Prof. Stefano Paraboschi

Prova del 06-06-06

A. Illustrare quali tra le modalità di cifratura ECB, CBC e CTR (Counter) risultano adatte alla gestione delle seguenti situazioni, motivando la risposta:

   - archiviazione su disco fisso di file di grandi dimensioni, con accesso casuale;
   - archiviazione su nastro di file, con accesso sequenziale;
   - trasmissione di dati in modo burst, con alta velocità di picco.

B. Illustrare le caratteristiche di base dei cifrari di Feistel.

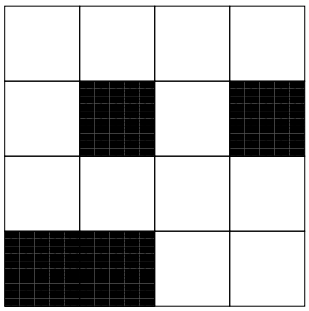
C. Si deve progettare un sistema software sicuro per garantire l'integrità di messaggi scambiati in rete. Si presentano due diversi scenari:

   1. per ogni messaggio inviato al gruppo di utenti, viene scrupolosamente verificata l'integrità del messaggio prima che esso venga utilizzato;
   2. l'integrità dei messaggi viene verificata molto di rado, solo in seguito a una precisa segnalazione di possibile malfunzionamento (come di norma avviene per le firme tradizionali).

   Quale tecnica tra RSA e DSA è quindi adatta a ciascuno dei contesti?

   Quali vantaggi e svantaggi porterebbe l'uso di una soluzione basata su HMAC?

D. (solo se avete tempo) Si realizza una soluzione di cifratura di messaggi di testo applicando in cascata una cifratura Playfair seguita da una permutazione con griglia di Cardano. Si sa che la parola chiave della cifratura Playfair è `CHIAVE`, che si esclude la lettera `J` dall'alfabeto, e si sa che la griglia utilizzata è la griglia seguente, utilizzata con rotazioni in verso orario:



   Decifrare quindi il seguente messaggio, mostrando una traccia dei passaggi (anche non commentata):

   `KTDI OBKP OSNT NTND` (3,2,2,5,4)