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)

"Key distribution and management"

Proposed exercises

Exercise 1:
Get the secret key that Alice and Bob negotiate using Diffie-Hellman algorithm. Suppose the following parameters: generator g=2, p=17, the secret random value chosen by Alice is x=2, and the secret random value chosen by Bob is y= 5.

Exercise 2:
Alice (A) and Bob(B) wish to exchange a key K using Diffie-Hellman algorithm. They choose the prime p=13 and the generator g=7 in Z_{13}.

a) If Alice chooses x=7 and Bob chooses y=8, calculate the key exchanged.
b) Charlie knows g and p and intercepts the communication. If he chooses c=10. What are the tasks he has to fulfill to deceive Alice and Bob and to carry out a man in the middle attack? Indicate the messages sent by Charles.
c) What can Alice and Bob do to avoid this active attack?

Exercise 3:
A and B agree on exchanging encrypted messages using a secret key. They will first exchange the secret key using the Diffie-Hellman algorithm. They agree to work mod p, with p=47, and the generator g=23.

a) Suppose that A and B randomly choose x=12 and y=33. Calculate the values they exchange through the communication channel and the shared secret key K they compute.
b) To encrypted a message M using the secret key K computed in the previous question, they use the algorithm $C = M^K \bmod n$, where the decryption algorithm computes $M = C^J \bmod n$ to retrieve the cleartext message. Calculate the value of J theoretically.
c) Using the previous encryption algorithm, calculate the ciphertext for M=16 with K=25 and p=47. Next, get the decryption key J and check that M is obtained from C when used in the decryption algorithm.

Exercise 4:
Anne (A) and Bob (B) want to exchange a secret key with Diffie-Hellman algorithm. They choose p=31.

a) Find the smallest g of Zp that they can use.
b) Ignore the previous result and consider that they choose g=11. A chooses the value $X_a = 5$ and B $X_b = 10$. Calculate the key K exchanged.

c) What would it happen if A and B choose a number g that is not a generator of Zp?
d) If they choose Z_{81} instead of Z_{31}, Would it be more secure? Why?