Rozkład liczb na czynniki.

9 grudnia 2013

Sito Eratostenesa
Korzystamy z faktów:
1) przy testowani pierwszości liczby a, można ograniczyć się do dzielników pierwszych nieprzekraczających $\sqrt{a}$
2) Jeśli liczba całkowita $a > 1$ nie dzieli się przez żadną liczbę pierwszą $p \leqslant \sqrt{a}$ to a jest pierwsza
Algorytm Eratostenesa polega na kolejnych wielokrotności z listy 2...n .
Przykład:
$2, 3, \not4, 5, \not6, 7, \not8, 9, \not10, 11, \not12, 13, \not14, 15, \not16, 17, \not18, 19, \not20, 21, \not22, 23, \not24, 25, \not26, 27, \not28, 29, \not30, 31, \not32, 33, \not34, 35, \not36, 37, /$
$38, 39, \not40$ krok 1 - skreślenie wielokrotności 2
$3, 5, 7, \not9, 11, 13, \not15, 17, 19, \not21, 23, 25, \not27, 29, 31, \not33, 35, 37, \not39$ krok 2 -kolejną liczbą na liście jest 3, skreślenie wielokrotności 3 (co 3 liczba)
$3, 5, 7, \not9, 11, 13, \not15, 17, 19, \not21, 23, \not25, \not27, 29, 31, \not33, \not35, 37, \not39$ krok 3 -kolejną liczbą na liście jest 5, skreślenie wielokrotności 5 (co 5 liczba)
$3, 5, 7, \not9, 11, 13, \not15, 17, 19, /\not21, 23, \not25, \not27, 29, 31, \not33, \not35, 37, \not39$ krok 4 -kolejną liczbą na liście jest 7, skreślenie wielokrotności 7 (co 7 liczba). Ponieważ ostatnia z liczb na liście (37) jest mniejsza od 7*7=49, to algorytm kończy działanie.
Rozszerzony algorytm Eklidesa
Algorytm ten oblicza największy wspólny dzielnik liczb a i b (NWD(a,b)=d) oraz liczby x i y takie, że xa+yb=d. Ponieważ:

$$\begin{aligned}
&a = bq_1 + r_1 \quad r_1 = ax_1 = by_1 \qquad (1)\\
&b = r_1q_2 + r_2 \quad r_2 = ax_2 + by_2\\
&r_1 = r_2q_3 + r_3 \quad r_3 = ax_3 + by_3\\
&r_2 = r_3q_4 + r_4 \quad r_4 = ax_4 + by_4\\
&r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \quad r_{n-1} = ax_{n-a} + by_{n-a}\\
&r_{n-2} = r_{n-1}q_n \quad r_n = 0
\end{aligned}$$

Dane można umieścić w tablicy gdzie $r_j = r_{j-2} - r_{j-1}q_j$ a $x_j = x_{j-2} - q_jx_{j-1}$, $y_j = y_{j-2} - q_jy_{j-1}$. Ponieważ $a = ax_{-1} + by_{-1}$,

a	q	x	y
a	-	x_{-1}	y_{-1}
b	-	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

$b = ax_0 + by_0$ to $x_{-1} = 1$, $x_{-1} = 0$,$x_0 = 0$,$y_0 = 1$. Kroki wykonuje się dopóki $q_j \neq 0$.
Algorytm RSA

1. Generowanie dwóch dużych liczb pierwszych P i Q przy pomocy sita Eratostenesa
2. Wyznaczenie N=PQ, $\varphi(N) = (P-1)(Q-1)$
3. wybór losowej liczby $1 < E < \varphi(N)$ dla której NWD(e, $\varphi(N)$)=1
4. Wyznaczanie liczby D odwrotnej do e modulo φ_N, czyli takiej, że ED = 1 mod φ_N - przy pomocy algorytmu Euklidesa (ostatnia liczba y)
5. kluczem publicznym jest (N,E) a prywatnym (N,D)
6. szyfrowanie c = m^E mod N
7. deszyfrowanie m= c^D mod N