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 y las firmas de Schnorr sobre grupos arbitrarios, y en particular que lo utilice sobre grupos generados por curvas elípticas. Para hacer esto, deberá completar el Jupyter notebook `pregunta1.ipynb`, en el cual primero deberá implementar el protocolo ElGamal y las firmas de Schnorr sobre una representación general de grupos, para luego probar su implementación sobre los grupos $\mathbb{Z}_p^*$ estudiados en clases, y finalmente probar su implementación sobre grupos generados por curvas elípticas como son definidos en el siguiente libro:

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

   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 `SecretKeyHolder`, `PublicKeyHolder` y `EllipticCurve`.

   Corrección. Para corregir esta pregunta se realizaran los 12 tests que son descritos en el Jupyter notebook con la solución de la tarea `sol_tests_p1.ipynb`. Por cada test que sea realizado correctamente, usted recibirá 0.5 puntos.