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

Criptografía y Seguridad Computacional - IIC3253
Tarea 3
Plazo de entrega: Sábado 1 de julio, 20:00hrs

Instrucciones

Cualquier duda sobre la tarea se deberá hacer en los *issues* del repositorio del curso. Si quiere usar alguna librería en sus soluciones debe preguntar primero si dicha librería está permitida. El foro es el canal de comunicación oficial para todas las tareas.

Configuración inicial. Para esta tarea utilizaremos *github classroom*. Para acceder a su repositorio privado debe ingresar al siguiente link, seleccionar su nombre y aceptar la invitación. El repositorio se creará automaticamente una vez que hagas esto y lo podrás encontrar junto a los repositorios del curso. Para la corrección se utilizará Python 3.10.

Entrega. Al entregar esta tarea, su repositorio se deberá ver exactamente de la siguiente forma:

```
Repositorio
├── Pregunta_1
│   ├── requirements.txt
│   └── pregunta1.ipynb
├── .gitignore
├── README.md
└── .git
```

Deberá considerar lo siguiente:

- El archivo `requirements.txt` dentro de la carpeta de una pregunta deberá especificar todas las librerías que se necesitan instalar para ejecutar el código de su respuesta a dicha pregunta. Este archivo debe seguir la especificación de Pip, es decir se debe poder ejecutar el comando `pip install -r requirements.txt` suponiendo una versión de `Pip` mayor o igual a 22.0 que apunte a la versión 3.10 de Python. Si su respuesta no requiere librerías adicionales, este archivo debe estar vacío (pero debe estar en su repositorio).
- Se recomienda utilizar tipado para las variables y funciones en Python.
- La solución de cada problema de programación debe ser entregada como un Jupyter Notebook (esto es, un archivo con extensión `ipynb`). Este archivo debe contener comentarios que

expliquen claramente el razonamiento tras la solución del problema, idealmente utilizando *markdown*. Más aún, su archivo deberá ser exportable a un módulo de Python utilizando el comando de consola

```
jupyter nbconvert --to python preguntaX.ipynb
```

Este comando generará un archivo `preguntaX.py`, del cual se deben poder importar las funciones y clases que se piden en cada pregunta. Por ejemplo, luego de ejecutar este comando, se debe poder importar desde otro archivo Python (ubicado en el mismo directorio) la clase `SecretKeyHolder` simplemente con `from pregunta1 import SecretKeyHolder`.

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, 2021.

   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`.