Kryptografia

http://www.liczbypierwsze.com

Duże liczby pierwsze są często wykorzystywane w kryptografii ze względu na swe specyficzne właściwości. Dla przykładu opiszę kryptosystem RSA. Wykorzystujemy tutaj dwie pary kluczy : klucz publiczny i klucz prywatny.

Algorytm RSA:

Najpierw generujemy klucz publiczny oraz klucz prywatny:

- wybieramy losowo dwie liczby pierwsze p i q.
- obliczamy iloczyn tych liczb n=pq
- obliczamy wartość funkcji Eulera dla n : $\varphi(n)=(p-1)(q-1)$
- wybieramy liczbę e z przedziału [1,n] względnie pierwszą z $\varphi(n)$
- znajdujemy liczbę d : $d=e^{-1} \bmod \varphi(n)$
- klucz publiczny to para liczb (n,e)
- klucz prywatny to para liczb (n,d)

Szyfrowanie i deszyfrowanie

- Aby zaszyfrować wiadomość dzielimy ją na bloki mi o wartości nie większej niż n
- Teraz każdy z bloków szyfrujemy według wzoru : $c_i = m_i^e \bmod n$
- Natomiast aby odszyfrować wiadomość musimy każdy z bloków c_i odszyfrować według wzoru : $m_i = c_i^d \bmod n$