CT255 Assignment 4

Diffie-Hellman Key Exchange

General

The objectives of this assignment are as follows:

1. Reinforce your understanding of the Diffie-Hellman Key exchange protocol.
2. Demonstrate a MitM attack on this protocol.

Problem 1: [7 marks]
Write a Java class that implements the following Diffie-Hellman functionality, using 32-bit integer arithmetic:

- A method that generates random DH parameters, i.e.
    - a prime number p with $10^4 < p < 10^5$. Please implement your own prime number test.
    - a matching primitive root a. Again, write your own code to test candidate numbers.
- A generator method (with argument X) that calculates values $Y = a^X \bmod p$. Make sure that numeric overflows are avoided.

Provide additional Java code that, using the above methods, emulates a key exchange between Alice and Bob using random values XA and XB (see also lecture notes). Show that both Alice and Bob calculate the same key K.

Problem 2: [3 marks]
Simulate a MitM attack with the malicious actor Mallory as exercised in the lecture notes. Show the different keys generated by Bob/Mallory and Alice/Mallory.

Assignment Submission

Please submit a zipped folder to Blackboard containing:

- Your (well-commented!) source code for problems 1 and 2 in PDF format.
- Screenshots showing your programs being compiled and emulating the key exchange / attacks.