Lucrarea de laborator #3
CRIPTAREA SIMETRICA

Criptare pe bloc. Standarde de criptare

Breviar teoretic

In prezenta lucrare de laborator vi se face o prezentare a noțiunii de cifru bloc, a modurilor de operare precumși a principalelor standarde in domeniu ale . În finalul capitolului se prezintă o serie de tehnici și metode de a cifrurilor bloc care vor fi exemplificate pe standardele de cifrare bloc DES si GOST 28147-89.

Cifrurile bloc procesează informația pe blocuri de o lungime stabilită apriori. În cele ce urmează vom nota prin n lungimea blocului procesat (exprimată în biți), V_n spațiul vectorilor n dimensionaliși prin K spațiul cheilor. Un bloc de text clar se va nota

prin M iar un bloc de text cifrat se va nota prin C.

Definiție Un cifru bloc pe n biți este o funcție $E : V_n \times K \to V_n$ astfel înc^at pentru orice cheie $k \in K$ funcția $E(\cdot, k)$ este o funcție inversabilă (funcția de cifrare cu ajutorul cheii k) din V_n în V_n. Funcția inversă este funcția de decifrareși

va fi notată prin $D_K(\cdot) = E^{-1}(\cdot)$.

Există două moduri principale de utilizare în practică a algoritmilor simetrici: cifrarea blocși cifrarea secvențială. Cifrarea bloc operează cu blocuri de text clarși cifrat-de regulă de 64 de biți, uneori chiar mai mari. Cifrarea secvențială operează cu secvențe de text clarși cifrat de un bit sau octet. Î^n cazul cifrării bloc, același bloc de text clar va fi cifrat de fiecare dată în același bloc de text cifrat, folosind aceeași cheie. Î^n cazul cifrării secvențiale, secvențele similare de text clar vor fi cifrate diferit în cazul unor cifrări repetate.

Modurile de cifrare constituie combinații ale celor două tipuri de bază, unele folosind metode feedback, altele realiz^and simple operații. Aceste operații sunt simple, deoarece securitatea este atributul cifrării și nu al modului în care se realizează schema de cifrare. Mai mult, modul de realizare a cifrării nu duce la compromiterea securității date de algoritmul de bază.

Un cifru bloc cifrează textul în blocuri de n biți de mărimi fixe. Î^n general este folosită valoarea n = 64 biți. Cele mai cunoscute moduri de operare sunt ECB (electronic code book), CBC (cipher block chaining), CFB (cipher feedback block)și OFB (output feedback block). Î^n funcție de modul de operare al cifrului bloc se vor aplica atacuri specifice. Vom nota în cele ce urmează, cu E_k se notează funcția de cifrare a blocului în timp ce cu D_k notăm funcția de descifrare.

Modul ECB (electronic code-book)

Modul ECB este cea mai obișnuită formă de cifrare bloc: un bloc de

text clar este transformat într-un bloc de text cifrat, fiecare bloc fiind cifrat independentși fiecare cheie fiind diferită de celelalte. Dacă același bloc de text clar se cifrează întotdeauna

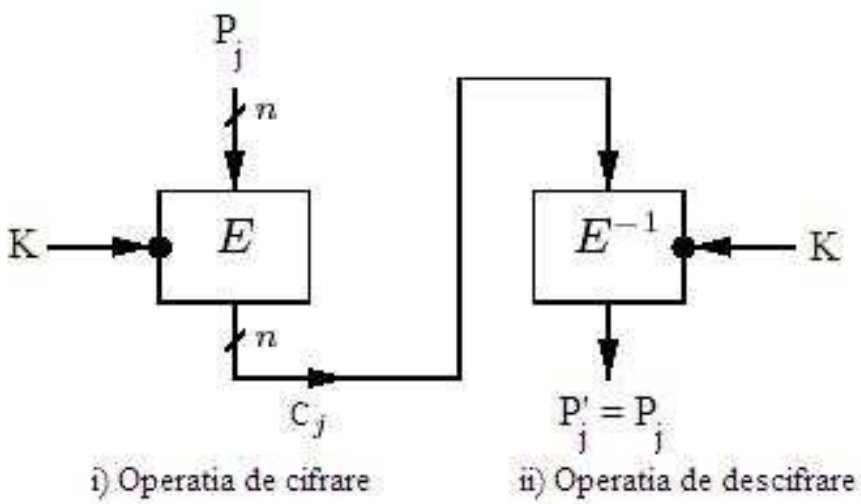
în același bloc de text cifrat, teoretic este posibilă o carte de coduri în care să se facă asocierea text clar-text cifrat. Pentru blocuri de 64 de biți rezultă un număr de 2^{64} intrări în cartea de coduri-mărime prea mare pentru a permite memorareași manipularea.

Modul ECB este cel mai simplu mod de lucru, fiecare bloc de text clar fiind cifrat independent. Cifrarea se poate face lu^and aleator blocuri din cadrul fișierului. Acest mod de cifrare este indicat pentru cifrarea documentelor care sunt accesate aleator, ca de exemplu baze de date, unde fiecare înregistrare poate fi adăugată,ștearsă, cifrată sau descifrată independent de celelalte.

Algoritmul ECB

Intrare: Cheia K de k biți, mesajul clar $M = M_1, \ldots, M_t$ pe blocuri de n biți.

Ieșire: Textul cifrat $C = C_1, \ldots, C_t$ care ulterior se descifrează pentru a descoperi textul original.



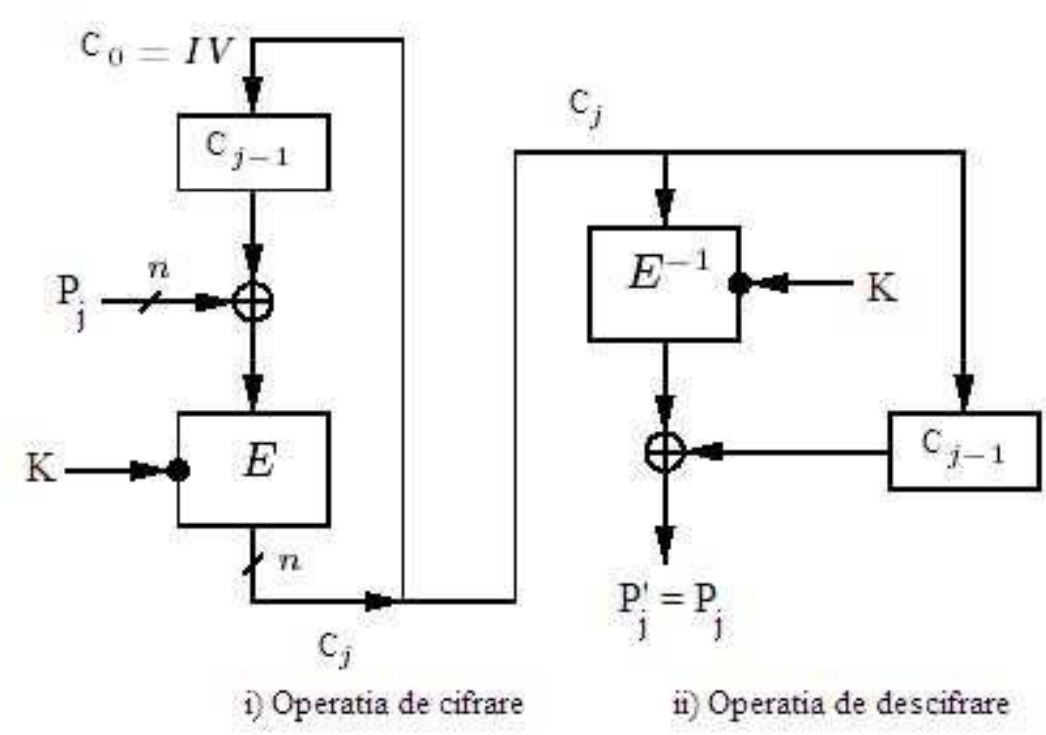
1. Cifrarea: pentru orice $i = 1, \ldots, t$ avem: $C_i = E_k(M_i)$.

2. Descifrarea: pentru orice i = 1, . . . , t avem: $M_i = D_K(C_i)$.

Modul CBC (cipher-block chaining)

Acest mod folosește un mecanism feedback, deoarece rezultatul cifrării unui bloc anterior revine prin buclăși intervine în cifrarea blocului curent. Cu alte cuvinte, blocul anterior este folosit pentru a modifica cifrarea următorului bloc. Ân acest fel, textul cifrat nu mai depinde doar de textul clar, cișsi de modul de cifrare al blocului anterior.

Ân modul CBC, textul clar, înainte de a intra în modul de cifrare propriu-zis, este însumat mod 2 cu blocul de text cifrat anterior. Diagrama de mai jos prezintă operația de cifrare/descifrare în modul CBC.
După ce blocul de text clar este cifrat, textul cifrat rezultat este stocat într-un registru al buclei de reacție. Ânainte ca următorul text clar să fie cifrat, el este sumat mod 2 cu blocul din registrul de reacțieși devine următoarea intrare în rutina de cifrare. După cifrare , conținutul registrului este înlocuit cu blocul cifrat. Ân acest fel, cifrarea blocului i depinde de toate cele i – 1 blocuri anterioare.



Într procesul de descifrare (care este exact procesul invers cifrării), textul cifrat este descifrat normalși depozitat în registrul de reacție. După ce următorul bloc este descifrat, el este făcut sumă mod 2 cu conținutul registrului de reacție.

Din punct de vedere matematic, procesul de cifrare arată astfel: $C_i = E_k(P_i \oplus C_{i-1})$.

Ecuațiile corespunzătoare operației de descifrare sunt: $P_i = C_{i-1} \oplus D_k(C_i)$.

Algoritmul CBC

Intrare: Cheia K pe k biți, vectorul inițial IV de n biți, mesajul clar M =

$M_1,...,M_t$ pe blocuri de n biți.
Ieșire: Textul cifrat $C = C_1, \ldots, C_t$ care ulterior se descifrează pentru a descoperi

textul original.

1. Cifrarea: C_0 = IV,și recursiv avem

$C_j = E_k(C_{j-1} \oplus M_j)$. 2.Descifrarea: C_0 =IV,pentruoricej=1,...,tavem

$M_j = C_{j-1} \oplus D_k(C_j)$.

SCOPUL LUCRARII DE LABORATOR

Studierea si analiza materialelor didactice a prezentului breviar la care aveti anexate textele originale a doua standarde, care vor fi si obiectul de studiu al algoritmilor dupa care s veti compune program de criptare-decriptare in conformitate cu standardul ales de voi.