
	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-PRLD-001	Página: 1

GUÍA DE LABORATORIO 05

INFORMACIÓN BÁSICA					
ASIGNATURA:	SEGURIDAD INFORMÁTICA				
TÍTULO DE LA PRÁCTICA:	CIFRADO ASIMÉTRICO RSA				
NÚMERO DE PRÁCTICA:	05	AÑO LECTIVO:	2023	NRO. SEMESTRE:	A
TIPO DE PRÁCTICA:	INDIVIDUAL				
	GRUPAL	MÍNIMO DE ESTUDIANTES	1	MÁXIMO DE ESTUDIANTES	2
FECHA INICIO:	30/06/2023	FECHA FIN:	06/07/2023	DURACIÓN:	7 días
RECURSOS Y EQUIPOS A UTILIZAR: PC, IDE de Programación					
DOCENTE(s): Juan Carlos Zuñiga					

OBJETIVOS/TEMAS Y COMPETENCIAS	
OBJETIVOS:	<ul style="list-style-type: none"> Conocer el algoritmo de cifrado asimétrico RSA Conocer los procesos de generación de claves RSA
TEMAS:	<ul style="list-style-type: none"> Generación de claves en RSA Cifrado RSA Condiciones de seguridad
COMPETENCIAS A ALCANZAR	<p>Mantiene responsablemente, software para que se adecue a las necesidades cambiantes del usuario, cliente o sociedad mediante la aplicación de técnicas y procedimientos establecidos que siguen estándares de calidad destinados a implementar la seguridad informática. (referencia C.n)</p> <p>Asegura la calidad del software mediante la aplicación de pruebas, validaciones y estándares de seguridad para garantizar el correcto funcionamiento del producto, en el marco de la seguridad informática, considerando el impacto productivo y social. (referencia C.o)</p> <p>Diseña soluciones informáticas apropiadas para proveer seguridad informática, utilizando los principios de ingeniería que integran consideraciones éticas, sociales, legales y económicas entiendo las fortalezas y limitaciones del contexto (referencia C.q)</p>

CONTENIDO DE LA GUÍA

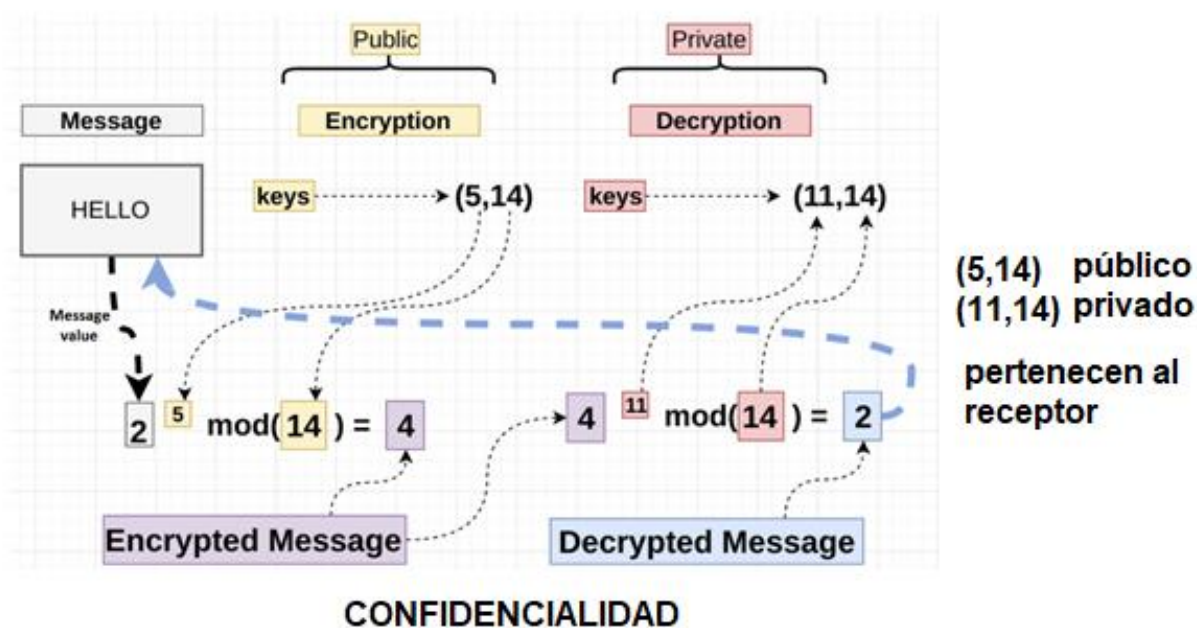
I. MARCO CONCEPTUAL

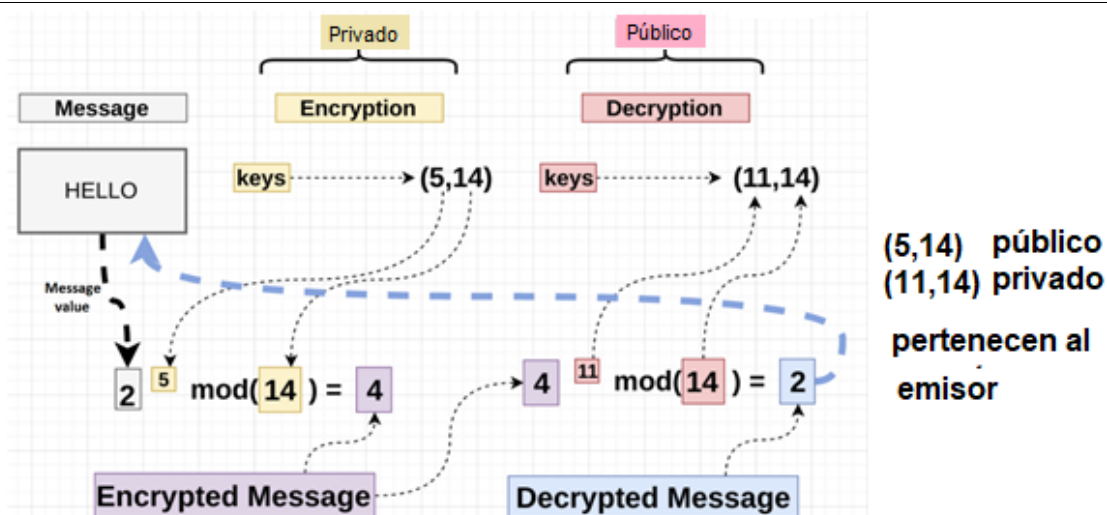
El algoritmo asimétrico RSA

RSA (Rivest, Shamir y Adleman) es un algoritmo asimétrico, por lo que requiere un par de claves (pública y privada), la pública se da a conocer a todo aquel con el que pudiera comunicarse y la privada se mantiene segura. Fue publicado en la década de los 70 por Ron Rivest, Adi Shamir y Leonard Adleman. RSA es bastante lento, por lo que casi no se usa para cifrar datos, su mayor aplicación es para cifrar y comunicar las claves simétricas usadas para proteger grandes cantidades de datos.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10^{300} , y se prevé que su tamaño puede crecer junto con el crecimiento computacional.

Por lo tanto, RSA será seguro mientras no se hallen formas rápidas de descomponer un número grande en producto de primos. El proceso de cifrado/descifrado se muestra a continuación:





FIRMA O AUTENTICACIÓN

Generación de claves

El algoritmo usado para la generación de las claves pública y privada RSA es el siguiente:

1. Alice y Bob eligen cada uno un grupo $n = p \times q$ distintos o no y se mantendrán secretos, primos y con longitudes superiores a 512 bits.
2. Alice y Bob hacen público el cuerpo o módulo de trabajo n , para Alice será $n_A = p_A \times q_A$ y para Bob $n_B = p_B \times q_B$.
3. Cada usuario calculará el **Indicador de Euler** Φ de ese módulo n :
 $\Phi n = (p - 1)(q - 1)$. Así, Alice calcula $\Phi n_A = (p_A - 1)(q_A - 1)$ y Bob calcula $\Phi n_B = (p_B - 1)(q_B - 1)$, este número es el secreto o trampa, a partir del cual se calculan la clave pública e y la correspondiente clave privada d .
4. Cada usuario elige una clave pública e tal que: $1 < e < \Phi(n)$ y que cumpla la condición $\text{mcd}[e, \Phi(n)] = 1$, ello asegura la existencia del inverso multiplicativo y por lo tanto que se pueda calcular la clave privada, la clave pública será el par (e, n) . Luego Alice elige $1 < e_A < \Phi_A$ y Bob elige $1 < e_B < \Phi_B$.
5. Usando el **Algoritmo Extendido de Euclides**, cada usuario calcula su clave privada d . Alice calcula $d_A = \text{inv}(e_A, \Phi_A)$ y Bob calcula $d_B = \text{inv}(e_B, \Phi_B)$. Valor que mantiene en secreto, entonces se guarda siempre p, q, d

En el ejemplo mostrado en el gráfico del acápite anterior se procedió de la siguiente manera:

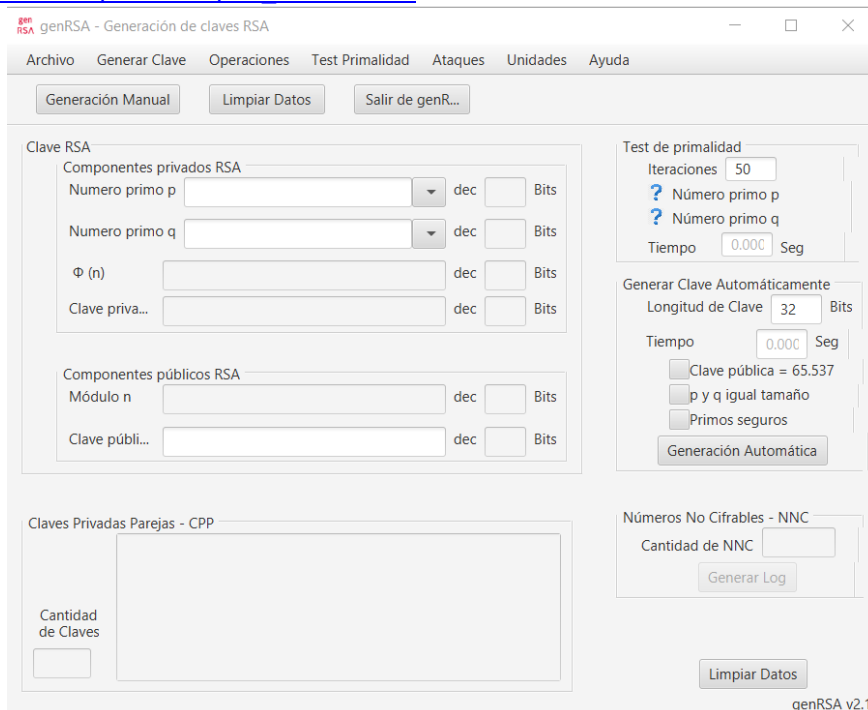
1. $p = 2, q = 7$ secretos y primos **31,97**
2. Luego el grupo $n = 14$ **3007**
3. El indicador de Euclides será $\Phi n = (2 - 1)(7 - 1) = 6$ **30*96=2880**
4. Se elige la clave pública e tal que $1 < e < 6$ y $\text{mcd}(e, 6) = 1$, la única opción $e = 5$, entonces la clave pública es (5, 14) **1<e<2880 mcd(e,2880)=1 e=7**
5. Usando el algoritmo extendido de Euclides se procede a calcular la clave privada $d = \text{inv}(5, 6) = 11$, entonces la clave privada es (11, 14), hay que recordar que $(d * e) \bmod(6) = 1$ **(d*7)mod(2880)=1 d=823**

II. EJERCICIO RESUELTO

Visualize el video <https://www.youtube.com/watch?v=CMe0COxZxb0>

Deberá descargar el software libre genRSA:

https://www.criptored.es/software/sw_m001d.htm





Familiarizarse con la herramienta.

III. EJERCICIOS PROPUESTOS

CÁLCULO MANUAL DE CLAVES

- 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
 - ¿cuántas claves privadas parejas hay? (deberá investigar a que se denominan claves parejas), ¿cuáles son y que longitud tienen?
- Cambie el valor de **e** por 11 y luego por 67, comente los resultados
- Verifique que **e=65537** sea un número de Fermat
- 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
- 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
- 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)

	<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;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 5</p>

CIFRADO Y DESCIFRADO

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

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.
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

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?

IV. CUESTIONARIO

1. Defina con sus propias palabras a que se denominan los números de Fermat
2. ¿Cuáles son las aplicaciones fundamentales de RSA?

V. REFERENCIAS Y BIBLIOGRAFÍA RECOMENDADAS:

Palacios, R., & Delgado, V. (2006, March). Aplicaciones prácticas de la criptografía. In *anales de mecánica y electricidad*.

TÉCNICAS E INSTRUMENTOS DE EVALUACIÓN	
TÉCNICAS: <i>Ejercicios propuestos</i>	INSTRUMENTOS: <i>Lista de cotejo</i>
CRITERIOS DE EVALUACIÓN Y LOGROS ALCANZADOS <i>Niveles de logro: inicio, proceso, logro esperado, logro destacado.</i>	