



“Criptosistemas asimétricos”

Ejercicios propuestos

Ejercicio 1:

Dados los siguientes criptosistemas RSA, calcule lo que se le indique en cada apartado, teniendo en cuenta que los datos de la clave que se dan pertenecen al receptor.

- $p = 5$, $q = 7$, y $d = 11$. Cifre el mensaje $M = 2$ y descifre el resultado.
- $p = 3$, $q = 11$, y $e = 7$. Cifre el mensaje $M = 5$ y descifre el resultado.
- $n = 55$, y $e = 7$. Cifre el mensaje $M = 10$ y descifre el criptograma $C = 35$.
- $n = 91$, y $d = 11$. Cifre el mensaje $M = 3$ y descifrar el criptograma $C = 41$.

Solución:

a)

$$N = p \cdot q \Rightarrow N = 5 \cdot 7 = 35$$
$$\phi(35) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24$$
$$d \cdot e \pmod{\phi(35)} = 1 \Rightarrow 11 \cdot e \pmod{24} = 1 \Rightarrow e = 11$$
$$C = 2^{11} \pmod{35}; \mathbf{C = 18}$$
$$M = 18^{11} \pmod{35}; \mathbf{M = 2}$$

b)

$$N = p \cdot q \Rightarrow N = 3 \cdot 11 = 33$$
$$\phi(33) = \phi(3) \cdot \phi(11) = 2 \cdot 10 = 20$$
$$d \cdot e \pmod{\phi(33)} = 1 \Rightarrow 7 \cdot d \pmod{20} = 1 \Rightarrow \mathbf{d = 3}$$
$$C = 5^7 \pmod{33}; \mathbf{C = 14}$$
$$M = 14^3 \pmod{33}; \mathbf{M = 5}$$

c)

$$N = 55 \Rightarrow p = 5, q = 11$$
$$\phi(55) = \phi(5) \cdot \phi(11) = 4 \cdot 10 = 40$$
$$d \cdot e \pmod{\phi(55)} = 1 \Rightarrow 7 \cdot d \pmod{40} = 1 \Rightarrow \mathbf{d = -17 = 23}$$
$$C = 10^7 \pmod{55}; \mathbf{C = 10}$$
$$M = 35^{23} \pmod{55}; \mathbf{M = 30}$$

d)

$$N = 91 \Rightarrow p = 7, q = 13$$
$$\phi(91) = \phi(7) \cdot \phi(13) = 6 \cdot 12 = 72$$
$$d \cdot e \pmod{\phi(91)} = 1 \Rightarrow 11 \cdot e \pmod{72} = 1 \Rightarrow \mathbf{e = -13 = 59}$$
$$C = 3^{59} \pmod{91}; \mathbf{C = 61}$$
$$M = 41^{11} \pmod{91}; \mathbf{M = 20}$$

Ejercicio 2:

- a) ¿En qué consiste la fortaleza del criptosistema RSA? ¿Qué longitudes deben tener las claves utilizadas en RSA? ¿En qué consiste la “trampa” para generar las claves RSA?
- b) Martín quiere enviar un mensaje cifrado a Laura utilizando el criptosistema RSA con los valores pertenecientes a Laura $p=5$, $q=11$ y $d=7$. Si el mensaje en claro que quiere enviar Martín es $M=10$ ¿qué valor recibirá Laura? ¿Es buena la elección que han hecho de p , q y d ? ¿Por qué?

Solución:

- a.1) la fortaleza del criptosistema RSA consiste en la dificultad de factorizar números grandes.
- a.2) Las claves utilizadas deben tener una longitud de entre 1024 y 2048 bits.
- a.3) Los números primos p y q , secretos, constituyen la trampa del sistema. Conocidos p y q es fácil calcular d a partir de e , mientras que la complejidad de factorizar N es del orden de $e((\ln(N)\ln(N))^{1/2})$.
- b) Para cifrar se necesita la clave pública de Laura que es el exponente de cifrado e . Tenemos que $d = 7$ y sabemos que $e \cdot d = 1 \pmod{\Phi(N)}$. Como $\Phi(55) = \Phi(5) \cdot \Phi(11) = 4 \cdot 10 = 40$ tenemos que $7 \cdot e = 1 \pmod{40}$ como $\text{m.c.d}(7,40)=1$ podemos aplicar t^a de Euler o método de Euclides modificado.
- T^a de Euler: $a^{-1} = a^{\Phi(n)-1} \pmod{n} \Rightarrow \Phi(n) = \Phi(40) = \Phi(23) \cdot \Phi(5) = (23-22) \cdot 4 = 16$
- $e = d^{-1} = d^{\Phi(40)-1} = 7^{15} \pmod{40} = (7^2)^7 \cdot 7 \pmod{40} = 9^7 \cdot 7 = (9^2)^3 \cdot 9 \cdot 7 = 81^3 \cdot 63 \pmod{40} = 63 \pmod{40} = 23$ Así $e = 23$
- Cifrar $M=10$ $C = M^e \pmod{N} = 10^{23} \pmod{55}$
- Sabemos que $10^2 \pmod{55} = -10$ y $10^3 \pmod{55} = -10 \cdot 10 = -100 \pmod{55} = 10$
- Así $10^{23} = (10^3)^7 \cdot 10^2 \pmod{55} = 10^7 \cdot (10^2) = 10^9 \pmod{55} = (10^3)^3 \pmod{55} = 10$
- p , q y d deberían ser primos grandes y además se observa que el mensaje que ha mandado Martín es invariante después de cifrarlo ($M = C$) lo que indica que la elección de p , q y d no es buena.

Ejercicio 3:

Alicia y Benito están practicando un juego popular a través de correo electrónico. El juego requiere mantener en secreto los mensajes intercambiados simultáneamente por ambos jugadores en cada partida. Para ello cifran sus mensajes y los envían codificados con 27 elementos de forma que $A=0$, $B=1, \dots$, $Z=26$. Hacen uso del algoritmo RSA para cifrar sus comunicaciones. Alicia hace público su módulo $N_A=33$ y su exponente $e_A=7$. Por su parte, Benito también publica su módulo $N_B=39$ y su exponente $e_B=5$.

Alicia recibe el mensaje: 26, 2, 15, 16, 6, 0, 13 Benito recibe: 22, 8, 10, 9, 18, 0.

Calcule en claro los tres primeros valores enviados y los tres primeros recibidos por Alicia.

Solución:

Alicia hace uso de su clave privada para descifrar el mensaje recibido. Primero se calcula la privada de Alicia, como sigue:

$\Phi(N_A) = 2 \cdot 10 = 20$

$e_A \cdot d_A = 1 \pmod{\Phi(N_A)}$; $d_A \cdot 7 = 1 \pmod{20}$ _ $d_A = 3$

Alicia va descifrando letra a letra el mensaje recibido:

$$26^3 \pmod{33} = 20 \rightarrow T$$

$$2^3 \pmod{33} = 8 \rightarrow I$$

$$15^3 \pmod{33} = 9 \rightarrow J$$

Cálculo de la clave privada de Benito:

$$\Phi(N_B) = 2 \cdot 12 = 24$$

$$e_B \cdot d_B = 1 \pmod{\Phi(N_B)}; d_B \cdot 5 = 1 \pmod{24} \rightarrow d_B = 5$$

Por su parte Benito también descifra con su privada letra a letra el mensaje enviado por Alicia:

$$22^5 \pmod{39} = 16 \rightarrow P$$

$$8^5 \pmod{39} = 8 \rightarrow I$$

$$10^5 \pmod{39} = 4 \rightarrow E$$

Ejercicio 4:

Alicia y Benito hacen uso del algoritmo RSA para cifrar sus comunicaciones con las siguientes claves públicas:

$$(n_A; e_A) = (55; 9) \text{ y } (n_B; e_B) = (39; 5)$$

a) Determine el criptograma C_B que Benito debe enviar a Alicia si el mensaje en claro es

MANDA DINERO

y determine también el envío que corresponde a la respuesta de Alicia

NO TENGO.

Las letras A – Z del alfabeto internacional (sin la Ñ) se codifican de 0 – 25, el punto es el 26 y el espacio en blanco es el 27.

b) Descifre el criptograma que recibe Benito, C_A

Solución:

a)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Benito debe enviar a Alicia el mensaje MANDA DINERO codificado de forma siguiente:

M -> 12 A -> 0 N -> 13 D -> 3 ' ' -> 27 I -> 8 E -> 4 R -> 17 O -> 14

Benito deberá usar la clave pública de Alicia, $(n_A; e_A) = (55; 9)$, para que sólo ella pueda abrir el criptograma C_B .

Utilizará $C_B = M^{e_A} \pmod{n_A}$.

$$C_B \rightarrow C\{M\} = 12^9 \pmod{55} = 12$$

$$C\{A\} = 0^9 \pmod{55} = 0$$

$$C\{N\} = 13^9 \pmod{55} = 28$$

$$C\{D\} = 3^9 \pmod{55} = 48$$

$C\{ } = 27^9 \text{ mód } 55 = 42$
 $C\{l\} = 8^9 \text{ mód } 55 = 18$
 $C\{E\} = 4^9 \text{ mód } 55 = 14$
 $C\{R\} = 17^9 \text{ mód } 55 = 2$
 $C\{O\} = 14^9 \text{ mód } 55 = 4$
Entonces $C_B = [12,0,28,48,0,42,48,18,28,14,2,4]$ (mód 55)

La respuesta de Alicia, NO TENGO., va cifrada. El mensaje codificado toma los valores: N->13 O->14 ‘
’->27 T->19 E->4 G->6 .->26

Alicia deberá usar la clave pública de Benito, $(n_B; e_B) = (39; 5)$, para cifrar.

Utilizará $C_A = M^{e_B} \text{ mód } n_B$.

$C_A \rightarrow C\{N\} = 13^5 \text{ mód } 39 = 13$
 $C\{O\} = 14^5 \text{ mód } 39 = 14$
 $C\{ } = 27^5 \text{ mód } 39 = 27$
 $C\{T\} = 19^5 \text{ mód } 39 = 28$
 $C\{E\} = 4^5 \text{ mód } 39 = 10$
 $C\{G\} = 6^5 \text{ mód } 39 = 15$
 $C\{.\} = 26^5 \text{ mód } 39 = 26$
Entonces, $C_A = [13,14,27,28,10,13,15,14,26]$ (mód 39)

b) Benito, en recepción, usará su privada para descifrar $C_A = [13,14,27,28,10,13,15,14,26]$ (mód 39).

Usará $M_A = C_A^{d_B} \text{ (mód } N_B)$

Calculo de d_B :

$$n_B = 3 \cdot 13 = 39$$

$$\Phi(n_B) = 2 \cdot 12 = 24$$

$$e_B \cdot d_B = 1 \text{ (mód } \Phi(n_B)) =; d_B \cdot 5 = 1 \text{ (mód } 24) \quad d_B = 5$$

$M_A \rightarrow M\{13\} = 13^5 \text{ mód } 39 = 13 \rightarrow N$
 $M\{14\} = 14^5 \text{ mód } 39 = 14 \rightarrow O$
 $M\{27\} = 27^5 \text{ mód } 39 = 27 \rightarrow ‘ ‘$
 $M\{28\} = 28^5 \text{ mód } 39 = 19 \rightarrow T$
 $M\{10\} = 10^5 \text{ mód } 39 = 4 \rightarrow E$
 $M\{13\} = 13^5 \text{ mód } 39 = 13 \rightarrow N$
 $M\{15\} = 15^5 \text{ mód } 39 = 6 \rightarrow G$
 $M\{14\} = 14^5 \text{ mód } 39 = 6 \rightarrow O$
 $M\{26\} = 26^5 \text{ mód } 39 = 26 \rightarrow .$
 $M_A = \text{NO TENGO.}$