Universidad
Carlos III de Madrid

Grupo COSEC · *Dpto. Informática*

Universidad Carlos III de Madrid

Cifrado asimétrico

Criptografía y Seguridad Informática
Seguridad en las Tecnologías de la Información
Curso 2016/2017

Pablo Martín

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.

a) p = 5, q = 7, y d = 11. Cifre el mensaje M = 2 y descifre el resultado.

b) p = 3, q = 11, y e = 7. Cifre el mensaje M = 5 y descifre el resultado.

c) n = 55, y e = 7. Cifre el mensaje M = 10 y descifre el criptograma C = 35.

d) n = 91, y d = 11. Cifre el mensaje M = 3 y descifrar el criptograma C = 41.

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?

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,..., Z=26. Hacen uso del algoritmo RSA para cifrar sus comunicaciones. Alicia hace público su módulo NA= 33 y su exponente eA=7. Por su parte, Benito también publica su módulo NB= 39 y su exponente eB=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.

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

5. Dos amigos comienzan a utilizar un conocido criptosistema basado en la complejidad del cálculo del logaritmo discreto con el fin de proteger sus comunicaciones.

Alicia ha decidido enviar todos sus mensajes cifrados a Benito siguiendo el algoritmo siguiente:

1. **Benito elige un primo grande ρ con valor ρ=11 y un generador θ del grupo multiplicativo de Z_ρ, con valor θ=2. Benito publica ambos.**

2. **Benito toma un entero α que cumpla que $0 < \alpha < \rho-1$. Benito elige $\alpha=8$ que le sirve para calcular el siguiente valor $\beta = \theta^{\alpha}$ mód. ρ.**
3. **Alicia, para enviar a Benito el cifrado de un mensaje M, primero representa dicho mensaje como un entero en el intervalo $[0, \rho - 1]$. A continuación, toma un entero ω aleatorio (primo relativo con $\rho-1$), por ejemplo $\omega=9$, con el que calcula, por un lado $\gamma = \theta^{\omega}$ mód. ρ, y por otro lado $\delta = M \bullet \beta^{\omega}$ mód. ρ.**
4. **Alicia enviará a Benito el criptograma C compuesto por (γ , δ).**
5. **En recepción, Benito descifra C mediante el cálculo siguiente:**

$$M = \gamma^{\rho-1-\alpha} \cdot \delta \text{ mód. } \rho$$

a) **Identifique y razone el esquema de cifrado elegido por los dos amigos.**

b) **Calcule el criptograma que Alicia envía a Benito sobre el mensaje M=5 mediante el criptosistema definido en el enunciado, y describa la operación de descifrado realizada**

RSA

p, q primos $n = p \cdot q$ $\phi(n) = \phi(p) \cdot \phi(q)$

$e \;//\; e \cdot d = 1 \bmod \phi(n)$ $\{\gcd(e, \phi(n)) = 1\}$

$C = M^e \bmod n$

$M = C^d \bmod n$

1.)

a) $p = 5$ $q = 7$ $d = 11$ Cifrar $M = 2$ y descifrar

$n = 5 \cdot 7 = 35$ $\phi(n) = 24$

$e \cdot d = 1 \bmod 24$; $e = d^{-1} \bmod 24 = 11^{-1} \bmod 24 = 11 \bmod 24$

$24 = 11 \cdot 2 + 2$ $1 = 11 - 5(24 - 11 \cdot 2) = \underset{\sim}{11} \cdot 11 - 5 \cdot 24$
$11 = 2 \cdot 5 + 1$ $1 = 11 - 5 \cdot 2$

$C = M^e \bmod n = 2^{11} \bmod 35 = 18$

$M = C^d \bmod n = 18^{11} \bmod 35 = 2$

b) $p = 3$ $q = 11$ $e = 7$ Cifrar $M = 5$

$n = 33$ $\phi(n) = 20$

$e \cdot d = 1 \bmod \phi(n)$; $d = e^{-1} \bmod \phi(n) = 7^{-1} \bmod 20 = 3 \bmod 20$

$20 = 7 \cdot 2 + 6$ $1 = 7 - 20 + 2 \cdot 7 = -20 + \underset{\sim}{3} \cdot 7$
$7 = 6 \cdot 1 + 1$ $1 = 7 - 6$
$6 = 1 \cdot 6$

$C = M^e \bmod n = 5^7 \bmod 33 = 14$

$M = C^d \bmod n = 14^3 \bmod 33 = 5$

c) $n=55$ $e=7$ Cifrar $M=10$ y Descifrar $C=35$

$n=55=p\cdot q=11\cdot 5$ $\phi(n)=10\cdot 4=40$

Cifrar 10 $\Rightarrow$ $C=M^e \bmod n=10^7 \bmod 55=10$

$d=e^{-1} \bmod \phi(n)=7^{-1} \bmod 40=-17 \bmod 40=23$

$40=7\cdot 5+5$ $\quad 1=-2\cdot 7+3\cdot(40-7\cdot 5)=3\cdot 40-17\cdot 7$
$7=5\cdot 1+2$ $\quad 1=5-2(7-5)=-2\cdot 7+3\cdot 5$ $\sim$
$5=2\cdot 2+1$ $\quad 1=5-2\cdot 2$

Descifrar 35 $\Rightarrow$ $M=C^d \bmod n=35^{23} \bmod 55=30$
$(35^5)^4\cdot 35^3=10^4\cdot 30$

d) $n=91$ $d=11$ Cifrar $M=3$ y Descifrar $C=41$

$n=p\cdot q=91=7\cdot 13$ $\phi(n)=6\cdot 12=72$

Descifrar 41 $\Rightarrow$ $M=C^d \bmod n=41^{11} \bmod 91=20$
$(41^5)^2\cdot 41=6^2\cdot 41$

$e=d^{-1} \bmod \phi(n)=11^{-1} \bmod 72=-13 \bmod 72=59$

$72=11\cdot 6+6$ $\quad 1=-11+2\cdot(72-11\cdot 6)=2\cdot 72-13\cdot 11$
$11=6\cdot 1+5$ $\quad 1=6-(11-6)=2\cdot 6-11$ $\sim$
$6=5\cdot 1+1$ $\quad 1=6-5$

Cifrar 3 $\Rightarrow$ $C=M^d \bmod n=3^{59} \bmod 91=9\cdot 27 \bmod 91=61$
$(3^{10})^5\cdot 3^9$
$81^5\cdot 3^9=9\cdot 27$

2.)

a) La dificultad de factorizar un n^2 grande.

Entre 1024 y 2048.

En el tamaño de los digitos que elegimos de p y q.

b.) $p=5 \quad q=11 \quad d=7$

$n=55 \quad \phi(n)=40$

$e \cdot d = 1 \bmod \phi(n)$; $e = 7^{-1} \bmod 40 = -17 \bmod 40 = 23$

$40 = 7 \cdot 5 + 5 \quad 1 = -2 \cdot 7 + 3 \cdot (40 - 7 \cdot 5) = 3 \cdot 40 - 7 \cdot 15 - 2 \cdot 7 = 3 \cdot 40 - 17 \cdot 7$

$7 = 5 \cdot 1 + 2 \quad 1 = 5 - 2(7-5) = -2 \cdot 7 + 3 \cdot 5$

$5 = 2 \cdot 2 + 1 \quad 1 = 5 - 2 \cdot 2$

$2 = 1 \cdot 2$

$C = 10^{23} \bmod 55 = 10$ $\quad M = 10$ No cifra, sale lo mismo.

3.) $n_A = 33 \quad e_A = 7 \qquad n_B = 39 \quad e_B = 5$

a) 26, 2, 15, 16 Alicia recibe

$p = 11$, $q = 3$ $\Rightarrow n_A = 33 \quad \phi(n) = 20$

$e_A = 7$

$d_A = 7^{-1} \bmod 20 = 3$

$20 = 2 \cdot 7 + 6 \quad 1 = 7 - 20 + 2 \cdot 7 = -20 + 3 \cdot 7$

$7 = 6 \cdot 1 + 1 \quad 1 = 7 - 6$

$6 = 1 \cdot 6$

$M = 26^3 \bmod 33 = 20 \rightarrow T$

$M = 2^3 \bmod 33 = 8 \rightarrow I$

$M = 15^3 \bmod 33 = 9 \rightarrow J$

Alicia cifra con la publica de Benito, y Benito lo descifra con su privada

b) 22, 8, 10 Benito recibe

$n_B = 39 \begin{cases} p = 13 \\ q = 3 \end{cases}$ $\quad \phi(n) = 24$ $\quad e_B = 5$ $\quad d = 5^{-1} \bmod 24 = 5$

$24 = 5 \cdot 4 + 4 \quad 1 = 5 - 24 - 4 \cdot 5 = -24 - 3 \cdot 5$

$5 = 4 \cdot 1 + 1 \quad 1 = 5 - 4$

$1 = 1$

$M = 22^5 \bmod 39 = 16 \rightarrow P$

$M = 8^5 \bmod 39 = 8 \rightarrow I$

$M = 10^5 \bmod 39 = 4 \rightarrow E$

4.) $n_A = 55$ $\quad n_B = 39$

$e_A = 9$ $\quad e_B = 5$

a) Benito envia a Alicia.

Benito cifra con la de Alicia

$n_A = 55 \quad e_A = 9$

$C = M^e \bmod n = 12^9 \bmod 55 = 12 \rightarrow M$

$C = 0^9 \bmod 55 = 0 \rightarrow A$

$C = 13^9 \bmod 55 = 28 \rightarrow C$

b.)

EG

p: primo g: generador

x_B: C. privada B

y_B: C. pública B $y_B = g^{x_B} \bmod p$

Cifrar:

Adige k / $1 \le k \le p$

$k = y_B^k \bmod p$

$C_1 = g^k \bmod p$

$C_2 = k \cdot M \bmod p$ $\Big\}$ $C_1, C_2 \rightarrow B$

Descifrar:

$k = C_1^{x_B} \bmod p$

$M = C_2 \cdot k \bmod p$

5.) B ⇒ Cifrado $\begin{cases} p = 11 \\ \theta = 2 \\ \alpha = 8 \end{cases}$ $\beta = \theta^\alpha \bmod p = 2^8 \bmod 11 = \underline{3 = \beta}$

A ⇒ Cifrado $w = 9$ $\begin{cases} \gamma = \theta^w \bmod p = 2^9 \bmod 11 = \underline{6 = \gamma} \\ \delta = M \beta^w \bmod p = 5 \cdot 3^9 \bmod 11 = 9 \end{cases}$

$A \xrightarrow[(6,9)]{\gamma, \delta} B$

ENB $M = \gamma^{p-1-\alpha} \bmod p$

$M = 6^{11-1-8} \cdot 9 \bmod 11 = 6^2 \cdot 9 \bmod 11 = 5$