Prof. Stefano Paraboschi

Prova in itinere dell'11-04-08

A. Una delle vulnerabilità del modo CBC è la sensibilità ad eventuali sostituzioni nella codifica dell'IV se questo viene presentato come prefisso del messaggio, che possono portare a realizzare sostituzioni mirate di bit nel testo in chiaro, indipendentemente dalla conoscenza della chiave di cifratura. Analizzare gli altri modi di cifratura e descrivere quali modi sono sensibili allo stesso attacco.

B. AES è la soluzione di cifratura simmetrica di riferimento al giorno d'oggi per la maggior parte delle applicazioni. Illustrare un paio di scenari, motivandoli, in cui il disegno del sistema può giustificare l'uso di una soluzione di cifratura come rispettivamente 3DES e Blowfish.

C. In un'applicazione si propone di incrementare il livello di protezione utilizzando in cascata l'algoritmo di cifratura AES (128 bit di blocco, 128 bit di chiave) seguito dall'algoritmo di cifratura 3DES (64 bit di blocco e 112 bit di chiave, applicato separatamente alla prima e seconda metà del blocco prodotto da AES). Stimare il costo di un attacco "brute force".