Laboratorium z kryptografii

Zajęcia 9-10: Algorytm RSA

1 Sito Eratostenesa

Sito Eratostenesa jest to algorytm znajdywania wszystkich liczb pierwszych nie większych od zadanej liczby p opierający się na następującym twierdzeniu:

Twierdzenie 1 .
Niech dana będzie liczba naturalna $n > 1$. Liczba n jest pierwsza jeżeli nie istnieje liczba (pierwsza) $2 \leqslant q \leqslant \sqrt{n}$, która dzieli n, tzn:

$$\forall_{2 \leqslant q \leqslant \sqrt{n}} \; n \mod q \neq 0 \tag{1}$$

Wykorzystując powyższe twierdzenie można kolejno eliminować liczby złożone z ciągu liczb naturalnych $\{2, 3, 4, \ldots, p - 2, p - 1, p\}$.
Przykładowy proces wyszukiwania wszystkich liczb pierwszych nie większych od $p = 30$:

1) Utworzenie początkowego ciągu liczb S:
$S = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30\}$

2) **PIERWSZY** element ciągu jest mniejszy od pierwiastka z ostatniego elementu ($2 \leqslant \sqrt{30}$) $\Rightarrow$ sprawdzanie (i usuwanie wszystkich, poza pierwszym), które elementy ciągu S dzielą się przez jego PIERWSZY element:

$$\begin{aligned} S &= \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30\} \\ & \Downarrow \\ S &= \{2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29\} \end{aligned}$$

3) **DRUGI** element ciągu jest mniejszy od pierwiastka z ostatniego elementu ($3 \leqslant \sqrt{29}$) $\Rightarrow$ sprawdzanie (i usuwanie wszystkich, poza pierwszym), które elementy ciągu S dzielą się przez jego DRUGI element:

$$\begin{aligned} S &= \{2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29\} \\ & \Downarrow \\ S &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29\} \end{aligned}$$

4) **TRZECI** element ciągu jest mniejszy od pierwiastka z ostatniego elementu ($5 \leqslant \sqrt{29}$) $\Rightarrow$ sprawdzanie (i usuwanie wszystkich, poza pierwszym), które elementy ciągu S dzielą się przez jego TRZECI element:

$$\begin{aligned} S &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29\} \\ & \Downarrow \\ S &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\} \end{aligned}$$

5) **CZWARTY** element ciągu jest **WIĘKSZY** od pierwiastka z ostatniego elementu ($7 > \sqrt{29}$) $\Rightarrow$ przerwanie algorytmu. Wszystkie liczby pierwsze nie większe od $p = 30$, to:

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$$

n	n-ta liczba pierwsza		n	n-ta liczba pierwsza
1	2		1	2
4	7		10	29
25	97		100	541
168	997		1 000	7 919
1 229	9 973		10 000	104 729
9 592	99 991		100 000	1 299 709
78 498	999 983		1 000 000	15 485 863

Tabela 1: Przykładowe liczby pierwsze

2 Rozszerzony algorytm Euklidesa

Algorytm pozwala na wyznaczenie największego wspólnego dzielnika d liczb a oraz b oraz dwóch liczb x oraz y takich, że spełniona jest równość (3):

$$d = NWD(a,b) \tag{2}$$
$$d = x \cdot a + y \cdot b \tag{3}$$

Algorytm:

1. Zapisanie liczby a jako sumy całkowitej wielokrotności q_1 liczby b i reszty r_1 z dzielenia $\frac{a}{b}$:
$$a = q_1 b + r_1$$
2. Zapisanie liczby b jako sumy całkowitej wielokrotności q_2 liczby r_1 i reszty r_2 z dzielenia $\frac{b}{r_1}$:
$$b = q_2 r_1 + r_2$$
3. Zapisanie liczby r_1 jako sumy całkowitej wielokrotności q_3 liczby r_2 i reszty r_3 z dzielenia $\frac{r_1}{r_2}$:
$$r_1 = q_3 r_2 + r_3$$
4. Przeprowadzenie kolejnych iteracji dopóki $r_n \neq 0$. Jeżeli $r_n = 0$ to
$$NWD(a,b) = r_{n-1}$$

Wyznaczając kolejne reszty z dzielenia r_j algorytm można podsumować za pomocą relacji rekurencyjnej:

$$\begin{cases} r_{-1} = a \\ r_0 = b \\ q_j = \left\lfloor \frac{r_{j-2}}{r_{j-1}} \right\rfloor \\ r_j = r_{j-2} - r_{j-1} q_j, \qquad j \geqslant 1. \end{cases} \tag{4}$$

Dodatkowo, rozpisując każdą kolejną iterację, otrzymuje się x, y spełniające (3):

$$\begin{aligned} r_1 &= a - q_1 b = \underbrace{1}_{x_1} \cdot a + \underbrace{(-q_1)}_{y_1} \cdot b \\ r_2 &= b - q_2 r_1 = b - q_2 (x_1 a + y_1 b) = \underbrace{-x_1 q_2}_{x_2} \cdot a + \underbrace{1 - y_1 q_2}_{y_2} \cdot b \\ r_3 &= r_1 - q_3 r_2 = \underbrace{x_1 - x_2 q_3}_{x_3} \cdot a + \underbrace{y_1 - y_2 q_3}_{y_3} \cdot b \\ &\vdots \\ r_i &= \underbrace{(x_{i-2} - x_{i-1} q_i)}_{x_i} \cdot a + \underbrace{(y_{i-2} - y_{i-1} q_i)}_{y_i} \cdot b \end{aligned}$$

Dla $i = n - 1$ otrzymuje się rozkład $d = NWD(a,b)$ na sumę postaci (3), gdzie $x = x_{n-1}$ oraz $y = y_{n-1}$.
Przykłady:

1. $a = 1920$ oraz $b = 162$

$$\begin{array}{rcl} r_1 & = & 1920 - 11 \cdot 162 = 138 \quad \Rightarrow \quad x_1 = 1 \quad y_1 = -11 \\ r_2 & = & 162 - 1 \cdot 138 = 24 \quad \Rightarrow \quad x_2 = -1 \quad y_2 = 12 \\ r_3 & = & 138 - 5 \cdot 24 = 18 \quad \Rightarrow \quad x_3 = 6 \quad y_3 = -78 \\ r_4 & = & 24 - 1 \cdot 18 = 6 \quad \Rightarrow \quad x_4 = -7 \quad y_4 = 83 \\ r_5 & = & 18 - 3 \cdot 6 = 0 \end{array}$$

$NWD(1920, 162) = 6$, $x = -7$, $y = 83$.

2. $a = 8280$ oraz $b = 990$

$$\begin{array}{rcl} r_1 & = & 8290 - 8 \cdot 990 = 360 \quad \Rightarrow \quad x_1 = 1 \quad y_1 = -8 \\ r_2 & = & 990 - 2 \cdot 360 = 270 \quad \Rightarrow \quad x_2 = -2 \quad y_2 = 17 \\ r_3 & = & 360 - 1 \cdot 270 = 90 \quad \Rightarrow \quad x_3 = 3 \quad y_3 = -25 \\ r_4 & = & 360 - 4 \cdot 90 = 0 \end{array}$$

$NWD(8280, 990) = 90$, $x = 3$, $y = -25$.

Uwaga! Liczby x oraz y nie są wyznaczone jednoznacznie, tzn:

$$d = xa + yb = \begin{cases} (x+b)a + (y-a)b \\ (x-b)a + (y+a)b \\ (x+2b)a + (y-2a)b \\ (x+57b)a + (y-57a)b \\ (x-101b)a + (y+101a)b \\ \vdots \end{cases} \tag{5}$$

3 Szyfr RSA

Generacja klucza publicznego i prywatnego

1. Generacja dwóch (dużych) liczb pierwszych p oraz q (np. sitem Eratostenesa).

2. Wyznaczenie liczb $n = p \cdot q$ oraz $m = (p-1)(q-1)$.

3. Wybór (losowej) liczby $1 < e < m$ takiej, że $NWD(e, m) = 1$.

4. Wyznaczenie liczby dodatniej d odwrotnej do e w ciele $\mathbb{Z}_m$, tzn. takiej, że:

$$e \cdot d = 1 \pmod m$$

W tym celu można posłużyć się algorytmem Euklidesa. Ponieważ z założenia $NWD(e, m) = 1$ to 1 można rozłożyć na sumę dwóch iloczynów (3):

$$1 = x \cdot e + y \cdot m \pmod m \tag{6}$$
$$= x \cdot e \pmod m \tag{7}$$

Więc poszukiwana liczba $d = x$, o ile jest dodatnia. Jeżeli tak nie jest należy wykorzystać zależność (5).

5. Kluczem publicznym jest para (n,e) a kluczem prywatnym para (n,d)

Szyfrowanie wiadomości t będącej pewną liczbą naturalną odbywa się przy wykorzystaniu klucza publicznego i polega na wyliczeniu

$$s = t^e \mod n$$

Deszyfrowanie szyfrogramu s będącej pewną liczbą naturalną odbywa się przy wykorzystaniu klucza prywatnego i polega na wyliczeniu

$$t = s^d \mod n$$

Przykłady:

a) Niech $p = 191$ i $q = 523$ (p i q odpowiednio 43 oraz 99 z kolei liczbą pierwszą). Wtedy:

$$\begin{aligned} n &= pq = 99893 \\ m &= (p-1)(q-1) = 99180 \end{aligned}$$

Należy „wylosować” e takie, że $NWD(e, m) = 1$, np. $e = 601$
Wykorzystując rozszerzony algorytm Euklidesa, sprawdzając, że $NWD(e, m) = 1$ wyznacza się liczbę $x = 6601$. Ponieważ $x > 0$ to poszukiwana $d = x$.
Otrzymuje się klucz publiczny (99893,601) oraz prywatny (99893,6601)
Dla przykładowej wiadomości $t = 1410$, szyfrogram s jest postaci:

$$s = 1410^{601} = 43521 \pmod{99893}$$

Deszyfrowania szyfrogramu s odbywa się w sposób:

$$t = 43521^{6601} = 1410 \pmod{99893}$$

b) Niech $p = 1489$ i $q = 2957$ (p i q odpowiednio 237 oraz 426 z kolei liczbą pierwszą). Wtedy:

$$\begin{aligned} n &= pq = 4402973 \\ m &= (p-1)(q-1) = 4398528 \end{aligned}$$

Należy „wylosować” e takie, że $NWD(e, m) = 1$, np. $e = 1703$
Wykorzystując rozszerzony algorytm Euklidesa, sprawdzając, że $NWD(e, m) = 1$ wyznacza się liczbę $x = -1301737$. Ponieważ $x < 0$ to poszukuje innego rozwiązania wykorzystując własność (5) otrzymując $d = 3096791$.
Otrzymuje się klucz publiczny (4402973,1703) oraz prywatny (4402973,3096791)
Dla przykładowej wiadomości $t = 1969$, szyfrogram s jest postaci:

$$s = 1969^{1703} = 1556059 \pmod{4402973}$$

Deszyfrowania szyfrogramu s odbywa się w sposób:

$$t = 1556059^{3096791} = 1969 \pmod{4402973}$$

c) Niech $p = 2131$ i $q = 677$ (p i q odpowiednio 321 oraz 123 z kolei liczbą pierwszą). Wtedy:

$$\begin{aligned} n &= pq = 1442687 \\ m &= (p-1)(q-1) = 1439880 \end{aligned}$$

Należy „wylosować” e takie, że $NWD(e, m) = 1$, np. $e = 7$.
Wykorzystując rozszerzony algorytm Euklidesa, sprawdzając, że $NWD(e, m) = 1$ wyznacza się liczbę $x = -205697$. Ponieważ $x < 0$ to poszukuje innego rozwiązania wykorzystując własność (5) otrzymując $d = 1234183$.
Otrzymuje się klucz publiczny (1442687,7) oraz prywatny (1442687,1234183)
Dla przykładowej wiadomości $t = 21969$, szyfrogram s jest postaci:

$$s = 21969^{7} = 1382858 \pmod{1442687}$$

Deszyfrowania szyfrogramu s odbywa się w sposób:

$$t = 1382858^{1234183} = 21969 \pmod{1442687}$$

4 ZADANIA

1. Dla dwóch zadanych w konsoli, dodatnich liczb naturalnych $i, j < 200\ 000$ napisać, przy wykorzystaniu sita Eratostenesa, program zwracający i-tą i j-tą liczbę pierwszą (np. dla $i = 78983$ oraz $j = 100000$ program ma zwrócić 999 983 oraz 1 299 709).

2. Dla dwóch zadanych w konsoli, dodatnich liczb naturalnych a oraz b napisać, przy wykorzystaniu rozszerzonego algorytmu Euklidesa program zwracający $d = NWD(a, b)$ oraz liczby x i y z rozkładu $d = xa + yb$

3. Dla zadanych w konsoli, dodatnich liczb naturalnych i, j oraz e napisać program generujący klucz prywatny oraz publiczny dla algorytmu RSA dla p i q będących (odpowiednio) i-tą oraz j-tą liczbą pierwszą. **Uwaga! Liczba „losowa"** e **ma być zadawana w konsoli!**

Punktacja:

- 1 punkty - Sito Eratostenesa dla $i, j < 10\ 000$
- 2 punkty - Sito Eratostenesa dla $i, j < 200\ 000$
- 4 punkty - Rozszerzony algorytm Euklidesa
- 3 punkty - Generacja kluczy RSA