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

Master in Computer Engineering

18 January 2015

NAME____ SERIAL NO.____________________

EXERCISE NO. 1 #MARKS: 10

With reference to perfect chipher,

1. Give the Shannon's definition;
2. Give an intuitive interpretation of the definition;
3. Prove that the number of keys cannot be smaller than the number of plaintexts.

EXERCISE NO. 2 #MARKS: 10

Let us consider the protocol below aimed at establishing a session key K_{AB} between Alice and Bob. In the protocol, n_A and n_B denote two nonces that are generated by Alice and Bob, respectively; K_B denotes the public key of Bob; and, finally, P_A denotes the shared secret password between Alice and Bob.

$$\begin{array}{lll} \text{M1} & A \rightarrow B & \{n_A, K_{AB}\}_{K_B} \\ \text{M2} & B \rightarrow A & \{n_B, n_A\}_{K_{AB}} \\ \text{M3} & A \rightarrow B & \{n_B, P_A\}_{K_{AB}} \end{array}$$

1. Analyze the protocol and verify whether it fulfils the key authentication and the key confirmation requirements. Specify the assumptions under which the requirements are fulfilled.
2. Let us suppose that a session key K_{AB} is compromised.
   a. Discuss the consequences.
   b. Improve the protocol in order to limit at the minimum the effects of compromising the session key.

EXERCISE NO. 3 #marks: 10

With reference to SSL, describe the Handshake protocol in the case of server authentication.

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
Master in Computer Engineering

18 January 2015

NAME____ SERIAL NO.____________________

SOLUTION

Exercise n.1

XXX

Exercise n.2

XXX

Exercise n. 3

XXX

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 September 2014