# INTE2401/2402 Lab 6

In this lab, we aim to implement the Diffie-Hellman Key Exchange protocol by calling the standard Java cryptographic libraries. The corresponding libraries are provided below.

* Apache commons codec lib provides binary encoding methods, e.g. Base64. Download at (<https://commons.apache.org/proper/commons-codec/download_codec.cgi> ). User guide is provided at (<https://commons.apache.org/proper/commons-codec/userguide.html> ).

## Task. Implementation of Diffie-Hellman key exchange method

Diffie-Hellman key agreement, shown in Figure 1, is an exponential key agreement to perform real-time key exchange over an untrusted network. It allows two users to change a secret key without requiring prior secrets. In this task, we use Java Crypto library to implement a prototype of Diffie-Hellman key agreement, and we output the public values and shared secret .

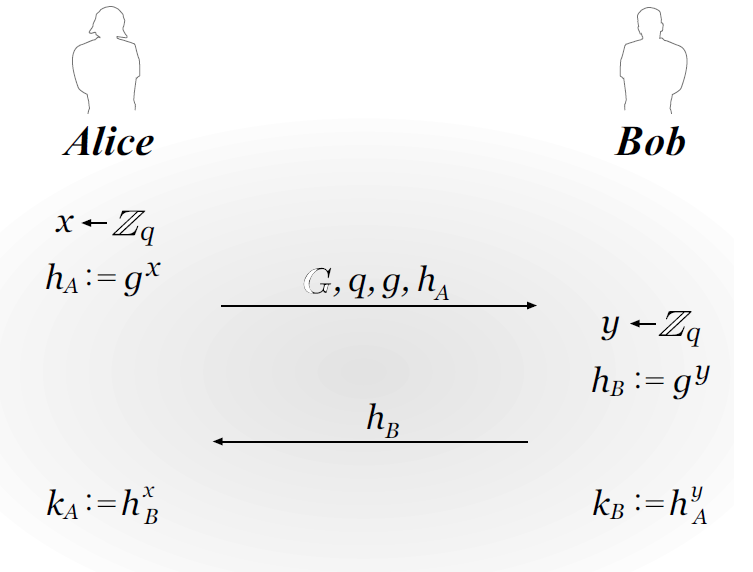


Figure Diffie-Hellman key exchange protocol

Q. Implement a Java program of Diffie-Hellman Encrypted Key Exchange protocol and output the intermediate results and shared secret between Alice and Bob.

Sample output:

