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)

"Digital signature schemes"

Proposed exercises

Exercise 1:
Consider an RSA system with p=13 and q=19. We want to sign the message M=10. If the exponent of our public key is e=11, compute the digital signature of M and verify it.

Exercise 2:
Two spies A and B exchange messages by email. They want to keep in secret these messages and also authenticate the origin, because A suspects that C wants to impersonate B. Accordingly, A and B digitally sign and encrypt their emails coded with 27 elements (A=00, B=01 ,…, Ñ=14 ,..., Z=26). They use RSA both to sign and encrypt with the following parameters.

A: N_A= 3 ·13 =39 e_A=5
B: N_B=5 ·11 = 55 e_B=9
A B C D E F G H I J K L M N Ñ 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 26

A and B has a plan and they only need to know if the city where they want to meet is PARIS (P) or LISBOA (L). They encrypt the first and the second letter of the city and only sign the first. Consider the city for A is Paris and for B is Lisboa.

a) Calculate the two messages encrypted: C_A y C_B.

b) To sign the messages. $F_A(M_A)$ y $F_B(M_B)$.

c) Decrypt the ciphertexts and verify the signatures

d) A and B do not agree in the city. Indicate a secure protocol where they only exchange the message PARIS

Exercise 3:
Calculate and verify the El Gamal signature of a message M=5, g=2, p=11, X_A=8 (signer's private key), and the random number k=9.

Exercise 4:
Alice wants to send to Bob a message M composed of hexadecimal digits, using a signature with appendix. She uses El Gamal with the hash function o-exclusive ($\oplus$), x $\oplus$ y = (x+y) mod 16, where x and y are hexadecimal digits. If M is

0 1 2 3 4 5 6 7 8 9 A B C D E F

a) Apply the hash function to get the message-digest R that is a hexadecimal digit long

b) If A chooses, p=17, g=7, X_A=5, Y_A=11, k=9 Does these parameters satisfy the conditions to be used in El Gamal signature algorithm?

c) Get the signature on message M.

d) Make the calculations that B does in order to verify the integrity of the message received. Is the signature valid?