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.

Solución:

a)

N = p • q => N = 5 • 7 = 35
ϕ (35) = ϕ (5) • ϕ (7) = 4 x 6 = 24
d • e mód ϕ (35) = 1 => 11 • e mód 24 =1 => e = 11
C = 2^{11} mód 35; **C = 18**
M = 18^{11} mód 35; **M = 2**

b)

N = p • q =>N=3 • 11=33
ϕ (33) = ϕ (3) • ϕ (11) = 2 • 10= 20
d • e mód ϕ (33) = 1 => 7 • d mód 20 = 1 => **d = 3**
C = 5^{7} mód 33; **C = 14**
M = 14^{3} mód 33; **M = 5**

c)

N = 55 => p = 5, q = 11
ϕ (55) = ϕ (5) • ϕ (11) = 4 • 10 = 40
d • e mód ϕ (55) = 1 => 7, d mód 40 = 1 => **d = -17 = 23**
C = 10^{7} mód 55; **C = 10**
M = 35^{23} mód 55; **M = 30**

d)

N = 91 => p = 7, q = 13
ϕ (91) = ϕ (7) • ϕ (13) = 6 • 12 = 72
d • e mód ϕ (91) = 1 => 11 • e mód 72 = 1 => **e = -13 = 59**
C = 3^{59} mód 91; **C = 61**
M = 41^{11} mód 91; **M = 20**

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)lnln(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 $e \cdot d = 1$ mód $\Phi(N)$.
Como Φ (55) = Φ (5) · Φ (11) =4 · 10 =40 tenemos que 7·e = 1 mód 40 como m.c.d(7,40)=1 podemos aplicar tª de Euler o método de Euclides modificado.
Tª de Euler: $a^{-1} = a^{\Phi(n)-1}$ mód. n => Φ (n) = Φ (40)= Φ (23) · Φ (5) = (23 – 22)·4 = 16
$e = d^{-1} = d^{\Phi(40)-1} = 7^{15}$ (mód 40) = $(7^2)^7 \cdot 7$ (mód 40) = $9^7 \cdot 7 = (9^2)^3 \cdot 9 \cdot 7 = 81^3 \cdot 63$ (mód 40) = 63 (mód 40) = 23 Así e = 23
Cifrar M=10 C = M^e (mód N) = 10^{23} mód 55
Sabemos que 10^2 (mód 55) = -10 y 10^3 (mód 55) = -10 · 10 = -100 (mód 55)= 10
Así $10^{23} = (10^3)^7 \cdot 10^2$ (mód 55) = $10^7 \cdot (10^2) = 10^9$ mód 55 = $(10^3)^3$ mód 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.

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 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:
$\Phi(N_A) = 2\cdot 10 = 20$
$e_A \cdot d_A = 1(\text{mód. } \Phi(N_A))$; $d_A \cdot 7 = 1(\text{mód. } 20)$ _ $d_A = 3$

Alicia va descifrando letra a letra el mensaje recibido:
26^3 (mód. 33) = 20 - > T
2^3 (mód. 33) = 8 - > I
15^3 (mód. 33) = 9 - > J

Cálculo de la clave privada de Benito:
$\Phi(N_B) = 2\cdot 12 = 24$
$e_B \cdot d_B = 1(\text{mód. } \Phi(N_B))$; $d_B \cdot 5 = 1(\text{mód. } 24)$ _ $d_B = 5$

Por su parte Benito también descifra con su privada letra a letra el mensaje enviado por Alicia:
22^5 (mód. 39) = 16 - > P
8^5 (mód. 39) = 8 - > I
10^5 (mód. 39) = 4 - > E

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

$(n_A; e_A) = (55; 9)$ 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 CB.

Utilizará CB = M^{eA} mód n_A.

CB -> C{M}= 129 mód 55 =12
C{A}= 0^9 mód 55 = 0
C{N}= 13^9 mód 55 = 28
C{D}= 3^9 mód 55 = 48
C{ }= 27^9 mód 55 = 42
C{I}= 8^9 mód 55 = 18
C{E}= 4^9 mód 55 = 14
C{R}= 17^9 mód 55 = 2
C{O}= 14^9 mód 55 = 4
Entonces CB = [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 CA = M^{eB} mód n_B.

CA -> C{N}= 13^5 mód 39 = 13
C{O}= 14^5 mód 39 = 14
C{ }= 27^5 mód 39 = 27

C{T}= 19^5 mód 39 = 28
C{E}= 4^5 mód 39 = 10
C{G}= 6^5 mód 39 = 15
C{.}= 26^5 mód 39 = 26
Entonces, CA = [13,14,27,28,10,13,15,14,26] (mód 39)

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

Usará $M_A=C_A^{dB}$(mód N_B)

Calculo de d_B :
n_B= 3 ·13 =39
$\Phi(n_B)$=2·12=24
$e_B \cdot d_B$=1(mód $\Phi(n_B)$)=; $d_B \cdot 5$=1(mód 24) d_B=5

MA -> M{13}= 13^5 mód 39= 13 -> N
M{14}= 14^5 mód 39= 14 -> O
M{27}= 27^5 mód 39= 27 -> ‘ ‘
M{28}= 28^5 mód 39= 19 -> T
M{10}= 10^5 mód 39= 4 -> E
M{13}= 13^5 mód 39= 13 -> N
M{15}= 15^5 mód 39= 6 -> G
M{14}= 14^5 mód 39= 6 -> O
M{26}= 265 mód 39= 26 -> .
MA = NO TENGO.

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 α=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 ρ-1), por ejemplo ω=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 por Benito.**

SOLUCIÓN:

a)El esquema detallado en el enunciado corresponde al algoritmo de cifrado de ElGamal.

b) Siguiendo el método de cifrado y los parámetros descritos en el enunciado:
ρ=11, θ=2, α=8, ω=9

La clave pública de Benito es $\beta = \theta^\alpha$ mód. $\rho = 2^8$ mód. $11 = 3$

Alicia calcula:
$\gamma = \theta^\omega$ mód. $\rho = 2^9$ mód. $11 = 6$
$\delta = M \bullet \beta^\omega$ mód. $\rho = 5 \cdot 3^9$ mód. $11= 9$

Benito recibe el criptograma (6,9). Su descifrado consiste en aplicar:
$M = \gamma^{\rho-1-\alpha} \cdot \delta$ mód. $\rho = 6^{11-1-8} \cdot 9$ mód. $11= 6^2 \cdot 9$ mód. $11= 5$