INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 5: Hard problems in cryptography *May 5, 2020*

Use a cryptographic library in your favorite programming language (C,C++, Java or Python) to solve the following exercises.

1. Programming exercises

1. Develop a program to solve the discrete logarithm problem, for the following instances.
   a) 11^x mód $1009 = 400$
   b) 5^x mód $10007 = 5235$
   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. Develop a program to find the prime factors of the following composite numbers.
   a) 100,160,063
   b) 10,006,200,817
   c) 250,035,001,189
   d) 250,000,009,000,000,081

2. Products

Write a brief report with the following:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. Briefly describe what you did to solve the exercises.

3. The answer for each exercise.

4. Screen shots, showing your program running.

You must submit your report to classroom as a pdf file, before **May 11, 2020**.