Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"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.

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.

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?

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,..., 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.

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