Universidad del Valle de Guatemala
Cifrado de Información
Sección 10
Docente: Alan Reyes

Jose Pablo Ponce 19092
Gabriel Quiroz 19255
Alexa Bravo 18831
Octubre 30, 2021

# REPORTE LABORATORIO 09

## INTRODUCCIÓN

El nombre RSA proviene de las iniciales de sus tres creadores, Rivest, Shamir y Adleman. RSA es un algoritmo de cifrado de clave pública que le permite al usuario conservar la confidencialidad de la información cuando es transmitida o compartida con otros usuarios. Es uno de los más utilizados en la actualidad, la mayor parte de los sitios web hoy integran seguridad SSL/TLS, y permiten la autenticación mediante RSA.

RSA, trabaja con dos claves, una pública y una privada. Todo el contenido de texto plano, o contenido sin cifrar, que se haya encriptado con la clave pública, podrá ser descifrado mediante la clave privada, y viceversa, todo contenido cifrado con la clave privada podrá ser descifrado mediante la clave pública.

La fortaleza del algoritmo RSA se basa en la complejidad de cálculo que tiene encontrar los dos factores primos de un número compuesto muy grande. Con este algoritmo los valores de los factores primos deben ser mínimo de 155 dígitos, lo que aproximadamente son unos 512 bits. El producto de estos factores tiene alrededor de 310 dígitos, que representa 1024 bits, lo cual puede dar una idea de lo complejo que puede llegar volverse su factorización en materia de recursos tecnológicos.

En este laboratorio se elaboró un cifrado RSA, qué incluye la generación de una clave pública, el cifrado y descifrado de un mensaje.

## METODOLOGÍA

### Generar Claves

Se creó un método qué genera dos primos aleatorios impares $p$ y $q$. Se construyó un módulo $N = pq$. Además se generó un número aleatorio $e$ y su inverso $d$. Como respuesta a todo lo mencionado anteriormente el método guarda una clave pública y otra privada. Ambas en formato *base64*.

### Encriptar

Se creó un método qué recibe como input una cadena de texto, qué es el mensaje a cifrar. Luego se implementó el cifrado RSA, se utilizó la función hash del método SHA-256, y el sistema de cifrado simétrico AES. Como respuesta el método devuelve el mensaje cifrado en formato *base64*.

**Decriptar**

El método recibe como input una cadena de texto, qué es el mensaje cifrado. Se implementó la descripción según RSA, con la función hash dada por el método SHA-256, y el sistema de cifrado simétrico AES. Como respuesta el método devuelve el mensaje original.

Para observar el funcionamiento de estos métodos, se creó un menú con las opciones de generar claves, encriptar y decriptar mensajes.

**RESULTADOS**

**Menú de Opciones**

```
1. Generar claves
2. Encriptar mensaje
3. Decriptar mensaje
4. Salir.
Ingresa el numero de opcion a elegir
```

**Generar Claves**

```
Generar Claves
p: 809
q: 313
n: 253217
phi_n: 252096
e: 97535
d: 240191
llave publica: 97535.253217
llave publica base 64: OTc1MzUuMjUzMjE3
240191.253217
llave privada base 64: MjQwMTkxLjI1MzIxNw==
```

**Encriptar**

```
Encriptar mensaje
Ingrese el mensaje a cifrar:
hola caracola
Mensaje encriptado:
NzkwNjUzOTc5NjY5MDM4NTIyNjEwODIzMDc1MTIyNjEwODMzMTUzNDIyNjEwODUxMzk3OTY2OTAzODUy
MjYxMDg=
```

**Decriptar**

```
1. Generar claves
2. Encriptar mensaje
3. Decriptar mensaje
4. Salir.
Ingresa el numero de opcion a elegir
3
Decriptar mensaje
Mensaje decriptado:
Hola Caracola
```

**CONCLUSIONES**

1. RSA es uno de los sistemas de cifrado asimétricos más exitosos de la actualidad.
2. El cifrado RSA se utiliza para las firmas digitales.
3. Conocer en qué consiste el cifrado RSA es la mejor opción para utilizarlo de forma adecuada y salvaguardar la información más sensible.

**LINK DEL REPOSITORIO**

https://github.com/JosePabloPonce/lab9cifrado