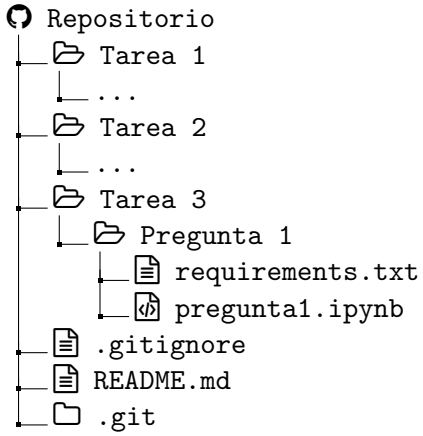
PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

**Criptografía y Seguridad Computacional - IIC3253**
**Tarea 3**
**Plazo de entrega: viernes 1 de julio**

# 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.

**Entrega.** Para entregar esta tarea deberá usar el mismo repositorio que utilizó para entregar las tareas 1 y 2. Al entregar esta tarea, su repositorio se deberá ver exactamente de la siguiente forma:




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 20.0 que apunta a la versión 3.9 de Python. Si su respuesta no requiere librerías adicionales, este archivo debe estar vacío (pero debe estar en su repositorio).
- 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 aun, 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 `EllipticCurve` simplemente con `from pregunta1 import EllipticCurve`.

## 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`.