Modelado y Programación
Proyecto 3

Aguirre Chávez Alejandra, 305772132

Junio 2022

1. Definición del problema

Generar un programa que permita cifrar y descifrar cualquier tipo de archivo usando el Esquema Secreto de Shamir y el estándar de cifrado de datos AES (el cual admite claves de cifrado de 256 bits), además para generar una contraseña de la longitud necesaria para deacuerdo con el estándar AES se debe utilizar la función de dispersión (hash) SHA-256. Esta última permite transformar la contraseña introducida por el usuario para que a partir de ella se obtenga una clave de la longitud requerida.

2. Análisis del problema

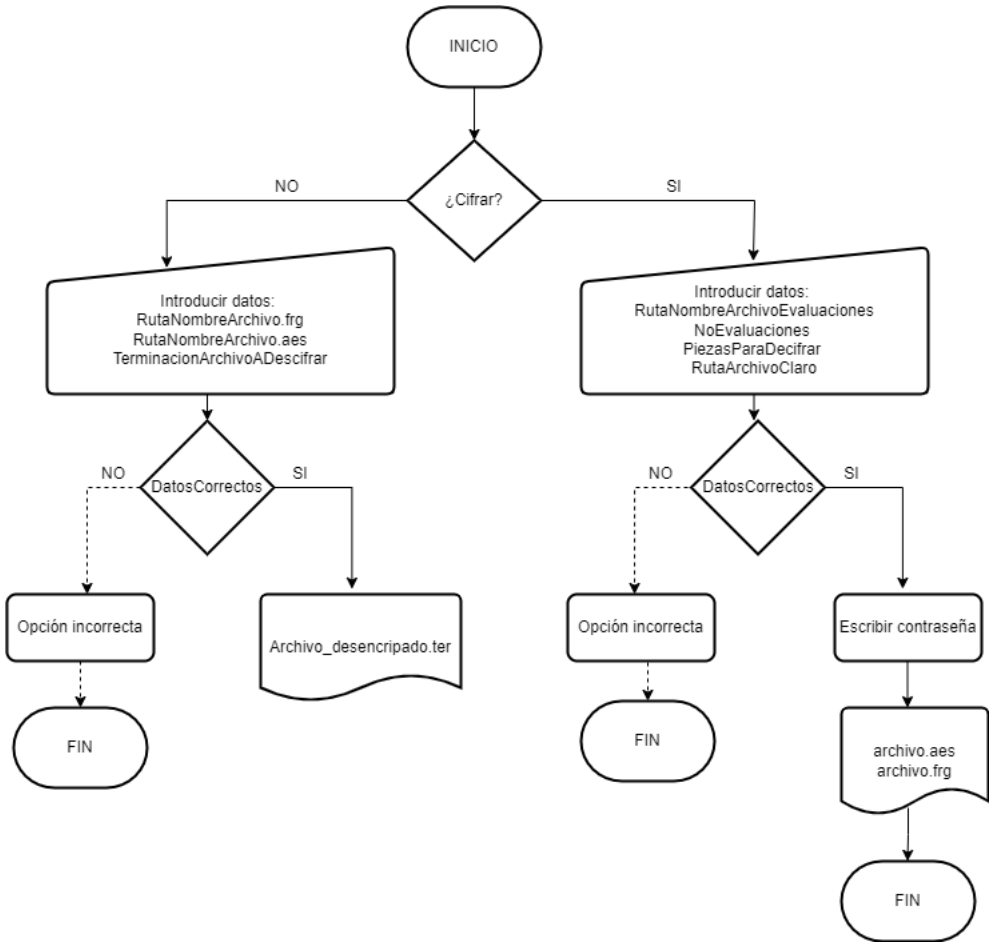
Se necesita cifrar y descifrar un archivo de cualquier tipo utilizando el esquema de cifrado de Shamir.

El método de Shamir lo que permite es esconder una clave K dentro de un polinomio de Lagrange de grado n y a partir de la reconstrucción de este polinomio, al evaluarlo en cero se puede recuperar la clave K que permite descifrar el archivo deacuerdo con el estándar AES.

Por otra parte, para cifrar el usuario debe proporcionar una contraseña, esta se pasa por la función de hashing SHA-256 para que tenga la longitud requerida con el estándar AES, se le agrega Sal y se cifra el archivo usando AES, además se generan n evaluaciones de un Polinomio de Lagrange de las cuales si se juntan al menos t con $1 < t \leq n$, es posible descifrar el archivo.

3. Diagrama de Flujo

El diagrama se realizó con el software $DRAWIO$ y los símbolos usados los escogí de acuerdo a como se explican en el programa $DRAWIO$



4. Como correr el programa

Primero para compilar se hace lo siguiente:
$ javac Main.java

Luego para **CIFRAR** un archivo se debe introducir en la terminal:

java shamir/Main c shamir/ArchivoClaro num num shamir/ArchivoClaro.ter

Los 5 argumentos usados son:

- Opción cifrar
- Ruta y nombre del archivo donde se guardaran las n evaluaciones de polinomio.
- Evaluaciones deseadas (n>2).
- No. de piezas necesarias para decifrar (1<= t <= n).
- Ruta y nombre del archivo que se va a cifrar.

Para **DESCIFRAR** un archivo que ha sido cifrado se introduce en la terminal

java shamir/Main d shamir/ArchivoClaro.frg shamir/ArchivoClaro.aes ter

Los 4 argumentos usados son:

- Ruta y nombre del archivo con extensión .frg que contiene al menos t de las n evaluaciones del polinomio.
- Ruta y nombre del archivo cifrado con extensión.aes
- Terminación del archivo que se va a descifrar (últimas 3 letras)

5. Qué hace falta a futuro

A continuación se identifican áreas de mejora o puntos que se podrían mejorar:

- Cobro: No cobraría mucho, pienso que a lo más 500$, siento que si le hace falta una interfaz gráfica que pueda ser portable. Y quizás que en lugar de tener las evaluaciones en un txt se generen varios archivos q uno pudiera esconder y recuperar para descifrar el documento claro de interés
- Cosas a corregir
    - Agregar una interfaz gráfica haría más fácil la introducción de los parámetros pues así como está si puede llegar a ser engorroso.
    - Identificar el tipo de archivo que se va a descrifrar en lugar de tener que introducir el tipo uno mismo.

- Apesar de que se utilizó SHA-256 y se agregó Sal al proceso del cifrado de la contraseña de acuerdo con el compilador se realizan operaciones poco seguras, así que corregir eso queda pendiente.
- Agregar alertas más específicas o diferenciadas para cada caso de error.
- Mejorar la organización de los archivos.

6. Fuentes consultadas

- https://howtodoinjava.com/java/java-security/how-to-generate-secure-password-hash-md5-sha-pbkdf2-bcrypt-examples/
- https://www.geeksforgeeks.org/path-touri-method-in-java-with-examples/
- https://docs.oracle.com/javase/7/docs/api/javax/crypto/spec/ SecretKeySpec.html
- https://docs.oracle.com/javase/7/docs/api/javax/crypto /Cipher.htmlENCRYPT_MODE
- https://docs.oracle.com/javase/7/docs/api/javax/crypto/ spec/GCMParameterSpec.html
- https://docs.oracle.com/javase/8/docs/api/javax/crypto/ spec/PBEKeySpec.html PBEKeySpec-char:A-byte:A-int-int-
- https://www.w3schools.com/java/ref_string_lastindexof.asp
- https://docs.oracle.com/javase/7/docs/api/java/io/FileOutputStream.html
- https://stackoverflow.com/questions/25428768/ java-eclipse-how-to-call-a-int-or-string-from-another-class-in-same-project