METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Tema: Cifruri bloc moderne

2.3.3.2 Analiza sistemului de criptare DES

Elementele constitutive ale cifrului DES au fost analizate cu scopul de a măsura rezistența criptografică a unor proprietăți caracteristice cifrului bloc.

2.3.3.2.1 Efectul de avalanșă și de completitudine DES

Orice cifru bloc modern trebuie să satisfacă proprietățile efectului de avalanșă și a efectului de completitudine.

Efectul de avalanșă se manifestă atunci când o modificare mică în biții textului clar (sau ai cheii) generează o modificare semnificativă în biții textului criptat rezultat. În raport cu această proprietate sistemul de criptare DES manifestă o rezistență criptografică remarcabilă.

SISTEMUL DE CRIPTARE DES

Exemplul 2.3.1. Cu scopul de a verifica efectul de avalanșă pentru cifrul DES vom cripta cu aceeași cheie două blocuri de text clar, care diferă doar printr-un singur bit, și vom contoriza numărul de biți distincți la fiecare rundă. Astfel, să considerăm următoarele date, obținute la aplicarea sistemului de criptare DES:

Cheia secretă	$(22234512987ABB23)_{16}$	$(22234512987ABB23)_{16}$
Textul clar	$(0000000000000000)_{16}$	$(4789FD476E82A5F1)_{16}$
Textul criptat	$(0000000000000001)_{16}$	$(0A4ED5C15A63FEA3)_{16}$

Deși blocurile de text clar diferă doar prin ultimul bit, blocurile de text criptat diferă prin 29 de biți:

SISTEMUL DE CRIPTARE DES

$$(4789FD476E82A5F1)_{16} =$$

$$(0100011110001001111111010100011101101110100000101010010111110001)_2,$$

$$(0A4ED5C15A63FEA3)_{16} =$$

$$(0000101001001110110101011100000101011010011000111111111010100011)_2.$$

Astfel, modificarea a circa 1.5 % din blocul de text clar a condus la modificarea a circa 45 % din textul criptat. În Tabelul 2.3.5 sunt prezentate date cu privire la numărul de biţi distincţi la fiecare rundă a cifrului. Din tabel se vede că modificările serioase intervin începând cu runda a treia.

Număr rundă	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Număr biți distincți	1	6	20	29	30	33	32	29	32	39	33	28	30	31	30	29

Tabelul 2.3.5. Numărul de biți distincți în textele criptate de la Exemplul 2.3.1

□

Efectul de completitudine constă în aceea că fiecare bit al textului criptat depinde de mai mulți biți ai textului clar. Difuzia și confuzia generată de către P-boxele și, respectiv, S-boxele DES, demonstrează un grad înalt de manifestare a efectului de completitudine.

2.3.3.2.2 Criteriile de proiectare a cifrului DES

Deși design-ul cifrului DES a fost prezentat oficial de către IBM în 1994, încă de la lansarea sa DES a fost supus unor analize minuțioase, însoțite de obiecții referitoare la S-boxe și P-boxe.

Toate calculele din cadrul algoritmului DES sunt liniare, cu excepția celora din cadrul S-boxelor. Astfel, în mare parte, securitatea sistemului DES se bazează pe acestea. Dar nimeni, cu excepția autorilor, nu știe cum au fost concepute S-boxele. Au fost persoane care erau convinse că ele ascund trape secrete ce le permit celor de la NSA (Agenția Națională de Securitate a SUA) să decripteze orice mesaj.

SISTEMUL DE CRIPTARE DES

În 1976 NSA a reacționat la observațiile făcute și a menționat unele criterii ce au stat la baza construcției S-boxelor DES:

1. Fiecare linie a S-boxei este o permutare a numerelor 0,...,15.
2. Fiecare S-boxă este o funcție neliniară, adică șirul de ieșire nu reperzintă o transformare afină a șirului de intrare.
3. Modificarea unui bit în șirul de la intrare în S-boxă conduce la modificarea a cel puțin doi biți în șirul de la ieșire din S-boxă.
4. Dacă șirurile de intrare $\alpha, \beta \in \{0,1\}^6$ în S-boxa S diferă doar prin biții de pe pozițiile 3 și 4, adică avem $\beta = \alpha \oplus (001100)_2$, atunci șirurile de ieșire $S(\alpha)$ și $S(\beta)$ diferă prin cel puțin doi biți.

SISTEMUL DE CRIPTARE DES

Alte două proprietăți au fost menționate ca fiind „consecințe ale criteriilor de construcție”:

5. Dacă pentru șirurile de intrare $\alpha, \beta \in \{0,1\}^6$ în S-boxa S diferă biții de pe pozițiile 1 și 2 și coincid biții de pe pozițiile 5 și 6, adică avem $\beta = \alpha \oplus (11ab00)_2$, $a, b \in \{0,1\}$, atunci șirurile de ieșire $S(\alpha)$ și $S(\beta)$ sunt distincte.
6. Pentru cele $2^6 = 32$ perechi de șiruri pe 6 biți (x_i, x_j) distincte, $x_i \oplus x_j \neq (000000)_2$, fie (y_i, y_j), $y_i := S(x_i)$, $y_j := S(x_j)$, 32 de perechi de șiruri pe 4 biți de ieșire din S-boxă. Din 32 de valori $d := y_i \oplus y_j$ nu mai mult de 8 vor coincide.

SISTEMUL DE CRIPTARE DES

7. Pentru orice S-boxă S, dacă un bit din șirul de intrare α este menținut constant și se variază arbitrar cu ceilalți 5 biți, urmărind locația șirului de ieșire $S(\alpha)$ corespunzătoare bitului fixat, se obține că numărul rezultat de biți 0 este „apropiat" de numărul de biți 1.

Alte criterii cu privire la S-boxe nu au fost făcute publice.

SISTEMUL DE CRIPTARE DES

În cadrul a două runde consecutive DES, între S-boxe sunt aplicate două transformări de permutare: transformarea de expansiune E (de la 32 la 48 biți) și transformarea de permutare P (de la 32 la 32 biți). Transformările E și P generează difuzia biților. La proiectarea P-boxelor s-a ținut cont de următoarele criterii:

1. Pentru fiecare S-boxă de la runda curentă șirul de la intrarea acesteia provine de la ieșirea altei S-boxe de la runda precedentă.
2. Cei 4 biți de la ieșirea din S-boxă în runda curentă sunt propagați către S-boxe distincte în runda următoare (fiecare doi biți sunt transmiși către S-boxe distincte).

SISTEMUL DE CRIPTARE DES

3. Dacă S-boxele sunt notate prin $S_1, \ldots, S_8$, atunci avem:

   a) Un bit de la ieșirea S-boxei S_{j-2} este direcționat către unul din primii doi biți ai lui S_j în runda următoare.

   b) Un bit de la ieșirea S-boxei S_{j-1} este direcționat către unul din ultimii doi biți ai lui S_j în runda următoare.

   c) Un bit de la ieșirea S-boxei S_{j+1} este direcționat către unul din doi biți de mijloc ai lui S_j în runda următoare.

SISTEMUL DE CRIPTARE DES

4. Pentru fiecare S-boxă doi biți de ieșire sunt direcționați către primii doi sau ultimii doi biți de intrare într-o S-boxă de la runda următoare. Ceilalți doi biți de ieșire sunt direcționați către biții de mijloc(3 și 4) de la intrarea în S-boxa de la runda următoare.
5. Dacă un bit de ieșire din S-boxa S_j este direcționat către unul din biții de mijloc de la intrarea în S_k (la runda următoare), atunci un bit de ieșire din S-boxa S_k nu poate să fie direcționat către un bit de mijloc de la intrarea în S_j la runda următoare. Dacă $j = k$, atunci nici unul din biții de mijloc ai unei S-boxe nu va fi direcționat către unul din biții de mijloc ai aceleași S-boxe de la runda următoare.

SISTEMUL DE CRIPTARE DES

Cea mai importantă observație față de cifrul DES se referă la dimensiunea mică de numai 2^{56} a spațiului de chei. În consecință, au fost construite mai multe mașini ce realizează eficient atacul prin forță brută. Pentru un bloc de text clar x pe 64 biți și blocul de text criptat corespunzător y, se verifică toate variantele de cheie secretă K (aproximativ 2^{55}), până se satisface condiția $E_K(x) = y$. De remarcat, că soluția există întotdeauna, dar poate să nu fie unică.

SISTEMUL DE CRIPTARE DES

Cifrul DES constă din 16 runde ale rețelei Feistel. De fapt, a fost arătat că după 8 runde, textul criptat obținut reprezintă o funcție de la fiecare bit al textului clar și fiecare bit al cheii secrete. Altfel spus, textul criptat este o funcție aleatoare de la textul clar și cheia secretă. Cu toate că s-ar părea că opt runde DES sunt suficiente pentru o criptare sigură, experimentele au arătat că variantele DES cu mai puțin de 16 runde sunt ceva mai vulnerabile în fața atacurilor analitice cu text clar cunoscut în raport cu atacul prin forță brută.

În mare parte, metodele analitice de criptanaliză elaborate (de exemplu, criptanaliza diferențială sau criptanaliza liniară) au fost testate pe exemplul sistemului de criptare DES.

2.3.3.2.3 Vulnerabilități ale cifrului DES

Vom menționa câteva vulnerabilități depistate la cifrul DES.

2.3.3.2.3.1 Vulnerabilități în proiectarea cifrului

Sunt cunoscute cel puțin trei vulnerabilități ale S-boxelor:

1. În S-boxa S_4 ultimii trei biți de ieșire pot fi obținuți în același mod ca și primul bit de ieșire, adică prin complementarea unor biți de intrare.
2. Două intrări special alese pentru un tabel de substituție corespunzător unei S-boxe, pot să genereze aceeași ieșire.
3. Este posibil să se obțină aceeași ieșire într-o singură rundă prin modificarea biților în trei S-boxe adiacente.

SISTEMUL DE CRIPTARE DES

În ceea ce privește design-ul P-boxelor, sunt două observații:

1. Nu este clar pentru ce autorii cifrului DES au folosit permutarea inițială și cea finală, deoarece acestea nu aduc careva beneficii de securitate.
2. În permutarea de expansiune E se repetă primul și al patrulea bit al fiecărui șir de patru biți.

SISTEMUL DE CRIPTARE DES

2.3.3.2.3.2 Vulnerabilități în cheia secretă

La fel au fost stabilite câteva vulnerabilități în legătură cu cheia secretă DES.

2.3.3.2.3.2.1 Lungimea cheii secrete

Cea mai serioasă vulnerabilitate DES o reprezintă lungimea mică de 56 de biți a cheii secrete. Pentru a realiza atacul prin forță brută se vor examina cel mult 2^{56} variante de chei.

a) Tehnologiile moderne permit să se verifice circa un milion de chei pe secundă. Aceasta înseamnă cu sunt necesari mai mult de 2000 ani pentru a realiza atacul prin forță brută în baza unui calculator cu un singur procesor.

SISTEMUL DE CRIPTARE DES

b) Dacă am construi un calculator cu un milion de chip-uri (pentru procesare paralelă), atunci am putea să verificăm toți pretendenții din spațiul de chei în circa 20 de ore. Când DES a fost introdus, costul unui astfel de calculator era de câteva milioane de dolari. Odată cu dezvoltarea tehnologiilor, a scăzut rapid și costul de construcție a unui astfel de supercalculator. Un calculator special pentru spargerea cifrului DES prin forță brută a fost construit în 1998. Acesta a găsit cheia secretă în circa 112 ore.

c) Se știe că rețelele de calculatoare pot să simuleze procesarea paralelă. În 1977 o echipă de cercetători (RSA Laboratories) au folosit 3500 de calculatoare pentru a găsi cheia secretă în 120 de zile. Spațiul de chei a fost partajat între calculatoarele rețelei, astfel încât fiecare calculator prelucra o anumită porțiune a acestuia.

d) Un grup de utilizatori din 42000 de membri pot să afle cheia secretă DES în 10 zile.

SISTEMUL DE CRIPTARE DES

2.3.3.2.3.2.2 Chei slabe DES

Dacă cheile de rundă satisfac condiția $K_1 = K_{16}$, atunci algoritmul de expandare a cheii va genera un șir de subchei cu proprietatea $K_i = K_{17-i}$, $i = \overline{1,8}$. Acestea sunt numite chei slabe.

Definiția 2.3.1. Cheie slabă (numită și cheie palindromică) DES este o cheie secretă K ce satisface proprietatea $E_K\left(E_K\left(x\right)\right) = x$ pentru orice bloc de text clar x (E_k definește o involuție). O pereche de chei DES $\left(K^1, K^2\right)$ este numită pereche de chei semi-slabe DES dacă se satisface condiția $E_{K^1}\left(E_{K^2}\left(x\right)\right) = x$.

SISTEMUL DE CRIPTARE DES

Textul criptat cu una din cheile perechii de chei semi-slabe poate fi decriptat cu cealaltă cheie.

Sistemul de criptare DES are 4 chei slabe și 6 perechi de chei semi-slabe. Probabilitatea ca să se aleagă aleator o cheie slabă sau semi-slabă este de aproximativ 2^{-52}. Uneori se solicită un test pentru stabilirea cheilor slabe, care nu afectează semnificativ timpul de criptare.

În Tabelul 2.3.6 sunt prezentate cele 4 chei slabe DES împreună cu variabilele corespunzătoare C_0 și D_0 pe 28 de biți din *Algoritmul de expandare a cheii DES*. Am notat prin $\{0\}^{28}$ șirul format din 28 biți de 0, iar prin $\{1\}^{28}$ - din 28 biți de 1. Deoarece C_0 și D_0 sunt șiruri cu toți biții zero sau cu toți biții 1, iar rotația acestora nu are efect, rezultă că toate subcheile K_i coincid, ceea ce conduce la o involuție.

SISTEMUL DE CRIPTARE DES

De regulă, octeții se reprezintă în format hexazecimal. Astfel, fiecare din cele două secvențe succesive de câte 4 biți (numite nibble-uri) din cadrul octetului este notată printr-un singur simbol hexazecimal (a se vedea *Tabelul 2.3.6*), iar octetul se reprezintă prin două simboluri în hexazecimal.

SISTEMUL DE CRIPTARE DES

Secvența de biți	Caracter hexazecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

Tabelul 2.3.6 Reprezentarea nibble-ului în hexazecimal

SISTEMUL DE CRIPTARE DES

Astfel, elementul $(01100011)_2$ se reprezintă sub forma $(63)_{16}$.

Cheile slabe (în hexazecimal)	C_0	D_0
0101010101010101	$\{0\}^{28}$	$\{0\}^{28}$
fefefefefefefefe	$\{1\}^{28}$	$\{1\}^{28}$
1f1f1f1f0e0e0e0e	$\{0\}^{28}$	$\{1\}^{28}$
e0e0e0e0f1f1f1f1	$\{1\}^{28}$	$\{0\}^{28}$

Tabelul 2.3.7. Patru chei slabe DES

SISTEMUL DE CRIPTARE DES

În Tabelul 2.3.7 sunt prezentate cele 6 perechi de chei semi-slabe DES. Cheile secrete K^1 și K^2 sunt semi-slabe atunci când subcheile de rundă $K_1^1,...,K_{16}^1$ formate în baza cheii secrete K^1 coincid corespunzător cu subcheile de rundă $K_{16}^2,...,K_1^2$ formate în baza cheii secrete K^2. Pentru a se satisface aceste condiții este necesar ca rotația circulară la stânga cu 1 bit a fiecăruia dintre șirurile C_0 și D_0, asociate cheii K^1 pe 56 de biți, să coincidă, respectiv, cu perechea (C_0, D_0) asociată cheii K^2 pe 56 biți. La fel, rotația circulară la stânga cu 1 sau 2 biți a șirurilor C_i și D_i asociați cheii K^1, trebuie să coincidă cu valorile corespunzătoare obținute prin rotația ciclică la dreapta cu 1 sau 2 biți a șirurilor asociate cheii K^2. Valorile din Tabelul 2.3.8 satisfac aceste condiții. Fiind dată o cheie semi-slabă K^1 pe 64 biți, se poate determina cheia K^2 asociată acesteia, prin divizarea în două jumătăți a șirului ce reprezintă cheia K^1 și rotația ciclică cu 8 biți a fiecărei jumătăți.

SISTEMUL DE CRIPTARE DES

C_0	D_0	perechi de chei semi-slabe (în hexazecimal)	C_0	D_0
$\{01\}^{14}$	$\{01\}^{14}$	*01fe01fe01fe01fe , fe01fe01fe01fe01*	$\{10\}^{14}$	$\{10\}^{14}$
$\{01\}^{14}$	$\{10\}^{14}$	*1fe01fe00ef10ef1 ,.... e01fe01ff10ef10e*	$\{10\}^{14}$	$\{01\}^{14}$
$\{01\}^{14}$	$\{0\}^{28}$	*01e001e001f101f1 , e001e001f101f101*	$\{10\}^{14}$	$\{0\}^{28}$
$\{01\}^{14}$	$\{1\}^{28}$	*1ffe1ffe0efe0efe ,.... fe1ffe1ffe0efe0e*	$\{10\}^{14}$	$\{1\}^{28}$
$\{0\}^{28}$	$\{01\}^{14}$	*011f011f010e010e ,.... 1f011f010e010e01*	$\{0\}^{28}$	$\{10\}^{14}$
$\{1\}^{28}$	$\{01\}^{14}$	*e0fee0fef1fef1fe , fee0fee0fef1fef1*	$\{1\}^{28}$	$\{10\}^{14}$

Tabelul 2.3.8. Șase perechi de chei semi-slabe DES (o pereche per linie)

SISTEMUL DE CRIPTARE DES

Fie E notația pentru algoritmul de criptare DES. Pentru fiecare din cele 4 chei slabe DES K există 2^{32} puncte fixe ale transformării E_K, adică blocuri de text clar x ce satisfac proprietatea $E_K(x) = x$. La fel, 4 din cele 12 chei semi-slabe K (acestea se află în partea superioară din Tabelul 2.3.7), au câte 2^{32} puncte anti-fixe, adică blocuri de text clar x astfel încât $E_K(x) = \overline{x}$ ($\overline{x}$ este șirul de biți obținut prin negarea fiecărui bit din x). Aceste 4 chei semi-slabe mai sunt numite și chei anti-palindromice, deoarece subcheile de rundă asociate sunt complementare: $K_1 = \overline{K_{16}}, K_2 = \overline{K_{15}}, \ldots$.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Istoria cifrului bloc DES nu s-a încheiat la retragerea calificativului de standard de criptare acestuia. Cifruri bloc ce reprezintă variante avansate ale lui DES sunt utilizate și în prezent. De exemplu, sistemul de criptare Triple DES (în română, Triplu DES) rămâne până în prezent un standard federal.

Pe parcursul anilor au fost propuse mai multe modalități de amplificare a securității DES, bazate pe modificarea componentelor algoritmului sau pe utilizarea DES în anumite construcții hibrid. În continuare, ne vom referi la unele din aceste construcții, care oferă alternative acceptabile în raport cu algoritmul original DES.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Sistemul de criptare Triple DES (3DES)

3DES sau Triple DES este un cifru bloc propus de către W. Tuchman și W. Diffie, M. Hellman, și este format în baza lui DES prin aplicarea acestuia de trei ori. Denumirea oficială a algoritmului utilizată în standarde este TDEA sau Triple DEA (Triple Data Encryption Algorithm). Atunci când s-a constatat că lungimea cheii pe 56 biți, utilizată de către DES, nu este suficientă pentru a proteja datele în fața atacurilor prin forță brută, 3DES a fost propus ca o modalitate simplă pentru a extinde lungimea cheii până la 168 biți, fără a fi necesară implicarea unui alt algoritm. Aplicarea a trei criptări DES este esențială pentru a evita atacul meet-in-the-middle (pe care îl vom examina în cadrul cursului de Criptanaliză), care este eficient în cazul criptării de două ori cu DES.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

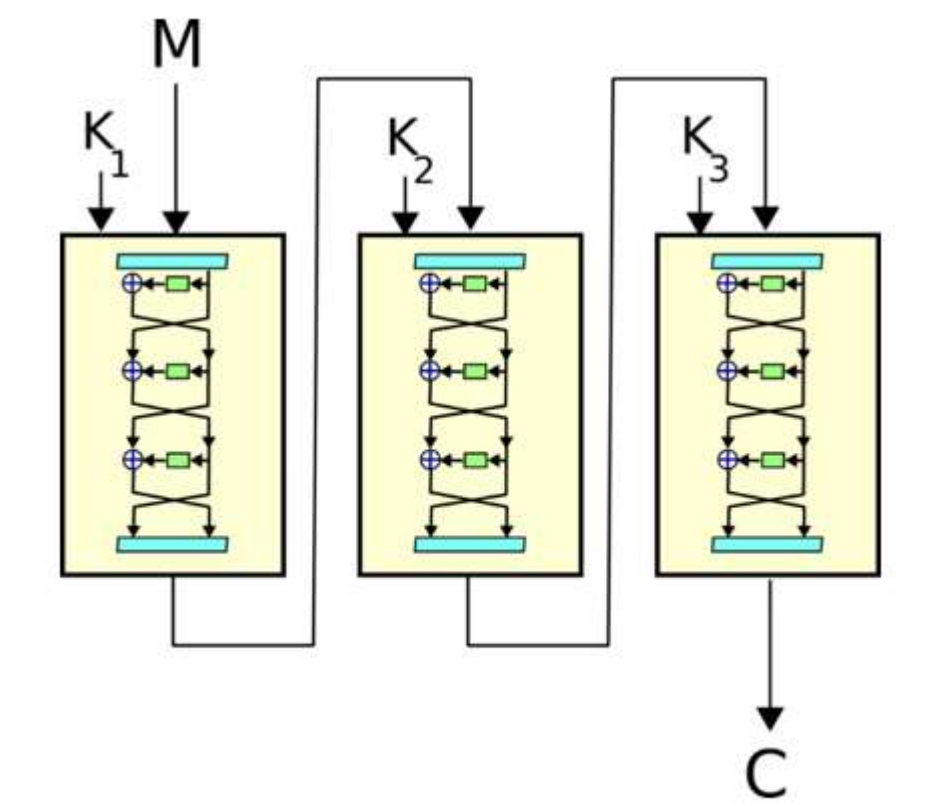

Figura 2.3.10. Algoritmul de criptare 3DES

SISTEME DE CRIPTARE ÎNRUDITE CU DES

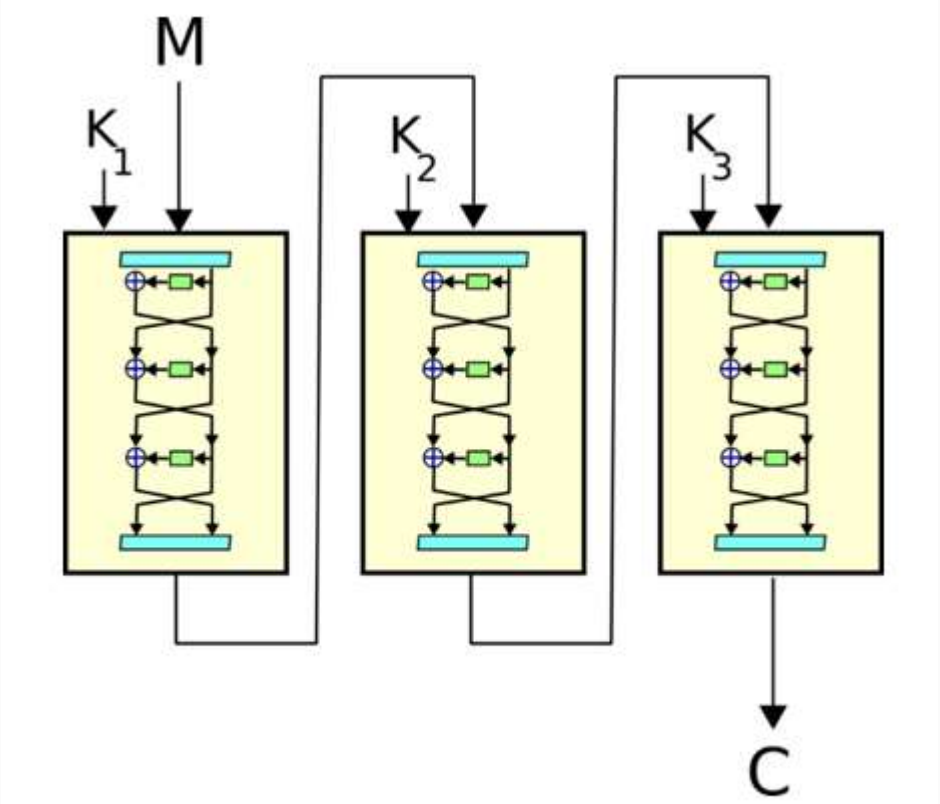

Figura 2.3.10. Algoritmul de criptare 3DES

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Schema standard 3DES este de forma $c = DES\left(k_3, DES\left(k_2, DES\left(k_1, m\right)\right)\right)$, unde k_1, k_2, k_3 sunt trei chei DES pe 56 biți fiecare, m un bloc de text clar pe 64 biți, iar c - blocul corespunzător de text criptat (a se vedea Figura 2.3.10). Viteza de criptare a lui 3DES este de 3 ori mai mică în raport cu DES, dar în schimb rezistența criptografică este cu mult mai mare. Astfel, 3DES reprezintă o modalitate simplă prin care se elimină vulnerabilitățile algoritmului DES.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

În practică pot fi utilizate trei variante ale algoritmului 3DES:

- DES-EEE3: Se criptează de 3 ori cu 3 chei diferite:

$$\text{Criptarea: } c = E_{k_3}\left(E_{k_2}\left(E_{k_1}(m)\right)\right),$$

$$\text{Decriptarea: } m = E_{k_1}^{-1}\left(E_{k_2}^{-1}\left(E_{k_3}^{-1}(c)\right)\right).$$

- DES-EDE3: Se efectuează o criptare DES, urmată de o decriptare DES și încă o criptare DES, cu 3 chei diferite:

$$\text{Criptarea: } c = E_{k_3}\left(E_{k_2}^{-1}\left(E_{k_1}(m)\right)\right),$$

$$\text{Decriptarea: } m = E_{k_1}^{-1}\left(E_{k_2}\left(E_{k_3}^{-1}(c)\right)\right).$$

Introducerea la pasul doi a transformării de decriptare, nu afectează securitatea algoritmului.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

- DES-EEE2 și DES-EDE2: Aceste variante sunt analoage precedenților 2 algoritmi, doar că operațiile 1 și 3 folosesc aceeași cheie. De exemplu, pentru DES-EDE2 avem:

$$\text{Criptarea: } c = E_{k_1}\left(E_{k_2}^{-1}\left(E_{k_1}(m)\right)\right).$$

$$\text{Decriptarea: } m = E_{k_1}^{-1}\left(E_{k_2}\left(E_{k_1}^{-1}(c)\right)\right).$$

Varianta cea mai populară este DES-EDE3. Cheile pentru cele trei etape pot fi alese astfel:

- k_1, k_2, k_3 sunt independente.
- k_1, k_2 sunt independente, iar $k_1 = k_3$.
- $k_1 = k_2 = k_3$.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Cea mai sigură variantă este atunci când toate trei chei sunt independente, deoarece lungimea cheii este de $3 \times 56 = 168$ biți. Pentru varianta a doua lungimea cheii este de $2 \times 56 = 112$ biți. În ceea ce privește siguranța, a treia variantă este echivalentă cu DES (lungimea cheii este de 56 biți) și nu este recomandată utilizarea acesteia.

Sistemul de criptare 3DES nu a fost spart, dar utilizarea sa practică este anevoioasă din cauza vitezei mici de criptare. Cu toate acestea, până relativ nu demult, cardurile bancare Mastercard erau configurate pe baza acestui sistem de criptare. De asemenea, sistemul de telefonie mobilă Zapp folosește 3DES ca sistem de criptare.

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Sistemul de criptare DES-X

DES-X reprezintă o altă variantă a sistemului de criptare DES dezvoltată pentru a rezista mai bine în fața unui atac prin forță brută, folosind tehnica key whitening.

Deoarece DES operează cu o cheie pe 56 biți, spațiul de chei conține 2^{56} elemente, unele elemente fiind chei slabe. Pentru a evita un atac direct, în anul 1984 R. Rivest a propus extinderea lungimii cheii K fără a modifica substanțial algoritmul DES.

Algoritmul DES-X folosește două chei suplimentare K_1, K_2 de câte 64 biți fiecare. Înainte de a aplica algoritmul DES, acesta combină printr-un XOR cei 64 biți ai cheii K_1 cu blocul de text clar m, iar după aplicarea DES cu cheia K, rezultatul se combină printr-un XOR cu cheia K_2:

$$DES\text{-}X(m) = K_2 \oplus DES_K(m \oplus K_1).$$

SISTEME DE CRIPTARE ÎNRUDITE CU DES

SISTEME DE CRIPTARE ÎNRUDITE CU DES

Astfel, lungimea totală a cheii devine $56+2\times64=184$ biți, deși experimentele au arătat că lungimea efectivă este de circa 119 biți.

DES-X amplifică rezistența algoritmului DES față de atacul prin criptanaliză diferențială sau prin criptanaliză liniară. Pentru un atac cu succes asupra lui DES-X, criptanaliza diferențială va necesita 2^{61} texte clare cunoscute (pentru DES sunt necesare 2^{47} texte clare), iar criptanaliza liniară - 2^{60} texte clare (pentru DES - 2^{43}) .

Există, la fel, o altă variantă a algoritmului DES-X, în care în loc de operațiile XOR este utilizată operația de adunare modulo 2^{64}.

Viteza algoritmului DES-X este aproximativ egală cu viteza lui DES.