Prof. Stefano Paraboschi

Prova dell'8-6-2005

A. Illustrare le modalità ECB, CBC, OFB.

B. Presentare una tecnica crittografia per la condivisione di segreti in cui è necessario che il segreto venga rivelato tramite la collaborazione di almeno 4 utenti normali o di 2 utenti normali e 1 utente manager.

C. Si consideri la realizzazione di schede per la gestione di ricariche telefoniche. La scheda che permette la ricarica presenta una certa quantità di informazioni in chiaro (ammontare, data di scadenza, codice identificativo) e un codice schermato da una banda argentata. Presentare le caratteristiche di sicurezza offerte da queste alternative per la produzione del codice nascosto:

   1. Valore random
   2. Hash SHA-1 delle informazioni in chiaro
   3. HMAC delle informazioni in chiaro (ovvero "hash con chiave")
   4. Firma digitale delle informazioni in chiaro

   Quali contesti giustificano l'uso delle diverse alternative?