SICUREZZA NELLE RETI — *Laurea Specialistica in Ingegneria Informatica*

SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU) — *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS
Computer Engineering

18 February 2014

NAME _____ **SERIAL NO.** _____

EXERCISE NO. 1 #MARKS: 12

Define a secure hash function and argue the relevance of its properties with respect to digital signature.

EXERCISE NO. 2 #MARKS: 6

In an access control system (ACS), Alice brings a personal device that is equipped with a symmetric cypher, a collision-resistant hash function, a random number generator, and a short-range wireless communication device. Alice and the ACS share a password Π_A.

Design a challenge-response protocol that allows Alice to prove ACS her presence. The key K_A shared by Alice and ACS for the challenge response protocol is derived from the password. The protocol must i) guarantee the authentication of Alice; ii) be resistant to replay-attacks; and iii) prevent offline password-guessing attack.

EXERCISE NO. 3 #marks: 12

Let (S, D) be a secure digital signature scheme with appendix. Let S and D be the signature and verification algorithm, respectively. Furthermore, let K_P be principal P's public key, and CA a Certification Authority that is trusted by all principals of the system. Finally let H be a secure hash function. Which of the following *certificates* are useful to establish a secure channel with Alice? Argue why.[1]

(A) "Alice" || K_A || S_{CA}(*Alice*)
(B) "Alice" || K_A || $S_{CA}(K_A)$
(C) "Alice" || K_A || $S_A(H$("Alice" || $K_A))$
(D) "Alice" || K_A || S_{CA}("Alice" || $H(K_A)$)
(E) "Alice" || K_A || S_{CA}(H("Alice" || $K_A)$)
(F) "Alice" || K_A || S_{Bob} ("Alice" || K_A) || "Bob" || K_B || S_{CA}("Bob" || K_B)
(G) "Alice" || K_A || S_{Bob}("Alice" || K_A) || "Bob, CA: yes" || K_B || S_{CA}("Bob, CA: yes" || K_B).

[1] Neglect any issue related to time.

29 January 2014

SOLUTION

EXERCISE #1

See theory.

EXERCISE #2.

$M1 \quad A \rightarrow S: \quad A$

$M2 \quad S \rightarrow A: \quad n_s$

$M3 \quad A \rightarrow S: \quad E_{K_A}\left(A, n_s, s_A\right)$

where $K_A = h(\Pi_A)\big|_k$ Notice that s_A is a random salting quantity aimed at avoiding an offline password-guessing attack.

EXERCISE #3.

A. Certificate A does not link KA to Alice
B. Certificate A does not link KA to Alice
C. Certificate B is self-signed and Alice is not a trusted authority
D. Certificate C is fine.
E. Certificate C is fine.
F. Bob, who is not a trusted authority, signed certificate D.
G. Certificate E is fine: CA delegates B to sign certificates.