Seminar 4 - 20 martie 2024

Rețele Feistel - stau la baza lui DES

Ex#1 Plaintext: 100110110111

Funcția F dată de: Litera 1 → Litera 3
Litera 2 → Litera 1
Litera 3 → Litera 2

Construiți o rețea Feistel cu trei runduri.

Dem

Algoritmul principal (care se repetă de un număr specificat de ori) este dat de:

PAS 1: Textul inițial se împarte în două părți L_0 și R_0

PAS 2: R_0 se codează folosind $F(R_0)$.

PAS 3: $L_1 = R_0$ și $R_1 = L_0 \oplus F(R_0)$.

PAS 4: Se concatenează L_1 și R_1 pentru a obține rezultatul.

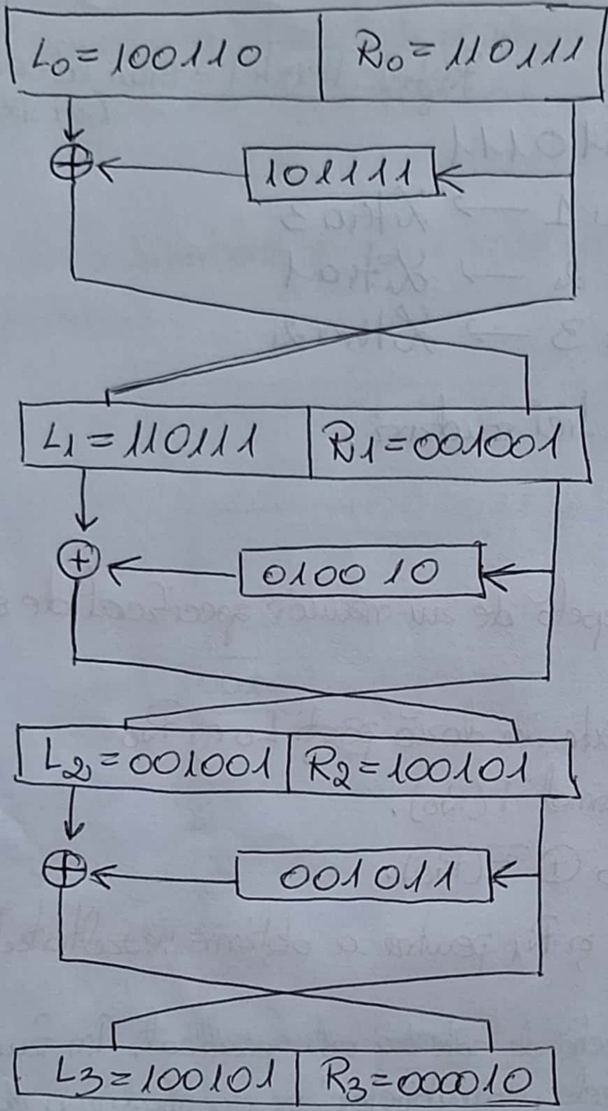
OBS 1: Algoritmul de mai sus se repetă de câte ori este specificat. În funcție de nivelul la care vă aflați, indicele „variabilelor" se va modifica ca atare.

OBS 2: Structura funcției F poate fi dată din problemă. Dacă nu se specifică, atunci inventați voi un algoritm pentru funcția F. În cazul nostru, problema ne spune cum se comportă F, deci doar trebuie aplicat pe datele pe care le avem.

OBS 3 DES conține 16 niveluri / nivele de tip Feisel.

DES = Data Encryption Standard

CamScanner



$L_0 = 100110$

$R_0 = 110111$

$F_1(R_0) = 101111$

$R_1 = F_1(R_0) \oplus L_0$

$R_1 = 001001$

$F_2(R_1) = 010010$

$R_2 = F_2(R_1) \oplus L_1$

$R_2 = 100101$

$F_3(R_2) = 001011$

$R_3 = F_3(R_2) \oplus L_2$

$R_3 = 000010$

Ciphertext: $L_3R_3 = 100101\,000010$

□

$\boxed{\text{Ex \#2}}$ Ciphertext: $L_3R_3 = 100101000010$

Se consideră funcția F ca în problema anterioară. Se știe că textul cifrat/codat este rezultat de pe urma unei rețele Feistel cu trei runduri.

Se cere textul inițial.

Dem.

Cel mai ușor mod de a efectua decriptarea este să

→ luăm textul criptat

→ îl spargem în două părți (în cazul nostru L_3 și R_3)

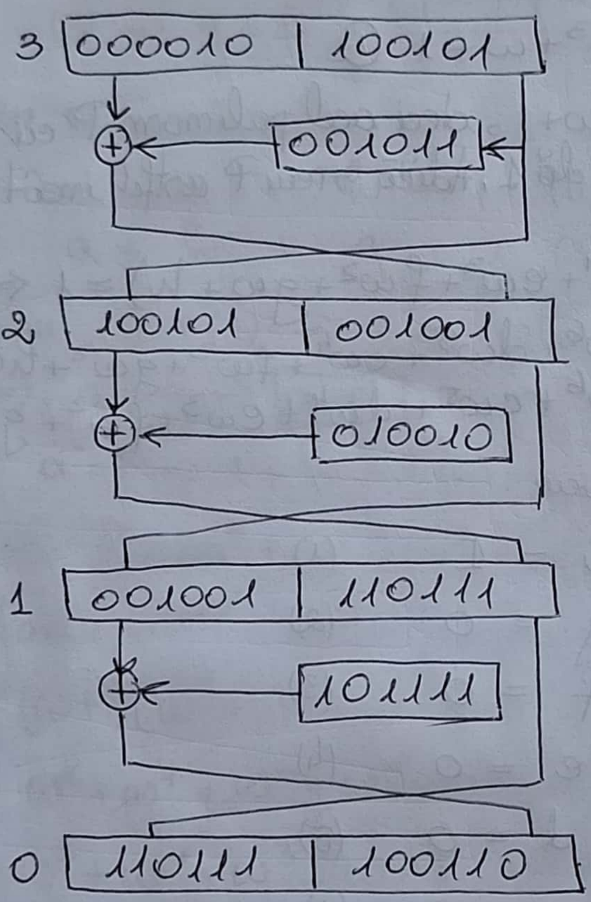
→ schimbăm pozițiile între ele

→ apl. alg. de criptare și schimbăm cele 2 bucăți de cod între ele la sf.

Inițial avem 100101000010.
Știm că s-a format de pe schema unui Feistel cu 3 niveluri.
Spargem în $L_3 = 100101$

$R_3 = 000010$

Le schimbăm pozițiile între ele și realizăm o rețea care respectă algoritmul



Schimbăm, acum, iar pozițiile celor două bucăți de mesaj și găsim textul în clar care a fost transmis inițial.

<u>Plaintext</u>: 100110110111 $= L_0R_0$

□

$\boxed{\text{Ex \#3}}$ La momentul în care algoritmul AES realizează operația S-Box (SubBytes), trebuie să se calculeze inversul elementului $x = \omega+1$. Aflați care este acesta.

Dem
ano

Din teorie, știm că aritmetica din $\mathbb{F}_{256}$ este dată de polinomul ireductibil

$$X^8+X^4+X^3+X+1$$

peste $\mathbb{F}_2$.

Așadar, dacă ω este soluție a polinomului de mai sus, putem scrie

$$\omega^8+\omega^4+\omega^3+\omega+1=0 \Leftrightarrow$$
$$\omega^8=\omega^4+\omega^3+\omega+1 \quad (1)$$

Căutăm inversul lui $x=\omega+1$, deci acel polinom P cu $\deg(P)\leq 7$ care înmulțit cu $x=\omega+1$ ne dă 1. Adică vrem P astfel încât $xP=1$.
Scriem

$$(\omega+1)(a\omega^7+b\omega^6+c\omega^5+d\omega^4+e\omega^3+f\omega^2+g\omega+h)=1 \Leftrightarrow$$
$$a(\omega^4+\omega^3+\omega+1)+b\omega^7+c\omega^6+d\omega^5+e\omega^4+f\omega^3+g\omega^2+h\omega+$$
$$+a\omega^7+b\omega^6+c\omega^5+d\omega^4+e\omega^3+f\omega^2+g\omega+h=1$$

Facem identificările și avem

$$a+h=1 \quad (1)$$
$$a+h+g=0 \quad (2)$$
$$g+f=0 \quad (3)$$
$$a+f+e=0 \quad (4)$$
$$a+e+d=0 \quad (5)$$
$$d+c=0 \quad (6)$$
$$c+b=0 \quad (7)$$
$$a+b=0 \quad (8)$$

Dacă sumăm egalitățile (5) - (8) găsim

$$2a+2b+2c+2d+e=0 \Leftrightarrow \boxed{e=0}$$

Din (5) $\Rightarrow a=d$
(6) $\Rightarrow d=c$
(7) $\Rightarrow b=c$

$$\left.\begin{array}{l} a=d \\ d=c \end{array}\right\} \Rightarrow a=c=d,\quad b=c \;\Rightarrow \boxed{a=b=c=d}$$

Rescriem, acum, egalitățile (1) – (4)

$$a + b = 1 \quad (1)$$
$$a + b + g = 0 \quad (2)$$
$$g + f = 0 \quad (3)$$
$$a + f = 0 \quad (4)$$

Din $(4) \Rightarrow a = f$, $(3) \Rightarrow g = f$ $\Rightarrow \boxed{a = f = g}$ (*)

Deci rămânem cu

$$a + b = 1 \quad (1)$$
$$a + b + g = 0 \quad (2)$$

Facem $(1) + (2) \Rightarrow 2a + 2b + g = 1 \Leftrightarrow \boxed{g = 1}$

Din (*), $a = g \Rightarrow \boxed{a = 1}$

Dacă $a = 1 \Rightarrow 1 + b = 1 \Leftrightarrow \boxed{b = 0}$ și deci

$$P = \omega^7 + \omega^6 + \omega^5 + \omega^4 + \omega^2 + \omega$$

Dacă facem verificările, observăm că

$$\pi P = (\omega+1)(\omega^7 + \omega^6 + \omega^5 + \omega^4 + \omega^2 + \omega) =$$
$$= \omega^8 + \cancel{\omega^7} + \cancel{\omega^6} + \cancel{\omega^5} + \omega^3 + \cancel{\omega^2} + \cancel{\omega^7} + \cancel{\omega^6} + \cancel{\omega^5} + \omega^4 + \cancel{\omega^2} + \omega =$$
$$= \omega^8 + \omega^4 + \omega^3 + \omega = 1 \quad (\text{din } (1))$$

Așadar, $\pi^{-1} = P$.

□

Ex#4 Explicați de ce operațiile ShiftRows și MixColumns (ca operații ce conțin matrice circulante) pot fi definite ca produs de polinoame modulo X^4+1.

Teorie: O matrice circulantă C, $n \times n$, are forma

$$C = \begin{bmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \ddots & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ c_{n-2} & & & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{bmatrix}$$

CamScanner

sau transpusa ei, în funcție de notațiile folosite. Când termenul C_i este o matrice $p \times p$, atunci matricea C de dimensiune $mp \times mp$ se numește matrice bloc-circulantă.

OBS O matrice circulantă este pe deplin descrisă de un vector c care apare ca fiind prima coloană (sau linie) din C. Restul coloanelor (și respectiv a liniilor) sunt permutări ciclice ale vectorului c.

Polinomul

$$f(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

se numește polinomul asociat matricei C.

Dem

Din teorie știm că lucrăm cu cuvinte care se identifică cu polinoame de grad cel mult 3 din $\mathbb{F}_{256}[X]$.

Așadar, considerăm următoarea multiplicare de polinoame

$$P = b_0 + b_1 X + b_2 X^2 + b_3 X^3 =$$

$$= (a_0 + a_1 X + a_2 X^2 + a_3 X^3)(c_0 + c_1 X + c_2 X^2 + c_3 X^3) \mod (X^4+1)$$

Facem calculele și avem

$$P = a_0 c_0 + (a_0 c_1 + a_1 c_0) X + (a_0 c_2 + a_1 c_1 + a_2 c_0) X^2 +$$
$$+ (a_3 c_0 + a_2 c_1 + a_1 c_2 + a_0 c_3) X^3 +$$
$$+ (a_1 c_3 + a_2 c_2 + a_3 c_1) X^4 + (a_2 c_3 + a_3 c_2) X^5 +$$
$$+ a_3 c_3 X^6 \mod (X^4+1)$$

Să observăm că dacă $X^4+1=0$ avem $X^4 = 1$, ie
$X^5 = X$ și
$X^6 = X^2$ deci

$$P = (a_0 c_0 + a_1 c_3 + a_2 c_2 + a_3 c_1) +$$
$$+ (a_0 c_1 + a_1 c_0 + a_2 c_3 + a_3 c_2) X +$$
$$+ (a_0 c_2 + a_1 c_1 + a_2 c_0 + a_3 c_3) X^2 +$$
$$+ (a_0 c_3 + a_1 c_2 + a_2 c_1 + a_3 c_0) X^3 \mod (X^4+1)$$

CamScanner

Matriceal avem

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

□

$\boxed{\text{EX\#5}}$ Operația MixColumns din AES presupune înmulțirea matricei stărilor cu matricea

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Operația are loc în $\mathcal{M}(4\times4;\mathbb{F}_{256})$. Arătați că în timpul decriptării, MixColumns presupune înmulțirea matricei de stare cu matricea

$$N = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}$$

tot în $\mathcal{M}(4\times4;\mathbb{F}_{256})$.

Dem

Ce trebuie să arătăm de fapt este că $N = M^{-1}$.

Evident putem arăta că $NM = I_4$ prin calcul direct. Din păcate, deoarece lucrăm în $\mathbb{F}_{256}$, calculele vor fi foarte urâte. Vom apela la altă metodă.

Știm că → în cazul AES, identificăm cuvintele cu polinoame
↳ aritmetica din $\mathbb{F}_{256}$ este dată de $X^8+X^4+X^3+X+1$

Pornind de la matricea M, identificăm elementele

$$\begin{cases} 1 = 10 = 1 \\ 2 = 01 = \omega \\ 3 = 11 = 1+\omega \end{cases}$$

$1 = 1$

$2 = 10 = \omega$

$3 = 11 = \omega + 1$

← binar, dar scris invers, ne arată gradul termenilor polinomului de la cel mai mare la cel mai mic

Uitându-ne la cea de-a doua matrice, găsim

$14 = 0111 = \omega + \omega^2 + \omega^3$

$13 = 1011 = 1 + \omega^2 + \omega^3$

$11 = 1101 = 1 + \omega + \omega^3$

$9 = 1001 = 1 + \omega^3$

OBS De două transformăm în binar și scrie invers, iar polinomul se scrie de la puterea cea mai mare la cea mai mică.

Și acum facem înmulțirea matricelor, dar cu identificarea făcută mai sus. Avem

$R_1^M \cdot C_1^N$:

$2\cdot 14 + 3\cdot 9 + 1\cdot 13 + 1\cdot 11 =$

$= \omega(\omega+\omega^2+\omega^3) + (\omega+1)(1+\omega^3) + \cancel{1}+\omega^2+\cancel{\omega^3}+\cancel{1}+\omega+\cancel{\omega^3} =$

$= \cancel{\omega^2}+\cancel{\omega^3}+\cancel{\omega^4}+\cancel{\omega}+\cancel{\omega^4}+1+\cancel{\omega^3}+\cancel{\omega^2}+\cancel{\omega} = 1$

$R_1^M \cdot C_2^N$:

$2\cdot 11 + 3\cdot 14 + 1\cdot 9 + 1\cdot 13 =$

$= \omega(1+\omega+\omega^3) + (\omega+1)(\omega+\omega^2+\omega^3) + \cancel{1}+\cancel{\omega^3}+\cancel{1}+\omega^2+\cancel{\omega^3} =$

$= \cancel{\omega}+\cancel{\omega^2}+\cancel{\omega^4}+\cancel{\omega^2}+\cancel{\omega^3}+\cancel{\omega^4}+\cancel{\omega}+\cancel{\omega^2}+\cancel{\omega^3}+\cancel{\omega^2} =$

$= 0$

$R_1^M \cdot C_3^N$:

$2\cdot 13 + 3\cdot 11 + 1\cdot 14 + 1\cdot 9 =$

$= \omega(1+\omega^2+\omega^3) + (\omega+1)(1+\omega+\omega^3) + \omega+\omega^2+\cancel{\omega^3}+1+\cancel{\omega^3} =$

$= \cancel{\omega}+\cancel{\omega^3}+\cancel{\omega^4}+\cancel{\omega}+\cancel{\omega^2}+\cancel{\omega^4}+\cancel{1}+\cancel{\omega}+\cancel{\omega^3}+\cancel{\omega}+\cancel{\omega^2}+\cancel{1} =$

$= 0$

$R_1^M \cdot C_4^N$:

$2\cdot 9 + 3\cdot 13 + 1\cdot 11 + 1\cdot 14 =$

$= \omega(1+\omega^3) + (\omega+1)(1+\omega^2+\omega^3) + 1 + \cancel{\omega} + \cancel{\omega^3} + \cancel{\omega} + \omega^2 + \cancel{\omega^3} =$

$= \cancel{\omega} + \cancel{\omega^4} + \cancel{\omega} + \cancel{\omega^3} + \cancel{\omega^4} + \cancel{1} + \cancel{\omega^2} + \cancel{\omega^3} + \cancel{1} + \cancel{\omega^2} =$

$= 0$

Datorită structurii circulare, observăm că ne putem opri aici cu calculele, deoarece, restul înmulțirilor /sumelor sunt identice cu cele calculate mai sus. Am găsit deci că

$$MN = I_4,$$

Prin urmare, $N = M^{-1}$ așa cum am dorit.

$\square$

$\boxed{\text{Ex \#6}}$ Găsiți o formulă pentru partea de multiplicare matriceală pentru operația SubBytes care se poate scrie într-o singură linie.

Dem

Avem următorul produs matriceal

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}$$

Observăm că indicii sunt de la 0 la 7, i.e fix resturile împărțirii la 8 => IDEE calcul modulor mod 8 pentru indici

Încercăm să găsim o formulă care să descrie operația de mai sus

$y_0 = x_0 + x_4 + x_5 + x_6 + x_7$ mod 2 (A)

$y_1 = x_0 + x_1 + x_5 + x_6 + x_7$ mod 2 (B)

$y_2 = x_0 + x_1 + x_2 + x_6 + x_7$ mod 2 (C)

$$A: \ y_0 \overset{2}{=} x_0 + x_{(0+4) \bmod 8} + x_{(0+5) \bmod 8} + x_{(0+6) \bmod 8} + x_{(0+7) \bmod 8}$$

$$B: \ y_1 \overset{2}{=} x_1 + x_{(1+4) \bmod 8} + x_{(1+5) \bmod 8} + x_{(1+6) \bmod 8} + x_{(1+7) \bmod 8}$$

$$C: \ y_2 \overset{2}{=} x_2 + x_{(2+4) \bmod 8} + x_{(2+5) \bmod 8} + x_{(2+6) \bmod 8} + x_{(2+7) \bmod 8}$$

Mai verificăm una aleatoare pentru siguranță

$$y_5 = x_1 + x_2 + x_3 + x_4 + x_5 \mod 2$$

$$y_5 = x_5 + x_{(5+4) \bmod 8} + x_{(5+5) \bmod 8} + x_{(5+6) \bmod 8} + x_{(5+7) \bmod 8} \mod 2$$

Prin urmare am găsit formula generală

$$y_i = x_i + x_{(i+4) \bmod 8} + x_{(i+5) \bmod 8} + x_{(i+6) \bmod 8} + x_{(i+7) \bmod 8} \mod 2$$

Pentru toți $i = \overline{0,7}$.

$\square$

10/10

Def A Feistel round is the function $f:\{0,1\}^{2n}\to\{0,1\}^{2n}$ defined as follows. Let $F:\{0,1\}^{n}\to\{0,1\}^{n}$ be an arbitrary function. One divides the words $x\in\{0,1\}^{2n}$ in equal halfs $x=(L,R)$ with $L,R\in\{0,1\}^{n}$. Then

$$f(x)=f(L,R)=(R,L\oplus F(R)).$$

Th The Feistel round is a bijection

- Feistel rounds are serially connected to build Feistel nets. The pseudo-random function F depends on a round key k_i. The action of a Feistel round can be written down as

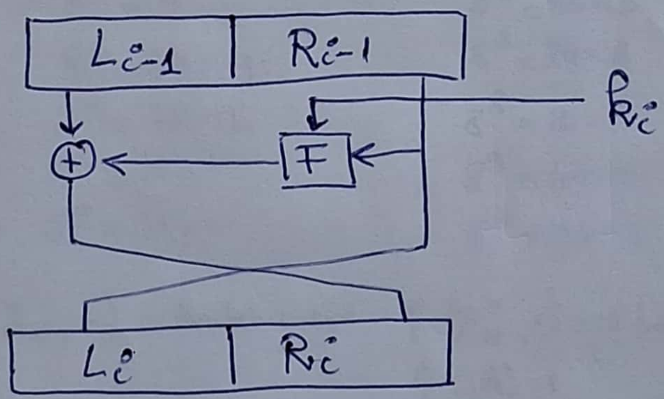
$$L_i = R_{i-1}$$
$$R_i = L_{i-1}\oplus F(k_i, R_{i-1})$$

and the decryption step is then:

$$R_{i-1} = L_i$$
$$L_{i-1} = F(k_i, L_i)\oplus R_i$$

DES = data encryption standard

OBS DES consists of 16 Feistel rounds



- DES is a block cipher
- DES is based on a Feistel network
- k_i is a subkey which is generally derived in some systematic way from the master key K

CamScanner

- f – the scrambling function
- the security of a Feistel-based code
  - → the construction of the scrambling function
  - → in the method of producing the subkeys k_i
- the invertibility – from properties of $\oplus$
- DES – uses 16 stage Feistel network
  - → the pair L_0R_0 is constructing from a 64-bit message by a fixed initial permutation

---

- When discussing „AES arithmetic on the field with 256 elements is given by the irreducible polynomial over $\mathbb{F}_2$" it means that operations in AES, such as substitution and mixing are performed using the specified finite field and its associated irreducible polynomial to ensure certain mathematics properties necessary for encryption.

CS CamScanner

$\boxed{\text{Ex\#4}}$ Calculați $31^{-1} \pmod{100}$ folosind algoritmul extins al lui Euclid.

<u>Dem</u>

$$100 = \underline{31 \cdot 3 + 7}$$
$$31 = \underline{7 \cdot 4 + 3}$$
$$7 = 3 \cdot 2 + 1$$
$$3 = 1 \cdot 3 + 0$$

k	r_k	q_k	t_k
0	100	–	0
1	31	3	1
2	7	4	-3
3	3	2	13
4	1	3	-29

Prin urmare

$$31^{-1} = -29 = 71 \pmod{100}$$

$\square$

CamScanner