INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 6: Hard problems in cryptography II   *May 11, 2020*

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

1. Programming exercises

1. Design an algorithm to find the private key in RSA, d, if you have the public key (e, n) Write the pseudocode of your algorithm. Give an example to explain how it works

2. Implement your algorithm. Take five public keys from those listed in google classroom and prove your algorithm

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. Pseudocode and your example for exercise 1.

3. Screen shots, showing your program running.

You must submit your report to classroom as a pdf file, before **May 14, 2020**.