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.

Solution:

A calculates:		B calculates:
$X = g^x \bmod p = 2^2 \bmod 17 = 4$	→	$X = 4$
$Y = 15$	←	$Y = g^y \bmod p = 2^5 \bmod 17 = 15$
$Y^x \bmod p = 15^2 \bmod 17 = 4$		$X^y \bmod p = 4^5 \bmod 17 = 4$
K = 4		**K = 4**

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?

Solution:

a)

A calculates:		B calculates:
$X = g^x \bmod p = 7^7 \bmod 13 = 6$	→	$X = 6$
$Y = 3$	←	$Y = g^y \bmod p = 7^8 \bmod 13 = 3$
$Y^x \bmod p = 3^7 \bmod 13 = 3$		$X^y \bmod p = 6^8 \bmod 13 = 3$
K = 3		**K = 3**

b)

A calculates:		C calculates:		B calculates:
$X = g^x \bmod p = 7^7 \bmod 13 = 6$	→	$X = 6$		
$Z = 4$		$Z = g^z \bmod p = 7^{10} \bmod 13 = 4$	←	$Z = 4$
		$Y = 3$	←	$Y = g^y \bmod p = 7^8 \bmod 13 = 3$
$Z^x \bmod p = 4^7 \bmod 13 = 4$		$X^z \bmod p = 6^{10} \bmod 13 = 4$		$Z^y \bmod p = 4^8 \bmod 13 = 3$
		Clave secreta: $\mathbf{K_{Alicia} = 4}$		
K = 4		$Y^z \bmod p = 3^{10} \bmod 13 = 3$		**K = 3**
		$\mathbf{K_{Berta} = 3}$		

c) The problem is that X and Y are not authenticated in the Diffie-Hellman algorithm. A countermeasure is to include some key authentication mechanism (for X and Y and other public key parameters). Possible approaches based on symmetric cryptography would be: compute the hash of these values and check them through a secure channel (phone conversation or other possibilities), attach a MAC tag (assuming that both parties share another secret key) or hash functions combined with symmetric encryption (also assuming another shared secret key). If public cryptography can be used, each party would have a pair of public/private keys, and their public keys would be linked to certain identity through a public key certificate; then, they can use these keys to sign the messages exchanged between them (or at least the values X and Y and associated parameters).

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.

Solution:

a)

A calculates:		B calculates:
$X = g^x \bmod p = 23^{12} \bmod 47 = 27$	→	$X = 27$
$Y = 33$	←	$Y = g^y \bmod p = 23^{33} \bmod 47 = 33$
$Y^x \bmod p = 33^{12} \bmod 47 = 25$		$X^y \bmod p = 27^{33} \bmod 47 = 25$
K = 25		**K = 25**

b)

$C = M^K \bmod n$ y $M = C^J \bmod n$, then

$$M = (M^K)^J \bmod n = M^{K \bullet J} \bmod n \qquad (1)$$

By Euler theorem, $M^{\phi(n)} \bmod n = 1$, therefore, multiplying both sides by M we get $M \times M^{\phi(n)} \bmod n = 1 \times M$, that is,

$$M^{\phi(n)+1} \bmod n = M \times 1 \qquad (2)$$

From (1) y (2) it can be derived that $M^{K \bullet J} \bmod n = M^{\phi(n)+1} \bmod n$, then $K \bullet J = \phi(n) + 1$. If we apply modulo $\phi(n)$, we get $K \bullet J \bmod \phi(n) = 1 \bmod \phi(n)$, that is, **$K \bullet J \bmod \phi(n) = 1$**, so K and J are multiplicative inverses modulo $\phi(n)$.

c)

M= 16, K=25, n=47
$C = M^K \bmod n$; $C = 16^{25} \bmod 47 = 21$; **C = 21**
$\phi(47) = 46$.
$25 \bullet J \bmod \phi(47) = 1$; $25 \bullet J \bmod 46 = 1 \Rightarrow J = -11 \bmod 46 = 35 \bmod 46$; **J= 35**
$M = C^J \bmod n$; $M = 21^{35} \bmod 47 \Rightarrow$ **M = 16**.

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?

Solution:

a)

A generator g of Z_{31} is a number $1<g<31$ y $g^a \bmod p \neq 1 \ \forall a \mid 0<a<30$.
Si p is prime, $x \in Z_p$ and $x^a \bmod p = 1$ to some $a<p$ then a is divisor of p-1.
p = 31; p-1 = 30 = 2x3x5; the divisor of 30 are 2,3,5,6,10,15:
$2^2 \bmod 31 = 4$; $2^3 \bmod 31 = 8$; $2^5 \bmod 31 = 1$; 2 no
$3^2 \bmod 31 = 9$; $3^3 \bmod 31 = 27$; $3^5 \bmod 31 = 3^3\ 3^2 \bmod 31 = (-4)\ 9 \bmod 31 = -5 \bmod 31 = 26$;
$3^6 \bmod 31 = 3\ (-5) \bmod 31 = 16$; $3^{10} \bmod 31 = (-5)\ (-5) \bmod 31 = 25$;
$3^{15} \bmod 31 = (-25)\ 5 \bmod 31 = 6\ 5 \bmod 31 = 30$;
Therefore 3 is the smallest generator in Z_{31}

b)

A sends to B: $g^{Xa} \bmod p = 11^5 \bmod 31 = 11^2\ 11^2\ 11 \bmod 31 = (-3)^2\ 11 \bmod 11 = 6$
B sends to A: $g^{Xb} \bmod p = 11^{10} \bmod 31 = 6*6 \bmod 31 = 5$
B calculates: $6^{Xb} \bmod p = 6^{10} \bmod 31 = 5^5 \bmod 31 = (-6)^2\ 5 \bmod 31 = 25$

A calculates: 5^{Xa} mod. p = 5^5 mod. 31 = $(-6)^2$ 5 mod. 31 = 25
K= 25 is the exchanged key between A and B.

c)

If A and B do not choose a generator in Zp, they can use the protocol, but in such a case it is easier to perform a brute force attack (not all remainders of Zp are generated).

d)

81 is not prime. Also, it is a small value: launching a brute force attack is still quite easy.