor relays and their encryption, the censor would only know that it is sending to Tor, but have no idea about the receiver.

Task2

In this Task I started with implementing the extend() function. By looking at the comment, I finished the onion_skin. The hint on the function signature helped me with getting the extend_cell and extended_cell. From the document, I get the value of shared_X__y and shared_X__b.
For the circuit_build_hops(), since we are using a three hop circuit, we just have to extend the circuit twice to the middle and exit router.

For the circuit_from_guard(), the random digest(X) is 20 bytes long, and since we are using CREATING_FAST optioin, the k0 here is just the concatenation of x and y.
With these three functions, it is easy to build a 3 hop Tor circuit and start a tcp stream connection.

Task3

In this task I think the most confusing part is the introduce_cell of the set_up_intro_point() I first input the X_bytes as the second entry, but the CellRelayIntroduce1 prompts us to use the public key of the introduce relay. The cell_acknowledgement also gave me a headache, since it took me a while to figure out what to input for the response argument.

In extend_to_hidden(), it also took me a while to figure out how to use generator functions to get hs_directory and routers.

The request_template and tor_stream skeleton code really helped me with the stream function in the telescoping.py.

Task4

Please see logs.tar.