Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 12/4/2012

A. Si consideri un cifrario simmetrico operante su blocchi di 64 bit costituito dalla concatenazione di un cifrario C1 con chiave a 48 bit e un cifrario C2 con chiave da 56 bit. Stimare il costo necessario, in termini di cicli di calcolo e di spazio di memoria, per rompere il crittosistema avendo a disposizione alcune coppie di blocchi in chiaro/cifrato.

B. Si consideri la realizzazione di una funzione hash concatenando in serie e in parallelo le funzioni hash MD5 e SHA1. Analizzare il costo e la robustezza delle due opzioni.

C. Si consideri un crittosistema RSA con chiave pubblica $K_{pub} = (n, e) = (119, 5)$.

1. Si emuli la funzione di cifratura del messaggio $M = \{10100\}_2 = 20 \bmod n$, dettagliando l'intero procedimento.
2. Sarebbe stato ammissibile avere esponente di cifratura $e = 3$? (Motivare la risposta)
3. Supponendo che il valore $\phi(n) = 96$ sia reso pubblico, indicare come fattorizzare il modulo n.
4. Indicare il costo computazionale medio delle funzioni di cifratura e decifrazione (senza CRT) per il crittosistema RSA in termini di moltiplicazioni modulari, assumendo $k_{\text{pub}} = (n, e)$, $k_{\text{priv}} = (p, q, j(n), d)$ con e e d aventi peso di Hamming pari al 50% del numero di bit con cui sono codificati. Specificare tali costi per i valori degli esponenti calcolati ai punti precedenti.
5. Sapendo che $\phi(n) = 96$, ricavare l'esponente di decifrazione d, giustificando ogni passaggio e facoltativamente indicando eventuali alternative di calcolo.