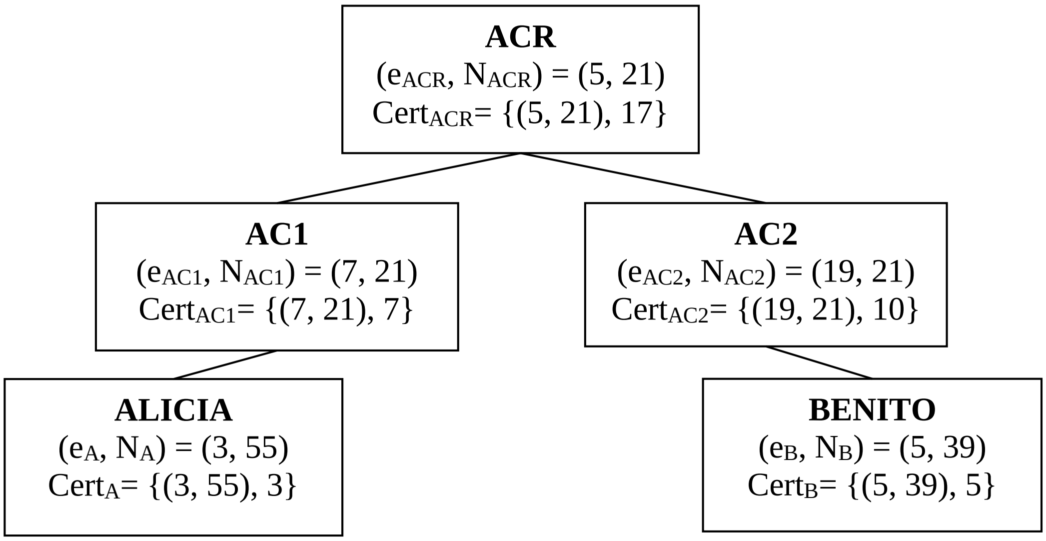
Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"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.

Solución:

a) Cálculo de d_A a partir de e_A:
$N_A = p_A \cdot q_A = 5 \cdot 11 \rightarrow \Phi(N_A) = \Phi(5) \cdot \Phi(11) = 4 \cdot 10 = 40$

Cálculo de inverso de 3 mod 40 por Euclides modificado:
$40 = 3 \cdot 13 + 1 \rightarrow 1 = 40 - 13 \cdot 3 \rightarrow d_A = 27$

Resultado = $F_A(M) = M^{d_A} \bmod N_A = 2^{27} \bmod 55 = (2^6)^4 \cdot 2^3 \bmod 55 = 9^4 \cdot 8 \bmod 55 = 26 \cdot 26 \cdot 8 =$ $\bmod 55 = 16 \cdot 8 \bmod 55 = 18$

b) Puntuación completa solo si está correctamente justificado. Alicia debe enviar:

- El mensaje
- La firma del mensaje
- Toda la cadena de certificación.

De esta manera Benito podrá comprobar la veracidad de todo lo enviado hasta el certificado de su confianza $Cert_{ACR}$.

c) 1º Benito comprueba que el mensaje está firmado utilizando el supuesto certificado de Alicia:

- Comprobación firma de Alicia:
  $F_A(M)^{e_A} \bmod N_A = 18^3 \bmod 55 = 2^3 \cdot 9^3 \bmod 55 = 72 \cdot 81 \bmod 55 = 26 \cdot 17 \bmod 55 = 2 = M$

2º Comprobación de la cadena de certificación:

- Comprobación de expedición del certificado de A por parte de AC1:
  Hay que comprobar que AC1 ha firmado el certificado de A
  $F(e_A)^{e_{AC1}} \bmod N_{AC1} = 3^7 \bmod 21 = 3^3 \cdot 3^3 \cdot 3 \bmod 21 = 6 \cdot 6 \cdot 3 \bmod 21 = 3 = e_A$

- Comprobación de expedición del certificado de AC1 por parte de ACR:
  Hay que comprobar que ACR ha firmado el certificado de AC1
  $F(e_{AC1})^{e_{ACR}} \bmod N_{ACR} = 7^5 \bmod 21 = 7 = e_{AC1}$

- Comprobación de expedición del certificado de ACR por parte de ACR:
  No hace falta comprobarlo, ya que Benito usa el que ya posee y confía en él. De hecho, la comprobación del certificado de AC1 se debería hacer con el $Cert_{ACR}$ que posee Benito y no con el recibido.

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 $(\mathbf{e_{AC_A}}, \mathbf{N}) = (\mathbf{e_{AC_A}}, \mathbf{55})$ 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.

Solución:

a) $8 = e_{AC_A}^{\ d_{AC}} \bmod N$ -> $e_{AC_A} = 8^{\,e_{AC}} \bmod N$

$e_{AC_A} = 8^7 \bmod 55 = 9 \cdot 9 \cdot 9 \cdot 8 \bmod 55 = 26 \cdot 17 \bmod 55 = 2$

La clave pública de AC_A calculada es: $(e_{AC_A}, N) = (2, 55)$

No es una clave pública válida debido a que $\mathbf{e_{AC_A}}$ no tiene inverso módulo $\Phi(N)$ dado que mcd $(2,40) \neq 1$.

b) Al no ser válida la clave pública de AC_A, no existe solución (como e no tiene inverso, no hay clave privada, y por tanto no puede haber firmado el certificado de A).

Si ignoramos este hecho, los cálculos serían los siguientes:

$7 = e_A^{\ d_{AC_A}} \bmod N$ -> $e_A = 7^{\,e_{AC_A}} \bmod N$

$e_A = 7^2 \bmod 55 = 49$

y la clave pública de A sería: $(e_A, N) = (49,55)$

c) $\Phi(N) = \Phi(55) = \Phi(5)\cdot\Phi(11) = 4\cdot10 = 40$

$e_A \cdot d_A = 1 \bmod 40$

$49\cdot d_A = 9 \cdot d_A = 1 \bmod 40$

$40 = 9\cdot4 + 4$

$9 = 4\cdot2 + 1$

$1 = 9 - 4\cdot2 = 9 - 2(40 - 9\cdot4) = 9 - 2\cdot40 + 8\cdot9 = 9\cdot9 - 2\cdot40$

$d_A = 9$

$F_A(M)$ $= 4^9 \bmod 55 = 2^{18} \bmod 55 = (2^6)^3 \bmod 55 = 9^3 \bmod 55 = 3^6 \bmod 55 =$

= $3^4 \cdot 3^2 \bmod 55 = 26 \cdot 9 \bmod 55 =$ **14**