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

"Asymmetric encryption"

Proposed exercises

Exercise 1:

Given the following RSA ciphers, perform the corresponding computation considering that the parameters provided correspond to the receiver:

a) p = 5, q = 7, and d = 11. Encrypt the message M = 2 and decrypt the result
b) p = 3, q = 11, and e = 7. Encrypt the message M = 5 and decrypt the result
c) n = 55, and e = 7. Encrypt the message M = 10 and decrypt the ciphertext C= 35
d) n = 91, and d=11. Encrypt the message M = 3 and decrypt the ciphertext C=41

Exercise 2:

a) What is the strength of RSA? What length must the keys in RSA have? What is the "trap-door" to generate the keys in RSA?
b) Martin wants to send an encrypted message to Laura using RSA, with p=5, q=11 and d=7. If the message is M=10. What does Laura receive? Is it a good election p, q and d? Why?

Exercise 3:

Alice and Bob are playing a popular game by e-mail. The game keeps in secret the messages exchanged by both players in each game. The messages are encrypted and sent with 27 elements where A=0 ,… …, Z=26. They use RSA algorithm to encrypt their communications. Alice's public key is $(e_A, N_A) = (7, 33)$. Bob's public key is $(e_B, N_B) = (5, 39)$.

Alice receives the ciphertext: 26 , 2 , 15 , 16 , 6 , 0 , 13 and Bob receives: 22 , 8 , 10 , 9 , 18 , 0.

Calculate the first three values sent and the first three values received by Alice.

Exercise 4:

Alice and Bob use RSA algorithm to encrypt their communications with the following public keys:

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

a) Calculate the ciphertext C_B that Bob must send to Alice if the message is:

MANDA DINERO

and calculate too the message corresponding to the answer of Alice

NO TENGO.

b) Decrypt the ciphertext C_A received by Bob

Note: Letters A-Z (without Ñ) are coded as 0-25, the dot as 26, and the blank as 27