



Task

© This file is provided by **Khagan Khan Karimov** - the first PhD student at the Kahlert School of Computing, **University of Utah**. It reflects Khagan's solutions for **Homework 2, CS 6490-001 Network Security, Spring 2023** course.

Contact



khagan.karimov@utah.edu



twitter.com/KhaganKarimov

Student: Khagan Khan Karimov

Course: CS 6490-001 Network Security

Instructor: Prof. Dr. Kasera

▼ Task Content:

Write client server programs (in Java, also acceptable in Python) using TCP sockets where the client (Alice) and the server (Bob) perform a Diffie-Hellman exchange. Let $g = 1907$, $p = 784313$, $S_A = 160031$ (Alice's secret), and $S_B = 12077$ (Bob's secret). Your output must show the numbers sent by Alice and Bob for the Diffie-Hellman exchange as well the shared key after the exchange.