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

22 July 2013

NAME____ SERIAL NO.____________________

EXERCISE NO. 1 #MARKS: 10

(A) Describe the CBC encryption mode;
(B) Discuss the advantages of CBC w.r.t. ECB;
(C) Discuss if ECB decryption and/or CBC decryption can be performed in parallel.

EXERCISE NO. 2 #MARKS: 10

Alice and Bob have each a smart-phone capable of performing the following cryptographic operations: (1) Diffie-Hellmann key establishment protocol; (2) symmetric encryption (*E* and *D*) and, (3) secure pseudo-random number generation (*G*). Alice and Bob meet face-to-face and want to establish a secure channel by means of DH without being fooled by the man-in-the-middle. To this regard, voice can be considered a secure, timely and authentic channel.

(A) Design an extended-DH protocol that allows Alice and Bob to establish a secure channel.
(B) Argue about a "reasonable" size (in bit) of random numbers involved in the protocol.
(C) Analyse the protocol by means of the BAN logic establishing.

EXERCISE NO. 3 #marks: 10

Let K_A be the public key of Alice, $S_P(x)$ be the digital signature of principal *P* on item *x*, CA be a Certification Authority (trusted by all principals of the system), and finally *H* a secure hash function. Which of the following certificates are useful to establish a secure channel with Alice? Argue why.

(A) "Alice" || S_{CA}(H("Alice"|| K_A))
(B) "Alice" || K_A || S_A("Alice" || K_A)
(C) "Alice" || K_A || S_{CA}("Alice" || H(K_A))
(D) "Alice" || K_A || S_{CA}(H("Alice" || K_A))
(E) "Alice" || K_A || S_{CA} (K_A)
(F) "Alice" || K_A || S_B("Alice" || H(K_A) || "issuer: Bob") || S_{CA}("Bob, CA=Yes" || K_B)

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

1 July 2013

SOLUTION

EXERCISE #1

Questions (A) and (B). See theory.

Question C. Decryption is ECB can be done in parallel because blocks are encrypted and decrypted separately. Decryption in CBC can be done in parallel too. Decryption of block p_i requires blocks c_i and c_{i-1} (or IV). Both blocks are available and therefore decryptions can proceed in parallel.

EXERCISE #2.

Question A. Each principal's smart phone generates a secret random number and displays it. Let r_A and r_B the secret number of Alice and Bob respectively. Each principal reads its own secret number to the other principal that types it into its smart phone. Then each principal computes a shared secret random number $r = r_A \oplus r_B$. Principals use this shared secret to authenticate the key establishment.

M1 $A \to B: \; \{A, B, X_A\}_r$

M2 $B \to A: \; \{B, A, X_B\}_r$

Question B. Secrets must not be smaller than 64 bits.

Question c. The key observation is that the first part of the protocol can be abstracted away by stating the two following assumptions:

1. Alice (Bob) believes that *r* is a shared key with Bob (Alice);
2. Alice (Bob) believes that *r* is fresh.

EXERCISE #3.

Options (A), (B) and (E) are not good. Option (A) is not good because there is no way to extract Alice's public key from the certificate. Option (B) is not good because it is a self-certified certificate. Finally, option (E) is not good because it does not link Alice's identifier "Alice" to Alice's public key K_A.

Options (C), (D), and (F) are good. In particular, option (F) describes a case of certificate chain.