Universidad del Norte
Departamento de Ingeniería de Sistemas y Computación
Criptografía

PROYECTO 1

Fecha de entrega: 22 de septiembre de 2024, 11:59 pm.

LUOV Digital Signature Scheme – Key Generation

El objetivo de este proyecto es comprender e implementar el proceso de generación de llaves de un criptosistema postcuántico, en específico el esquema de firma digital LUOV (Lifted Unbalanced Oil Vinegar).

Para ello se deben apoyar en la documentación oficial que se encuentra cargada en el curso de Brightspace, en específico, deben implementar el Algoritmo 4 (**KeyGen**) teniendo en cuenta la información contenida en las tablas 1 y 2.

El algoritmo de generación de llaves debe funcionar **obligatoriamente** para los siguientes conjuntos de parámetros:

- LUOV-7-57-197
- LUOV-7-83-283
- LUOV-7-110-374

Opcionalmente, el algoritmo de generación de llaves debe funcionar para los siguientes conjuntos de parámetros:

- LUOV-47-42-182
- LUOV-61-60-261
- LUOV-79-76-341

Además de los códigos desarrollados se debe realizar un informe en el que se exponga:

- Una explicación (con sus propias palabras) del funcionamiento del esquema de firma digital, detallando el funcionamiento de la generación de la llave.
- Los códigos desarrollados para solucionar el problema y una explicación de estos, donde se detalle las estrategias, criptosistemas y librerías utilizadas para resolver cada una de las tareas intermedias.

Para tener en cuenta:

- La solución (análisis) debe ser original.
- Puede utilizar el lenguaje de su elección para desarrollarlo, se recomienda el uso de Python o Rust.
- Todos los códigos deben estar documentados por los integrantes del equipo.
- Este proyecto es para desarrollar en grupos de **3** integrantes.
- Todo el código debe ser subido a un repositorio de **GitHub**.