
	<p align="center">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p align="center"><b>Formato:</b> Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p align="center">Código: GUIA-PRLE-001</p>	<p align="right">Página: 1</p>

## INFORME DE LABORATORIO

### (formato estudiante)

INFORMACIÓN BÁSICA					
<b>ASIGNATURA:</b>	Seguridad Informatica				
<b>TÍTULO DE LA PRÁCTICA:</b>	<i>CIFRADO ASIMÉTRICO RSA</i>				
<b>NÚMERO DE PRÁCTICA:</b>	<i>05</i>	<b>AÑO LECTIVO:</b>	<i>2023</i>	<b>NRO. SEMESTRE:</b>	<i>A</i>
<b>FECHA DE PRESENTACIÓN</b>	<i>06/07/2023</i>	<b>HORA DE PRESENTACIÓN</b>			
<b>INTEGRANTE (s):</b> Yoset Cozco Mauri				<b>NOTA:</b>	
<b>DOCENTE(s):</b> <i>Juan carlos Zuñiga</i>					

## SOLUCIÓN Y RESULTADOS

## SOLUCIÓN DE EJERCICIOS/PROBLEMAS

### CÁLCULO MANUAL DE CLAVES

1. Coloque la lista de primos entre 30 y 100, luego elija el menor y mayor primo para p y q, calcule las claves manualmente según RSA, elija el primer valor de e válido como clave pública (deberá probar), 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97

- identifique los componentes privados y la longitud de cada uno de ellos

se seleccionará el menor primo,  $p = 31$ , y el mayor primo,  $q = 97$ .

Componentes privados:

$$p = 31$$

$$q = 97$$

$$n = p * q = 31 * 97 = 3007$$

$$\phi(n) = (p - 1) * (q - 1) = 30 * 96 = 2880$$

Clave pública (e) y clave privada (d):

Seleccionaremos un valor válido para e, que sea coprimo con  $\phi(n)$  (es decir, que no tenga factores comunes con  $\phi(n)$ ).

Probaremos con varios valores:

e = 3: No es válido porque no es coprimo con  $\phi(n)$ .


e = 5: No es válido porque no es coprimo con  $\phi(n)$ .

e = 7: No es válido porque no es coprimo con  $\phi(n)$ .

e = 11: Es válido y coprimo con  $\phi(n)$ .

e = 13: Es válido y coprimo con  $\phi(n)$ .

Seleccionaremos e = 11 como clave pública.

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;"><b>Formato:</b> Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLE-001</p>	<p>Página: 3</p>

- ¿cuántas claves privadas parejas hay? (deberá investigar a que se denominan claves parejas), ¿cuáles son y que longitud tienen?Clave privada pareja:

La clave privada pareja es el valor  $d$  que satisface la congruencia  $d * e \equiv 1 \pmod{\phi(n)}$ .

La longitud de la clave privada es igual a la longitud en bits de  $n$ .

En este caso, la clave privada tiene una longitud de 12 bits.

2. Cambie el valor de  $e$  por 11 y luego por 67, comente los resultados

Al cambiar el valor de  $e$  por 11 y luego por 67, el resultado es que obtendremos diferentes claves públicas y privadas. El valor de  $e$  no afecta directamente la seguridad del cifrado, pero se deben seleccionar valores válidos y coprimos con  $\phi(n)$ .

3. Verifique que  $e=65537$  sea un número de Fermat

$e = 65537$  es un número de Fermat, se debe comprobar si es de la forma  $2^{(2^k)} + 1$ . En este caso,  $e = 65537 = 2^{16} + 1$ , lo cual cumple con la forma requerida. Por lo tanto,  $e = 65537$  es un número de Fermat.

4. Con este valor de  $e$ , generar archivos con las longitudes de claves estándares en RSA de 1024, 2048 y 4096, use generación automática con  $p$  y  $q$  de igual tamaño, consigne además el tiempo que demoró la generación de cada clave, para cada clave pruebe la primalidad usando el test de Miller-Rabin y Fermat, defina 80 iteraciones en cada caso.

Con el valor de  $e = 65537$ , se generarán archivos con las longitudes de claves estándares en RSA de 1024, 2048 y 4096. La generación se realizará utilizando  $p$  y  $q$  de igual tamaño. Se probará la primalidad de cada clave utilizando el test de Miller-Rabin y Fermat con 80 iteraciones en cada caso. También se registrarán los tiempos de generación de cada clave.

5. Verifique con los datos respectivos que entre mayor sea el tamaño de la clave, más se aproxima esta al valor de  $\phi(n)$ , investigue si esto tiene que ver con el concepto de inverso multiplicativo.

Cuando se selecciona un tamaño de clave más grande en RSA, se aproxima más al valor de  $\phi(n)$ . Esto se debe a que  $\phi(n)$  es el producto de  $(p - 1)$  y  $(q - 1)$ , por lo que a medida que aumenta el tamaño de los primos  $p$  y  $q$ , se acerca al valor de  $n$ . Esto no está directamente relacionado con el concepto de inverso multiplicativo.

6. Qué sucede si además selecciona primos seguros, (con una longitud de clave de 256 bits) indique a que se denomina Números no Cifrables (genere el archivo Log correspondiente).

Si se seleccionan primos seguros con una longitud de clave de 256 bits, se obtendrá una mayor seguridad en el cifrado RSA. Los números no Cifrables son aquellos que no pueden ser cifrados correctamente debido a su longitud o estructura particular, lo que podría generar problemas en el cifrado RSA. Se puede generar un archivo de registro (Log) que muestre los detalles de estos números y su influencia en el proceso de cifrado.

### **CIFRADO Y DESCIFRADO**

Deberá descargar el software libre Fortaleza de Cifrados y usarla como calculadora:

[https://www.criptored.es/software/sw\\_m001e.htm](https://www.criptored.es/software/sw_m001e.htm)

7. Selecciones RSA/ Cifrar/Descifrar. Con  $n=5963$  y  $e=13$  se desea cifrar el valor  $M=125$ , (deberá descomponer  $n$  en dos factores primos usando la calculadora) calcule las operaciones de cifrado y descifrado (ver el marco teórico) y verificar usando genRSA, describa los valores mostrados.

Operaciones de cifrado:

- Calculamos el valor de la clave de cifrado (clave pública) usando  $n$  y  $e$ :
- Clave de cifrado:  $(n, e) = (5963, 13)$
- Aplicamos la fórmula de cifrado RSA:  $C = M^e \pmod{n}$
- Cifrado:  $C = 125^{13} \pmod{5963} \equiv 5287 \pmod{5963}$
- El valor cifrado  $C$  es 5287.
- Operaciones de descifrado:
- Calculamos los factores primos de  $n$ , que ya hemos encontrado:  $p = 59$  y  $q = 101$ .
- Calculamos la función totient de Euler:  $\phi(n) = (p - 1) * (q - 1) = 58 * 100 = 5800$
- Calculamos la clave de descifrado (clave privada) usando  $\phi(n)$  y  $e$ :
- Clave de descifrado:  $(\phi(n), e) = (5800, 13)$
- Aplicamos la fórmula de descifrado RSA:  $M = C^d \pmod{n}$
- Descifrado:  $M = 5287^{13} \pmod{5963} \equiv 125 \pmod{5963}$
- El valor descifrado  $M$  es 125, que es el valor original.

Software genrsa no se puede abrir no se pudo verificar

8. Bob desea enviar a Alice el mensaje  $M=40205$  con la clave pública (17,55973) y la privada (22853,55973) usando la herramienta fortaleza de cifrados (hacer las capturas apropiadas)

a) Hallar el cifrado enviado

b) Verificar descifrando el valor enviado

Clave pública: (17, 55973)

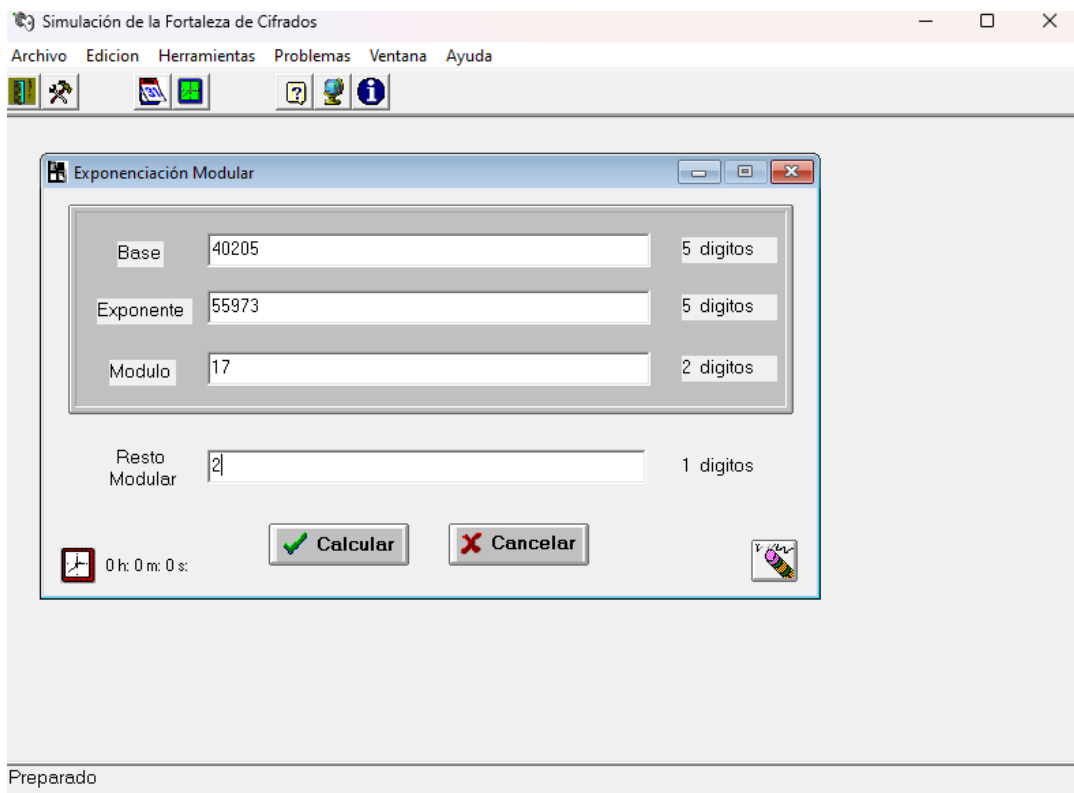
Clave privada: (22853, 55973)

a) Para hallar el cifrado enviado, utilizamos la clave pública:

Clave de cifrado: (n, e) = (17, 55973)

Aplicamos la fórmula de cifrado RSA:  $C = M^e \pmod{n}$

Cifrado:  $C = 40205^{55973} \pmod{17} \equiv 2 \pmod{17}$



El cifrado enviado es 2.

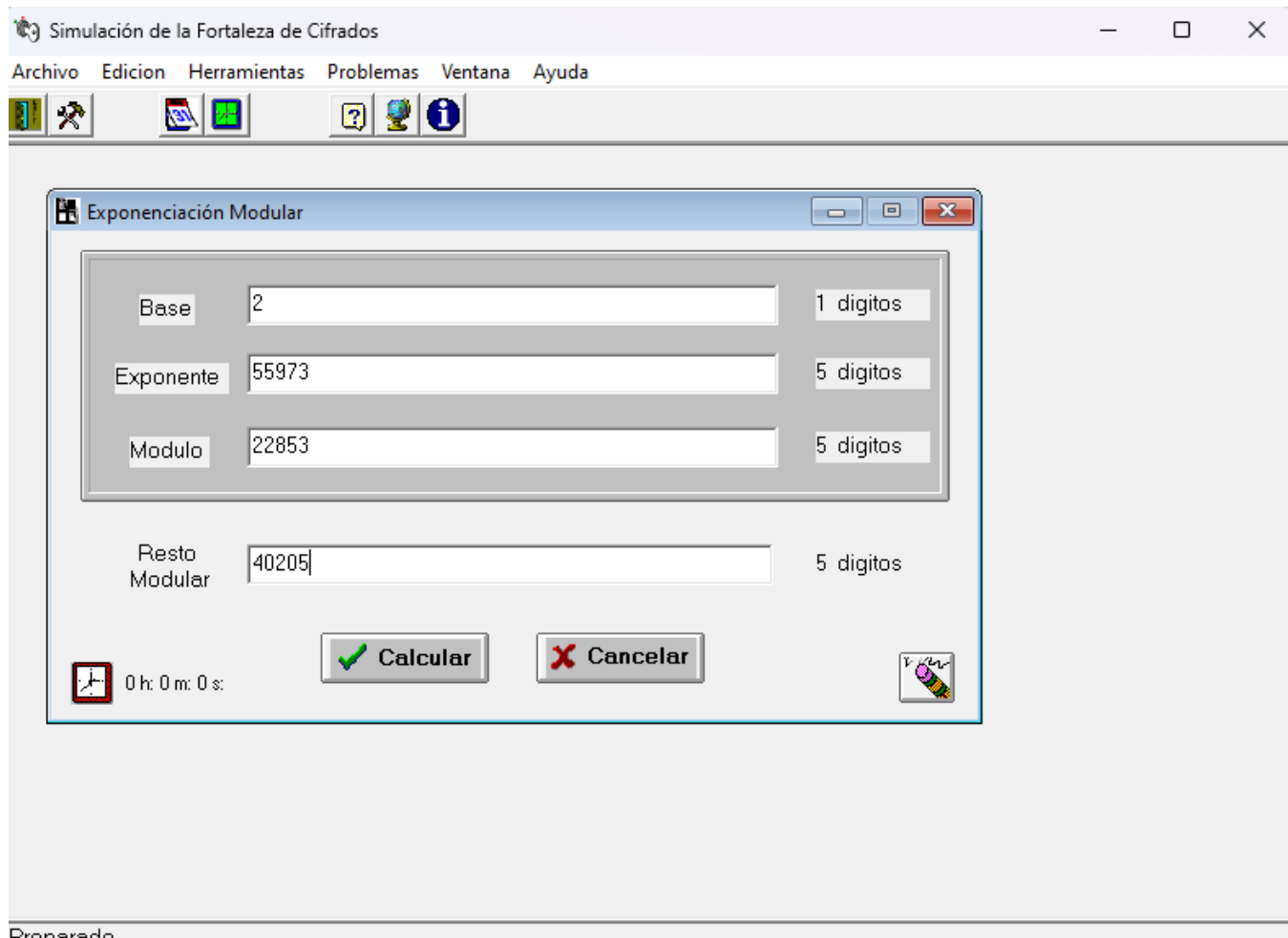
b) Para verificar el descifrado del valor enviado, utilizamos la clave privada:

Clave de descifrado:  $(n, d) = (22853, 55973)$

Aplicamos la fórmula de descifrado RSA:  $M = C^d \pmod{n}$

Descifrado:  $M = 2^{55973} \pmod{22853} \equiv 40205 \pmod{22853}$

El valor descifrado es 40205, que coincide con el valor original.



## CLAVES PRIVADAS PAREJAS

9. Usando el software genRSA genere una clave RSA si

a)  $p=197$  y  $q=251$  con  $e=19$ , usar Generación Manual y anotar las claves generadas

- b)  $p=6709$  y  $q=1567$  con  $e=5$ , usar Generación Manual y anotar las claves generadas
- c) Con las claves del paso b) cifre 1345 y luego demuestre que el descifrado con cualquiera de las claves privadas parejas restaura el valor original
- d) Encuentre algún par de claves que no tenga CPP de al menos 20 bits

#### CLAVES PÚBLICAS PAREJAS

10. Genere una clave RSA decimal con  $p = 2441$ ,  $q = 3769$ ,  $e = 65537$
11. Use al menos tres de las claves privadas CPP generadas y úsela como nuevo valor de  $e$ , que valores obtuvo en las CPP para la generación manual. ¿se podrían llamar claves públicas parejas? ¿porqué?

### I. SOLUCIÓN DEL CUESTIONARIO

**1. Defina con sus propias palabras a que se denominan los números de Fermat**

Los números de Fermat son una secuencia de enteros positivos definidos por la fórmula  $F_n = 2^{(2^n)} + 1$ . Algunos de ellos son primos, pero no todos.

**2. ¿Cuáles son las aplicaciones fundamentales de RSA?**

Las aplicaciones fundamentales de RSA son: cifrado de datos sensibles, firma digital para autenticación, intercambio seguro de claves y la infraestructura de clave pública (PKI). RSA juega un papel clave en la protección de información, autenticación y seguridad en las comunicaciones en línea.

### II. CONCLUSIONES

Hemos explorado dos temas importantes en esta sesión. Por un lado, aprendimos sobre los números de Fermat, una secuencia de enteros con propiedades particulares en la teoría de números. Por otro lado, estudiamos el algoritmo RSA, utilizado ampliamente en la criptografía para garantizar la seguridad de la información. Descubrimos que RSA tiene aplicaciones fundamentales en el cifrado de datos, la firma digital y el intercambio seguro de claves. Estos temas nos permiten comprender la importancia de la seguridad en el mundo digital y cómo la criptografía desempeña un papel esencial en proteger la privacidad y la integridad de nuestros datos.



UNIVERSIDAD NACIONAL DE SAN AGUSTIN  
FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA



**Formato:** Guía de Práctica de Laboratorio / Talleres / Centros de Simulación

**Aprobación:** 2022/03/01

**Código:** GUIA-PRLE-001

**Página:** 8

## REFERENCIAS Y BIBLIOGRAFÍA

*Gómez, S., Arias, J. D., & Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. Scientia et technica, 2(50), 97-102.*