Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 9/4/2015

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, ciascuno dei quali è diviso in un certo numero di pezzi. Ad esempio, una risorsa da 1 GiB può essere divisa in 1024 blocchi da 1 MiB, ciascuno diviso in 1024 pezzi da 1 KiB. Per garantire l'integritá, il protocollo prevede di fornire assieme al descrittore della risorsa una struttura per la verifica dell'integrità che presenta il valore di hash su 32 bit per ogni blocco e una firma digitale DSA su 2048 bit calcolata su uno hash SHA-3 a 512 bit per l'intera risorsa. Discutere i vantaggi dell'uso congiunto di uno hash e di una firma digitale, tenendo conto che il protocollo P2P prevede di scaricare i pezzi di un blocco dai peer presenti sulla rete, operando contemporaneamente anche su molti pezzi, con molti peer coinvolti, gestendo pochi (al limite uno solo) blocchi alla volta, passando ai blocchi successivi solo dopo aver terminato il download di un blocco.

   Si supponga poi di aggiungere allo scenario sopra descritto l'elenco dei valori di hash di ogni singolo pezzo all'interno del descrittore della risorsa. Discutere il trade-off di sicurezza/performance di questa estensione.

B. Si consideri la costruzione di un cifrario ottenuto mediante l'applicazione in sequenza di 4 cifrature AES-128. Analizzare la robustezza di questo cifrario, che opera su blocchi di 128 bit con chiavi di 512 bit.

C. Discutere brevemente la sorgente della robustezza dell'algoritmo RSA. Confrontare il profilo di prestazioni di RSA rispetto a DSA e presentare quindi uno scenario adatto all'uso di ciascuno dei due critto-sistemi.