Prof. Stefano Paraboschi

Prova in itinere del 13-04-07

A. Si ha una griglia di Cardano quadrata con lato n pari. Determinare il costo di un attacco "brute force", espresso nei termini del numero di configurazioni che è necessario considerare per svolgere un'analisi esaustiva.

B. In un'applicazione si propone di incrementare il livello di protezione utilizzando in cascata 4 volte l'algoritmo di cifratura AES (128 bit di blocco, 128 bit di chiave). Confrontare il costo stimato per un attacco "brute force" quando si utilizza la stessa chiave ad ogni iterazione e quando si usano 4 chiavi diverse.

C. Si riporti nel proprio foglio e si compilino almeno 3 colonne della seguente tabella, per la quale si assume che i modi di cifratura siano applicati all'algoritmo di cifratura AES:

	a	b	c	d	e
ECB					
CBC					
CFB					
CFB-8bit					
OFB					
CTR					

In ciascuna cella bisogna inserire il valore che caratterizza ciascun modo di cifratura, secondo i seguenti parametri:

a Numero di cifrature AES richieste per la gestione di un messaggio lungo 136 bit

b Ritardo nell'invio di un messaggio di 136 bit in termini di numero di cifrature da eseguire (si assuma che il ritardo sia causato solo dall'esecuzione della funzione di cifratura e che ci sia stato tempo e spazio di memoria per preparare tutto ciò che può servire).

c Numero di decifrature richieste per decifrare l'intero contenuto del quarto blocco (ovvero, il blocco che inizia con il $3*128+1$-esimo bit del messaggio e termina con il $4*128$-esimo bit).

d Numero di bit del messaggio cifrato che è necessario considerare per decifrare l'intero contenuto del quarto blocco (ovvero, il blocco che inizia con il $3*128+1$-esimo bit del messaggio e termina con il $4*128$-esimo bit).

e Numero di bit del messaggio in chiaro corrotti in seguito a una modifica di valore di un bit del messaggio cifrato.