Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova dell'11/6/2013

A. Discutere l'applicazione di un modello MAC multilvello per l'integritá di tipo Biba nell'ambito del sistema informativo di un'universitá, ipotizzando che vi siano il dominio "amministrativo", che tratta di tasse di iscrizione, e il dominio "accademico", che descrive l'erogazione dei corsi e la carriera degli studenti.

B. I sistemi di autenticazione hardware possono essere soggetti ad attacchi di tipo "replay" e di tipo "relay". Descrivere sinteticamente queste due tipologie diverse di attacco e fornire una classificazione delle tecniche che si possono usare per proteggersi da essi.

C. Keccak ha unna struttura che consente di poter essere usato in modalitá keyed-hash senza bisogno di utilizzare una struttura HMAC. Giustificare i motivi di questa proprietá e i benefici che ne possono derivare. Mostrare inoltre un possibile uso di Keccak per la realizzazione di un protocollo di bit commitment.