COMP 522: Privacy and Security
Lab session 5

Lecturer: Alexei Lisitsa

Diffie-Hellman Key Exchange

Download, compile and run the following simple program available at the web page `www.csc.liv.ac.uk/~alexei/COMP522/index.html` of COMP522 course:

- Diffie-Hellman Key Exchange between Two parties (`DHKeyAgreement2.java`)

Look into the code and see how the key exchange is implemented and how the shared secret is further used in the AES encryption.
Then try the folloiwng:

- Find a key size setting in the code. It should be 2048 bits. Try to increase it to 4096, compile and run again. What do you observe? (*Hint*: It should not work, the compiler will report a possible range of key sizes)
- Try to set the key size to the minimal possible value, compile and run the program again. Try other possible values. Notice how the size of the shared secret changes.
- Measure a time (see Lab 3 for the details) required to perform key generation and key agreement for the minimal and maximal possible key sizes.
- Download, compile and run the program implementing DH key exchange between three parties (`DHKeyAgreement3.java`). Look into the code and see how the key exchange is implemented.
- Write the process of key exchange for three parties in terms of the modular exponent, similar to the case of two parties described at pages 6-8 of Lecture Notes on DH Key Exchange:
  `/~alexei/COMP522/COMP522-DiffieHellman-18.pdf`
- Based on the three parties case, can you propose a variant of DH protocol for key exchange between 4 parties? Time permitting, you can implement it by an appropriate modification of the program `DHKeyAgreement3.java`