

Kryptografia z elementami algebry, laboratorium 1

Maciej Grześkowiak

27 października 2020

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 $y = 1; i = l - 1;$
- 2 **while** $i \geq 0$
- 3 $y = y^2 \pmod{n}$
- 4 **if** $n_i == 1$ **then** $y = yx \pmod{n}$
- 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 $(x, N) = d.$

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

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

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

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

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

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

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

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 $q = A \text{ div } B$

④
$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} A \\ B \end{bmatrix}$$

⑤
$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} U \\ V \end{bmatrix}$$

⑥ **until** $B == 0$

⑦ $d = A, u = U, v = (d - xu)/N$

⑧ **return** (u, v, d)

Definicja: Niech $a \in \mathbb{F}_p$, $p > 2$. Element a jest resztą kwadratową modulo p jeśli istnieje $b \in \mathbb{F}_p$ 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 liczbą pierwszą. Definiujemy symbol Legendre'a

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

Twierdzenie (Eulera)

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n}. \quad (1)$$

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

$$\{b_1, b_2, \dots, b_n\}$$

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 $b_1 b_2^{-1}$.

Zatem dla s różnych reszt

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

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.