Facultad de Ciencias, UNAM

Modelado y programación

Proyecto 3: Shamir Secret Sharing

18 de junio de 2022

Garzón Castro Oscar René

Profesor: José de Jesús Galaviz Casas
Ayudante: Ximena Lezama
Ayud. Lab.: Miren Jessamyn Hernández Leyva

1. Definición del problema

Implementar el Esquema de Secreto Compartido de Shamir. El cual consiste en distribiuir una llave de encriptación en múltiples partes. Y al unir cierto número de partes, recuperar la llave para desencriptar el archivo

2. Análisis del problema.

Para encriptar el arichvo se va utilizar el estandar de cifrado de datos AES. Además se utiliza el modo de encriptación Galois/Counter Mode (GCM) para garantizar la confiabilidad y la integridad del mensaje.

La llave de encriptación va ser generada a partir de una contraseña a la cual se va aplicar hash256 para obtenerla.

Dado que la llave va ser escondida como el término independiente de un polinomio tenemos que caluclar dicho polinomio en varios valores por lo que usaremos el método de horner para que el algoritmo sea eficiente.

3. Selección de la mejor alternativa.

En este programa se ocupa trabajar con números enenteros muy grandes. Python se encarga automaticamente de lidiar con números de tantos dígitos, por eso python va ser el lenguaje utilizado. Además cuanto con una libreria, PyCryptodome, que esta muy bien documentada y cuenta con todos los recursos necesarios para la encriptar y desencriptar archivos.

4. Pseudocódigo.

Cifrar

1. Crear la clase Cifrador. Con argumentos: key, evaluaciones, evaluaciones mínimas y un cifrador
2. Esta clase va tener métodos para cifrar un archivo y para obtener las evaluaciones (los puntos necesarios para después reconstruir la llave)
3. El algoritmo de horner genera las evaluaciones necesarias de forma eficiente

Descifrar

1. Crear la clase Descifrador la cual tiene argumentos: key, evaluaciones y el documento cifrado.
2. Esta clase tiene un solo método público para descifrar el archivo
3. Tiene además dos métodos privados get_key y evalua_poli que reconstruyen el polinomio a partir de las evaluaciones y así obtienen la key para desencriptar el archivo.
4. Además se creará un módulo main desde el cual se harán las llamadas correspondientes a cada clase para encriptar y desencriptar los archivos.

El nombre original del archivo se guarda en el documento generado al momento de realizar la encriptación para posteriormente recuperarlo y contar con el nombre original.

5. Proyección a futuro.

Se puede crear una interfaz gráfica para que el programa sea mas user-friendly. Tal vez se pueda trabajar mas en el area de criptografía pero eso requeriría un estudio profundo de la misma.

Este programa podría ser valioso para empresas o personas que manejan data muy sensible y no se pueda confiar en un solo actor para guardarla. Haciendo estimaciones en internet se calcula que el programa podria costar 10,000 pesos si tuviera una interfaz gráfica mas amigable.

6. Referencias

https://www.pycryptodome.org/en/latest/src/cipher/modern.html
https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
https://www.geeksforgeeks.org/shamirs-secret-sharing-algorithm-cryptography/