Criptografía Práctica y Blockchain

Trabajo Práctico 1

Condiciones

- La resolución de las consignas deberá ser de manera **individual**.
- Deberá implementarse en uno de estos lenguajes de programación a elección: **Rust o Python**.
- La entrega deberá realizarse antes del día 10 de mayo a las 18 hs por medio de un formulario Google que será comunicado.
- Las entregas tendrán una calificación numérica, que se utilizará en el cálculo de la nota final de la cursada.

Consignas

1. Implementar un tipo de dato para un elemento de cuerpo finito, junto con sus operaciones aritméticas fundamentales (adición, sustracción, multiplicación y división).
2. Implementar un tipo de dato para puntos de una curva elíptica, junto con las operaciones de grupo (suma de puntos distintos y duplicación de puntos), utilizando la forma de Weierstrass. Hacer pruebas con la curva $y^2=x^3-3x-3$ y $p=1021$, determinando la cantidad de puntos que tiene la curva. Usando $P=(379,1011)$, obtener kP, siendo $k=655$.
3. Implementar un esquema básico de acuerdo de clave de Diffie-Hellman usando curvas elípticas. Usar la curva con $p=43$, $y^2=x^3+6$ y como generador $g=(13,15)$. ¿Qué sucede si se emplea el punto $g=(9,2)$?
4. Considerar la curva $y^2=x^3+905x+100$ definida sobre el cuerpo primo de orden 1021 y el punto generador (1006,416). Desarrollar alguna estrategia que permita resolver el problema del logaritmo discreto $kP=(612,827)$.