CSC427 Week 12 – Tor Lab Handout

Circuit Extension Protocol

# Set up

1. On your local machine, set up a python virtual environment:
   * python3 –m venv venv
   * source venv/bin/activate
2. The lab requires the fernet package for encryption. Download the package as shown:
   * pip install fernet
3. Make sure tor\_lab.py runs without ModuleNotFoundError.
   * python3 tor\_lab.py

# Files

## tor\_lab.py

This is the file you will work on. It includes several important classes

* **Directory Authority**: A simple Directory Authority with a static consensus.
* **Relay**: A doubly-linked list node with diffie-hellman key exchange and encryption/decryption capabilities (the latter part to be done in the lab)
* **Server**: Single server that sends a single response back to the client
* **Client**: Tor client that has access to guard relay, equipped with diffie-hellman key exchange and circuit extension capabilities (the latter part to be done in the lab)

## tor\_encrypt.py

A file that contains encryption and decryption utilities and prime number generation.

# Instructions

You are tasked to implement the circuit extension protocol in the Tor **clients** and **relays**. The implementation of diffie-hellman calculations is done for you. See the 11 TODOs for details.

## Hints

* Important functions: Relay/Client.send\_payload, encrypt, decrypt
* Think of the number and order of encryptions/decryptions in each TODO

When you completed the lab, you should be able to see a message:

## ***“Congrats for completing CSC427!!”***