Exerciții*

17 aprilie 2024

1. *RSA* Un mesaj este criptat cu RSA modulo 35 și cheia publică $e = 5$. Mesajul criptat este $c = 33$. Găsiți mesajul original.

2. *Elgamal Aditiv* modulo $n = 1000$ cu generator $g = 667$. Cheia publică este $h = 21$ iar mesajul criptat este $(c_1, c_2) = (81, 27)$. Găsiți mesajul original m.

3. *Elgamal Multiplicativ* modulo $p = 29$ în grupul generat de $g = 2$. Cheia publică este $h = 24$, mesajul criptat este $(c_1, c_2) = (7, 21)$. Găsiți mesajul clar m.

4. *Corpuri finite.* Arătați că polinomul $x^3 + x + 1$ este ireductibil peste corpul $\mathbb{F}_2$. Fie ω o rădăcină a polinomului. Calculați elementul ω^{-2} în $\mathbb{F}_8 = \mathbb{F}_2[\omega]$.

5. *Shamir Secret Sharing.* Fie $P \in \mathbb{Z}_{29}[X]$ un polinom de grad 2. Considerați perechile $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ și $P(\alpha) \in \mathbb{Z}_{29}$. Dacă 3 asemenea perechi sunt $(1, 15)$, $(2, 6)$ și $(3, 7)$, deduceți secretul partajat $s = P(0) \in \mathbb{Z}_{29}$.

6. *Secret Multiparty Computation.* Alice, Bob și Cathy dețin valorile secrete $x = 2$, $y = 3$ și respectiv $z = 4$. Ei vor să calculeze împreună valoarea $xz + yz$, fără ca vreunul dintre ei să destăinuie secretul x, y, respectiv z. Pentru partajarea valorilor inițiale, ei folosesc polinoame de forma $X + a$, $2X + b$ și respectiv $3X + c$. Pentru partajările de la operația de înmulțire, ei folosesc polinoame de forma $3X + a$, $2X + b$ și respectiv $X + c$. Efectuați protocolul.

*Pentru fiecare exercițiu primiți 1.5 puncte. Pentru orice invers modular sau exponențiere modulară fără calcul explicit se scad câte 0.375 puncte.

1

RSA Un mesaj este criptat cu RSA modulo 35 și cheia publică $e = 5$. Mesajul criptat este $c = 33$. Găsiți mesajul original.

Soluție: Cum $35 = 5 \cdot 7$, $\lambda(35) = \text{lcm}(5-1, 7-1) = 12$. Cum $5 \cdot 5 = 25 = 24 + 1$, cheia secretă este $d = e^{-1} \bmod \lambda(N) = 5^{-1} \bmod 12 = 5$. Mesajul original este:

$$m = 33^5 \bmod 35 = (-2)^5 \bmod 35 = -32 \bmod 35 = 3,$$

□

2

Elgamal Aditiv modulo $n = 1000$ cu generator $g = 667$. Cheia publică este $h = 21$ iar mesajul criptat este $(c_1, c_2) = (81, 27)$. Găsiți mesajul original m.

Soluție: Se lucrează pe grupul $(\mathbb{Z}_{1000}, +, 0)$. Cum operația de grup este $+$, semnificația formulei a^b este abși semnificația formulei a^{-1} este $-a$. În asemenea grupuri se poate afla ușor cheia secretă sau cheia temporară calculând întâi inversul $g^{-1} \bmod N$. Observați că g este un generator al lui $\mathbb{Z}_N$ dacă și numai dacă $\gcd(g, N) = 1$, ceea ce este echivalent cu existența lui $g^{-1} \bmod N$.

$$\begin{aligned} 1000 &= \underline{667} + \underline{333} \\ \underline{667} &= 2 \cdot \underline{333} + 1 \end{aligned}$$

$$1 = \underline{667} - 2 \cdot \underline{333} = \underline{667} - 2(-\underline{667}) = 3 \cdot 667,$$

deci $667^{-1} \bmod 1000 = 3$.

Prima metodă: Găsim cheia x:

$$x = g^{-1}h = (3 \cdot 21) \bmod 1000 = 63,$$

după care găsim m:

$$m = c_2 - xc_1 = (27 - 63 \cdot 81) \bmod 1000 = 924.$$

A doua metodă: Găsim cheia temporară y:

$$y = g^{-1}c_1 = (3 \cdot 81) \bmod 1000 = 243,$$

după care găsim m:

$$m = c_2 - yh = (27 - 243 \cdot 21) \bmod 1000 = 924.$$

Nu contează ce metodă alegeți. Este suficient să găsiți rezultatul folosind o singură metodă. □

3

Elgamal Multiplicativ modulo $p = 29$ în grupul generat de $g = 2$. Cheia publică este $h = 24$, mesajul criptat este $(c_1, c_2) = (7, 21)$. Găsiți mesajul clar m.

Soluție: Lucrăm în grupul multiplicativ $(\mathbb{Z}_{29}^{\times}, \cdot, 1)$. Cheia secretă a lui Alice este protejată de dificultatea logaritmului discret. Totuși puterile lui 2 se calculează ușor prin înmulțire succesivă cu 2, și 29 e un număr relativ mic. Calculăm puterile lui 2 modulo 29.

Prima metodă: Găsim cheia secretă x:

$$2^n \bmod 29 = 2, 4, 8, 16, 3, 6, 12, 24 = h.$$

Deci $x = 8$.

$$m = c_2 c_1^{(-x)} = 21 \cdot (7^8)^{-1}.$$

Prin ridicare succesivă la pătrat:

$$7 \rightsquigarrow 7^2 = 20 = -9 \rightsquigarrow 7^4 = 81 = -6 \rightsquigarrow 7^8 = 36 = 7,$$

totul modulo 29. Rezultă:

$$m = 21 \cdot 7^{-1} = 3 \cdot 7 \cdot 7^{-1} = 3.$$

Metoda a doua: Găsim cheia temporară y:

$$2^n \bmod 29 = 2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7 = c_1.$$

Deci $y = 12$.

$$m = c_2 h^{-y} = 21 \cdot (24^{12})^{-1}.$$

Prin ridicare succesivă la pătrat:

$$24 = -5 \rightsquigarrow 24^2 = 25 = -4 \rightsquigarrow 24^4 = 16 = -13 \rightsquigarrow 24^8 = 13^2 = 24,$$

totul modulo 29. Rezultă:

$$24^{12} = 24^8 \cdot 24^4 = 24 \cdot 16 = 48 \cdot 8 = -10 \cdot 8 = 7.$$

$$m = 21 \cdot 7^{-1} = 3 \cdot 7 \cdot 7^{-1} = 3.$$

Nu contează ce metodă alegeți. Este suficient să găsiți rezultatul folosind o singură metodă. □

4

Corpuri finite. Arătați că polinomul $x^3 + x + 1$ este ireductibil peste corpul $\mathbb{F}_2$. Fie ω o rădăcină a polinomului. Calculați elementul ω^{-2} în $\mathbb{F}_8 = \mathbb{F}_2[\omega]$.

Soluție: Fie $f(x) = x^3 + x + 1$. Observăm ca f nu are soluție în $\mathbb{F}_2$ deoarece $f(0) = 0 + 0 + 1 = 1$ și $f(1) = 1 + 1 + 1 = 1$ modulo 2. Dacă f ar fi reductibil, ar trebui să se scrie ca produs de polinoame, și singura posibilitate este ca un polinom să aibă grad 1 și celălalt să aibă grad 2. Dar polinoamele de gradul 1 sunt doar x și $x + 1$. Aceste polinoame au în $\mathbb{F}_2$ rădăcinile 0, respectiv 1. Deci ele nu divid polinomul f deoarece acesta ar avea și el una din aceste rădăcini.

Dacă ω este o rădăcină a lui f, regula de calcul din $\mathbb{F}_8 = \mathbb{F}_2[\omega]$ este:

$$\omega^3 = \omega + 1,$$

iar elementele lui $\mathbb{F}_8$ au forma $a + b\omega + c\omega^2$ cu $a, b, c \in \mathbb{F}_2$. Vrem să găsim un asemenea element astfel încât:

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

adică

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

Din regula de calcul știm că $\omega^3 = \omega + 1$ și deducem că $\omega^4 = \omega^2 + \omega$. Prin înlocuire deducem că:

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

Prin identificarea coeficienților lui 1, ω și respectiv ω^2 din cele două părți, deducem următorul sistem de ecuații liniare peste corpul $\mathbb{F}_2$:

$$\begin{aligned} b &= 1 \\ b + c &= 0 \\ a + c &= 0 \end{aligned}$$

Sistemul are soluția evidentă $(a, b, c) = (1, 1, 1)$. Verificați că $\omega^2(\omega^2 + \omega + 1) = 1$! Deci $\omega^{-2} = \omega^2 + \omega + 1$. □

5

Shamir Secret Sharing. Fie $P \in \mathbb{Z}_{29}[X]$ un polinom de grad 2. Considerați perechile $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ și $P(\alpha) \in \mathbb{Z}_{29}$. Dacă 3 asemenea perechi sunt $(1, 15)$, $(2, 6)$ și $(3, 7)$, deduceți secretul partajat $s = P(0) \in \mathbb{Z}_{29}$.

Soluție: Fie $P(x) = s + ax + bx^2$. Trebuie să găsim coeficienții lui $P(x)$. Deducem următorul sistem de ecuații liniare peste corpul $\mathbb{Z}_{29}$:

$$\begin{aligned} s + a + b &= 15 \\ s + 2a + 4b &= 6 \\ s + 3a + 9b &= 7 \end{aligned}$$

Scădem prima ecuație din celelalte ecuații și obținem:

$$\begin{aligned} s + a + b &= 15 \\ a + 3b &= 20 \\ 2a + 8b &= 21 = -8 \end{aligned}$$

Ultima ecuație poate fi simplificată cu 2 și devine:

$$a + 4b = -4.$$

Ultimele două ecuații alcătuiesc sistemul:

$$\begin{aligned} a + 4b &= -4 \\ a + 3b &= 20 \end{aligned}$$

Prin scăderea ecuațiilor obținem $b = -24 = 5$. Înlocuim b în a doua ecuație și obținem $a + 15 = 20$, deci $a = 5$. Înlocuim a și b în prima ecuație și obținem $s + 5 + 5 = 15$, deci $s = 5$. Acesta este secretul partajat. □

6

Secret Multiparty Computation. Alice, Bob și Cathy dețin valorile secrete $x = 2$, $y = 3$ și respectiv $z = 4$. Ei vor să calculeze împreună valoarea $xz + yz$, fără ca vreunul dintre ei să destăinuie secretul x, y, respectiv z. Pentru partajarea valorilor inițiale, ei folosesc polinoame de forma $X + a$, $2X + b$ și respectiv $3X + c$. Pentru partajările de la operația de înmulțire, ei folosesc polinoame de forma $3X + a$, $2X + b$ și respectiv $X + c$. Efectuați protocolul.

Solution: Cum $xz + yz = (x + y)z$, partenerii decid să efectueze doar două operații: întâi o adunare, apoi o înmulțire.

Distribuția valorilor inițiale:

Alice calculează valorile lui $X+2$, Bob pe ale lui $2X+3$ și Cathy calculează valorile lui $3X+4$. Ei partajează următoarele numere:

$$\begin{pmatrix} & A & B & C \\ X+2 & 3 & 4 & 5 \\ 2X+3 & 5 & 7 & 9 \\ 3X+4 & 7 & 10 & 13 \end{pmatrix}$$

Coloanele conțin calorile primite de fiecare participant.

Adunări locale: Fiecare participant calculează $x+y$ local, și obține:

Alice $3+5=8$.

Bob $4+7=11$.

Cathy $5+9=14$.

Înmulțiri locale: Fiecare participant calculează $(x+y)z$ local, și obține:

Alice $8 \cdot 7 = 56$.

Bob $11 \cdot 10 = 110$.

Cathy $14 \cdot 13 = 182$.

Înmulțire colaborativă: Partenerii partajează rezultatele înmulțirilor locale. Alice folosește polinomul $3X+56$, Bob folosește poinomul $2X+110$ iar Cathy folosește polinomul $X+182$:

$$\begin{pmatrix} & A & B & C \\ 3X+56 & 59 & 62 & 65 \\ 2X+110 & 112 & 114 & 116 \\ X+182 & 183 & 184 & 185 \end{pmatrix}$$

Coloanele indică valorile primite de către fiecare participant

Recombinări locale: Fiecare participant află prin recombinare acel rezultat al înmulțirii criptate, pe care trebuie să îl dețină el.

Alice $3 \cdot 59 - 3 \cdot 112 + 183 = 24$.

Bob $3 \cdot 62 - 3 \cdot 114 + 184 = 28$.

Cathy $3 \cdot 65 - 3 \cdot 116 + 185 = 32$.

Recombinarea finală: Partenerii publică rezultatele criptate pe care le dețin și recombină rezultatul final:

$$3 \cdot 24 - 3 \cdot 28 + 32 = 20.$$

Această valoare este egală cu valoarea $2 \cdot 4 + 3 \cdot 4$ care trebuia calculată. Protocolul a funcționat. $\square$