E0254: Network and Distributed Systems Security

Assignment No. 3

Date given: Oct. 31, 2017

Submission Due Date: Nov. 30, 2017

Write a program in Java or C++ to establish 128-bit shared secret key between two processes in different machines with the help of Authenticated Diffie-Hellman key establishment protocol. That is, the processes already have a shared secret key, and they want to establish a new shared secret key ensuring perfect forward secrecy. For authentication, you can use any of the MAC function. The program should use the following two types of groups to establish the shared secret key.

(i) Multiplicative residue group Z_p^*, where p is a 512-bit prime number.

(ii) Elliptic curve group $E(GF(p))$, where p is a 512-bit is a prime number.

For the case (i), you need to get a prime subgroup of Z_p^*, where Diffie-Hellman key establishment protocol can be run. For the case (ii), you can use some standard elliptic curve, where Diffie-Hellman key establishment protocol can be run in a prime subgroup of the main group. Please do not use any library function to compute the exponentiation function. The program should display the common key established in a separate window for each process, and the time required to compute the key (excluding communication delay) in each of the group. Note that this assignment would be required in assignment 4 which is different for each student. Please submit the tar and compressed file of your program, and the output of your program within the due date along with explanation for how to run the program. You will be required to give the demo of your program later.