Laboratorium z kryptografii

Zajęcia 7-8: Liczby pierwsze - test Millera-Rabina

1 Algorytm szybkiego potęgowania modulo

Obliczanie reszty z dzielenia pewnej liczby naturalnej a podniesionej do potęgi b przez c (tj. $a^b \mod c$), gdzie $a, b, c \in \mathbb{N}$ wymaga przeprowadzenia $b-1$ mnożeń oraz jednego dzielenia. Dodatkowo dla dużych liczb a oraz b liczba a^b przed wyciągnięciem reszty z dzielenia może osiągać ogromne wartości. Wykorzystując jedną z podstawowych własności arytmetyki modularnej:

$$((a \mod c) \cdot (b \mod c)) \mod c = (a \cdot b) \mod c$$

oraz rozkład wykładnika b na reprezentację binarną $(b_n, b_{n-1}, \ldots, b_1, b_0)$:

$$b = b_0 2^0 + b_1 2^1 + \ldots + b_n 2^n$$

liczbę $a^b \mod c$ można zapisać jako:

$$\begin{aligned} a^b &= a^{b_0 2^0 + b_1 2^1 + \ldots + b_n 2^n} \pmod c \\ &= a^{b_0 2^0} a^{b_1 2^1} \cdot \ldots \cdot a^{b_n 2^n} \pmod c \end{aligned}$$

Przykładowo niech dane będzie wyrażenie $4^{21} \mod 7$, wtedy:

$$\begin{aligned} 4^1 \mod 7 &= 4 \\ 4^2 \mod 7 &= (4^1)^2 = 16 \mod 7 = 2 \\ 4^4 \mod 7 &= (4^2)^2 = 4 \mod 7 = 4 \\ 4^8 \mod 7 &= (4^4)^2 = 16 \mod 7 = 2 \\ 4^{16} \mod 7 &= (4^8)^2 = 4 \mod 7 = 4 \end{aligned}$$

ponieważ wykładnik $b = 21$ w postaci binarnej wynosi $b = (10101)$, to:

$$\begin{aligned} 4^{21} &= 4^1 \cdot 4^4 \cdot 4^{16} \pmod 7 \\ &= 4 \cdot 4 \cdot 4 \pmod 7 \\ &= 1 \pmod 7 \end{aligned}$$

Przykład $1897^{50498} \mod 16112$

$$\begin{aligned} 1897^1 \mod 16112 &= 1897 \\ 1897^2 \mod 16112 &= (1897^1)^2 \mod 16112 = 5633 \\ 1897^4 \mod 16112 &= (1897^2)^2 \mod 16112 = 6161 \\ 1897^8 \mod 16112 &= (1897^4)^2 \mod 16112 = 14161 \\ 1897^{16} \mod 16112 &= (1897^8)^2 \mod 16112 = 3969 \\ 1897^{32} \mod 16112 &= (1897^{16})^2 \mod 16112 = 11537 \\ 1897^{64} \mod 16112 &= (1897^{32})^2 \mod 16112 = 1137 \\ 1897^{128} \mod 16112 &= (1897^{64})^2 \mod 16112 = 3809 \\ 1897^{256} \mod 16112 &= (1897^{128})^2 \mod 16112 = 7681 \\ 1897^{512} \mod 16112 &= (1897^{256})^2 \mod 16112 = 11729 \\ 1897^{1024} \mod 16112 &= (1897^{512})^2 \mod 16112 = 5185 \\ 1897^{2048} \mod 16112 &= (1897^{1024})^2 \mod 16112 = 9409 \\ 1897^{4096} \mod 16112 &= (1897^{2048})^2 \mod 16112 = 9953 \\ 1897^{8192} \mod 16112 &= (1897^{4096})^2 \mod 16112 = 5633 \\ 1897^{16384} \mod 16112 &= (1897^{8192})^2 \mod 16112 = 6161 \\ 1897^{32768} \mod 16112 &= (1897^{16384})^2 \mod 16112 = 14161 \end{aligned}$$

Ponieważ $50498 = (1100010101000010)_2$, to:

$$\begin{aligned} 1897^{50498} &= 1897^{32768+16384+1024+256+64+2} \pmod{16112} \\ &= 14161 \cdot 6161 \cdot 5185 \cdot 7681 \cdot 1137 \cdot 5633 \pmod{16112} \\ &= 8993 \pmod{16112} \end{aligned}$$

Inne przykłady

i) $5^{41} \mod 137 = 62$

ii) $15^{12347} \mod 707 = 113$

iii) $73^{987654} \mod 613 = 195$

iv) $2234^{1234567} \mod 9876 = 2900$

2 Test Millera-Rabina

Twierdzenie 1 *Małe twierdzenie Fermata*
Jeżeli n jest liczbą pierwszą, to dla dowolnej liczby całkowitej q, liczba $q^n - q$ jest wielokrotnością liczby n, tzn.:

$$q^n = q \pmod{n}.$$

Powyższe twierdzenie można także zapisać w postaci:

$$q^{n-1} = 1 \pmod{n}.$$

Ponieważ centrum zainteresowania stanowią liczby pierwsze $n > 2$, to $n - 1$ na pewno jest liczbą parzystą, dzięki czemu można dokonać rozkładu:

$$n - 1 = 2^s d \tag{1}$$

Rozważając ciąg $q_r = (q^{2^r d} \mod n)_{r=0}^{s}$, nietrudno zauważyć, że każdy kolejny element jest kwadratem poprzedniego:

$$\begin{aligned} q^{2^0 d} &\mod n \\ q^{2^1 d} \mod n &= (q^{2^0 d} \mod n)^2 \\ q^{2^2 d} \mod n &= (q^{2^1 d} \mod n)^2 \\ &\vdots \\ q^{2^s d} \mod n &= (q^{2^{s-1} d} \mod n)^2 \end{aligned} \tag{2}$$

natomiast ostatni element (wykorzystując małe twierdzenie Fermata) spełnia równość:

$$q^{2^s d} = q^{n-1} = 1 \pmod{n} \tag{3}$$

Ponieważ element ten także jest kwadratem innego elementu ciągu q_r to można zapisać, że:

$$x^2 = 1 \pmod{n} \tag{4}$$

czego rozwiązaniem są:

$$x_1 = 1 \pmod{n} \tag{5}$$

$$x_2 = -1 \pmod{n} \tag{6}$$

dając dwie możliwe sytuacje dla całego ciągu q_r:

1) „Zerowy" element ciągu q_0 równy jest jeden ($q^d = 1 \pmod{n}$), wtedy każdy następny także jest jedynką.

2) „Zerowy" element ciągu q_0 jest różny od jeden ($q^d \neq 1 \pmod{n}$), wtedy aby ostatni wyraz ciągu równy był jeden ($q^{n-1} = 1$) musi istnieć element q_R, gdzie $R \in \{0, \ldots, s-1\}$, równy -1 ($q^{2^R d} = -1 \pmod{n}$).

Twierdzenie 2 *Test Millera-Rabina*
Niech $n > 2$ będzie pewną naturalną liczbą nieparzystą, natomiast liczba całkowita q losowana będzie ze zbioru $\{2, 3, \ldots, n-1\}$. n jest liczbą złożoną jeżeli spełnione są dwa następujące warunki:

1. $q^d \neq 1 \pmod{n}$
2. $q^{2^r d} \neq -1 \pmod{n}$ *dla każdego* $r \in \{0, \ldots, s-1\}$,

gdzie s, d zdefiniowane są przez rozkład $n - 1 = 2^s d$.

Twierdzenie 2 wyznacza test złożoności danej liczby nieparzystej n. Jeżeli warunek 1. bądź 2. nie są spełnione to n jest **PRAWDOPODOBNIE** pierwsza - dowodzi się, że prawdopodobieństwo to wynosi 75%. Aby zwiększyć prawdopodobieństwo, że dana liczba jest liczbą pierwszą test Millera-Rabina należy przeprowadzić wielokrotnie dla różnych losowych wartości q.
Przykłady:

a) $n = 252601$ i $q = 85132$, wtedy $n - 1 = 2^3 \cdot 31575$ oraz:

$$\begin{aligned} 85132^{31575} &= 191102 \pmod{252601} \\ 85132^{2 \cdot 31575} &= 184829 \pmod{252601} \\ 85132^{2^2 \cdot 31575} &= 1 \pmod{252601} \end{aligned}$$

Wniosek - n jest liczbą złożoną

b) $n = 280001$ i $q = 105532$, wtedy $n - 1 = 2^6 \cdot 4375$ oraz:

$$\begin{aligned} 105532^{4375} &= 236926 \pmod{280001} \\ 105532^{2 \cdot 4375} &= 168999 \pmod{280001} \\ 105532^{2^2 \cdot 4375} &= 280000 = -1 \pmod{280001} \end{aligned}$$

Wniosek - n jest prawdopodobnie liczbą pierwszą

3 ZADANIA

1. Zaimplementować algorytm szybkiego potęgowania modulo ($a^b \mod c$) działający w zakresie $a, c <32\,000$ oraz $b <2\,000\,000\,000$. Liczby a, b i c mają być wczytywane z konsoli. Program ma wyświetlać wynik.
2. Zaimplementować test Millera-Rabina dla liczby nieparzystej n i pewnej liczby q. Obie liczby mają być wczytywane z konsoli. Program ma wyświetlać kolejne elementy ciągu $q_r = (q^{2^r d} \mod n)_{r=0}^{s}$ i zwracać odpowiedni wniosek „liczba n jest złożona/prawdopodobnie pierwsza”

Punktacja - łącznie 10 punktów

- 2 punkty - poprawnie działający algorytm szybkiego mnożenia dla $a, c < 10\,000$
- 2 punkty - poprawnie działający algorytm szybkiego mnożenia dla $a, c \geqslant 10\,000$
- 3 punkty - poprawnie działający test Millera-Rabina dla $n < 10\,000$
- 3 punkty - poprawnie działający test Millera-Rabina dla $n \geqslant 10\,000$