Seminar 6 - 3 Aprilie 2024

→ Exercițiile rămase din seminarul 5 → decriptarea de la Ex#5
→ Ex#6, Ex#7, Ex#8

$\boxed{\text{Ex\#1}}$ Pentru $n = 77$, $e = 7$ și $m = 9$ parcurgeți criptosistemul RSA atât cu $\varphi(n)$ cât și cu $\lambda(n)$. Ce observați?

Dem

$n = 77 = 7 \cdot 11$

$e = 7$

$m = 9$

$\varphi(n)$

$\varphi(n) = \varphi(77) = (7-1)(11-1) = 6 \cdot 10 = 60$

$\Rightarrow \varphi(n) = 60$

- Cheia privată

$de \equiv 1 \pmod{\varphi(n)}$

$d \equiv e^{-1} \pmod{\varphi(n)}$

$d \equiv 7^{-1} \pmod{60}$

$d = 43$ (cu Euclid)

$60 = 7 \cdot 8 + 4$
$7 = 4 \cdot 1 + 3$
$4 = 3 \cdot 1 + 1$
$3 = 1 \cdot 3 + 0$

$\Rightarrow 1 = 4 - 3 = 4 - (7-4) = 4 \cdot 2 - 7 = 2(60 - 7 \cdot 8) - 7 = 2 \cdot 60 - 7 \cdot 17$

$\Rightarrow 1 \equiv -7 \cdot 17 \pmod{60}$

$\Rightarrow 7^{-1} \equiv -17 \equiv 43 \pmod{60}$

- Criptarea

$c \equiv m^e \pmod n$

$c \equiv 9^7 \pmod{77}$

(Exponențiere rapidă)

$c = 37$

- Decriptarea

$m \equiv c^d \pmod n$

$m \equiv 37^{43} \pmod{77}$

(Exponențiere rapidă)

$m = 9$.

ok

$\lambda(n)$

$\lambda(n) = \lambda(77) = \text{lcm}(7-1, 11-1) = \text{lcm}(6, 10) = \frac{6 \cdot 10}{2} = 30$

$\Rightarrow \lambda(n) = 30$

- Cheia privată

$de \equiv 1 \pmod{\lambda(n)}$

$d \equiv e^{-1} \pmod{\lambda(n)}$

$d \equiv 7^{-1} \pmod{30}$

$d = 13$ (cu Euclid)

$30 = 7 \cdot 4 + 2$
$7 = 2 \cdot 3 + 1$
$2 = 1 \cdot 2 + 0$

$\Rightarrow 1 = 7 - 2 \cdot 3 = 7 - 3 \cdot (30 - 7 \cdot 4) = 7 \cdot 13 - 3 \cdot 30$

$\Rightarrow 1 \equiv 7 \cdot 13 \pmod{30}$

$\Rightarrow 7^{-1} \equiv 13 \pmod{30}$

- Criptarea

$c \equiv m^e \pmod n$

$c = 37$

- Decriptarea

$m \equiv c^d \pmod n$

$m \equiv 37^{13} \pmod{77}$

(Exponențiere rapidă)

$m = 9$.

ok

OBS: $\lambda(n)$ are poate da o cheie de decriptare mai mică. □

$\boxed{\text{Ex \#2}}$ Folosind algoritmul lui Cipolla, găsiți rădăcina pătrată a lui 13 modulo 43, dacă există.

· Alg. lui Cipolla pt calculul rădăcinii pătrate mod p

SE DĂ $n \in Sq(\mathbb{F}_q^*)$

VREM $a \in \mathbb{F}_q^*$ a.î. $a^2 - n \notin Sq(\mathbb{F}_q^*)$

$\omega = \sqrt{a^2 - n} \notin \mathbb{F}_q$

$x = (\omega + a)^{\frac{q+1}{2}}$

OUTPUT x

Simbolul lui Legendre

Simbolul lui Legendre a lui a în raport cu p este dat de

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ dacă } a \text{ este rest pătratic mod } p \\ -1, \text{ dacă } a \text{ este rest nepătratic} \end{cases}$$

Criteriul lui Euler

Dacă p este număr prim impar și $gcd(a,p)=1$, atunci

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

Proprietăți – Aplicații ale criteriului lui Euler

(P1) Dacă $a \equiv b \pmod p$, atunci $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(P2) $\left(\frac{a_1 a_2 \ldots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \ldots \left(\frac{a_n}{p}\right)$

(P3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Teoremă Avem $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Legea de reciprocitate pătratică (Gauss)

Dacă p și q sunt numere prime impare distincte, atunci

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Dem

Prima dată verificăm dacă 13 este rest pătratic modulo 43, deci vrem simbolul lui Legendre a lui 13 în raport cu 43, $\left(\frac{13}{43}\right)$.

$$\left.\begin{array}{l}\bullet\ 43 \text{ prim impar} \\ \bullet\ \gcd(13,43)=1\end{array}\right\} \xrightarrow[\text{Euclid}]{\text{Crit}} 13^{\frac{43-1}{2}} = 13^{\frac{42}{2}} = 13^{21} = \left(\frac{13}{43}\right) \pmod{43}.$$

Folosind exponențierea rapidă, calculăm 13^{21}.

Calcule $\Rightarrow 13^{21} = 1$.

Așadar $\left(\frac{13}{43}\right)=1$, deci 13 este rest pătratic mod 43.

Prin urmare putem calcula $\sqrt{13}$ mod 43 (folosind Cipolla).

$$\left.\begin{array}{l}\bullet\ a=1 \Rightarrow a^2-13 = 1-13 = -12 = 31 \bmod 43 \\ \left(\frac{31}{43}\right) = 31^{\frac{43-1}{2}} = 31^{21} = (\text{Exp. rapidă}) = 1\end{array}\right\} \Rightarrow 31 \in sq(\mathbb{F}_{43}^{*})$$

$\bullet\ a=5 \Rightarrow a^2-13 = 25-13 = 12 \bmod 43$

$$\left(\frac{12}{43}\right) = \left(\frac{2^2\cdot 3}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{2}{43}\right)\left(\frac{3}{43}\right) = (-1)^{\frac{43^2-1}{8}}\cdot(-1)^{\frac{43^2-1}{8}}\cdot\left(\frac{3}{43}\right) =$$

$$= \left[(-1)^{\frac{43^2-1}{8}}\right]^2 \cdot 3^{\frac{43-1}{2}} = 3^{21} = (\text{Exp. rapidă}) = 42 = -1 \pmod{43}$$

$\Rightarrow 12 \notin sq(\mathbb{F}_{43}^{*})$.

Vom executa alg. lui Cipolla pornind cu $a=5$.

Punem $\omega^2 = 12$ și calculăm $x = (\omega+5)^{\frac{43+1}{2}}$, i.e. $x = (\omega+5)^{22}$

Exponențiere rapidă. Observăm că $22 = 2+4+16$. Avem

- $(5+\omega)^2 = 25 + 10\omega + \omega^2 = 25+12+10\omega = 37+10\omega \pmod{43}$

  $(5+\omega)^2 = 10\omega - 6$
- $(5+\omega)^4 = (10\omega-6)^2 = 100\omega^2 + 36 - 120\omega = 14\cdot 12 + 36 + 9\omega \pmod{43}$

  $(5+\omega)^4 = 32 + 9\omega = 9\omega - 11$
- $(5+\omega)^8 = (9\omega-11)^2 = 81\omega^2 + 121 - 9\cdot 22\omega = 38\cdot 12 + 35 + 17\omega \pmod{43}$

  $(5+\omega)^8 = 18 + 17\omega$

$\bullet\ (5+\omega)^{16} = (18+17\omega)^2 = 23 + 31\cdot 12 + 10\omega \pmod{43}$

$(5+\omega)^{16} = 8 + 10\omega$

Așadar

$$x = (5+\omega)^{22} = (5+\omega)^2 (5+\omega)^4 (5+\omega)^{16} =$$
$$= (10\omega - 6)(9\omega - 11)(8+10\omega) =$$
$$= (90\omega^2 - 110\omega - 54\omega + 66)(8+10\omega) =$$
$$= (5 + 8\omega + 23)(8+10\omega) =$$
$$= (28 + 8\omega)(8+10\omega) =$$
$$= 28\cdot 8 + 280\omega + 64\omega + 80\omega^2 =$$
$$= 9 + 37\cdot 12 = 23.$$

$\Rightarrow$ În concluzie, $x = 23$ și $x = 43 - 23 = 20$ sunt rădăcini pătrate. $\square$

$\boxed{\text{Ex\#3}}$ (Examen 2021-2022) Cipolla.

a) Arătați că 2 este rest pătratic modulo 23.

b) Găsiți rădăcina pătrată a lui 2 modulo 23. Arătați întâi că $a = 0$ este o bună alegere astfel ca $a^2 - 2$ să nu fie pătrat modulo 23 și apoi calculați în $\mathbb{F}_{23}[\sqrt{21}]$.

Dem:

a) $\left.\begin{array}{l}\bullet\ 23 \text{ prim impar} \\ \bullet\ \gcd(2,23)=1\end{array}\right\} \xrightarrow[\text{Euclid}]{\text{Crit}} 2^{\frac{23-1}{2}} = \left(\frac{2}{23}\right) \pmod{23}$

unde $\left(\frac{2}{23}\right)$ este simbolul lui Legendre a lui 2 în raport cu 23.

$$2^{\frac{23-1}{2}} = 2^{11} = 2^{1+2+8} = 2\cdot 4\cdot 2^8$$

Folosind exponențierea rapidă, avem

$$2^2 = 4 \pmod{23}$$
$$2^4 = 16 \pmod{23}$$
$$2^8 = 3 \pmod{23}$$

Așadar $2^{11} = 2\cdot 4\cdot 3 = 24 = 1 \pmod{23}$

Prin urmare $\left(\frac{2}{23}\right)=1$ și deci 2 este rest pătratic modulo 23.

b) Vrem $\sqrt{2}$ in $\mathbb{F}_{23}$.

Dacă $a=0$, atunci $a^2-2=-2=21 \pmod{23}$. Putem aplica criteriul lui Euclid și avem

$$(-2)^{\frac{23-1}{2}}=(-2)^{11}=-(2^{11})$$

Din punctul anterior am văzut că $2^{11}=1 \pmod{23}$. Așadar

$$21^{\frac{23-1}{2}}=-(2^{11})=-1=\left(\frac{21}{23}\right)$$

Prin urmare 21 este rest nepătratic modulo 23 și deci $a=0$ este o alegere potrivită pentru a începe alg. lui Cipolla.

Acum avem că $\omega^2=a^2-2$, ie $\omega^2=-2=21 \pmod{23}$

Calculăm $x=(\omega+a)^{\frac{23+1}{2}}$, ie $x=\omega^{12}$ cu $a=0$

Observăm că $12=4+8$, așadar, folosind exponențierea rapidă, avem
- $\omega^2=-2 \pmod{23}$
- $\omega^4=4 \pmod{23}$
- $\omega^8=16 \pmod{23}=-7 \pmod{23}$

Deci

$$x=\omega^{12}=\omega^4\cdot\omega^8=4\cdot(-7)=-28 \Leftrightarrow$$
$$x=-5=18 \pmod{23}$$

În concluzie $x=18$ și $x=23-18=5$ sunt rădăcini pătrate. $\square$

$\boxed{\text{EX\#4}}$ RSA. Știind $N=77$ și $\varphi(77)=60$, găsiți o factorizare pentru N.

Dem.

Știm că $N=pq$ cu p și q prime. Mai mult, știu că $\varphi(N)=(p-1)(q-1)$.

Calculăm

$$\varphi(N)=(p-1)(q-1)=pq-p-q+1=pq+1-(p+q) \Leftrightarrow$$
$$\varphi(N)=N+1-(p+q) \Leftrightarrow p+q=N-\varphi(N)+1 \Leftrightarrow$$
$$\Leftrightarrow p+q=77-60+1 \Leftrightarrow p+q=18$$

Știm suma, știm produsul, considerăm ecuația

$$x^2 - sx + p = 0 \Leftrightarrow$$
$$x^2 - 18x + 77 = 0$$

Calculăm $\Delta = 18^2 - 4\cdot 77 \Leftrightarrow \Delta = 16$. Avem, atunci

$$x_{1,2} = \frac{18 \pm \sqrt{16}}{2} \Leftrightarrow \begin{cases} x_1 = \frac{18+4}{2} = 11 \\ x_2 = \frac{18-4}{2} = 7 \end{cases}$$

Prin urmare $N = 11 \cdot 7 = 77$.

□

! Aceasta este motivul pentru care p și q (deci, implicit $\varphi(n)$) sunt păstrate secret.

$\boxed{\text{Ex \#5}}$ Folosind atacul lui Fermat, factorizați $N = 697$.

Algoritm – Factorizare Fermat

ȘTIM: $n = pq$

VREM: p, q

Considerăm $k = [\sqrt{n}] + 1$

$p^2 = k^2 - n$

- cât timp p^2 nu este pătrat perfect
  - $k = k + 1$
  - $p^2 = k^2 - n$

  □

$p = k - [\sqrt{p^2}]$

$q = k + [\sqrt{p^2}]$

Afișează p și q.

Deci

Calculăm $k = [\sqrt{697}] + 1 = 26 + 1 = 27$

Calculăm $p^2 = 27^2 - 697 = 32$

- 32 nu este pătrat perfect

  $k = k + 1 \Rightarrow k = 28$

  $p^2 = 28^2 - 697 = 87$

• 87 nu este pătrat perfect

$k = k+1 \Rightarrow k = 29$

$p^2 = 29^2 - 697 = 144 = 12^2$

Ne oprim și găsim $\left.\begin{array}{l} p = 29-12 \Rightarrow p = 17 \\ q = 29+12 \Rightarrow q = 41 \end{array}\right\} \Rightarrow pq = 697.$

$\square$

$\boxed{\text{Ex \#6}}$ Folosind metoda de factorizare $p-1$ a lui Pollard, factorizați numărul $N = 91$.

<u>Algoritm</u>

→ Alegem un număr a astfel încât $\gcd(a, n) = 1$

→ Calculează $a^{B!}$ pentru $B = 1, 2, 3, \ldots$

→ Găsește $\gcd(a^{B!} - 1 \pmod{n}, n) = d$

Dacă d este netrivial, am găsit un factor pentru n.

Dem

Alegem $a = 2$. Observăm că $\gcd(2, 91) = 1$. <u>ok</u>

Calculăm

• $B = 1$ $\quad 2^{1!} = 2$; $\gcd(2-1, 91) = \gcd(1, 91) = 1$

• $B = 2$ $\quad 2^{2!} = 2^2 = 4$; $\gcd(4-1, 91) = \gcd(3, 91) = 1$

• $B = 3$ $\quad 2^{3!} = 2^6 = 64$; $\gcd(64-1, 91) = \gcd(63, 91) = 7$

Euclid: $91 = 63 \cdot 1 + 28$

$63 = 28 \cdot 2 + 7 \Rightarrow \gcd(63, 91) = 7$

$28 = 7 \cdot 4 + 0$

Prin urmare 7 este un factor a lui 91, să spunem $p = 7$. Deci $q = 91 : 7$, i.e. $q = 13$.

$\square$

$\boxed{\text{Ex \# 7}}$ Pollard $p-1$. Factorizați $N = 1927$ plecând cu $a = 10$.

Dem

Observăm că $\gcd(10, 1927) = 1$ <u>ok</u>

Calculăm

• $B = 2$ $\quad 10^{2!} = 10^2$; $\gcd(100-1, 1927) = 1$

• $B=3$ $\quad 10^{3!}=10^{6}$; $gcd(10^{6}-1, 1927)=gcd(1814-1, 1927)=1$

• $B=4$ $\quad 10^{4!}=10^{24}$; $gcd(10^{24}-1, 1927)=gcd(37-1, 1927)=1$

• $B=5$ $\quad 10^{5!}=10^{120}$; $gcd(10^{120}-1, 1927)=gcd(862-1, 1927)=41$

Așadar $p=41$ și $q=1927:41$, ie $q=47$

$N=1927=41\cdot 47$.

□

$\boxed{Ex\ \#8}$ Folosind algoritmul de factorizare ρ a lui Pollard, factorizați numărul $N=1927$, având ca valoarea de start $x=10$.

<u>Algoritm</u>

1. Alege aleator x și c. Definește $f(x)=x^2+c \pmod n$

   Începem cu $x=y$ și $d=1$.

2. Cât timp $d=1$

   a. $x \leftarrow f(x)$

   b. $y \leftarrow f(f(y))$

   c. $d \leftarrow gcd(n, |x-y|)$

   d. dacă $d \neq 1$

      i) dacă $d=n$, reia cu un nou (x, y, c)

      ii) altfel, d este un factor

<u>OBS</u>: În aplicațiile școlărești mai mereu se lucrează cu $c=1$

Dem

Pornim cu $x_0=y_0=10$.

Considerăm $f(x)=x^2+1$ și $x_i=f(x_{i-1})$

$y_i=f(f(y_{i-1}))$

Obținem

• $x_1=f(x_0)=101 \pmod{1927}$

$y_1=f(f(0))=f(101)=101^2+1=567$

$d=gcd(567-101, 1927)=gcd(466, 1927)=1$

- $x_2 = f(x_1) = 567$
  $y_2 = f(f(y_1)) = f(1608) = 1558$
  $d = \gcd(|x_2 - y_2|, n) = \gcd(991, n) = 1$

- $x_3 = f(x_2) = 1608$
  $y_3 = f(f(y_2)) = f(1272) = 1232$
  $d = \gcd(|x_3 - y_3|, n) = \gcd(376, n) = 47$

Ne oprim și găsim $p = 47$ și $q = 1927 : 47 = 41$. Deci

$$N = 47 \cdot 41 = 1927.$$

$\square$