Kryptografia z elementami algebry, laboratorium 1

Maciej Grześkowiak

21 października 2021

Potęgowanie binarne, implementacja (Left-to-right)

Dane: $x \in \mathbb{Z}_n^*$, $k, n \in \mathbb{N}$, $k = (k_{l-1}k_{l-2}\ldots k_0)_2$
Wynik: $y \in \mathbb{Z}_n^*$ takie, że $y = x^k \pmod{n}$

1. $y = 1$; $i = l - 1$;
2. **while** $i \geqslant 0$
3. $\quad$ $y = y^2 \pmod{n}$
4. $\quad$ **if** $k_i == 1$ **then** $y = yx \pmod{n}$
5. $\quad$ $i = i - 1$
6. **return** y

Potęgowanie binarne, implementacja (Right-to-left)

Dane: $x \in \mathbb{Z}_n^*$, $k, n \in \mathbb{N}$, $k = (k_{l-1}k_{l-2}\dots k_0)_2$
Wynik: $y \in \mathbb{Z}_n^*$ takie, że $y = x^k \pmod{n}$

1. $y = 1; z = x\ i = 0;$
2. **while** $i < l$
3.   **if** $k_i == 1$ **then** $y = yz \pmod{n}$
4. $y = y^2 \pmod{n}$
5. $i = i + 1$
6. **return** y

Rozszerzony algorytm Euklidesa, idea

Dane: $x = 10, N = 13$, $x < N$,
Wynik: (u, v, d) takie, że $xu + vN = d$ oraz $(x, N) = d$.

$$13 = 1 \cdot 10 + 3$$

$$10 = 3 \cdot 3 + 1$$

$$3 = 1 \cdot 3 + 0$$

$$13 = 13 \cdot 1 + 0 \cdot 10$$

$$10 = 13 \cdot 0 + 1 \cdot 10$$

$$3 = 13 \cdot 1 - 1 \cdot 10$$

$$1 = 13 \cdot (-3) + 4 \cdot 10$$

Rozszerzony algorytm Euklidesa, implementacja

Dane: x, N, $x < N$,
Wynik: (u, v, d) takie, że $xu + vN = d$ oraz $(x, N) = d$.

1. $A = N;\ B = x;\ U = 0;\ V = 1;$
2. **repeat**
3. $\qquad q = A \text{ div } B$
4. $\qquad \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} A \\ B \end{bmatrix}$
5. $\qquad \begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} U \\ V \end{bmatrix}$
6. **until** $B == 0$
7. $d = A,\ u = U,\ v = (d - xu)/N$
8. **return** (u, v, d)

Reszty kwadratowe modulo n

Definicja: Niech $a \in \mathbb{Z}_p$, $p > 2$. Element a jest resztą kwadratową modulo p jeśli istnieje $b \in \mathbb{Z}_p$ taki, że $a = b^2 \pmod{p}$. Jeśli takie b nie istnieje, to mówimy, że a nie jest reszta kwadratową modulo p.

Definicja: Niech $a \in \mathbb{Z}$ oraz niech $p > 2$ będzie liczba pierwszą. Definiujemy symbol Legendre'a

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{jeśli} \quad p \mid a \\ 1 & \text{jeśli} \quad a \text{ jest resztą kwadratową} \pmod{p} \\ -1 & \text{jeśli} \quad a \text{ nie jest resztą kwadratową} \pmod{p} \end{cases}$$

Twierdzenie (Eulera)

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

Reszty kwadratowe modulo n, implementacja

Twierdzenie (Eulera) Niech $p = 3 \pmod 4$ będzie liczbą pierwszą. Niech a będzie resztą kwadratową modulo p. To znaczy istnieje $b \in \mathbb{Z}_p$ takie, że $b^2 = a \pmod p$. Wtedy

$$\pm b = a^{(p+1)/4} \pmod p.$$

Test pierwszości

Twierdzenie (Fermata) Niech n będzie liczbą pierwszą. Dla dowolnej liczby b takiej, że $(b, n) = 1$, mamy

$$b^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

Definicja Jeśli n jest liczbą nieparzystą liczbą złożoną oraz b jest dowolną liczbą taką, że $(b, n) = 1$ oraz zachodzi (1), to n nazywamy pseudopierwszą przy podstawie b.

Twierdzenie Jeśli n nie spełnia testu (1) przy pewnej podstawie $b \in \Phi(n)$, to n nie spełnia testu (1) dla co najmniej połowy możliwych podstaw $b \in \Phi(n)$.

Dowód Niech

$$\{b_1, b_2, \ldots, b_s\}$$

będzie zbiorem wszystkich podstaw, przy których n jest pseudopierwsza.
Niech b będzie ustaloną podstawą, przy której n nie jest pseudopierwszą.
Gdyby, n była pseudopierwsza przy podstawie bb_i, to byłaby pseudopierwsza przy podstawie

$$(bb_i)b_i^{-1} \equiv b \pmod n,$$

co jest sprzeczne z założeniem.
Ponieważ, jeśli n jest pseudopierwsza przy podstawach b_1, b_2, to n jest pseudopierwsza przy podstawach $b_1 b_2$ oraz $b_1 b_2^{-1}$.

Test pierwszości, dowód cd.

Zatem dla s różnych reszt

$$\{bb_1, bb_2, \ldots, bb_s\}$$

liczba n nie spełnia testu (1).

Istnieje zatem co najmniej tyle podstaw w $\Phi(n)$, przy których n nie jest liczbą pseudopierwszą, co podstaw, przy których (1) zachodzi. To kończy dowód.