SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering

12 January 2015

NAME_____ **SERIAL NO.**_____

EXERCISE NO. 1 #MARKS: 12

With reference to the Diffie-Hellmann key establishment protocol,

1. Describe the protocol;
2. Argue about the security of the protocol w.r.t. to a passive adversary;
3. Argue about the security of the protocol w.r.t. to an active adversary;
4. Discuss a possible solution to the MIM attack

EXERCISE NO. 2 #MARKS: 8

Alice e Bob utilizzano il protocollo di Diffie-Hellman per stabilire una chiave di sessione. Siano Y_A ed Y_B i rispettivi parametri pubblici. Al fine di evitare l'attacco dell'uomo-nel-mezzo, Alice e Bob mantengono una relazione di fiducia con una terza entità fidata Trent che agisce da autorità di certificazione. Tali relazioni di fiducia si concretizzano nelle chiavi K_a e K_b, che, rispettivamente, Alice e Bob condividono a priori con l'autorità.

Assumendo che gli orologi di Alice, Bob e Trent non siano sincronizzati, progettare un protocollo per la certificazione dei parametri pubblici che permetta di raggiungere i seguenti *belief*

$$A \mid\equiv \overset{Y_B}{\mapsto} B$$

$$B \mid\equiv \overset{Y_A}{\mapsto} A$$

EXERCISE NO. 3 (♥) #marks: 10

1) Describe the key generation algorithm of the RSA encryption scheme.
2) Discuss the complexity of each algorithm step.

SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering

12 January 2015

NAME_____ **SERIAL NO.**_____

SOLUTION

Exercise n.1

See theory

Exercise n.2

TBD

Exercise n. 3

See theory

SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

18 September 2014