Universidad Nacional Autónoma de México

Facultad de Ciencias

Modelado y Programación

Esquema de Secreto Compartido de Shamir

Integrantes de equipo:
Mario Letepichia Romero
Celic Aislinn Liahut Ley
Ivette González Mancera

Junio 15,2022

Definición del problema

Mantener la cofidencialidad y seguridad de documentos al ser compartidos, para eso se les necesita encriptar. Para eso en este caso lo que debemos lograr con el esquema de secreto compartido de Shamir es que apartir de un dato ocultado(encriptado), a partir de él, se generan n diferentes datos y que con, al menos t $\leq$ n cualesquiera de ellos sea posible recuperar el dato original.

Análisis del problema

Primero lo que se debe hacer para este problema es recibir el dato(documento) para esto se le pedira la ruta del archivo o documento y una contraseña al usuario. Sin embargo las contraseñas que teclea el usuario suelen ser un poco simples y poco seguras, por lo que se le aplicara el algoritmo SHA-256, para que asi la contraseña sea segura, pues sera la llave para encriptar y desencriptar.El algoritmo que se aplica para ocultar el dato(encriptarlo) y decifrarlo (es decir volver al original) es AES-256 , el cual en como se implementara encripta y decencripta documentos claros(es decir cualquier tipo de archivo). Para recuperar el archivo original se deberá reunir minimo t de valores, el cual establece el grado del polinomio; también podrá establecer la n, talque t $\leq$ n, las cuales son la evaluaciones deseadas por el usuario. Esto incrementara la seguridad pues la llave esta repartida entre varias personas. Reuniendo t contribuciones puedes recuperar la llave y de esa manera poder decifrar ya si obtenr el dato original.

Mantenimiento del programa

Un problema que puede surgir con esta implementación es la falta de interfaz gráfica, dado que cada que se ejecuta se generaran nuevos archivos, al paso de varios ejecuciones, puede haber un poco de desorden en los archivos.

Costo del programa

En este programa no se utilizo ninguna herramienta de paga, mas que el tiempo y esfuerzo de los programadores de trabajo de investigación, documentación, estructuración y programación, el tiempo estimado que se empleó fueron dos semanas. Por lo tanto nuestro equipo cobraria un total de 250 dolares.

Lo que nuestro equipo cobraría por este programa son 200 dolares considerando el trabajo hecho, mas lo que costaría un plan viable de OpenWeather que es el plan de 3,801 pesos.

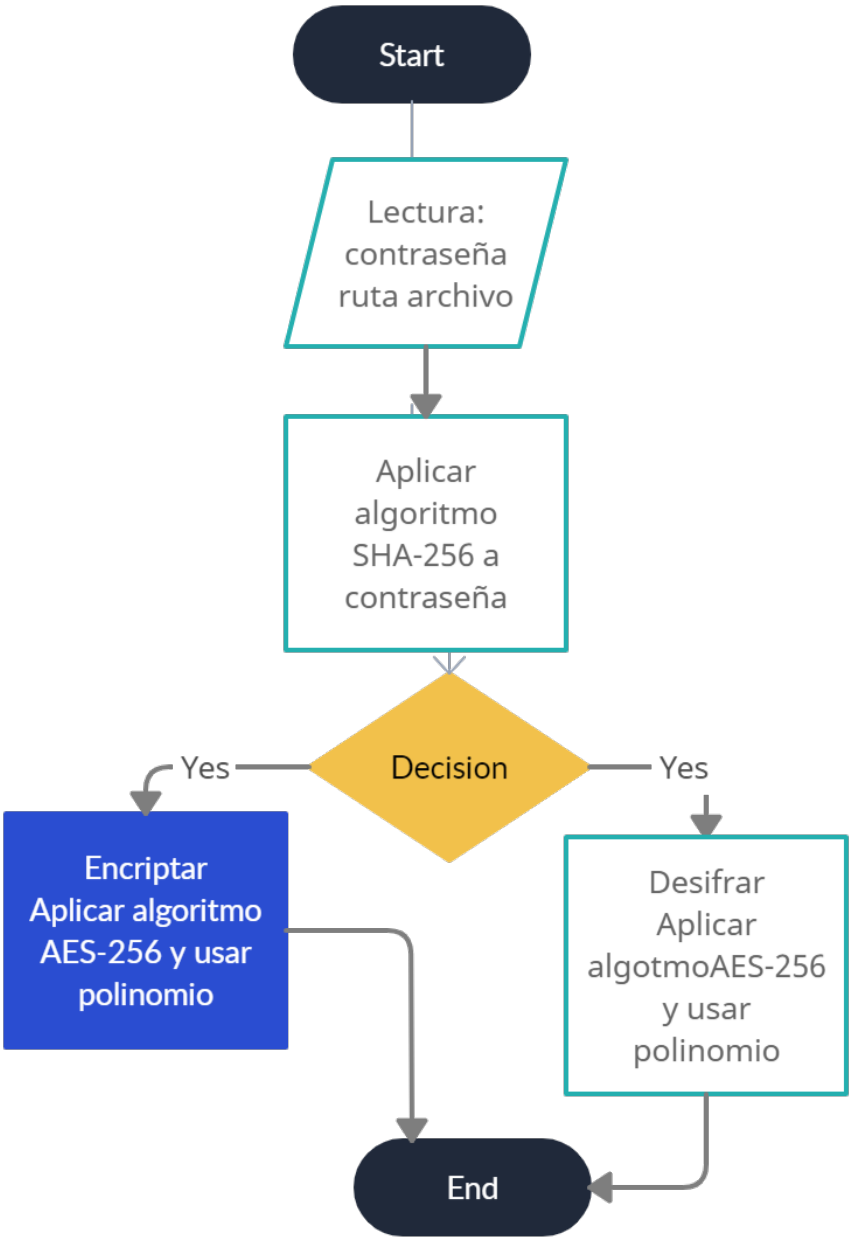

Figure 1: Diagrama de flujo

Justificaciones

Decidimos implementar el proyecto con el lenguaje de java, ya que es mas sencillo hacer el debugging. Se utiliza el algoritmo AES-256 porque de todos los algoritmos AES es el mas seguro.También se utilizo Mave para facilitar el trabajo ya que desde ahi usamos las librerias , test y demas herramientas.

Fuentes consultadas:

- Esquema de Secreto Compartido de Shamir y algoritmos
  1. Shamir's Secret Sharing
  2. Shamir's Keystore
  3. SHA-256 Hash in Java

4. How to hast some string wih sha-256
5. Java AES-256 Encryption and Decryption
6. Java Program to Convert File to a Byte Array
7. Convert byte[] array to File using Java
8. Java AES Encryption and Decryption
9. Encriptación AES en Java

- Videos consutados:

1. AES Explained (Advanced Encryption Standard)
2. Shamir Secret Sharing Scheme 1/2
3. Shamir Secret Sharing Scheme 2/2
4. CSV column to Python List

- Maven:

1. Descarga Maven
2. Instalación
3. Poner dependencias dentro del jar
4. CSV column to Python List

- Librerias usadas:

1. Cypher
2. BigInteger
3. JavaTuples