Planeación del Proyecto: Secreto Compartido

February 16, 2025

Equipo de Trabajo

- **Scrum Master:** Thomas Molina Molina
- **Product Owner:** Catalina Metaute Gonzalez
- **Desarrolladores:** Juan Miguel Paez Tatis
- **Desarrolladores:** Juan Jose Jimenez Maya

Duración y Metodología

- **Tiempo total:** 4 semanas
- **Metodología:** Scrum
- **Sprints:** 2 sprints de 2 semanas
- **Reuniones:** Diarias de 15 min (Daily Stand-Up) y retrospectiva al final de cada sprint. Reunión con cliente una vez por semana

Objetivos del Proyecto

- Implementar un protocolo de comunicación para cálculo conjunto de funciones con datos privados.
- Aprender y programar operaciones en el campo primo $\mathbb{Z}_p$, incluyendo suma, multiplicación e inverso multiplicativo/aditivo modular.

- Ejecutar el algoritmo de Shamir para realizar la fragmentación de datos y hacer el reparto de estos 'secretos' de manera segura.
- Simular una red P2P y definir la estructura de los mensajes para la comunicación entre nodos.
- Implementar y evaluar la interpolación de Lagrange en $\mathbb{Z}_p$ para la reconstrucción de datos secretos.
- Optimización del código para mejorar eficiencia.
- Medir tiempos de cómputo y evaluar el uso de la red en la implementación del protocolo.

Plan de Trabajo (Backlog)

Sprint 1 (Semana 1-2)

- ✓Definir estructura del proyecto y entorno de desarrollo.
- ✓Implementar generación y reparto de secretos.
- ✓Simular red P2P y definir estructura de mensajes.
- ✓Interpolación de Lagrange para reconstrucción.

Sprint 2 (Semana 3-4)

- ✓Implementar medidas de seguridad (SSL en fase final).
- ✓Optimización con primos de Mersenne.
- ✓Medición de tiempos y pruebas de concepto.
- ✓Documentación y preparación de la entrega.

Entregables

- Código funcional con implementación del protocolo.
- Informe técnico con metodología, resultados y pruebas.
- Presentación final del proyecto.

Herramientas y Tecnologías

- **Lenguaje:** Python
- **Gestión de código: GitHub**

Distribución de tareas

Distribución de tareas en Excel