Criptografía y Cifrado de Información 2021

Lab 10

02.noviembre.2021

En este laboratorio implementamos el método de cifrado de clave pública ElGamal.

1. Elaborar un esquema de cifrado de clave pública ElGamal. Para ello, deberá implementar una clase CifradoElGamal con los siguientes métodos:

   - GenerarClaves,
   - Encriptar,
   - Decriptar.

   El método **GenerarClaves** debe generar un primo aleatorio grande p, en el rango dado por dos parámetros $(minn, maxx)$. Usaremos el grupo de unidades $G = U(p)$. El método luego debe generar un valor aleatorio $\mathbf{g} \in [2, p-1]$ el cual servirá como generador de G, y un entero aleatorio $\mathbf{a}$ que sirve como clave privada. El método debe producir la clave $\mathbf{h} = \mathbf{g}^{\mathbf{a}}$.
   Como respuesta, el método debe guardar la clave privada $\mathbf{a}$, y la clave pública $(\mathbf{g}, \mathbf{h})$. Tome como rango para los primos: $minn = 10000$ y $maxx = 100000$.

   El método **Encriptar** debe recibir como input una cadena de texto (mensaje a cifrar), o bien, si lo prefieren, debe recibir un *path* y un nombre de archivo donde se encuentra el mensaje a cifrar $\mathbf{m}$.
   Luego, deberá implementar el cifrado ElGamal. Puede usar H la función hash del método SHA-256, y el sistema de cifrado simétrico de su elección.
   Como respuesta, el método debe devolver el mensaje cifrado $(\mathbf{u}, \mathbf{c})$ en formato base64, o en su defecto, guardarlo en un archivo en el mismo path que el texto original.

   Finalmente, el método **Decriptar** debe recibir como input una cadena de texto (mensaje cifrado), o bien, si lo prefieren, debe recibir un *path* y un nombre de archivo donde se encuentra el mensaje cifrado $(\mathbf{u}, \mathbf{c})$.
   Luego, deberá implementar la decripción según ElGamal, con H la función hash dada por el método SHA-256, y el sistema de cifrado simétrico elegido.
   Como respuesta, el método debe devolver el mensaje original $\mathbf{m}$, o en su defecto, guardarlo en un archivo en el mismo path que el texto original.
   Ambas funciones o métodos Encriptar y Decriptar, deben usar la claves generadas por el método GenerarClaves.

   Para hacer más manejable los métodos. Debe implementar una plataforma interactiva con el usuario, digamos un menú simple, donde el usuario puede elegir la opción a ejecutar:

```
Cifrado ElGamal:
1.  Generar claves
2.  Encriptar mensaje
3.  Decriptar mensaje
4.  Salir.
```