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

Criptografía y Seguridad Computacional - IIC3253
Tarea 4
Plazo de entrega: jueves 26 de junio

Instrucciones

Cualquier duda sobre la tarea se deberá hacer en los *issues* del repositorio del curso. Los issues son 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 haga esto y lo podrá encontrar junto a los repositorios del curso. Para la corrección se utilizará Python 3.12.

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

```
Repositorio
├── Tarea4
│   └── Pregunta1
│       └── pregunta1.ipynb
├── .gitignore
├── README.md
└── .git
```

Preguntas

1. En esta pregunta usted deberá implementar el protocolo de firmas de anillo visto en clases, el cual utiliza las firmas de Schnorr también vistas en clases.

   Recuerde que una firma de Schnorr se define de la siguiente forma. Suponga que los siguiente objetos son públicos: un grupo $(G, *)$, un elemento $g \in G$, un número primo q tal que $|\langle g \rangle| = q$ y una función de hash h. La clave secreta de un usuario A es un número $x_A \in \{1, \ldots, q-1\}$ y su clave pública es el elemento del grupo $y_A = g^{x_A}$. Si el usuario A quiere generar una firma de Schnorr para un mensaje m, entonces debe realizar los siguientes pasos:

   (a) Genera al azar $r \in \{1, \ldots, q-1\}$ y calcula $c = h(g^r \| m)$ considerando g^r como un string.

   (b) Calcula $s = r + c \cdot x_A$ interpretando c como un número natural.

(c) Define (c, s) como la firma de Schnorr de m.

Un usuario B puede verificar si (c, s) es una firma del mensaje m hecha por el usuario A chequeando que la siguiente condición se cumpla:

$$c \;=\; h(g^s * y_A^{q-c} \| m).$$

Utilizando este protocolo, mostraremos cómo se define una firma de anillo para un caso particular. Usted deberá generalizarlo. Suponga que tiene un grupo formado por los usuarios 1, 2 y 3, donde la clave secreta del usuario i es x_i y la clave pública del usuario i es $y_i = g^{x_i}$. Si el usuario 1 quiere generar una firma de anillo de un mensaje m, entonces debe realizar los siguientes pasos:

(a) Genera al azar $r_1 \in \{1, \ldots, q-1\}$ y calcula $c_2 = h(g^{r_1} \| m)$.

(b) Genera al azar $s_2 \in \{1, \ldots, q-1\}$.

(c) Calcula $g^{r_2} = g^{s_2} * y_2^{q-c_2}$ y $c_3 = h(g^{r_2} \| m)$. Note que en este paso el usuario 1 no calcula r_2, sólo calcula $g^{s_2} * y_2^{q-c_2}$ y sabe que esto es igual a un elemento del grupo de la forma g^{r_2}. Además, el usuario 1 utiliza g^{r_2} para calcular c_3.

(d) Genera al azar $s_3 \in \{1, \ldots, q-1\}$.

(e) Calcula $g^{r_3} = g^{s_3} * y_3^{q-c_3}$ y $c_1 = h(g^{r_3} \| m)$.

(f) Calcula $s_1 = r_1 + c_1 \cdot x_1$. Note que este paso lo puede realizar el usuario 1 ya que conoce la clave secreta x_1.

(g) Saca al azar $i \in \{1, 2, 3\}$ y define (s_1, s_2, s_3, c_i, i) como la firma de anillo de m.

Supongamos que $i = 2$. Si un usuario B quiere verificar que $(s_1, s_2, s_3, c_2, 2)$ es una firma de anillo válida para el grupo formado por los usuarios 1, 2 y 3, entonces debe hacer lo siguiente:

(a) Calcula $c_3 = h(g^{s_2} * y_2^{q-c_2} \| m)$

(b) Calcula $c_1 = h(g^{s_3} * y_3^{q-c_3} \| m)$

(c) Revisa si $h(g^{s_1} * y_1^{q-c_1} \| m)$ igual al valor c_2 de la firma.

Note que si esta última condición es cierta, entonces B sabe que la firma es válida, pero no sabe cuál de los usuarios firmó el mensaje m (ya que el valor de i se sacó al azar).

Para responder esta pregunta, usted debe entregar el notebook `pregunta1.ipynb` habiendo completado exclusivamente los bloques marcados con `##### POR COMPLETAR`. Su notebook deberá correr de principio a fin. Además, se evaluará con un programa externo su implementación de las clases `Signer` y `Verifier`.