INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Lab Session 3: Discrete logarithm problem and DHKE *September 18, 2024*

Please solve the following exercises in pairs. You can use C/C++, Java or Python do develop your source code, but please use only one of this languages to develop all the exercises.

1. Programming exercises

1. Design and implement a function to solve the discrete logarithm problem. Your function must receive a primer number p, a generator $g \in \mathbb{Z}_p^*$, and any element $\beta in \mathbb{Z}_p^*$. Use your function to find x for each of the following instances of the problem

   a) 5^x mód $10007 = 9012$

   b) 2^x mód $100003 = 100002$

   c) 2^x mód $100,000,000,003 = 1,922,556,950$

   d) 3^x mód $500,000,009 = 406,870,124$

   e) 3^x mód $500,000,009 = 187,776,257$

2. Design and implement a function to solve the discrete logarithm problem in elliptic curves. Your function must receive a primer number p,the parameters for an elliptic curve $a, b \in \mathbb{Z}_p^*$, a generator point $G \in \mathbb{E}(a, b)$, and any point $P \in \mathbb{E}(a, b)$. Use your function to find x for each of the following instances of the problem

   a) $p = 113, a = 1, b = 9, G = (47, 22, 1), P = (52, 53, 1)$

   b) $p = 503, a = 11, b = 1, G = (457, 404, 1), P = (459, 58, 1)$

   c) $p = 5009, a = 1, b = 1, G = (359, 1928, 1), P = (1942, 2938, 1)$

   d) $p = 1,000,003, a = 1000, b = 1, G = (917459, 678095, 1), P = (798677, 191330, 1)$

   e) $p = 500,000,009, a = 1, b = 9, G = (377863415, 222914743, 1), P = (477613302, 314579681, 1)$

3. Design and implement the Diffie-Hellman key exchange protocol between two entities. You can use a library to do arithmetic with large numbers, but you **MUST NOT USE a cryptographic function that already implements Diffie-Hellman**. Your program must randomly generate a large prime number p, i.e. $|p| \geq 1024$ bits. Then you must obtain a generator $g \in \mathbb{Z}_p^*$, you can use a cryptographic library for this purpose. Your program must perform modular exponentiation using the library to do arithmetic on large numbers. To test your program, every student must use her/his own computer and proceed as follows:

a) Agree a large prime number p and a generator $g \in \mathbb{Z}_p^*$ with your partner.

b) One student will play the role of Alice and the other one will play the role of Bob.

c) Alice randomly choose exponent a and compute $A = g^a$ mód p. Share A with Bob.

d) Bob randomly choose exponent b and compute $B = g^b$ mód p. Share B with Alice.

e) Once Alice received the value B from the other student, must calculate B^a mód p

f) Once Bob received the value A from the other student, must calculate A^b mód p

2. Products

Every student must write her/his own report including the following information:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. The source code for each point 1.1 , 1.2, 1.3. Please include a brief paragraph explaining your functions.
3. Answers you found for points 1.1 and 1.2.
4. Examples that you used to test your program for point 1.3
5. Screenshots of your programs running.

3. Evaluation

- Advances in class: 2 point
- Source code: 3 points
- Program running: 3 points
- Report: 2 points

Deadline : September 24, 2024.