Seminar 7 - 08 mai 2025

El Gamal

Algoritm - varianta multiplicativă

- Alice îi trimite mesajul m lui Bob, $m \in \{0, 1, \dots, p-1\}$

I Generarea cheilor

- Alice generează aleator un număr prim p
- Alice generează aleator o rădăcină primitivă g mod p.
- Se calculează aleator $k \in \mathbb{Z}$ cu $1 < k \leq p-2$
- Calculează $g^k \pmod p$
- Obține cheia publică (p, g, g^k) și cheia privată k

II Criptarea mesajului

- Bob preia cheia publică
- Alege aleator un număr natural $b < p-1$
- Calculează $g^b \pmod p$ și $m g^{kb} \pmod p$
- Obține mesajul $c = (g^b, m g^{kb})$ pe care îl trimite

III Decriptarea

- Alice folosește cheia privată și calculează

$$(g^b)^{-k} = (g^b)^{p-1-k} \pmod p$$

← Mica teoremă a lui Fermat

$x^{p-1} \equiv 1 \pmod p$

$x^{-a} = x^{-a} \cdot 1 = x^{-a} x^{p-1} = x^{p-1-a} \bmod p$.

- Calculează

$$(g^b)^{-k} m g^{kb} = m g^{kb-kb} = m \pmod p$$

! Dezavantaj ElGamal → textul cifrat își dublează dimensiunea în raport cu textul în clar m

Rădăcină primitivă mod n

Se numește rădăcină primitivă modulo n numărul $a \in \mathbb{Z}$ cu $\gcd(a,n)=1$, dacă satisface

$$\begin{cases} a^{\varphi(n)} = 1 \pmod n \\ a^{\alpha} \neq 1 \pmod n \end{cases}$$

pentru orice $\alpha \in \mathbb{Z}$ cu $\alpha \in (0, \varphi(n))$.

Ex#1 Alice și Bob folosesc El Gamal multiplicativ modulo 11 cu generatorul $g=2$. Alice alege cheia secretă $k=9$. Calculează cheia publică și îi transmite lui Bob. Bob alege cheia $y=7$ și, folosind cheia publică, criptează mesajul $m=8$. Faceți toate calculele.

Dem

Alice calculează cheia publică $h = g^k \pmod{11}$, ie $h = 2^9 \bmod 11$.

Exponențiere rapidă

$$2^2 = 4 \pmod{11}$$
$$2^4 = 16 = 5 \pmod{11}$$
$$2^8 = 25 = 3 \pmod{11}$$

Deci $h = 2^9 = 2^{1+8} = 2 \cdot 2^8 = 2 \cdot 3 = 6 \pmod{11}$

Alice face publice h și g.

Bob calculează

- $c_1 = g^y \pmod{11} \Leftrightarrow c_1 = 2^7 = 2^{1+2+4} = 2 \cdot 4 \cdot 5 =$
$= 40 = 33 + 7 = 7 \pmod{11}$

$\boxed{c_1 = 11}$

- $c_2 = m h^y \pmod{11} \Leftrightarrow c_2 = 8 \cdot 6^7 \pmod{11}$

$$6^7 = 6^{1+2+4} \pmod{11}$$
$$6^2 = 36 = 33 + 3 = 3 \pmod{11}$$
$$6^4 = 9 \pmod{11}$$
$$6^7 = 6 \cdot 3 \cdot 9 = 18 \cdot 9 = (11+7) \cdot 9 = 63 = 55 + 8 = 8 \bmod 11$$

$C_2 = 8\cdot 8 = 64 = 55+9 = 9 \pmod{11}$

$\boxed{C_2 = 9}$

Alice trebuie să decripteze $(c_1, c_2) = (7, 9)$ pentru a obține m.

$m = c_2 (c_1^k)^{-1} = m\, h^y (g^{-y})^k = m\, (g^k)^y (g^{-y})^k = m$ ok

$m = 9 \cdot (7^9)^{-1} \pmod{11}$

Calculăm

$7^9 = 7^{1+8} = 7 \cdot 7^8 \pmod{11}$

$7^2 = 49 = 44+5 = 5 \pmod{11}$

$7^4 = 25 = 22+3 = 3 \pmod{11}$

$7^8 = 9 \pmod{11}$

Deci $7^9 = 7 \cdot 9 = 63 = 8 \pmod{11}$

Deci $m = 9 \cdot 8^{-1} \pmod{11}$

Calculăm $8^{-1} \pmod{11}$ folosind Euclid extins:

$11 = 8\cdot 1 + 3$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 1$

$\Rightarrow 1 = 3 - 2 = 3 - (8 - 3\cdot 2)$

$= 3 \cdot 3 - 8 = 3 \cdot (11 - 8) - 8$

$= 3 \cdot 11 - 4 \cdot 8 \pmod{11}$

Deci $1 = -8 \cdot 4 \equiv 8 \cdot 7 \pmod{11}$, adică $8^{-1} = 7 \bmod 11$.

Prin urmare, $m = 9 \cdot 7 \equiv 63 \equiv 8 \pmod{11}$

$\boxed{m = 8}$ ok.

A

Concluzie: calcule complicat de efectuat, siguranță crescută

Varianta aditivă → ridicarea la putere devine înmulțire
→ înmulțirea devine adunare

$\boxed{Ex\#2}$ Alice și Bob folosesc ElGamal aditiv modulo 100 cu generatorul $g = 31$. Alice alege cheia secretă $k = 17$. Calculează cheia publică și i-o transmite lui Bob. Bob alege cheia $y = 11$. El folosește cheia publică și criptează mesajul $m = 72$. Alice își folosește cheia și găsește mesajul în clar. Faceți toate calculele.

Dem

• $(\mathbb{Z}_{11}, +) =: G$; $\gcd(31, 100) = 1 \Rightarrow 31$ este generator pt. G.

Cum ne situăm în cadrul aditiv, cheia publică este dată de
$h = gk \pmod{100}$, ie $h = 31 \cdot 17 \pmod{100}$
(Alice) $h = 27 \pmod{100}$

Bob calculează
$(c_1, c_2) = (gy, m + hy) = (31 \cdot 11, 27 \cdot 11 + 72) = (41, 97 + 72)$
$(c_1, c_2) = (41, 69)$

Alice primește (c_1, c_2). Pentru a afla m, ea calculează
$m = c_2 - kc_1 = hy + m - kgy = gky + m - kgy = m$ ok
$m = 69 - 17 \cdot 41 = 69 - 97 = 72$. $\pmod{100}$.

$\square$

$\boxed{Ex\#3}$ În ipotezele problemei anterioare, Oscar interceptează mesajul $(41, 69)$ și vrea să afle cheia secretă k. Ce trebuie să facă acesta?

Dem

Oscar cunoaște cheia publică $h = 27 \pmod{100}$
$h = gk \pmod{100} \to k = g^{-1} h \pmod{100}$

Să observăm că și g este public. Așadar Oscar trebuie doar să calculeze inversul modular al lui g. Aplicăm Euclid extins

$$\begin{aligned} 100 &= 31\cdot 3+7 \\ 31 &= 7\cdot 4+3 \\ 7 &= 3\cdot 2+1 \end{aligned} \Rightarrow 1 = 7-3\cdot 2 = 7-(31-7\cdot 4)\cdot 2$$

$$= 7\cdot 9 - 31\cdot 2 = (100-31\cdot 3)\cdot 9 - 31\cdot 2$$

$$= 100\cdot 9 - 31\cdot 29 \pmod{100}$$

Deci $1 = 31\cdot(-29) = 31\cdot 71 \pmod{100}$, ie $31^{-1} = 71 \pmod{100}$

Prin urmare $g^{-1} = 71 \pmod{100}$

Găsește că $k = g^{-1}h \pmod{100}$

$k = 71\cdot 27 \pmod{100}$

$k = 17 \pmod{100}$

$\square$

! Concluzie: Siguranță inexistentă.

Shamir Secret Sharing

Problema: Să spunem că avem un grup de n persoane care dețin un secret. Se pune problema ca fiecare submulțime de t persoane să NU poată reconstrui secretul, dar fiecare submulțime de $t+1$ poate și va avea acces la secret.

$\hookrightarrow$ vezi povestea cu bomba nucleară: două persoane trebuie să folosească, simultan, o cheie pentru a avea acces și pentru a o lansa

Shamir a propus o metodă de rezolvare a acestei probleme

1) Se alege un corp $\mathbb{Z}_p$ cu $p > n$

2) Elementul secret este un element $s \in \mathbb{Z}_p$ ales aleator.

Se aleg t elemente aleatoare, ~~neep~~ nu neapărat diferite, $f_1, \dots, f_t \in \mathbb{Z}_p$ și se construiește polinomul

$$f(x) = s + f_1 x + f_2 x^2 + \dots + f_t x^t \in \mathbb{Z}_p[x]$$

3) Fiecare persoană primește o cheie unică $x_i \in \mathbb{Z}_p$. Persoana i primește perechea $s_i = (x_i, f(x_i))$.

Teoremă. Dată fiind construcția anterioară, fiecare submulțime de $t+1$ persoane poate reconstrui elementul secret $s=f(0)$, dar fiecare submulțime de t, nu poate.

$\boxed{\text{Ex\#4}}$ Fie $P \in \mathbb{Z}_{29}[x]$ un polinom de grad 2. Se consideră perechile $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ și $P(\alpha) \in \mathbb{Z}_{29}$. Date trei astfel de perechi $(2,11), (4,27), (8,25)$ găsiți elementul secret $s = P(0) \in \mathbb{Z}_{29}$.

Sol

Considerăm polinomul $P(x) = s + \alpha x + \beta x^2 \in \mathbb{Z}_{29}[x]$. Vrem să aflăm s, α, β. Prin urmare, considerăm sistemul

$$(S)\begin{cases} s + 2\alpha + 4\beta = 11 \\ s + 4\alpha + 16\beta = 27 \\ s + 8\alpha + 64\beta = 25 \end{cases} \Longleftrightarrow \begin{cases} s + 2\alpha + 4\beta = 11 \\ s + 4\alpha + 16\beta = 27 \\ s + 8\alpha + 6\beta = 25 \end{cases} \pmod{29}$$

$$\left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 1 & 4 & 16 & 27 \\ 1 & 8 & 6 & 25 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 2 & 12 & 16 \\ 0 & 6 & 2 & 14 \end{array}\right] \xrightarrow[\frac{1}{2}L_3]{\frac{1}{2}L_2} \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 1 & 6 & 8 \\ 0 & 3 & 1 & 7 \end{array}\right] \xrightarrow{L_3 - 3L_2}$$

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

$$\left[\begin{array}{c|c} Id_3 & \begin{matrix} 3 \\ 2 \\ 1 \end{matrix} \end{array}\right].$$ Așadar $\begin{cases} s = 3 \\ \alpha = 2 \\ \beta = 1. \end{cases}$

$\square$

$\boxed{\text{Ex\#5}}$ Shamir Secret Key Sharing în corpul $\mathbb{Z}_{41}$. Considerăm $f \in \mathbb{Z}_{41}[x]$ de grad 2. Trei utilizatori au perechile $(x, f(x)) \in \mathbb{Z}_{41}^2$ mai exact $(1,10), (2,26), (3,14)$. Găsiți cheia secretă $s = f(0)$.

Sol

Considerăm polinomul $f(x) = s + ax + bx^2$. Avem următorul sistem:

$$\begin{cases} s + a + b = 10 \\ s + 2a + 4b = 26 \\ s + 3a + 9b = 14 \end{cases}$$

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 1 & 2 & 4 & 26 \\ 1 & 3 & 9 & 14 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 2 & 8 & 4 \end{array}\right] \xrightarrow{1/2 L_3} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 1 & 4 & 2 \end{array}\right]$$

$$\xrightarrow{L_3 - L_2} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 0 & 1 & 27 \end{array}\right] \xrightarrow[L_1 - L_3]{L_2 - 3L_3} \left[\begin{array}{ccc|c} 1 & 1 & 0 & 24 \\ 0 & 1 & 0 & 17 \\ 0 & 0 & 1 & 27 \end{array}\right] \xrightarrow{L_1 - L_2} \left[\begin{array}{c|c} I_3 & \begin{matrix} 7 \\ 17 \\ 27 \end{matrix} \end{array}\right].$$

Prin urmare $\begin{cases} s = 7 \\ a = 17 \\ b = 27 \end{cases}$, deci elementul secret $s = f(0) = 7$.

□

Multiparty Computation

Problema Să presupunem că (minim) trei persoane A, B, C vor să calculeze, împreună, o funcție aritmetică (adunări și înmulțiri) $f(x_A, x_B, x_C)$, dar fără a face cunoscute cantitățile x_A, x_B, x_C (adică A, B și C își cunosc doar propriile valori). Cum putem face asta?

- Detalii complete → Curs p 83
  ↳ Secure circuit evaluation III

Pași principali

- Persoana A_i deține valoarea secretă x_i

1) Distribuirea valorilor.

Fiecare A_i alege, aleator, $f_1, \dots, f_t \in \mathbb{Z}_p$ și își construiește polinomul de distribuție $h_i(x) = x_i + f_1 x + f_2 x^2 + \dots + f_t x^t$

A_i trimite către A_j un reprezentant al valorii sale secrete, adică (și pt $i=j$) $x_i^{(j)} = h_i(j)$

↑ x_i trimis către A_j

Mai departe, fiecare utilizator va lucra cu cantitățile primite de la ceilalți.

<u>Adunarea</u> Se face așa cum ne-am obișnuit.

<u>Înmulțirea</u>

<u>OBS</u> Interpolare Lagrange. Vezi detalii.

Avem $f(x)$ un polinom. Distribuim valorile $f(j)$. Există un vector $(r_1, \dots, r_n)$ a.î. $f(0) = \sum_{i=\overline{1,n}} r_i f(i)$ care funcționează pt orice polinom de $\deg \leq n-1$.

Poartă numele de <u>vector de recombinare</u>

<u>Principiu</u>: • fiecare utilizator are o val. distribuită pt a și b

ex $a^{(i)} = f(i)$ și $b^{(i)} = g(i)$ unde $a = f(0)$ și $b = g(0)$.

VREM $c^{(i)} = h(i)$ unde $h(x)$ este un polinom a.î. $h(0) = c = ab$.

a) Fiecare utilizator calc. local $d^{(i)} = a^{(i)} b^{(i)}$

b) Fiecare utilizator creează local un polinom $\delta_i(x)$ de grad cel mult t a.î. $\delta_i(0) = d^{(i)}$

c) i trimite către j (și $i=j$) valoarea $d_i^{(j)} = \delta_i(j)$

d) Fiecare utilizator i calculează

$$c^{(i)} = \sum_{j=\overline{1,n}} r_j d_i^{(j)}$$

Valorile finale se fac publice și se aplică iar vectorul de recombinare. ↖ Collaborative disclosure

$\boxed{\text{Ex\#6}}$ Secure Multiparty Computation over $\mathbb{Z}$.

Valoarea secretă a lui Alice este $x_1 = 3$

Bob $x_2 = 4$

Cesar $x_3 = 5$

Vor să calculeze $x_1 x_2 + x_3$, fără a face cunoscute x_1, x_2, x_3.

Pentru partajarea valorilor, folosesc polinoame de $deg = 1$.

- partajarea inițială Alice $x+3$
  Bob $2x+4$
  Cesar $3x+5$

- partajarea înmulțirilor Alice $4x + a$
  Bob $5x + b$
  Cesar $6x + c$

Efectuați calculele.

Sol.

VREM $\underbrace{x_1 x_2}_{\text{Pas 1 - Înmulțirea}} + x_3$

Pas 2 - Adunarea.

Partajarea valorilor inițiale $\quad x_i^{(j)} = f_i(j)$

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

Pas 1 Înmulțirea. $x_1 x_2$ $\quad (x_1 \to A, x_2 \to B)$.

a) Calcul local: $A = 4 \cdot 6 = 24$

$B = 5 \cdot 8 = 40$

$C = 6 \cdot 10 = 60$

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

A: $4x + 24$

B: $5x + 40$

C: $6x + 60$

c) Partajarea înmulțirilor $\quad d_i^{(j)} = \delta_i(j)$.

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

d) Aplicăm vectorul de recombinare $(3,-3,1)$

↳ funcționează pentru toate polinoamele de $\deg \leq 2$

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 Adunarea. $\quad x_1x_2 + x_3$

A: $15+8 = 23$

B: $18+11 = 29$

C: $21+14 = 35$

Pas 3 Collaborative disclosure

Se fac publice rezultatele finale și se aplică vectorul de recombinare:

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

Verificare: $x_1x_2 + x_3 = 3\cdot 4 + 5 = 12 + 5 = 17.$

$\square$