Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 26 giugno 2011

Nome e Cognome _____ **Matricola** _____

ESERCIZIO 1 **PUNTI:10**

Con proprietà di linguaggio e precisione matematica, il candidato definisca un cifrario perfetto secondo la teoria di Shannon. Inoltre, il candidato dimostri che a) in un cifrario perfetto il numero di chiavi non può essere inferiore al numero dei messaggi; e che b) un cifrario asimmetrico può essere sicuro solo da un punto di vita computazionale.

ESERCIZIO 2 **punti: 10**

Alice e Bob utilizzano il protocollo di Diffie-Hellman per stabilire una chiave di sessione. Al fine di evitare l'attacco dell'uomo-nel-mezzo, Alice e Bob mantengono una relazione di fiducia con una terza entità fidata Trent, relazioni che si concretizzano nelle chiavi condivise *a priori* K_a e K_b, rispettivamente. Assumendo che gli orologi di Alice, Bob e Trent non siano sincronizzati, progettare un protocollo di distribuzione di una chiave di sessione K_{ab} che soddisfi i consueti requisiti di key authentication, key confirmation e non-replay.

ESERCIZIO 3 **punti:10**

Con proprietà di linguaggio e precisione matematica, il candidato descriva il protocollo di autenticazione di WEP e la sua vulnerabilità.