Ejercicios:
Infraestructura de clave pública

6.1) Una autoridad certificadora (AC) tiene clave pública RSA e_{AC}= 19, siendo n_{AC}= 23·31 = 713. Un usuario, A, tiene clave pública RSA e_A= 3, siendo n_A= 11·23 = 253.
¿Qué protocolo aplica AC para certificar la clave pública del usuario A? Efectúa los cálculos pertinentes para obtener el certificado de A, c_A.

6.2) Consideremos la autoridad certificadora, AC, del ejercicio anterior (RSA, e_{AC}= 19, n_{AC}=23·31=713), el usuario A (RSA, e_A=3, n_A=11·23=253) de ese ejercicio y un usuario B con clave pública RSA, e_B= 5, n_B= 13·19 = 247 y un certificado expedido por AC, c_B=408.

a) El usuario A envía a B su clave pública e_A, n_A y su certificado c_A. ¿Qué protocolo aplica B para comprobar que la clave es auténtica? Realiza los cálculos.
b) El usuario B cifra el mensaje m=12 para A y le envía el criptograma c obtenido y A lo descifra para obtener m. Calcula c y realiza el descifrado que hace A de c para obtener m.
c) El usuario B firma digitalmente el mensaje m y le envía la firma digital, s, al usuario A. Calcula s.
d) El usuario A verifica que la clave pública de B es de ese usuario y aplica el protocolo de firma digital para comprobar que el mensaje recibido del usuario B es auténtico. Haz los cálculos para ambas verificaciones.

6.3) Explica, brevemente, qué es un certificado digital.