Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 28/4/2011

A. Descrivere l'applicazione dei principi di "confusione" e "diffusione" nel disegno dell'algoritmo Blowfish.

B. Si consideri l'applicazione dei modi di cifratura ECB, CBC, CTR e OFB per la protezione di un messaggio di lunghezza elevata che non fa uso di MAC. Descrivere per ciascuna tecnica se e come si puó realizzare un attacco in cui, senza conoscere la chiave di cifratura, viene commutato il valore di uno specifico bit del messaggio in chiaro (si consideri solo il caso in cui il bit appartiene a un blocco intermedio).

C. Mostrare come la tecnica di Diffie-Hellman puó essere usata per realizzare un crittosistema a chiave pubblica (suggerimento: Alice puó mostrare come chiave pubblica la tripla di valori (p, g, g^a), e Bob puó combinare la tecnica DH con le normali tecniche di cifratura simmetrica).

D. Si consideri la costruzione di una funzione hash mediante l'applicazione della tecnica HMAC con chiave k nota. Si illustri brevemente se la ricerca di una collisione per questa funzione é ancora suscettibile all'attacco del compleanno.