Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 15-6-2005

A. Illustrare il modello di controllo dell'accesso HRU.

B. Illustrare il problema dell'aggiornamento di tuple per basi di dati multilivello che usano una politica di poliistanziazione con la granularità della tupla.

C. È stata sviluppata di recente una tecnica che consente di creare coppie di documenti o certificati digitali che presentano lo stesso risultato della funzione MD5. Discutere le vulnerabilità che vengono introdotte nei sistemi a causa di queste nuove tecniche.

D. Illustrare i vantaggi e le debolezze della modalità di cifratura OFB.

E. Si presenti l'architettura di soluzioni di sicurezza informatica che si potrebbero adottare per rendere sicura la gestione di un servizio per la gestione di scommesse online, in cui sia necessario gestire scommesse in modo estremamente rapido e robusto rispetto a malfunzionamenti del sito della società che gestisce le scommesse. Si supponga ad esempio che le quote possono essere inviate in tempo reale sul canale televisivo e che si voglia consentire al cliente di scommettere una cifra specificando il proprio codice, il codice dell'opzione e l'ammontare della scommessa, coinvolgendo eventualmente una terza parte responsabile di gestire le transazioni finanziarie (la banca o il gestore della propria carta di credito).