METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Tema: Cifruri bloc moderne

OBIECTIVELE TEMEI

Vom examina unele concepte generale ce stau la baza sistemelor de criptare simetrice moderne și o clasă specială de algoritmi criptografici – cifrurile *bloc* cu cheie simetrică. Obiectivele urmărite sunt următoarele:

- A evidenția diferențele dintre cifrurile simetrice clasice și cele moderne;
- A introduce conceptul de sistem de criptare bloc și a examina caracteristicile definitorii ale cifrurilor bloc moderne;
- A defini transformările criptografice utilizate în construcția cifrurilor bloc;
- A examina sisteme de criptare bloc moderne, precum DES, 3DES, IDEA, AES, Serpent, Twofish ș.a.

OBIECTIVELE TEMEI

O atenție sporită vom acorda sistemelor de criptare DES (Data Encryption Standard) și AES (Advanced Encryption Standard), care sunt cele mai cunoscute cifruri bloc cu cheie simetrică. De la apariția lui DES au fost elaborate multe alte scheme de criptare eficiente, mai mult, DES a fost înlocuit cu AES . Cu toate acestea, studiul detaliat al sistemului de criptare DES permite înțelegerea conceptelor ce stau la baza altor cifruri bloc simetrice.

SUBIECTELE ABORDATE ÎN CADRUL TEMEI

1.1 Sisteme simetrice de criptare bloc

1.1.1 Conceptul general al cifrului bloc cu cheie simetrică

1.1.2 Transformări criptografice utilizate în construcția cifrurilor bloc

1.1.2.1 Cifruri compuse

1.1.2.2 Confuzia și difuzia Shannon

1.1.2.3 Rețeaua substituție-permutare

1.1.2.4 Rețeaua Feistel

1.1.3 Sistemul de criptare DES (Data Encryption Standard)

1.1.3.1 Descrierea sistemului de criptare DES

1.1.3.1.1 Prezentarea generală a sistemului DES

1.1.3.1.2 Algoritmul de criptare DES

SUBIECTELE ABORDATE ÎN CADRUL TEMEI

1.1.3.1.3 Algoritmul de expandare a cheii DES

1.1.3.1.4 Algoritmul de decriptare DES

1.1.3.2 Analiza sistemului de criptare DES

1.1.3.2.1 Efectul de avalanșă și de completitudine DES

1.1.3.2.2 Criteriile de proiectare a cifrului DES

1.1.3.2.3 Vulnerabilități ale cifrului DES

1.1.3.2.3.1 Vulnerabilități în proiectarea cifrului

1.1.3.2.3.2 Vulnerabilități în cheia secretă

1.1.4 Sisteme de criptare înrudite cu DES

1.1.4.1 Sistemul de criptare Triple DES (3DES)

1.1.4.2 Sistemul de criptare DES-X

SUBIECTELE ABORDATE ÎN CADRUL TEMEI

1.1.5 Sistemul de criptare AES

1.1.5.1 Finalistele la concursul pentru AES

1.1.5.2 Detalii ale sistemului de criptare AES

1.1.5.2.1 Elemente teoretice folosite în implementarea algoritmului AES

1.1.5.2.1.1 Corpul finit

1.1.5.2.1.2 Operații definite peste corpul finit GF(2^8)

1.1.5.2.1.3 Notații pentru octeți și biți

1.1.5.2.1.4 Polinoame cu coeficienți în GF(2^8)

1.1.5.2.2 Specificarea algoritmului AES

1.1.5.2.2.1 Tabloul de stare, cheia secretă și numărul de runde

1.1.5.2.2.2 Algoritmul de criptare AES

SUBIECTELE ABORDATE ÎN CADRUL TEMEI

1.1.5.2.2.3 Algoritmul de expandare a cheii Rijndael

1.1.5.2.2.4 Algoritmul de decriptare AES

1.1.5.2.2.5 Procedura echivalentă de decriptare

1.1.6 Moduri de operare a cifrurilor bloc

1.1.6.1 Modul ECB (Electronic CodeBook)

1.1.6.2 Modul CBC (Cipher Block Chaining)

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

2.3.1 Conceptul general al cifrului bloc cu cheie simetrică

Sistemul de criptare simetrică bloc (prescurtat cifru bloc) este un algoritm criptografic deterministic ce acționează la nivel de grupuri de biți de lungime fixă ale mesajului, numite blocuri, folosind o transformare inversabilă, specificată în baza cheii secrete. Atât algoritmii de criptare cu cheie simetrică, cât și cei cu cheie publică pot fi cifruri bloc.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Design-ul modern al cifrurilor bloc este bazat pe conceptul cifrurilor compuse iterative. C. Shannon a propus utilizarea cifrurilor compuse bazate pe transformări simple, precum substituțiile și permutările, ca și tehnici criptografice ce asigură o securitate sporită. Ideea nu este una nouă, deoarece a fost utilizată la cifrurile clasice, diferența aici fiind că simbolurile asupra cărora se vor aplica transformări de permutare și de substituție sunt biți.

Cifrurile compuse iterative realizează procedura de criptare în mai multe runde, fiecare dintre care folosește o subcheie distinctă, derivată din cheia inițială. O implementare eficientă a acestor cifruri, cunoscută sub numele de rețea Feistel, a fost utilizată în schema de criptare DES. Alte cifruri bloc, precum AES, se bazează pe rețele de tip substituție-permutare. Rețelele substituție-permutare și Feistel vor fi examinate la secțiunea 2.3.2.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Cifrurile bloc sunt prevăzute pentru criptarea sigură, cu o cheie fixată, doar a unui singur bloc de date a mesajului. Însă pentru a cripta mesaje formate din mai multe blocuri au fost elaborați algoritmi speciali, numiți moduri de operare a cifrurilor bloc, care permit aplicarea sigură de mai multe ori a cifrului bloc (cu aceeași cheie).

Cifrul bloc constă din doi algoritmi: transformarea de criptare E și transformarea de decriptare D. Ambii algoritmi au doi parametri de intrare – un bloc de mesaj și cheia secretă, iar în calitate de parametru de ieșire – un bloc de aceeași lungime ca și blocul de la intrare (a se vedea Figura 2.3.1).

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

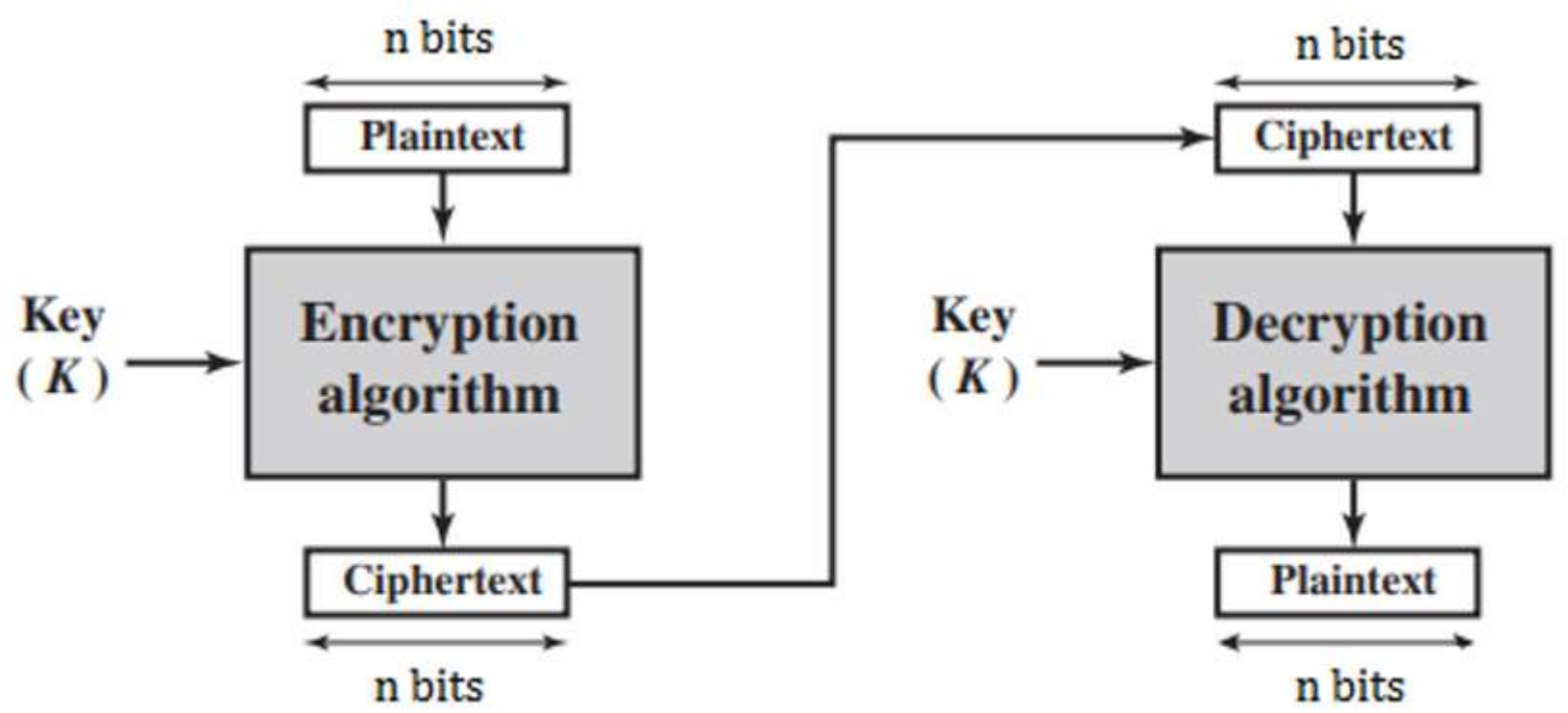

Figura 2.3.1. Modelul cifrului bloc

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Din punct de vedere matematic, transformarea de criptare a cifrului bloc este o funcție

$$E_k(P):\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n,$$

care preia la intrare cheia k pe m biți și blocul de mesaj clar P pe n biți, și, întoarce blocul de text criptat C pe n biți. Valoarea menționată n este numită lungime a blocului, iar m - lungime a cheii. Pentru fiecare cheie k este necesar ca transformarea de criptare $E_k(P)$ să fie inversabilă din $\{0,1\}^n$ în $\{0,1\}^n$. Inversa lui E este transformarea de decriptare $D_k(C)$,

$$D_k(C):=E_k^{-1}(C):\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^n,$$

care preia cheia k și textul criptat C, și întoarce blocul de text clar P, astfel încât să se satisfacă relațiile $D_k(E_k(P))=P$ și $E_k(D_k(C))=C$.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Cheia k se alege aleator, dar este aceeași, atât la criptare, cât și la decriptare. Numărul de chei posibile este egal cu cardinalul spațiului de chei $\mathcal{K}$ (numărul elementelor mulțimii șirurilor pe m biți).

Pentru ca decriptarea să fie unică, transformarea de criptare trebuie să fie o funcție bijectivă (fiecărui element al domeniului de definiție îi corespunde un singur element al domeniului de valori și reciproc). Pentru blocurile de text clar și de text criptat pe n biți și o cheie fixată, transformarea de criptare definește o permutare pe șirurile de n biți. Fiecare cheie definește o permutare distinctă dintr-o mulțime de $(2^n)!$ permutări posibile.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Deși lungimea fixă a blocului de mesaj pare a fi o importantă limitare a gradului de utilizare a cifrului bloc, dificultatea este depășită prin divizarea mesajului în părți de lungime egală cu cea a blocului, care sunt criptate (decriptate) separat, iar blocurile de text criptat (text clar) obținute sunt concatenate pentru a constitui mesajul criptat (decriptat). Dacă după divizarea pe blocuri a mesajului ultimul grup de biți are lungime mai mică ca cea a blocului, la acesta se aplică *procedura de padding,* adică grupul este completat cu un șir de biți, a cărui structură este predefinită, până atunci când lungimea acestuia devine egală cu cea a blocului.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Deși teoretic sunt acceptabile orice lungimi de bloc, în practică se va ține cont de următoarele aspecte:

- Dacă lungimea n a blocului este exagerat de mică, cifrul poate fi vulnerabil în fața atacurilor criptanalitice de tip dicționar. Într-adevăr, deoarece sunt posibile 2^n combinații de biți în blocul de text clar, dacă n este mic, atunci adversarul, pentru diferite variante de cheie secretă, poate să formeze rapid toate perechile text clar/text criptat. Astfel, adversarul poate forma în timp de calcul util un dicționar al perechilor text clar/text criptat în raport cu diferite variante de cheie secretă. Încă o vulnerabilitate o prezintă și faptul că fiecare bloc este criptat cu aceeași cheie, dar acest dezavantaj poate fi anihilat prin utilizarea unui mod specific de implementare a algoritmului cifrului bloc, iar procedeele corespunzătoare vor fi examinate la secțiunea 2.3.6.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

- Dacă lungimea n a blocului se alege exagerat de mare, atunci codificarea în baza cifrului poate să fie una ineficientă, deoarece consumă prea multe resurse de calcul. În practică, pentru valori mai mari ale lui n sunt necesare funcții pseudoaleatoare mai simplu de implementat.

De regulă, în calitate de lungime a blocului se alege un multiplu al lui 8, deoarece majoritatea procesoarelor gestionează date sub formă de multipli ai lui 8 biți.

CONCEPTUL GENERAL AL CIFRULUI BLOC CU CHEIE SIMETRICĂ

Pentru a realiza o comparație simplă a cifrurilor fluide și a cifrurilor bloc, amintim că cifrul fluid criptează textul clar bit cu bit, combinând prin XOR acești biți cu biții șirului pseudoaleator ce definește cheia fluidă, iar cifrul bloc criptează blocuri de biți ai textului clar cu aceeași cheie. Atât în cazul utilizării cifrurilor fluide, cât și a cifrurilor bloc, utilizatorii ce comunică în rețea partajează cheia de criptare simetrică. Majoritatea aplicațiilor bazate pe criptografie cu cheie simetrică folosesc cifrurile bloc (cu utilizarea unor moduri specifice de implementare), deoarece acestea asigură un nivel mai înalt de securitate, cu toate că unele cifruri bloc au o viteză de calcul mai mică.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Un număr mare de algoritmi de criptare bloc cu cheie simetrică sunt bazați pe structuri precum rețeaua Feistel și cifrurile compuse, ale căror principii de proiectare le vom prezenta în continuare.

Cifruri compuse

Cifrul compus reprezintă un concept propus de către C. Shannon, conform căruia se combină două sau mai multe transformări criptografice astfel încât cifrul rezultat să aibă o rezistență criptografică mai mare ca și componentele individuale ale acestuia. De regulă, transformările criptografice utilizate sunt bazate pe substituții, permutări și operații de aritmetică modulară.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Definiția cifrului compus utilizează conceptul compoziției de funcții. Dacă S, T, U sunt mulțimi finite, iar $f : S \to T$ și $g : T \to U$ sunt două funcții definite pe aceste mulțimi, atunci prin compunere a lui g cu f vom înțelege funcția $g \circ f$ (uneori notată și prin gf) din S în U, definită astfel:

$$(g \circ f)(x) = g(f(x)), \forall x \in S.$$

Operația de compunere poate fi extinsă la un număr finit arbitrar de funcții.

Dacă rezultatul compunerii $f \circ f$ este funcția identică $I(x) = x$, atunci f este numită involuție.

Dacă $E_{k_1}, \ldots, E_{k_t}$ sunt involuții, atunci inversa lui $E_k := E_{k_1} \ldots E_{k_t}$ este $E_k^{-1} := E_{k_t} \ldots E_{k_1}$, adică este compunerea de involuții, considerată în ordine inversă.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Fie $\mathcal{A}$ un alfabet de q simboluri, care servește în calitate de alfabet al textelor clare și, la fel, al textelor criptate. La fel, vom considera mulțimea M a tuturor șirurilor de lungime t peste $\mathcal{A}$.

Fie o schemă de criptare bloc cu cheie simetrică a cărei lungime de bloc este t, iar $\mathcal{K}$ mulțimea tuturor permutărilor de elemente din $\{1,\ldots,t\}$. Pentru fiecare $e \in \mathcal{K}$ se definește *cifrul cu transpoziție* E_e ca și transformarea $E_e(m) = \left(m_{e(1)} \ldots m_{e(t)}\right)$, unde $m := \left(m_1 \ldots m_t\right) \in M$. Un șir de simboluri ale textului clar este înlocuit printr-o permutare a acestora. Permutările se referă la manipularea ordinii biților conform unui algoritm.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Fie $\mathcal{K}$ mulțimea tuturor permutărilor pe mulțimea $\mathcal{A}$. Pentru fiecare $e \in \mathcal{K}$ se definește *cifrul cu substituție* E_e ca și transformarea $E_e(m) = (e(m_1)...e(m_t))$, unde $m := (m_1...m_t) \in M$. Elementul de text clar m_i este înlocuit în mod unic prin elementul de text criptat corespunzător $e(m_i)$. Substituțiile se referă la înlocuirea unor biți cu altii, conform unor reguli definite.

Separat transformările de transpoziție și de substituție nu promovează un nivel înalt de securitate. Dar prin combinarea acestor transformări este posibil de obținut cifruri compuse a căror rezistență criptografică este una înaltă. Un exemplu de cifru compus este compoziția a $t \geq 2$ transformări $E_k := E_{k_1}...E_{k_t}$, unde E_{k_i}, $i = \overline{1,t}$, este un cifru cu substituție sau un cifru cu transpoziție.

2.3.2.2 Confuzia și difuzia Shannon

Într-o compoziție a unei substituții și a unei permutări, se zice că substituția adaugă confuzie procesului de criptare, iar permutarea – difuzie.

Confuzia are ca scop să facă pe cât e posibil de complexă (în particular, neliniară) relația dintre cheia de criptare și textul criptat (camuflând legătura dintre acestea), iar difuzia constă în rearanjarea sau împrăștierea biților mesajului astfel încât orice redundanță (surplus de informație statistică) în textul clar este „răspândită" (disipată) peste tot în textul criptat. Fiecare bit de text clar afectează valoarea a mai multor biți de text criptat și reciproc. Deci, mecanismul difuziei face ca relația statistică dintre textul clar și textul criptat să fie pe cât e posibil de complexă.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Difuzia înseamnă că dacă se modifică un singur bit în textul clar, atunci, sub aspect statistic, se vor modifica jumătate din biții textului criptat, și analog, dacă se modifică un bit al textului criptat, atunci se vor modifica aproximativ jumătate din biții textului clar. În particular, dacă pentru un text clar ales aleator se va modifica bitul cu numărul i, atunci probabilitatea că se va modifica bitul cu numărul j din textul criptat este de $1/2$ (pentru oricare valori i și j), caz în care se spune că algoritmul criptografic satisface criteriul de avalanșă strictă. Această proprietate, conform căreia o modificare ușoară a textului clar sau a cheii conduce la modificări serioase, „în avalanșă", în textul criptat (fiecare dintre biții de ieșire se modifică cu probabilitatea $1/2$), este numită efect de avalanșă. Mai general, se poate cere ca modificarea unei mulțimi fixate de biți în textul clar să conducă la modificarea fiecărui bit din textul criptat cu probabilitatea $1/2$.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Dacă cifrul bloc nu satisface proprietatea efectului de avalanșă la un nivel suficient de înalt, atunci, posibil, criptanalistul va putea să facă predicții referitoare la textul clar, bazându-se doar pe textul criptat. Acest fapt poate să fie suficient pentru a sparge parțial sau chiar complet algoritmul de criptare. Construcția cifrurilor bloc ce satisfac proprietatea efectului de avalanșă este unul dintre obiectivele primare ale proiectării acestora.

Atât confuzia, cât și difuzia urmăresc să împiedice încercările de a restabili cheia, chiar dacă se cunoaște un număr mare de perechi *text clar – text criptat*, generate cu aceeași cheie. Modificarea unui bit al cheii va modifica complet textul criptat. Chiar dacă adversarul află careva informație cu privire la statistica textului criptat, calea prin care cheia a fost utilizată pentru a genera acest text criptat este atât de complexă, încât este computațional dificil de determinat această cheie. Astfel, proprietățile de difuzie și de confuzie constituie *pietrele de temelie* în proiectarea cifrurilor bloc.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Transformările de criptare și de decriptare din majoritatea cifrurilor bloc moderne utilizează în mod repetat compunerea de substituții și de permutări. În general, cifrurile bloc se bazează pe transformări de criptare complexe ce presupun aplicarea unor transformări liniare și neliniare, operații în aritmetica modulară (XOR, multiplicarea și exponențierea modulară), astfel încât cifrul rezultat să dobândească o rezistență criptografică mai mare ca și componentele utilizate în construcția acestuia.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

2.3.2.3 Rețeaua substituție-permutare

Pentru ca sistemele de criptare să reziste în fața atacurilor cu text criptat cunoscut este necesar ca textul criptat să satisfacă proprietățile de difuzie și de confuzie. Pentru a satisface aceste proprietăți, în cadrul cifrurilor bloc moderne se apelează la structuri criptografice special elaborate în acest scop. Un exemplu consacrat de astfel de structură criptografică îl reprezintă *rețeaua substituție-permutare* (prescurtat SP), care este un cifru compus, ce combină transformări de substituție și de permutare pe parcursul mai multor etape (a se vedea Figura 2.3.2).

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Rețeaua SP preia la intrare un bloc de text clar și cheia secretă, în baza cărora este efectuat un anumit număr de etape (numite runde), fiecare etapă conținând o transformare de permutare (numită P-boxă) și mai multe transformări de substituție (numite S-boxe). În locul unei singure S-boxe, care ar necesita un spațiu relativ mare de stocare, se folosesc mai multe S-boxe de capacitate redusă (a se vedea Figura 2.3.2).

Boxele de substituție și de permutare transformă biții de intrare în biți de ieșire în baza unor operații ce pot fi implementate eficient la nivel de hardware (de exemplu, XOR sau rotații de biți). La fiecare rundă este utilizată subcheia de rundă derivată din cheia secretă (a se vedea Figura 2.3.2). Decriptarea este efectuată prin inversarea procesului de criptare, folosind inversele pentru S-boxe și P-boxe și, aplicând cheile de rundă în ordine inversă.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

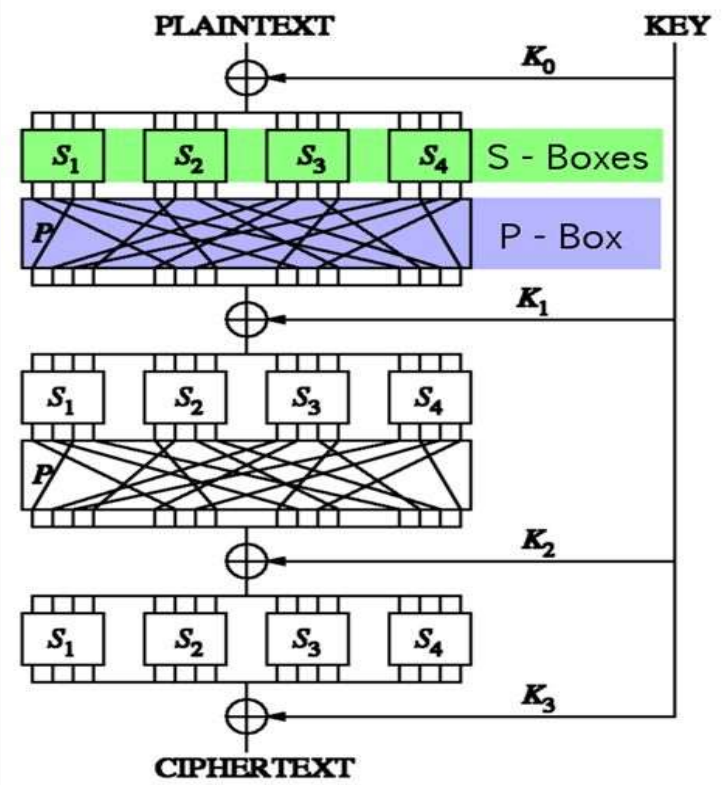

Figura 2.3.2. Rețeaua substituție-permutare (SP)

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

S-boxa efectuează o transformare neliniară, mixând biții cheii secrete cu biții textului clar. Astfel este mascată relația statistică dintre cheie (la fel, și textul clar) și textul criptat, creându-se *confuzie* în sens Shannon. O S-boxă de dimensiune $m \times n$ poate fi implementată ca un tabel ce conține 2^m cuvinte pe n biți fiecare. În unii algoritmi, precum DES, tabelele de substituție sunt fixate, iar în alți algoritmi - acestea sunt generate dinamic în baza cheii (de exemplu, în sistemele de criptare Blowfish și Twofish).

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Corespondența dintre blocul biților de intrare și blocul biților de ieșire este una bijectivă (oricărui element din domeniul de definiție îi corespunde un singur element din domeniul de valori și reciproc) pentru a asigura inversabilitatea transformării de criptare (adică posibilitatea decriptării). S-boxa posedă proprietatea conform căreia la modificarea unui bit al datelor de intrare în S-boxă se vor modifica circa jumătate din biții de ieșire din ea (efectul de avalanșă). La fel, S-boxele trebuie să satisfacă proprietatea că orice bit de ieșire depinde de fiecare bit de intrare.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

P-boxa realizează o permutare (liniară) a tuturor biților, distribuind redundanța (surplusul) peste tot în textul criptat, generând astfel *difuzie* în sens Shannon. Aceasta preia datele de la ieșirile tuturor S-boxelor unei runde, permută toți biții și îi transmite către S-boxele următoarei runde. Boxele de permutare satisfac proprietatea că biții de ieșire ai oricărei S-boxe sunt distribuiți la cât e posibil de multe intrări către alte S-boxe.

La fiecare rundă este combinată subcheia de rundă cu rezultatul obținut la etapa precedentă, folosind operația XOR.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Ținând cont că S-boxa poate fi considerată ca un cifru cu substituție, iar P-boxa ca un cifru cu permutare, o singură S-boxă sau P-boxă nu asigură rezistență criptografică înaltă. Însă o rețea SP bine proiectată, cu mai multe runde ce conțin S-boxe și P-boxe alternante, satisface proprietățile de confuzie și de difuzie în sens Shannon, care în acest caz, se descriu astfel:

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

- *Difuzie* - dacă se modifică un bit de text clar, atunci acesta este transmis într-o S-boxă a cărei ieșire se va modifica în mai mulți biți, după care, aceste modificări de biți vor fi distribuite prin intermediul P-boxelor către mai multe S-boxe. La ieșirea din fiecare S-boxă se vor obține un anumit număr de biți modificați ș.a.m.d. Efectuând câteva runde, fiecare bit este modificat de câteva ori, iar textul criptat rezultat va fi un șir pseudoaleator. Reciproc, dacă se modifică un bit al textului criptat, atunci încercările de decriptare a textului criptat rezultat vor conduce la un text clar total diferit de textul clar inițial.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

- *Confuzie* – modificarea unui bit al cheii va modifica mai multe chei de rundă și fiecare modificare în cheia de rundă este dispersată printre toți biții, modificând textul criptat într-o manieră pseudoaleatoare.
- Chiar dacă un adversar obține un text clar ce corespunde unui text criptat, confuzia și difuzia fac dificilă problema de recuperare a cheii.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Standardul internațional actual în materie de cifruri bloc cu cheie simetrică, AES (Advanced Encryption Standard), este bazat pe o rețea SP.

De regulă, rețelele SP sunt cifruri bloc iterative, care efectuează calcule repetate succesiv în baza unei funcții interne, numită funcție de rundă. În acest sens, sunt utilizați următorii parametri: numărul de runde r, lungimea în biți n a blocului, lungimea în biți k a cheii secrete K din care sunt derivate r subchei K_i (numite chei de rundă). Pentru a asigura inversabilitatea transformării de criptare (fapt ce permite decriptare unică) este necesar ca pentru fiecare valoare K_i funcția de rundă să fie o bijecție în raport cu input-ul de rundă.

2.3.2.4 Rețeaua Feistel

O alternativă pentru rețeaua substituție-permutare o reprezintă rețeaua Feistel, care, la fel, definește o metodă de construcție a cifrurilor bloc cu proprietăți ce asigură la criptare un grad înalt de confuzie și de difuzie. Fie $f:\{0,1\}^t \to \{0,1\}^t$ o funcție pseudoaleatoare (care dă impresia că cei t biți din imaginea lui f sunt aleși fără nici o regulă).

Textul clar inițial este divizat pe blocuri de lungime fixată n. În cazul în care lungimea ultimului bloc este mai mică ca n, se aplică procedura de padding (de exemplu, se completează ultimul grup de biți cu biți de zero până atunci când lungimea grupului devine egală cu lungimea blocului). În continuare, examinăm operațiile utilizate la prelucrarea unui singur bloc de text clar, întrucât acestea sunt aceleași pentru fiecare bloc.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Blocul de text clar de $2t$ biți ce urmează a fi criptat este divizat în două părți - blocurile L_0 (jumătatea de stânga) și R_0 (jumătatea de dreapta), fiecare de t biți. Rețeaua Feistel este un cifru iterativ ce transformă blocul de text clar pe $2t$ biți (L_0, R_0) în blocul de text criptat (R_r, L_r) pe $2t$ biți, în cadrul unui proces din r runde ($r \geq 1$) de același tip (a se vedea Figura 2.3.3). În cadrul rundei $i \in \{1,...,r\}$, pornind de la subcheia K_i, este transformată perechea (L_{i-1}, R_{i-1}) în (L_i, R_i) în baza relațiilor $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, unde fiecare subcheie K_i este derivată din cheia secretă K a cifrului bloc printr-o procedură de expandare a cheii. Jumătatea de stânga L_{i-1} este supusă unei transformări de substituție în modul următor: este aplicată funcția de rundă f la jumătatea de dreapta R_{i-1} și subcheia K_i, după care, rezultatul obținut $f(R_{i-1}, K_i)$ este combinat printr-un XOR cu

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

jumătatea de stânga L_{i-1}. Ținând cont că după o rundă de criptare jumătatea din dreapta R_{i-1} nu a fost prelucrată (aceasta a fost doar deplasată în jumătatea de stânga), pentru a o cripta este necesară încă o rundă. De regulă, într-o rețea Feistel numărul de runde este $r \geq 3$ și r este un număr par.

Funcția de rundă f are aceeași structură generală pentru fiecare rundă, dar este parametrizată de subcheia de rundă K_i. După realizarea substituției, este aplicată o permutare, care constă în interschimbul celor două jumătăți.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Transformarea Feistel este bijectivă, ceea ce înseamnă, că pornind de la perechea (R_r, L_r), se poate determina (L_0, R_0), procedând analog ca și la procesul de criptare. Astfel, la decriptare este aplicat același algoritm din r runde, în care mesajul de intrare este textul criptat, iar subcheile sunt folosite în ordine inversă, de la K_r la K_1. Ultima rundă este anulată prin simpla repetare a ei. Operațiile efectuate la decriptare sunt: $L_{i-1} := R_i$, $R_{i-1} := L_i \oplus f(R_i, K_i)$, $i = \overline{r,1}$.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Funcția de rundă f a rețelei Feistel poate să fie un cifru compus și nu este necesar ca transformarea f să fie inversabilă, deoarece inversa transformării ce descrie rețeaua Feistel nu depinde de inversabilitatea lui f. De regulă, aplicația f este formată din operații simple, care sunt executate rapid de calculator. Exemple de astfel de operații sunt:

- Permutări de biți (implementate sub forma unor tabele de permutare, numite P-boxe);
- Funcții simple neliniare (implementate sub forma unor tabele de substituție, numite S-boxe);
- Operații liniare (deplasări ciclice de biți, adunări modulo pe biți, multiplicări modulo pe biți, XOR).

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Toate aceste operații pot fi implementate direct pe structuri hardware, ceea ce le face extrem de rapide.

În Figura 2.3.3 sunt ilustrate rundele succesive ale rețelei Feistel, care operează pe jumătăți ale textului parțial criptat.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

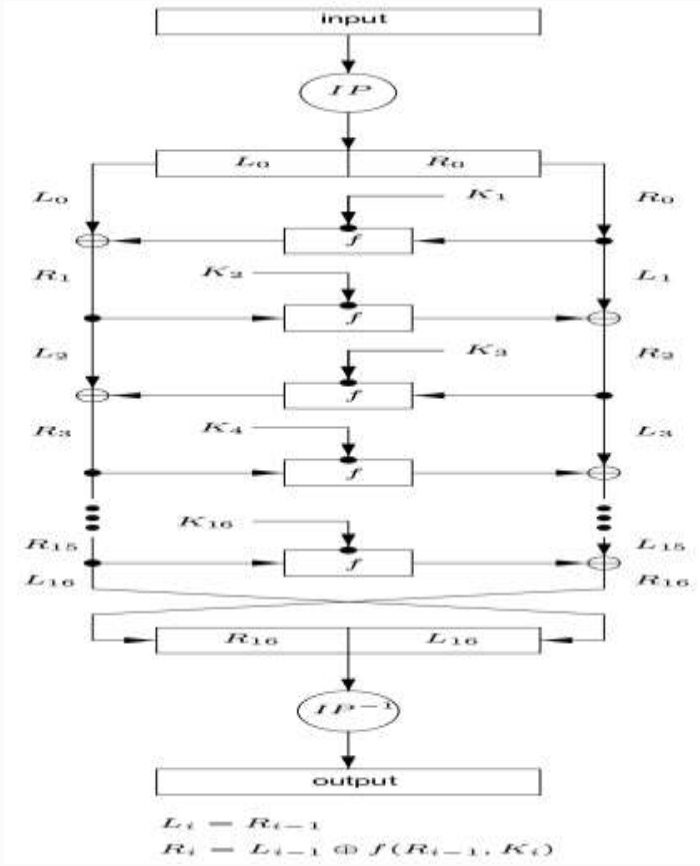

Figura 2.3.3. Rundele succesive ale rețelei Feistel

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Rețelele Feistel apar prima oară în 1971 la sistemul de criptare Lucifer, construit pentru IBM de o echipă condusă de H. Feistel și D. Coppersmith. Succesul a fost asigurat odată cu desemnarea sistemului DES ca standard federal de criptare în SUA.

Ca și rețeaua substituție-permutare, rețeaua Feistel reprezintă o realizare practică a propunerii lui C. Shannon de a dezvolta un cifru compus care să alterneze transformările ce generează confuzie și difuzie. Deși până la rețelele Feistel erau cunoscuți algoritmi de construcție a funcțiilor pseudoaleatoare, nu se știau însă algoritmi de construcție a funcțiilor pseudoaleatoare bijective.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Spre deosebire de rețeaua SP, în care S-boxele trebuie să fie inversabile, în rețeaua Feistel nu sunt impuse astfel de restricții și acestea sunt construite ca și funcții unidirecționale (știind argumentul, se calculează simplu valoarea funcției, dar știind valoarea funcției, este dificil de calculat argumentul corespunzător). Avantajul rețelei Feistel constă în aceea că aceasta realizează în mod similar operațiile de criptare și de decriptare (acestea sunt chiar identice în unele cazuri), ceea ce permite o reducere a dimensiunii codului ce implementează sistemul de criptare.

Dimensiuni mai mari pentru lungimea blocului și a cheii conduc la o rezistență criptografică mai mare a algoritmului, dar reduc din viteza de criptare/decriptare. De regulă, se folosesc dimensiuni de 64 sau 128 de biți pentru lungimea blocului și de 128 sau 256 de biți pentru lungimea cheii.

TRANSFORMĂRI CRIPTOGRAFICE UTILIZATE ÎN CONSTRUCȚIA CIFRURILOR BLOC

Rezistența criptografică a algoritmului definit printr-o rețea Feistel sporește atunci crește numărul de runde efectuate. De regulă, numărul de runde într-o rețea Feistel este de cel puțin 16.

O listă a celor mai cunoscute sisteme de criptare bazate pe rețeaua Feistel cuprinde: Blowfish, Camellia, CAST-128, DES, FEAL, KASUMI, LOKI97, Lucifer, MAGENTA, RC5, RC6, TEA, Triple DES, Twofish, XTEA. După elaborarea și adoptarea sistemului AES (2001) a început o perioadă de regres al structurilor de tip Feistel în construirea sistemelor de criptare.