Criptografía y Cifrado de Información 2021

Lab 09

21.octubre.2021

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

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

   - GenerarClaves,
   - Encriptar,
   - Decriptar.

   El método **GenerarClaves** debe generar dos primos aleatorios impares p y q, con $p \neq q$, ambos entre un rango dado por dos parámetros $(minn, maxx)$. Luego debe construir el módulo $N = pq$.
   Además, deberá generar un número aleatorio $e \pmod N$, con $e \not\equiv 1 \pmod N$ y $e \not\equiv N-1 \pmod N$, y su inverso d módulo $\varphi(N)$. Esto es, e y d deben satisfacer $ed \equiv 1 \pmod{\varphi(N)}$.
   Como respuesta, el método debe guardar la clave pública (e, N), y la clave privada (d, N). Ambas claves se deben guardar en formato base64. Tome como rango para los primos: $minn = 200$ y $maxx = 1000$.

   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 RSA (Iso estándar o Libro de Texto, ustedes eligen). Puede usar H la función hash del método SHA-256, y el sistema de cifrado simétrico AES.
   Como respuesta, el método debe devolver el mensaje cifrado $\mathbf{c}$ 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 $\mathbf{c}$.
   Luego, deberá implementar la decripción según RSA Iso estándar, con H la función hash dada por el método SHA-256, y el sistema de cifrado simétrico AES.
   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 RSA:
1.  Generar claves
2.  Encriptar mensaje
3.  Decriptar mensaje
4.  Salir.
```

2. Cada grupo debe generar una clave pública RSA (e, N) en base64 (aquí se debe concatenar una cadena con el valor de e, un punto (separador) y la cadena que contiene el valor de N, y luego codificar de ASCII a base64).

   En combinación con otro equipo de trabajo (los cuales se indican a continuación), hacer lo siguiente:

   - Enviar un mensaje al otro equipo (un archivo de texto pequeño conteniendo algún mensaje a responder).
   - El mensaje cifrado recibido, deberá ser descifrado, respondido y enviado de vuelta al otro equipo.

   Los equipo a trabajar en conjunto son: 1 y 7, 2 y 8, 3 y 9, 4 y 10, 5 y 11, 6 y 12.