Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 28/4/2010

A. Una semplice soluzione per la costruzione di un MAC con funzione hash sicura consiste nell'applicare la funzione hash a un input che ha come prefisso una chiave seguita dal messaggio che si desidera autenticare. Illustrare la fragilitá di questa soluzione e discutere le alternative che rendono il sistema piú sicuro.

B. Si consideri un crittosistema RSA con chiave pubblica $K_{\text{pub}} = (n, e) = (91, 13)$:

   1. Si emuli la funzione di cifratura del messaggio $M = \{10010\}_2 = 18 \; mod \; n$, dettagliando l'intero procedimento.
   2. Sarebbe stato ammissibile avere esponente di cifratura $e = 3$? (Motivare la risposta)

C. Il modo di cifratura CTR rappresenta una delle soluzioni piú interessanti. Realizzare un'analisi approssimata che valuti il numero di bit b da usare per il contatore tenendo conto che una certa chiave deve essere usata per cifrare 2^x messaggi di dimensione pari a 2^y byte con una probabilitá al massimo pari a 2^{-p} che si verifichi una sovrapposizione tra gli intervalli coperti da una qualunque coppia di messaggi. (Verrá valutata la qualitá del ragionamento, aldilá della correttezza delle formule presentate)