Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 12 febbraio 2011

Nome e Cognome_____ Matricola _____

ESERCIZIO 1 — PUNTI:10

Lo schema di cifratura RSA e la sua relazione con il problema della fattorizzazione.

ESERCIZIO 2 — punti: 10

In un sistema cliente servitore, si consideri il seguente protocollo di autenticazione tra il server *S* ed un cliente *C*:

M1 C $\rightarrow$ S: "Hello", C M2 S $\rightarrow$ C: $\mathcal{C}_A(S)$ M3 C $\rightarrow$ S: $\mathcal{P}_S(K, C)$, $\mathcal{E}_K(n)$ M4 S $\rightarrow$ C: n M5 C $\rightarrow$ S: $\mathcal{E}_K(C, PWD)$ M6 S $\rightarrow$ C: $\mathcal{E}_K$("OK")	**Legenda** a. $\mathcal{C}_A(S)$ denota il certificato rilasciato al server S dall'autorità *A* di cui *S* e *C* si fidano (si assuma che la chiave pubblica di *A* sia ben nota); b. $\mathcal{P}_S(x)$ denota la cifratura della quantità x con la chiave pubblica di S; c. *K* denota una chiave segreta generata da C ad ogni nuova sessione; d. $\mathcal{E}_K(x)$ denota la cifratura della quantità *x* con la chiave simmetrica *K*; e. *n* denota un numero random generato da C ad ogni nuova sessione; ed infine f. PWD denota la password di C memorizzata sul server S.

Domanda a. Al termine del protocollo, il cliente *C* può ritenere di stare effettivamente interagendo con il server S? Motivare la risposta.

Domanda b. Al termine del protocollo, il server *S* può ritenere di stare effettivamente interagendo con il cliente *C*? Motivare la risposta.

Domanda c. Al termine del protocollo, la chiave *K* può essere utilizzata per garantire la segretezza della sessione tra *S* e *C*. Motivare questa affermazione rispetto alla presenza di un avversario passivo.

ESERCIZIO 3 — punti:10

Con riferimento al sistema Kerberos, il candidato illustri il protocollo base, discuta le ipotesi sotto le quali il protocollo di autenticazione è sicuro, discuta il dimensionamento delle finestre temporali.