Seminar 8 - 17 Aprilie 2024

→ Exercițiul #8 din Seminarul 7

Examen Protocoale 19 mai 2022

Ex #1 ElGamal aditiv modulo $n = 100$ cu generator $g = 11$.

a) Alice alege cheia secretă $x = 12$. Bob alege cheia efemeră $y = 13$. Calculați cheia publică a lui Alice. Arătați cum criptează Bob mesajul $m = 14$ și cum decriptează Alice mesajul criptat.

b) Agenta Eva calculează $g^{-1} \mod n$ și găsește cheia secretă a lui Alice folosind cheia ei publică. Efectuați calculele

Dem

Lucrăm în $(\mathbb{Z}_{100}, +)$.

a) Știm
- generatorul $g = 11$
- cheia secretă $x = 12$ (Alice)
- cheia efemeră (Bob) $y = 13$
- mesajul în clar $m = 14$

Vrem
- cheia publică h (Alice)
- criptare mesaj (Bob)
- decriptare mesaj (Alice)

În cazul aditiv, cheia publică este dată de relația $h = gx$, unde g este un generator, iar x este cheia secretă. În cazul acesta, avem

$$h = gx \pmod n \iff$$
$$h = 11 \cdot 12 \pmod{100} \iff$$
$$h = 32 \pmod{100}.$$

Vedem acum cum criptează Bob mesajul m. Știm că $y = 13$, așador calculăm

1) $gy \pmod n = 11 \cdot 13 \pmod{100} = 43 \pmod{100} =: c_1$

2) $m + hy \pmod n = 14 + 32 \cdot 13 \pmod{100} = 30 \pmod{100} =: c_2$

Am obținut astfel mesajul criptat $(c_1, c_2) = (43, 30)$.

Alice primește mesajul și vrea să îl decripteze. Pentru asta calculează

$$m = c_2 - x c_1 \pmod n$$

Avem

$m = 30 - 12 \cdot 43 = 14 \pmod{100}$. OK

b) Noi știm că $h = g^x \pmod{n}$ este cunoscut. Dacă Eva calculează $g^{-1} \pmod{n}$, poate găsi cheia secretă x dată de

$$x = g^{-1} h \pmod{n}.$$

Calculăm, folosind alg. lui Euclid, $g^{-1} = 11^{-1} \pmod{100}$.

$$100 = 11 \cdot 9 + 1$$
$$11 = 1 \cdot 11 + 0 \Rightarrow 1 = 100 - 11 \cdot 9 \pmod{100}$$
$$1 = 11 \cdot (-9) \pmod{100}$$
$$11^{-1} = 91 \pmod{100}$$

Așadar $g^{-1} = 91 \pmod{100}$ și deci

$$x = 91 \cdot 32 \pmod{100}$$
$$x = 12.$$

ok

□

Ex #2 El Gamal multiplicativ, modulo $p = 19$ în grupul generat de $g = 2$. Alice are cheia publică $h = 6$. Bob trimite mesajul criptat $(c_1, c_2) = (12, 18)$. Decriptați mesajul.

Dem

Lucrăm în $(\mathbb{Z}_{19}^*, \cdot)$.

Știm că $h = g^x \pmod{p}$, unde x este cheia secretă. Așadar

$$2^x = 6 \pmod{19}.$$

Lucrăm cu numere mici, deci avem

$2^1 = 2 \pmod{19}$
$2^2 = 4 \pmod{19}$
$2^3 = 8 \pmod{19}$
$2^4 = 16 \pmod{19}$
$2^5 = 13 \pmod{19}$
$2^6 = 7 \pmod{19}$
$2^7 = 14 \pmod{19}$
$2^8 = 9 \pmod{19}$
$2^9 = 18 \pmod{19}$
$2^{10} = 17 \pmod{19}$
$2^{11} = 15 \pmod{19}$
$2^{12} = 11 \pmod{19}$
$2^{13} = 3 \pmod{19}$
$2^{14} = 6 \pmod{19}$

Prin urmare, $x = 14$.

Altă metodă pentru a afla x (a rezolva DLP)

Baby Step - Giant Step

Știm y, g și p. Vrem x a.î. $g^x = y \pmod p$

x n.n. logaritmul discret al lui y și se notează $x = \log_g y \pmod p$

Algoritm

Se folosește faptul că fiecare $x < p$ se poate scrie ca

$$x = \lceil \sqrt{p} \rceil x_1 + x_2, \text{ unde } 0 \le x_1, x_2 \le \lfloor \sqrt{p} \rfloor$$

Așadar

$$y = g^x = g^{\lceil \sqrt{p} \rceil x_1 + x_2} = \left(g^{\lceil \sqrt{p} \rceil}\right)^{x_1} \cdot g^{x_2} \iff$$

$$y \cdot (g^{-1})^{x_2} = \left(g^{\lceil \sqrt{p} \rceil}\right)^{x_1}$$

Se calculează $g^{-1} \bmod p =: z$ și $g^{\lceil \sqrt{p} \rceil} \pmod p = w$

Se scriu listele

$$L_1 = \{(x_1, w^{x_1}) : x_1 = 0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$$

$$L_2 = \{(x_2, y z^{x_2}) : x_2 = 0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$$

Se caută o coliziune de tipul $(x_1, k) \in L_1, (x_2, k) \in L_2$. Atunci $x = \lceil \sqrt{p} \rceil x_1 + x_2$ este logaritmul discret căutat.

Folosind algoritmul BS-GS, avem: OBS: $\sqrt{19} \approx 4.35$

$\lceil \sqrt{19} \rceil = 5$, iar $\lfloor \sqrt{19} \rfloor = 4$

Căutăm $x < p$ cu $x = 5x_1 + x_2$, unde $0 \le x_1, x_2 \le 4$

Calculăm $g^{-1} \bmod p = 2^{-1} \pmod{19}$ (cu alg lui Euclid)

$$\left.\begin{aligned} 19 &= 2 \cdot 9 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}\right\} \Rightarrow 1 = 19 - 2 \cdot 9 \pmod{19}$$

$$1 = 2(-9) \pmod{19}$$

$$2^{-1} = 10 \pmod{19} \Rightarrow \boxed{z = 10}$$

Acum calculăm $g^{\lceil \sqrt{p} \rceil} \pmod p = 2^5 \pmod{19}$ (cu exp. rapidă)

$$2^1 = 2 \pmod{19}$$

$$2^2 = 4 \pmod{19}$$

$$2^4 = 16 \pmod{19}$$

$$\Rightarrow 2^5 = 32 = 13 \pmod{19} \Rightarrow \boxed{w = 13}$$

Construim listele

$L_1 = \{(0,1), (1,13), (2,17), (3,12), (4,4)\}$

$L_2 = \{(0,6), (1,3), (2,11), (3,15), (4,17)\}$

$\omega^0 = 13^0 = 1$
$\omega^1 = 13^1 = 13$
$\omega^2 = 13^2 = 17 = (-2) \pmod{19}$
$\omega^3 = 13^3 = 12$
$\omega^4 = 13^4 = 4$

$hz^0 = 6 \cdot 10^0 = 6$
$hz^1 = 6 \cdot 10 = 3$
$hz^2 = 6 \cdot 10^2 = 11$
$hz^3 = 6 \cdot 10^3 = 15$
$hz^4 = 6 \cdot 10^4 = 17$
$\pmod{19}$

Găsim ecuația
- $(x_1, 8) = (2, 17) \in L_1$
- $(x_2, 8) = (4, 17) \in L_2$

și calculăm $x = 5x_1 + x_2 \pmod p$, ie $x = 5 \cdot 2 + 4 = 14 \pmod{19}$

$x = 14 \pmod{19}$.

Știind cheia secretă, putem decripta mesajul $m = c_2 (c_1^x)^{-1} \pmod p$

Calculăm $c_1^x = 12^{14} \pmod{19}$.

Observăm că $14 = 2 + 4 + 8$. Avem

$12^2 = 11 \pmod{19}$
$12^4 = 7 \pmod{19}$
$12^8 = 11 \pmod{19}$

Deci $12^{14} = 12^2 \cdot 12^4 \cdot 12^8 = 11 \cdot 7 \cdot 11 = 7 \cdot 7 = 11 \pmod{19}$.

Calculăm $11^{-1} \pmod{19}$.

$19 = 11 \cdot 1 + 8$
$11 = 8 \cdot 1 + 3$
$8 = 3 \cdot 2 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

$\Rightarrow 1 = 3 - 2 = 3 - (8 - 3 \cdot 2) =$
$= 3 \cdot 3 - 8 = (11 - 8) \cdot 3 - 8 =$
$= 11 \cdot 3 - 8 \cdot 4 =$
$= 11 \cdot 3 - (19 - 11) \cdot 4 =$
$= 11 \cdot 7 - 19 \cdot 4 \pmod{19}$

$\Rightarrow 11 \cdot 7 = 1 \pmod{19}$, ie

$11^{-1} = 7 \pmod{19}$

Acum putem obține $w = 18 \cdot 7 \pmod{19} \Rightarrow \boxed{w = 12.}$

□

EX#3 RSA. Un mesaj cu modulo 91 este criptat cu cheia publică $e = 5$ și se obține $c = 25$. Decriptați mesajul cu funcția $\lambda(N)$.

Deci
w

Știm $N = 91$, $e = 5$, $c = 25$. Să observăm că $N = 91 = 7 \cdot 13$. Așador putem calcula

$$\lambda(N) = \lambda(91) = \lambda(7 \cdot 13) = \text{lcm}(7-1, 13-1) = \text{lcm}(6, 12) = \frac{6 \cdot 12}{6} = 12$$

Așador $\lambda(91) = 12$.

Știm că $ed \equiv 1 \pmod{\lambda(N)}$, deci $d = e^{-1} \pmod{\lambda(N)}$. Noi avem

$$d = 5^{-1} \pmod{12}.$$

Calculăm $5^{-1} \pmod{12}$ cu alg. lui Euclid

$$\left.\begin{aligned} 12 &= 5 \cdot 2 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}\right\} \Rightarrow 1 = 5 - 2 \cdot 2 = 5 - (12 - 5 \cdot 2) \cdot 2 = 5 \cdot 5 - 12 \cdot 2 \pmod{12}$$

Avem $5 \cdot 5 = 1 \pmod{12}$, ie $5^{-1} = 5 \pmod{12}$

Știm că $w = c^d \pmod{N}$, deci $w = 25^5 \pmod{91}$. Observăm că $5 = 4 + 1$. Aplicăm alg. de exp rapidă și avem

$$25^1 = 25 \pmod{91}$$
$$25^2 = 79 \pmod{91}$$
$$25^4 = 53 \pmod{91}.$$

Așador $w = 25 \cdot 25^4 = 25 \cdot 53 = 51 \pmod{91} \Rightarrow \boxed{w = 51}$

□

EX#4 Goldwasser-Micali. Un mesaj criptat modulo 133 este format din numerele 120, 13, 123, 10. Decriptați mesajul.

Goldwasser-Micali

→ se folosește pt a cripta bit cu bit
→ se bazează pe problema stabilirii dacă un număr este pătrat mod p sau nu

SETUP (Alice)

1) Se alg două numere prime $p \neq q$. Fie $N = pq$
2) Se alege k din $\mathbb{Z}_N$ a.î.

$$\left(\frac{k}{p}\right) = -1 \wedge \left(\frac{k}{q}\right) = -1$$

Vezi în curs cum se poate face alegerea

3) Cheia publică → (N, k)
4) Cheia secretă → (p, q)

PROTOCOL

Bob: 1) Criptează mesajul $m \in \{0,1\}$
2) Alege $r \in \mathbb{Z}_N^*$ aleator
3) Calculează și trimite $c = k^m r^2 \bmod N$

Alice: Calculează $\left(\frac{c}{p}\right) = c^{\frac{p-1}{2}} \bmod p$. Dacă c este pătrat, atunci $m = 0$. Altfel, $m = 1$.

Demo

Observăm că $N = 133 = 7 \cdot 19$.
Modulo 7, șirul $(120, 13, 123, 10)$ devine $(1, 6, 4, 3)$. Așadar

- $\left(\frac{1}{7}\right) = 1 \Rightarrow m_1 = 0$
- $\left(\frac{6}{7}\right) = 6^3 = 6 = -1 \Rightarrow m_2 = 1$
- $\left(\frac{4}{7}\right) = 4^3 = 1 \Rightarrow m_3 = 0$
- $\left(\frac{3}{7}\right) = 3^3 = 6 = -1 \Rightarrow m_4 = 1$

Mesajul m este $m = (0, 1, 0, 1)$.

□

Ex #5 Shamir Secret Sharing. Fie $P \in \mathbb{Z}_{19}[X]$ un polinom de grad 2. Se consideră următoarele perechi $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{19}^*$ și $P(\alpha) \in \mathbb{Z}_{19}$: $(10, 16)$, $(11, 0)$ și $(12, 5)$. Deduceți secretul partajat $s = P(0) \in \mathbb{Z}_{19}$.

Deci

Avem $P = a + \alpha X + \beta X^2$ cu $\alpha, \beta \in \mathbb{Z}_{19}$ și $a \in \mathbb{Z}_{19}$.

Avem sistemul $\begin{cases} a + 10\alpha + 100\beta = 16 \\ a + 11\alpha + 121\beta = 0 \\ a + 12\alpha + 144\beta = 5 \end{cases} \Leftrightarrow \begin{cases} a + 10\alpha + 5\beta = 16 \\ a + 11\alpha + 7\beta = 0 \\ a + 12\alpha + 11\beta = 5 \end{cases}$

Calculăm

$$\Delta = \begin{vmatrix} 1 & 10 & 100 \\ 1 & 11 & 121 \\ 1 & 12 & 144 \end{vmatrix} = (11-10)(12-10)(12-11) = 1 \cdot 2 \cdot 1 = 2 \neq 0$$

Cum $\gcd(2, 19) = 1$, sistemul are soluții. Rezolvăm

$$\left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 1 & 11 & 7 & 0 \\ 1 & 12 & 11 & 5 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 6 & 8 \end{array}\right] \xrightarrow{1/2 L_3} \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \end{array}\right] \xrightarrow{L_3 - L_2}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[L_1 - 5L_3]{L_2 - 2L_3} \left[\begin{array}{ccc|c} 1 & 10 & 0 & 11 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow{L_1 - 10L_2} \left[\begin{array}{c|c} Id_3 & \begin{matrix} 1 \\ 1 \\ 1 \end{matrix} \end{array}\right]$$

Așadar, am găsit că $a = \alpha = \beta = 1$.

□

Ex #6 Secure Multiparty Computation over $\mathbb{Z}$. Valoarea secretă a lui Alice este $x_1 = 3$, valoarea secretă a lui Bob este $x_2 = 4$ și valoarea secretă a lui Cesar este $x_3 = 5$. Ei vor să calculeze împreună combinația $x_1 x_2 + x_3$ fără a-și dezvălui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajările inițiale, Alice folosește $X+3$, Bob folosește $2X+4$, iar Cesar folosește $3X+5$. Pentru a partaja înmulțirile locale, Alice folosește $4X+a$, Bob folosește $5X+b$, iar Cesar folosește $6X+c$. Efectuați protocolul pas cu pas.

OBS: Pentru teorie, vezi Secure circuit evaluation III din curs.

↓ interpolare Lagrange

7/12

Deci

Știm secretele valori secrete

Alice $x_1 = 3$

Bob $x_2 = 4$

Cezar $x_3 = 5$

Mai știm că pentru partajările inițiale folosim polinoamele

A: $X + 3$

B: $2X + 4$

C: $3X + 5$

iar pentru partajarea înmulțirilor locale se folosesc

A: $4X + a$

B: $5X + b$

C: $6X + c$

Vrem să calculăm $x_1 x_2 + x_3$, fără a face cunoscuți x_1, x_2 și respectiv x_3. Pentru asta considerăm

PAS 1 Multiplicative gate

PAS 2 Additive gate

Din teorie știm că A $\rightsquigarrow$ 1

B $\rightsquigarrow$ 2

C $\rightsquigarrow$ 3

PAS 1 Construim the multiplicative gate

Partajarea valorilor inițiale

	A	B	C
$X + 3$	4	5	6
$2X + 4$	6	8	10
$3X + 5$	8	11	14

Efectuarea înmulțirilor locale x_1, x_2:

A: $4 \cdot 6 = 24$

B: $5 \cdot 8 = 40$

C: $6 \cdot 10 = 60$

8/12

Partajarea înmulțirilor locale

	A	B	C
$4X+24$	28	32	36
$5X+40$	45	50	55
$6X+60$	66	72	78

Aplicăm, acum, vectorul de recombinare $(3,-3,1)$ ce funcționează pentru polinoame de grad ≤ 2. Avem

A: $3\cdot 28 - 3\cdot 45 + 66 = 15$

B: $3\cdot 32 - 3\cdot 50 + 72 = 18$

C: $3\cdot 36 - 3\cdot 55 + 78 = 21$

PAS 2 Additive gate.

Calculăm

A: $8 + 15 = 23$

B: $11 + 18 = 29$

C: $14 + 21 = 35$

În final ajungem în partea de collaborative disclosure în care fiecare își anunță rezultatul final. Se aplică vectorul de recombinare și avem

$$3\cdot 23 - 3\cdot 29 + 35 = 17$$

Verificare: $x_1 x_2 + x_3 = 3\cdot 4 + 5 = 12 + 5 = 17$.

□

Ex #7 Examen Protocoale 18 mai 2023

Cipolla. Arătați că 8 este pătrat modulo 17. Pentru $a=1$, arătați că a^2-8 nu este nici pătrat modulo 17. Folosiți algoritmul lui Cipolla și $a=1$ pentru a calcula $\sqrt{8}$ modulo 17.

Dem

Observăm că 17 este prim impar, iar $\gcd(8,17)=1$. Așadar, conform criteriului lui Euler avem că $\left(\frac{8}{17}\right) = 8^{\frac{17-1}{2}}$. Calculăm

$8^{(17-1):2} = 8^{16:2} = 8^8 \pmod{17}$.

Aplicăm alg. de exponențiere rapidă și avem

$8^2 = 13 \pmod{17}$

$8^4 = 16 \pmod{17}$

$8^8 = 1 \pmod{17}$

Prin urmare $\left(\frac{8}{17}\right) = 1$ și deci 8 este pătrat modulo 17.

Acum, pentru $a = 1$, avem $a^2 - 8 = 1 - 8 = -7 = 10 \pmod{17}$.

Calculăm

$$\left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = 1 \cdot (-1) = -1$$

Așadar 10 nu este pătrat modulo 17.

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ dacă } p \equiv 1 \text{ sau } 7 \pmod 8 \\ -1, \text{ dacă } p \equiv 3 \text{ sau } 5 \pmod 8 \end{cases}$

- $\left(\frac{5}{p}\right) = (-1)^{\left\lfloor \frac{2p+2}{5} \right\rfloor} = \begin{cases} 1, \text{ dacă } p \equiv 1 \text{ sau } 4 \pmod 5 \\ -1, \text{ dacă } p \equiv 2 \text{ sau } 3 \pmod 5 \end{cases}$

p prim impar, $p \neq 5$

Executăm acum algoritmul lui Cipolla cu $a = 1$.

Pentru $\omega^2 = 10$ și calculăm $x = (\omega+1)^{\frac{17+1}{2}}$, ie $x = (\omega+1)^9$

Aplicăm alg. de exponențiere rapidă pentru $9 = 1 + 8$. Avem

- $(\omega+1)^2 = \omega^2 + 2\omega + 1 = 11 + 2\omega \pmod{17}$
- $(\omega+1)^4 = (11+2\omega)^2 = 121 + 44\omega + 4\omega^2 = 121 + 40 + 44\omega =$
  $= 8 + 10\omega \pmod{17}$
- $(\omega+1)^8 = (8+10\omega)^2 = 64 + 100\omega^2 + 160\omega = 13 + 150 + 7\omega =$
  $= 10 + 7\omega \pmod{17}$

Așadar

$$x = (\omega+1)^9 = (\omega+1)^8(\omega+1) = (10+7\omega)(\omega+1) =$$
$$= 10\omega + 10 + 7\omega^2 + 7\omega =$$
$$= 17\omega + 10 + 7 =$$
$$= 12$$

Așadar concluzie, $x = 12$ și $x = 17 - 12 = 5$ sunt rădăcini pătrate modulo 17.

□

10/12

Ex#8 Secure Multiparty Computation peste $\mathbb{Z}$. Valoarea secretă a lui Alice este $x_1=3$, valoarea secretă a lui Bob este $x_2=3$ și valoarea secretă a lui Cezar este $x_3=3$. Ei vor să calculeze împreună cantitatea $x_3(x_1+x_2)$ fără a-și dezvălui valorile secrete. Pentru a partaja valori, ei folosesc polinoame liniare (de gradul 1). Pentru partajările inițiale, Alice folosește $X+3$, Bob folosește $2X+3$, iar Cezar folosește $3X+3$. Pentru a partaja înmulțirile locale, Alice folosește $3X+a$, Bob folosește $X+b$, iar Cezar folosește $2X+c$. Efectuați protocolul pas cu pas.

Deci

Știm că $x_1=x_2=x_3=3$.

Vrem $x_3(x_1+x_2)$.

PAS 1 Adunarea

PAS 2 Înmulțirea

a) Partajarea valorilor inițiale

	A	B	C
$X+3$	4	5	6
$2X+3$	5	7	9
$3X+3$	6	9	12

b) Adunarea locală

A: $4+5=9$

B: $5+7=12$

C: $6+9=15$

c) Înmulțirea locală

A: $9\cdot 6=54$

B: $12\cdot 9=108$

C: $15\cdot 12=180$

d) Înmulțirea colaborativă:

	A	B	C
$3X+54$	57	60	63
$X+108$	109	110	111
$2X+180$	182	184	186

e) Recombinarea locală

A: $3\cdot 57-3\cdot 109+182=26$

B: $3\cdot 60-3\cdot 110+184=34$

C: $3\cdot 63-3\cdot 111+186=42$

f) Recombinarea finală

$3\cdot 26-3\cdot 34+42=18$

Verificare

$x_3(x_1+x_2)=3(3+3)=$

$=3\cdot 6=$

$=18$

Ex#9 Shamir Secret Sharing. Fie $P \in \mathbb{Z}_{19}[X]$ un polinom de grad 2. Și considerăm următoarele perechi $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{19}^*$ și $P(\alpha) \in \mathbb{Z}_{19}$: $(10,16)$, $(11,0)$ și $(12,5)$. Deduceți secretul partajat $\delta = P(0) \in \mathbb{Z}_{19}$.

Dem
ow

Fie $P = \delta + \alpha x + \beta x^2 \in \mathbb{Z}_{19}[x]$.

Avem următorul sistem

$$\begin{cases} \delta + 10\alpha + 100\beta = 16 \\ \delta + 11\alpha + 121\beta = 0 \\ \delta + 12\alpha + 144\beta = 5 \end{cases} \Leftrightarrow \begin{cases} \delta + 10\alpha + 5\beta = 16 \\ \delta + 11\alpha + 7\beta = 0 \\ \delta + 12\alpha + 11\beta = 5 \end{cases}$$

Rezolvăm sistemul

$$\left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 1 & 11 & 7 & 0 \\ 1 & 12 & 11 & 5 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 6 & 8 \end{array}\right] \xrightarrow{1/2 L_3}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \end{array}\right] \xrightarrow{L_3 - L_2} \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[L_1 - 5L_3]{L_2 - 2L_3}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 10 & 0 & 11 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow{L_1 - 10L_2} \left[\begin{array}{c|c} I_3 & \begin{matrix} 1 \\ 1 \\ 1 \end{matrix} \end{array}\right]$$

Așadar $\delta = \alpha = \beta = 1$. $\Rightarrow P = 1 + x + x^2$

Secretul partajat este $P(0) = \delta = 1$.

□