Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 6/6/2016

A. Si consideri un crittosistema RSA con chiave pubblica Kpub-A = $(n, e) = (133, 17)$:

   1. Si emuli la funzione di cifratura del messaggio $M = \{001000010\}_2 = 66 \bmod n$, dettagliando l'intero procedimento.
   2. Sapendo che $\phi(n) = 108$, ricavare l'esponente di decifrazione d giustificando ogni passaggio e indicare eventuali alternative di calcolo.
   3. Indicare il criterio usualmente adottato per la scelta dell'esponente di cifratura di una chiave pubblica RSA, commentando la risposta.

B. Discutere le motivazioni all'origine della poliistanziazione e fornire una valutazione della loro applicabilità nei moderni sistemi informatici.

C. Considerando le soluzioni di autenticazione basate su possesso, illustrare le possibili strategie di protezione agli attacchi di tipo *relay*.