Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 23/4/2013

A. Si considerino i modi di cifratura CBC, OFB e CTR. Per tutti questi modi, la trasformazione del testo dipende dalla chiave di cifratura e da un valore di inizializzazione IV applicato alla protezione del primo blocco. Supponendo che la chiave di cifratura sia costante, analizzare il comportamento di ciascun modo in queste due situazioni:

   1. riuso dello stesso IV su messaggi diversi;
   2. sostituzione da parte dell'avversario di un blocco durante la fase di cifratura, prima che il blocco venga eventualmente usato come input per la costruzione del blocco successivo.

B. Svolgere ad alto livello l'analisi del cifrario DES-4, che prevede di applicare in cascata 4 cifrature DES.

C. Si consideri un Crittosistema RSA con chiave pubblica $K_A^{\text{pub}} = (n, e) = (133, 17)$.

   1. Si emuli la funzione di cifratura del messaggio $M = \{001100010\}_2 = 98 \bmod n$, 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.