**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*

**6 July 2013**

**NAME** _____ **SERIAL NO.** _____

## EXERCISE NO. 1 #MARKS: 10

With respect to the Diffie-Hellman key establishment protocol, (1) present it, and discuss its security with respect to both a (2) passive and an (3) active adversary

## 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.

M1 $A \rightarrow B \quad \{n_A, K_{AB}\}_{K_B}$

M2 $B \rightarrow A \quad \{n_B, n_A\}_{K_{AB}}$

M3 $A \rightarrow B \quad \{n_B, P_A\}_{K_{AB}}$

1) Analyse 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 session key compromization.

## EXERCIZE NO. 3 #marks: 10

Let us consider the Vernarm Cipher (One-Time Pad),

1) discuss whether, and to what extent, it is resistant to a ciphertext-only attack;
2) discuss whether, and to what extent, it is resistant to a known-plaintex attack.

**Appello del 17 luglio 2012**