

## Seminar 8 - Iunie 2025

- Teorie MPC din Seminor #.
- Exercițiu MPC din Seminor #.

**Ex#1** Se cunosc MPC peste  $\mathbb{Z}$ . Valoarea secretă a lui A este  $x_1 = 3$ , valoarea secretă a lui B este  $x_2 = 3$  și valoarea secretă a lui Cesar este  $x_3 = 3$ . El vor să calculeze împreună cantitatea  $x_3(x_1 + x_2)$  fără să facă publică valoarea secretă. Pentru partajarea acestia folosesc polinoame Zniare (de grad 1). Pentru partajările inițiale

$$A : x + 3$$

$$B : 2x + 3$$

$$C : 3x + 3$$

Pentru partajarea înmulțirilor

$$A : 3x + a$$

$$B : x + b$$

$$C : 2x + c$$

Efectuati protocolul pas cu pas.

Dez  
m

VREM  $x_3(x_1 + x_2)$ .

Observăm că prima fază ar efectua o adunare, după care urmează o înmulțire.

Cantitățile secrete sunt  $x_1 = x_2 = x_3 = 3$ .

Partajarea valoante inițiale  $x_i^{\circ}(j) = h_i^{\circ}(j)$

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

Pas 1 Adunarea:  $\alpha_1 + \alpha_2$  ( $\alpha_1 \rightarrow A, \alpha_2 \rightarrow B$ )

A:  $4+5=9$

B:  $5+7=12$

C:  $6+9=15$

Pas 2 Înmulțirea cu  $\alpha_3$

a) Înmulțiri locale

A:  $6 \cdot 9 = 54$

B:  $9 \cdot 12 = 108$

C:  $12 \cdot 15 = 180$

b) Polinoamele de partajare  $\rightarrow$  date din ipoteză

A:  $3\alpha + 54$

B:  $\alpha + 108$

C:  $2\alpha + 180$

c) Partajarea înmulțirilor

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

d) Aplicarea vectorului de recombinare  $(3, -3, 1)$

A:  $3 \cdot 54 - 3 \cdot 109 + 182 = 26$

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

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

Pas 3 Collaborative disclosure – se fac publice rezultatele finale și se aplică încă vectorul de recombinare:

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

Verificare:  $\alpha_3(\alpha_1 + \alpha_2) = 3 \cdot (3+3) = 3 \cdot 6 = 18.$

Ex#2

Secure MPC.

- Valorile secrete: A  $x_1 = 6$   
B  $x_2 = 11$   
C  $x_3 = 13$

• Vor să calculeze  $\frac{1}{2}(x_1 + x_3)$ ,

- Pentru partajarea valorilor inițiale
- A  $3x + 6$   
B  $5x + 11$   
C  $9x + 13$

• Pentru partajarea înmulțirii

- A  $a + x$   
B  $3x + b$   
C  $6x + c$

Relații protocolul.

Denumire PAS 1. Adunare

PAS 2. Înmulțire

PAS 3. Collaborative Disclosure

Partajarea valorilor inițiale

	A	B	C	
A	$3x + 6$	9	12	15
B	$5x + 11$	16	21	26
C	$9x + 13$	22	31	40

PAS 1 Adunarea  $x_1 + x_3$

$$A: 9 + 22 = 31$$

$$B: 12 + 31 = 43$$

$$C: 15 + 40 = 55$$

PAS 2 Înmulțirea cu  $x_2$

a) Înmulțirile locale

$$A: 16 \cdot 31 = 496$$

$$B: 21 \cdot 43 = 903$$

$$C: 26 \cdot 55 = 1430$$

b) Polinoamele de partajare  $\rightarrow$  date în ipoteză

A :  $x+496$

B :  $3x+903$

C :  $6x+1430$

c) Partajarea înmulțirilor

	A	B	C	
A	$x+496$	497	498	499
B	$3x+903$	906	909	912
C	$6x+1430$	1436	1442	1448

d) Aplicare metoda de reconstruire  $(3, -3, 1)$

$$A: 3 \cdot 497 - 3 \cdot 906 + 1436 = 209$$

$$B: 3 \cdot 498 - 3 \cdot 909 + 1442 = 209$$

$$C: 3 \cdot 499 - 3 \cdot 912 + 1448 = 209$$

Pass 3 Colaborative disclosure - facem publice rezultatele finale  
și aplicăm din nou metoda de reconstruire.

$$3 \cdot 209 - 3 \cdot 209 + 209 = 209.$$

Verificare:  $x_2(x_1 + x_3) = 11 \cdot (6 + 13) = 11 \cdot 19 = 209.$

□

**Ex#3** Arătați că polinomul  $x^3 + x^2 + 1$  este ireductibil pe  $\mathbb{F}_2$ .  
Fie  $w$  o rotație a polinomului. Calculați elementul  
 $(w^2 + w + 1)^{-1}$  în  $\mathbb{F}_8 = \mathbb{F}_2[w]$ .

Denumire

Fie  $f(x) = x^3 + x^2 + 1$ . Observăm că  $f$  nu are soluții în  $\mathbb{F}_2$   
deoarece  $f(0) = 0 + 0 + 1 = 1 \pmod 2$  și

$$f(1) = 1 + 1 + 1 = 1 \pmod 2$$

Dacă ar fi fost ireductibil, ar fi trebuit să aibă factori de  
grad 1 și 2.

Dacă  $\omega$  este o radacină a lui  $f$ , rezultă din  $F_8 = F_2[\omega]$  că  $\omega^3 = \omega^2 + 1$ . Iar elementele din  $F_8$  au forma  $a + b\omega + c\omega^2$  cu  $a, b, c \in F_2$ . Corectării zilei astfel că elementele să satisfacă

$$(1 + \omega + \omega^2)(a + b\omega + c\omega^2) = 1.$$

Calculăm

$$(1 + \omega + \omega^2)(a + b\omega + c\omega^2) = 1 \iff$$

$$a + b\omega + c\omega^2 + a\omega + b\omega^2 + c\omega^3 + a\omega^2 + b\omega^3 + c\omega^4 = 1$$

Observăm că dacă  $\omega^3 = \omega^2 + 1$ , atunci

$$\omega^4 = \omega^3 + \omega = \omega^2 + \omega + 1$$

Revenim la calcul și avem

$$a + (b+a)\omega + (c+b+a)\omega^2 + (c+b)\omega^3 + c\omega^4 = 1 \text{ adică}$$

$$a + (b+a)\omega + (c+b+a)\omega^2 + (c+b)\omega^3 + c(\omega^2 + \omega + 1) = 1, \text{ ic}$$

$$(a+c) + (a+b+c)\omega + (a+b+2c)\omega^2 + (b+c)\omega^3 = 1$$

$$(a+c) + (a+b+c)\omega + (a+b)\omega^2 + (b+c)(\omega^2 + 1) = 1$$

$$(a+b+2c) + (a+b+c)\omega + (a+2b+c)\omega^2 = 1$$

$$(a+b) + (a+b+c)\omega + (a+c)\omega^2 = 1$$

$$\Rightarrow \begin{cases} a+b &= 1 \\ a+b+c &= 0 \\ a+c &= 0 \end{cases} \Rightarrow \begin{array}{l} a=1 \\ b=0 \\ c=1 \end{array}$$

Așadar  $(a, b, c) = (1, 0, 1)$ , deci

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

Dacă efectuăm verificarea, avem

$$\begin{aligned} (1 + \omega + \omega^2)(1 + \omega^2) &= 1 + \omega + \omega^2 + \omega^2 + \omega^3 + \omega^4 \\ &= 1 + \omega + \omega^2 + 1 + \omega^2 + \omega + 1 \\ &= 1 \end{aligned}$$

□

**Ex#4** Shanon Secret Sharing. Fie  $P \in \mathbb{Z}_{19}[x]$  un polinom de grad 2. Si consideram zirnumtoarele perechi  $(\alpha, P(\alpha))$  unde  $\alpha \in \mathbb{Z}_{19}^*$  si  $P(\alpha) \in \mathbb{Z}_{19}$ :  $(10, 16), (11, 0)$  si  $(12, 5)$ . Deduceti secretul partajat  $A = P(0) \in \mathbb{Z}_{19}$ .

**Ex#5** RSA. Un mesaj cu modul 20 si este criptat cu cheie publica  $e=5$  si obtinut  $c=25$ . Decriptati mesajul cu functia  $\lambda(N)$ .

Denumire

$$\text{Stim } N=91$$

$$e=5$$

$$c=25$$

Să observăm că  $N=91=7 \cdot 13$ . Astfel putem calcula

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

$$=\text{lcm}(6, 12) = \frac{6 \cdot 12}{6} = 12.$$

$$\text{Așadar } \lambda(91)=12.$$

Stim că  $ed \equiv 1 \pmod{\lambda(N)}$ , deci  $d=e^{-1} \pmod{\lambda(N)}$ .  
Noi avem  $d=5^{-1} \pmod{12}$

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

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

Audem  $5 \cdot 5 \equiv 1 \pmod{12}$ , ie  $5^{-1} \equiv 5 \pmod{12}$

Stim că  $m=c^d \pmod{N}$ , deci  $m=25^5 \pmod{91}$ .

Observăm că  $5=4+1$ . Aplicăm alg. de exponentiere rapidă și avem

$$25^1 = 25 \pmod{91}$$

$$25^2 = 49 \pmod{91}$$

$$25^4 = 53 \pmod{91}$$

Așadar  $m=25 \cdot 25^4 = 25 \cdot 53 = 51 \pmod{91} \rightarrow \boxed{m=51}$

EX#6 Examen Protocole - 19 mai 2022

ElGamal aditiv: modul  $n = 100$  cu generatorul  $g = 11$ .

- a) Alice alege cheia secretă  $\alpha = 12$ . Bob alege cheia efemero  $y = 13$ . Calculati cheia publică a lui Alice. Arătați cum criptat Bob mesajul  $m = 14$  și cum decriptat Alice mesajul criptat.
- b) Agentul Eve calculează  $g^{-1} \pmod{n}$  și găsește cheia secretă a lui Alice folosind cheia ei publică. Efectuați calculurile.

Dacă

Lucrările sunt:

Vrem: • cheia publică  $h$  (Alice)  
• criptare mesaj (Bob)  
• decriptare mesaj (Alice)

- a) Stiu: • generatorul  $g = 11$   
• cheia secretă  $\alpha = 12$  (Alice)  
• cheia lui Bob  $y = 13$   
• mesajul în clor  $m = 14$ .

În cazul aditiv, cheia publică este dată de relația  $h = g^\alpha$ , unde  $g$  este un generator, iar  $\alpha$  este cheia secretă. În ceea ce urmă, avem  
 $h = g^\alpha \pmod{n} \Leftrightarrow h = 11 \cdot 12 \pmod{100}$   
 $\Leftrightarrow h = 32 \pmod{100}$

Vedem acum cum criptat Bob mesajul  $m$ . Stiu că  $y = 13$ , asadar calculăm 1)  $g^y \pmod{n} = 11 \cdot 13 \pmod{100} = 43 \pmod{100}$

$$C_1 := 43$$

$$2) m + h^y \pmod{n} = 14 + 32 \cdot 13 = 30 \pmod{100}$$

$$C_2 := 30$$

Așa am obținut astfel mesajul criptat  $(C_1, C_2) = (43, 30)$ .

Alice primește mesajul și vrea să-l decripteze. Pentru acesta calc.

$$m = C_2 - \alpha C_1 \pmod{n}$$

Aveam

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

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

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

Calculăm, folosind algoritmii 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

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

$$x = 12.$$

□

**Ex #7** ElGamal multiplicativ modulo  $p=19$ . În general de  $g=2$ . Alice are cheia publică  $h=6$ . Bob trimite mesajul criptat  $(c_1, c_2) = (12, 18)$ . Decriptează mesajul.

Denumire

Mesajul este din  $(\mathbb{Z}_{19}^*)^*$ .

Stim că  $h = g^x \pmod{p}$ , unde  $x$  este cheia secretă. Așadar  $2^x = 6 \pmod{19}$ .

Varianta 1 Fiecare brută

Varianta 2 Algoritm de afilare a logaritmului discret.

Varianta 1 Calculăm

$$2^1 = 2$$

$$2^8 = 9$$

$$2^2 = 4$$

$$2^9 = 18$$

$$2^3 = 8$$

$$2^{10} = 17$$

$$2^4 = 16$$

$$2^{11} = 15$$

$$2^5 = 13$$

$$2^{12} = 11$$

$$2^6 = 7$$

$$2^{13} = 3$$

$$2^7 = 14$$

$$2^{14} = 6$$

$\pmod{19}$

Prim exercițiu,  $p = 14$ .

Varianta 2 Algoritm de afilare a logaritmului discret

Baby Step - Giant Step

Stim  $y, g \neq 1$ . Vrem să afili  $x$  cu  $y \equiv g^x \pmod{p}$

$x$  D.m. Logaritmul discret a lui  $y$  înseamnă că există

$$x = \log_g y \pmod{p}.$$

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

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

Așadar

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

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

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

Se scriu liste

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

$$L_2 = \{(x_2, yz^{x_2}) \mid x_2 = 0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$$

Se caută o combinație de tipul  $(x_1, z) \in L_1, (x_2, y) \in L_2$ , astfel încât  $x = \lceil \sqrt{p} \rceil x_1 + x_2$  să fie logaritmul discret căutat.

Folosind algoritm BS-GS, avem:

OBS:  $\sqrt{19} \approx 4.35$

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

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

Calculăm  $g^{-1} \pmod{19} = 2^{-1} \pmod{19}$  (folosind algoritm Euclid)

$$19 = 2 \cdot 9 + 1 \Rightarrow 1 = 19 - 2 \cdot 9 \pmod{19}$$

$$1 = 2 \cdot (-9) = 2 \cdot 10 \pmod{19}$$

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

Ameni calculăm  $\sqrt[p]{g}$  mod p = 2<sup>5</sup> mod 19 (cu exp. rapidă)

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

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

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

$$\rightarrow 2^5 = 2 \cdot 2^4 = 2 \cdot 16 = 32 \equiv 13 \pmod{19}$$

$$\rightarrow \boxed{w=13}$$

Construim liste

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

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

$$w^0 = 13^0 = 1$$

$$w^1 = 13^1 = 13$$

$$w^2 = 13^2 = 17 \equiv -2$$

$$w^3 = 13^3 = 12$$

$$w^4 = 13^4 = 4$$

$$\pmod{19}$$

$$h_2^0 = 6 \cdot 10^0 = 6$$

$$h_2^1 = 6 \cdot 10^1 = 3$$

$$h_2^2 = 6 \cdot 10^2 = 11$$

$$h_2^3 = 6 \cdot 10^3 = 15$$

$$h_2^4 = 6 \cdot 10^4 = 17$$

$$\pmod{19}$$

Găsim coliziunea  $\bullet (x_1, \delta) = (2, 17) \in L_1$

$\bullet (x_2, \delta) = (4, 17) \in L_2$

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

Stând cheia secretă, putem decripta mesajul

$$m = c_2(c_1, x)^{-1} \pmod{p}$$

Calculăm  $c_1^x = 12^{14} \pmod{19}$ . Obs. că  $14 = 2+4+8$ . Ameni

$$12^2 = 11 \pmod{19}$$

$$12^4 = 7 \pmod{19}$$

$$12^8 = 11 \pmod{19}$$

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

Calculăm  $m^{-1} \pmod{19}$ .

$$\begin{array}{l}
 19 = 11 \cdot 1 + 8 \\
 11 = 8 \cdot 1 + 3 \\
 8 = 3 \cdot 2 + 2 \\
 3 = 2 \cdot 1 + 1
 \end{array}
 \quad \left| \begin{array}{l}
 \Rightarrow 1 = 3 - 2 = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8 \\
 = (11 - 8) \cdot 3 - 8 = 11 \cdot 3 - 8 \cdot 4 \\
 = 11 \cdot 3 - (19 - 11) \cdot 4 = 11 \cdot 7 - 19 \cdot 4 \pmod{19}
 \end{array} \right.$$

Sei  $\lambda = 11 \cdot 7 \pmod{19}$ , also  $11^{-1} = 7 \pmod{19}$ .

Aber  $w = 18 \cdot 7 \pmod{19} \Rightarrow \boxed{w = 12}$ .

□