Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 12/6/2012

A. Confrontare le tecniche di autenticazione basate su certificati (di tipo one-way, two-way e three-way) con le modalitá di gestione di un dialogo su rete basata sull'uso della tecnica di Diffie-Hellman.

B. Illustrare il funzionamento delle tecniche di generalizzazione per realizzare la k-anonymity.

C. Si ha la seguente tabella IMPIEGATO, gestita da una base di dati multilivello con poliistanziazione a livello di tupla.

IMPIEGATO

Nome	L_Nome	Stipendio	L_Stipendio	Citta	L_Citta
Anna	C	100K	C	Milano	C
Bruno	U	50K	C	Bergamo	U

Si ipotizzi di utilizzare un approccio per la gestione dinamica low water-mark per soggetti applicato a DB multilivello con poliistanziazione a livello di tupla. Si supponga quindi che un utente con livello S esegua is eguenti comandi SQL:

- `insert into Impiegato values (Anna, 200K, Bergamo)`
- `select * from Impiegato where Nome = 'Bruno'`
- `insert into Impiegato values (Anna, 50K, Dalmine)`

Illustrare il comportamento del sistema e mostrare la configurazione finale della tabella.