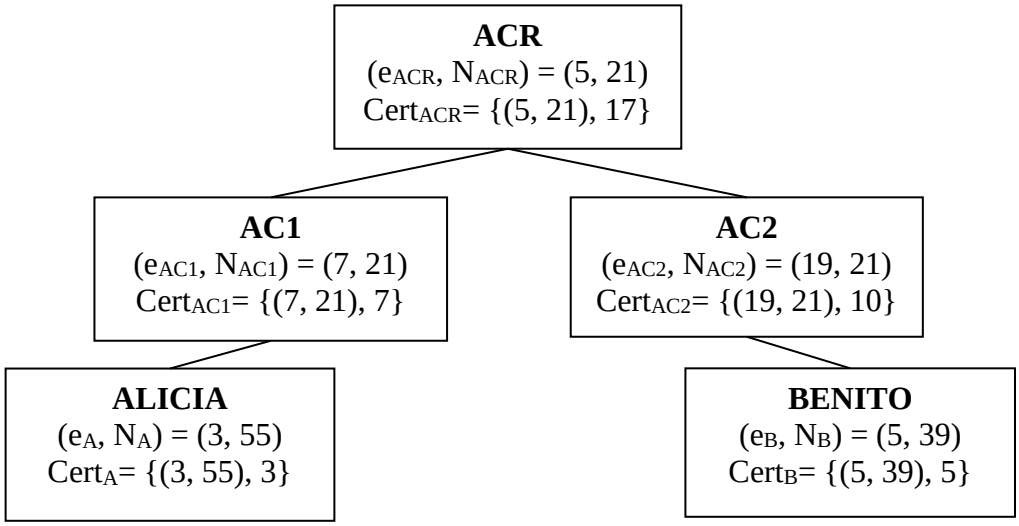
Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Infraestructuras de clave pública"

Ejercicios propuestos

Ejercicio 1:

Alicia quiere mandar un mensaje firmado a Benito. La jerarquía de autoridades de certificación y las claves públicas y certificados en cuestión son los que se muestran en la figura a continuación.



Teniendo en cuenta las siguientes consideraciones:

El certificado de cada entidad *i* está compuesto por su clave pública y la firma del exponente de esa clave pública por parte de la entidad emisora del certificado, es decir, $Cert_i = \{(e_i, N), F_{emisor}(e_i)\}$, siendo $F_{emisor}(e_i)$ la firma RSA realizada por la entidad emisora del certificado (entidad inmediatamente superior).

La autoridad raíz firma su propio certificado.

No se usan funciones resumen.

Cada entidad posee y confía en los certificados de toda su cadena de certificación (e.g., Benito posee $Cert_{AC2}$ y $Cert_{ACR}$ y confía en ellos).

Se pide:

a) Calcule la firma RSA del mensaje M = 2 realizada por Alicia.

b) ¿Qué tendrá que enviar Alicia a Benito para que éste pueda comprobar que el mensaje fue enviado por Alicia? Justifique su respuesta.

c) Suponiendo que Alicia le envía a Benito {M, $F_A(M)$, $Cert_A$, $Cert_{AC1}$, $Cert_{ACR}$}, siendo M = 2 y $F_A(M)$ el resultado calculado en el apartado a), realice TODOS los cálculos que tendría que realizar Benito para comprobar la autoría del mensaje enviado.

Ejercicio 2 :

Alicia desea enviar a Benito un mensaje M firmado mediante RSA. Las claves públicas de Alicia y Benito están certificadas por las Autoridades de Certificación AC_A y AC_B respectivamente. Existe una tercera Autoridad, AC, que certifica a AC_A y AC_B. Suponga que los certificados de las tres Autoridades de Certificación constan exclusivamente de la firma RSA del exponente de la clave pública de los clientes, es decir, F(e).

Datos:

- Todas las Autoridades de Certificación trabajan con el mismo módulo N=55.
- La clave pública de AC es ($e_{AC,}$ N) = (7, 55).
- Los exponentes públicos de las claves públicas de AC_A $\mathbf{(e_{AC_A}, N) = (e_{AC_A}, 55)}$ y A ($e_{A,}$ N) = (e_A, 55) no se proporcionan.
- El certificado de AC_A emitido por AC es 8.
- El certificado de A emitido por AC_A es 7.

Se pide:

a) Calcule la clave pública de AC_A. Analice si es un exponente público válido.
b) Calcule la clave pública de A. ¿Sería posible en vista del resultado del apartado anterior?
c) Independientemente del resultado del apartado anterior, suponga que la clave pública de A es ($e_{A,}$ N) = (49, 55). Calcule la firma RSA por parte de A del mensaje M = 4.