uc3m | Universidad Carlos III de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY

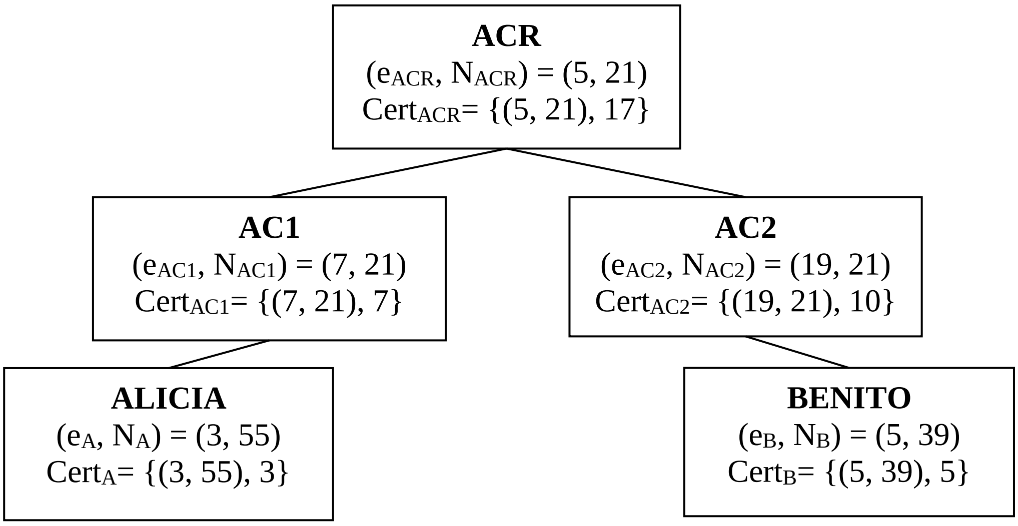
Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Public key infrastructures"

Proposed exercises

Exercise 1:

Alicia wants to send a signed message to Benito. The certification authorities' hierarchy and the public key and public key certificates in use are shown in the following figure.



Considerations:

- The certificate of an entity *i* consists of her public key and the signature on the public exponent of the public key issued by the certificate issuer. That is, $Cert_i = \{(e_i, N), S_{issuer}(e_i)\}$, being $S_{issuer}(e_i)$ the RSA signature generated by the certificate issuer (the entity immediately precedent within the shown hierarchy).
- Root certification authority self-signs her certificate.
- No hash functions are used.
- Each entity owns a local copy and trust the certificates within the certificate chain of her own certificate (e.g., Benito owns $Cert_{AC2}$ and $Cert_{ACR}$, and he trusts the local copy of their certificates).

Answer the following questions:

a) Compute Alice's RSA signature of message M = 2.

b) What should send Alicia to Benito so he can check that the message was sent by Alicia? Argument your answer.

c) Assuming that Alicia sends Benito {M, $S_A(M)$, $Cert_A$, $Cert_{AC1}$, $Cert_{ACR}$}, being M = 2 and $S_A(M)$ the result computed in question a), show ALL the computations that Benito should perform to check the authenticity of the received message.

Solution:

a) Computation of d_A from e_A:
$N_A = p_A \cdot q_A = 5 \cdot 11 \rightarrow \Phi(N_A) = \Phi(5) \cdot \Phi(11) = 4 \cdot 10 = 40$
Computation of the multiplicative inverse of 3 mod 40 using the extended Euclidean algorithm:
$40 = 3 \cdot 13 + 1 \rightarrow 1 = 40 - 13 \cdot 3 \rightarrow d_A = 27$
Result = $S_A (M) = M^{d_A} \bmod N_A = 2^{27} \bmod 55 = (2^6)^4 \cdot 2^{3} \bmod 55 = 9^4 \cdot 8 \bmod 55 = 26 \cdot 26 \cdot 8 = \bmod 55$
$= 16 \cdot 8 \bmod 55 = 18$

b) Alicia must send:

- The message
- The signature on the message
- The certificate chain.

Thus, Benito may check their authenticity and trust till one of his trust anchors, $Cert_{ACR}$.

c) 1º Benito checks that the message is signed using the purported Alicia's certificate:

- Verification of Alicia's signature:
  $S_A(M)^{e_A} \bmod N_A = 18^3 \bmod 55 = 2^3 \cdot 9^3 \bmod 55 = 72 \cdot 81 \bmod 55 = 26 \cdot 17 \bmod 55 = 2 = M$

2º Verification of the certificate chain:

- Verification of Alicia's certificate:
  Verification of AC1's signature on Alicia's certificate
  $S(e_A)^{e_{AC1}} \bmod N_{AC1} = 3^7 \bmod 21 = 3^3 \cdot 3^3 \cdot 3 \bmod 21 = 6 \cdot 6 \cdot 3 \bmod 21 = 3 = e_A$

- Verification of AC1's certificate:
  Verification of ACR's signature on AC1's certificate
  $S(e_{AC1})^{e_{ACR}} \bmod N_{ACR} = 7^5 \bmod 21 = 7 = e_{AC1}$

- Verification of ACR's certificate:

It is not necessary as Benito already trusts ACR and owns a local copy of her certificate. Verification of AC1's certificate should be done using Benito's local copy of $Cert_{ACR}$.

Exercise 2 :

Alice wants to send to Benito a message M signed with RSA. The public keys of Alice and Benito are certified by the certification authorities CA_A and CA_B respectively. A third certification authority (CA) exists, that certifies CA_A and CA_B. Consider that the three certificates are only composed of the signature of the public key exponent of the subject of the certificate.

Data:

- All certification authorities have the same modulo: N=55
- AC public key is $(e_{CA}, N)=(7, 55)$
- Public exponents of AC_A and A are not provided
- AC_A 's public key is $(e_{CA_A}, N) = (e_{CA_A}, 55)$
- A's public key is $(e_A, N)=(e_A, 55)$
- The certificate of CA_A issued by CA is 8
- The certificate of A issued by AC_A is 7

Questions:

a) Calculate the public key of CAA.

b) Calculate the public key of A.

c) Consider the public key of A is $(e_A, N) = (49, 55)$, compute the RSA signature on the message M=4 by Alice.

Solution:

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

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

AC_A 's public key is: $(e_{AC_A}, N) = (2, 55)$

It is not a valid public key as $\mathbf{e}_{\mathbf{AC_A}}$ does not have multiplicative inverse in modulo $\Phi(N)$ as gcd $(2,40) \neq 1$.

b) Due to the public key of CA_A is not valid, solution does not exist. If we ignore this fact, the calculations would be:

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

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

and A's public key would be: $(e_{A,}N) = (49,55)$

c) $\Phi(N) = \Phi(55) = \Phi(5)\cdot\Phi(11) = 4\cdot10 = 40$
$e_A \cdot d_A = 1 \mod 40$
$49\cdot d_A = 9 \cdot d_A = 1 \mod 40$
$40 = 9\cdot4 + 4$
$9 = 4\cdot2 + 1$
$1 = 9 - 4\cdot2 = 9 - 2(40 - 9\cdot4) = 9 - 2\cdot40 + 8\cdot9 = 9\cdot9 - 2\cdot40$
$d_A = 9$

$\mathbf{S_A(M)} = 4^9 \mod 55 = 2^{18} \mod 55 = (2^6)^3 \mod 55 = 9^3 \mod 55 = 3^6 \mod 55 =$
$\mathbf{=}\ 3^4 \cdot 3^2 \mod 55 = 26 \cdot 9 \mod 55 = \mathbf{14}$