**Sicurezza dei Sistemi Informatici**
**Prof. Stefano Paraboschi**
*Prova in itinere del 19/4/2016*

A. Si consideri un protocollo P2P per la distribuzione di file di grandi dimensioni. Il protocollo prevede di dividere la risorsa in un certo numero di blocchi. Ad esempio, una risorsa da 1 GiB può essere divisa in 1024 blocchi da 1 MiB. Per garantire l'integritá, il protocollo prevede di fornire assieme al descrittore della risorsa una struttura per la verifica dell'integritá che presenta un valore di hash su 256 bit per l'intera risorsa. Discutere i vantaggi dell'uso di un albero di hash costruito sui valori di hash dei singoli blocchi (con il valore radice che caratterizza la risorsa globalmente) rispetto a fornire un valore di hash unico per l'intera risorsa (applicando la funzione hash all'intero GiB di dati). Analizzare anche il profilo di una struttura di hash ad albero binario rispetto a un albero con fan-out maggiore, rispetto infine a una soluzione che calcola il valore di hash di sintesi considerando la concatenazione dei 1024 valori di hash da 64 bit.

B. Si consideri la costruzione di un cifrario ottenuto mediante un'architettura di Feistel in cui la funzione *round* é ottenuta mediante una funzione DES con chiave fissa. Si consideri una soluzione in cui si esegue una sola applicazione dell'architettura di Feistel e una in cui si eseguono 4 o piú iterazioni. Si analizzi brevemente il profilo di sicurezza di queste due configurazioni.

C. Alcuni dei modi di cifratura possono essere usati per inviare messaggi che hanno una lunghezza diversa da un multiplo del blocco, troncando semplicemente il messaggio protetto in corrispondenza dell'ultimo bit/byte del messaggio. Classificare i modi di cifratura in base a questa caratteristica. Considerare quindi il disegno di un modo di cifratura ibrido, che utilizzi solo per l'ultimo blocco del messaggio l'uso di un modo di cifratura che consenta il troncamento. Analizzare il profilo di questa soluzione.