PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Rúbrica Tarea 3

Preguntas

1. El objetivo de esta pregunta es que usted implemente el protocolo criptográfico ElGamal sobre grupos arbitrarios, y en particular que lo utilice sobre grupos generados por curvas elípticas. Para hacer esto, primero deberá leer la sección 9.3.4 del texto guía del curso:

   - Jonathan Katz y Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, tercera edición, 2020.

   Luego de esto, deberá completar el Jupyter notebook `pregunta1.ipynb`. Para que su pregunta sea considerada correcta, su notebook deberá correr de principio a fin habiendo modificado exclusivamente las clases y funciones marcadas con `##### POR COMPLETAR`. En particular, se evaluará con un programa externo la implementación de sus clases `ElGamalSender`, `ElGamalReceiver` y `EllipticCurve`.

   Corrección. La correción de esta pregunta está basada en 13 tests. La descripción de estos tests y del puntaje asignado por cada uno de ellos se encuentra en el Jupyter notebook `https://github.com/UC-IIC3253/2022/tree/main/Tareas/Tarea%203/rubrica/pregunta1.ipynb`.