El cifrado RSA

En criptografía, **RSA (Rivest, Shamir y Adleman**) es un **sistema criptográfico de clave pública** desarrollado en 1979, que **utiliza factorización de números enteros**. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

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**, conocido, **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 siempre crezca con el aumento de la capacidad de cálculo de los ordenadores.

Como en todo sistema de clave pública, **cada usuario posee dos claves de cifrado: una pública y otra privada**. Cuando se quiere enviar un mensaje confidencial, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

En el caso de querer firmar (propiedades de autenticidad, integridad y no repudio), el emisor obtiene un hash del mensaje a firmar y lo procesa con su clave privada obteniendo así la firma; se envía el mensaje y la firma; el receptor recalcula el hash y descifra el hash original con la clave pública del emisor, validando así (o no) la firma del mensaje.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. Aunque se cree que la computación cuántica podría proveer de una solución al problema de factorización, existen investigadores que dudan que dichos avances vayan a volver obsoletos estos algoritmos.

Para generar las claves pública y privada, se sigue el siguiente procedimiento:

Generación de claves

1. Seleccionar dos números primos: p , q
2. Calcular: n = p * q
3. Calcular: z = (p - 1) * (q - 1)
4. Seleccionar un entero k que cumpla:

   $$\gcd(z, k) = 1;\ 1 < k < z$$

   gcd: greatest common divisor (máximo común divisor)
5. Elegir j de modo que cumpla:

   $$k * j = 1 \pmod{z}$$

   En la práctica: elegir un j entero que verifique
   $j = (1+x*z)/k$
   para algún valor entero de k

Clave Pública:

(n , k)

Clave Privada:

(j)

Para el cifrado y descifrado del mensaje se sigue el siguiente procedimiento:

Cifrado y descifrado	
Texto cifrado: C, que verifica: $M^k = C \pmod n$ Que puede calcularse así: **$C = M^k \% n$** (donde '%' calcula el módulo)	Texto plano: M, que verifica: $C^j = M \pmod n$ Que puede calcularse así: **$M = C^j \% n$** (donde '%' calcula el módulo)

EJEMPLO:

p		5
q		11
n	p*q	55
ϕ(n)	(p-1)*(q-1)	40
e e y ϕ(n) han de ser coprimos	1 < e < ϕ(n)	7
d	e*d mod ϕ(n) =1	23
llave pública	(e,n)	(7, 55)
llave privada	(d,n)	(23, 55)

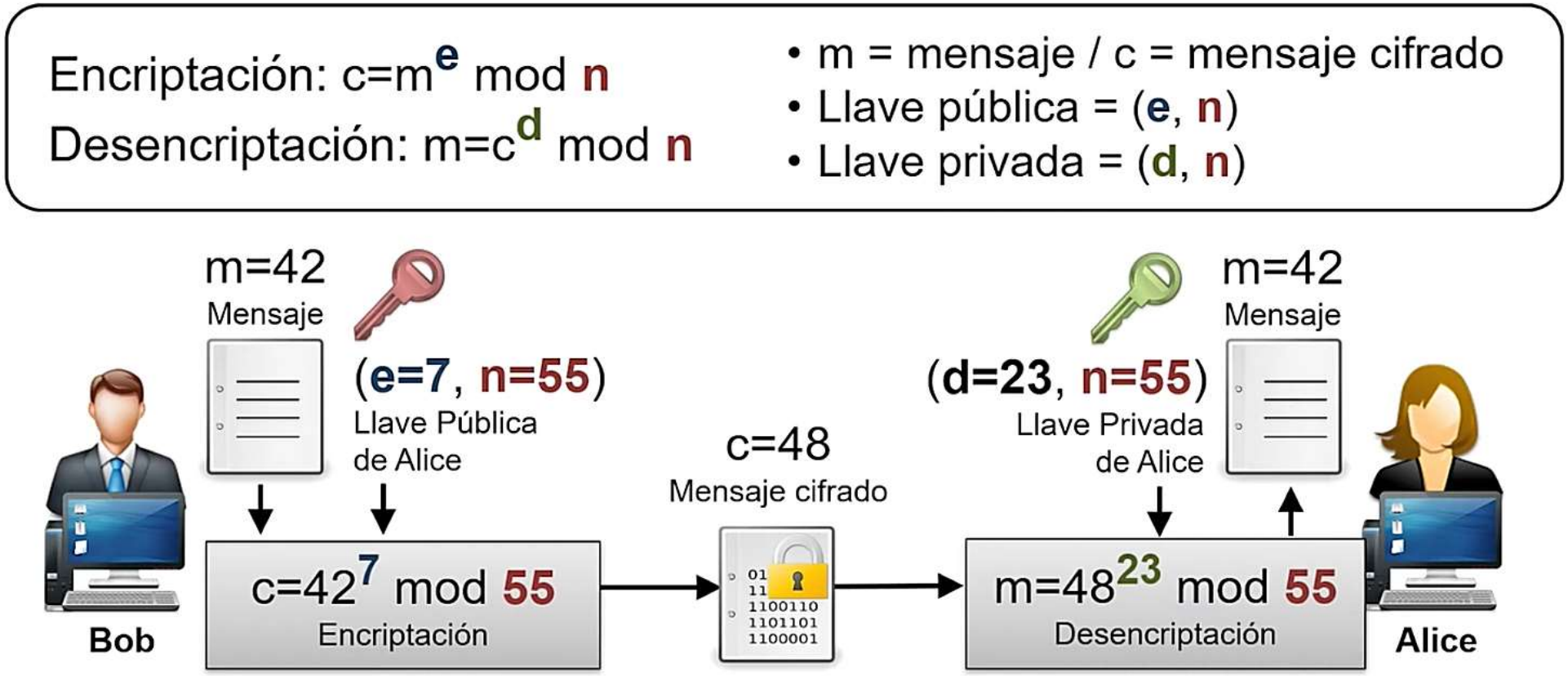
Encriptacion mensaje M

$C = M^e \bmod n$

Desencriptacion mensaje C

$M = C^d \bmod n$

EJEMPLO:


Encriptación: c=m^e mod n
Desencriptación: m=c^d mod n
• m = mensaje / c = mensaje cifrado
• Llave pública = (e, n)
• Llave privada = (d, n)
m=42
Mensaje
(e=7, n=55)
Llave Pública
de Alice
c=42^7 mod 55
Encriptación
c=48
Mensaje cifrado
01
11
1100110
1101101
1100001
(d=23, n=55)
Llave Privada
de Alice
m=48^23 mod 55
Desencriptación
m=42
Mensaje
Bob
Alice

En los siguientes artículos se habla sobre el algoritmo de cifrado RSA:

- RSA: ¿Cómo funciona este algoritmo de cifrado?
- ¿Qué es el cifrado RSA y cómo se compara con otros métodos de cifrado?
- ¿Qué es RSA en criptografía?
- ¿Cómo funcionan las claves RSA?
- ¿Qué es el cifrado RSA y cómo funciona?

En los siguientes vídeos se habla sobre el algoritmo de cifrado RSA:

- ¿Cómo funciona el algoritmo RSA?
- El sistema RSA
- RSA