Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 03 marzo 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

I processi A e B utilizzano un cifrario simmetrico $E()$ ed una funzione hash con chiave $h_k()$. A e B condividono le chiavi segrete K_e e K_a da utilizzare con E ed h rispettivamente. Infine A e B utilizzano un servizio anti-replay basato su di un meccanismo contatore-finestra (come quello di IPsec). Supponendo che il formato dei messaggi sia $\langle ciphertext, counter, mac \rangle$, con *counter* valore del contatore del mittente, specificare quale, o quali, dei seguenti schemi fornisce il servizio anti-replay:

1. $ciphertext = E(K_e, m)$; $mac = h(K_a, counter)$
2. $ciphertext = E(K_e, m||counter)$; $mac = h(K_a, counter)$
3. $ciphertext = E(K_e, m)$; $mac = h(K_a, ciphertext||counter)$
4. $ciphertext = E(K_e, m)$; $mac = h(K_a, m)$
5. $ciphertext = E(K_e, m||h(K_a, m))$; $mac = h(K_a, counter)$

ESERCIZIO 3 — punti:10

Con proprietà di linguaggio e precisione matematica, il candidato descriva il protocollo WEP. Il candidato discuta anche il *key reuse attack* a cui WEP é soggetto.