29.05.2018

Patryk Kaczmarek
Mateusz Rędzia

Emedia

Algorytm szyfrowania RSA

RSA - Jest to niesymetryczny algorytm szyfrujący, którego zasadniczą cechą są dwa klucze: publiczny do kodowania informacji oraz prywatny do jej odczytywania.

Działanie algorytmu RSA krok po kroku:

1. Generowany jest klucz publiczny oraz klucz prywatny. Klucz publiczny jest ogólnodostępny, natomiast prywatny należy chronić przed światem zewnętrznym.
2. Użytkownik może szyfrować swoje dane za pomocą klucza publicznego. (Taka wiadomość nie może zostać rozszyfrowana za pomocą tego samego klucza)
3. Adresat wiadomości może rozszyfrować ją jedynie w przypadku kiedy posiada klucz prywatny.

Generowanie kluczy RSA:

1. Należy znaleźć dwie duże liczby pierwsze (mające przykładowo po 128 bitów)
2. Należy obliczyć wartość funkcji Eulera dla tych liczb oraz ich iloczyn
3. Z wykorzystaniem algorytmu Euklidesa należy znaleźć liczbę E, która jest względnie pierwsza z wyliczoną wartością funkcji Eulera
4. Należy obliczyć liczbę odwrotną modulo funkcji Eulera do liczby E.
5. Kluczem publicznym jest para liczb - liczba E oraz iloczyn wygenerowanych na początku liczb pierwszych.
6. Klucz prywatny to również para liczb - liczba odwrotna modulo funkcji Eulera do liczby E (podpunkt 4.) oraz iloczyn wygenerowanych na początku liczb pierwszych.

Generowanie dużych liczb pierwszych z wykorzystaniem testu Millera-Rabina:

1. Losujemy dużą liczbę
2. Rozpoczynamy sprawdzenie czy wylosowana liczba jest pierwsza (za pomocą testu Millera-Robina)
3. Należy obliczyć s, czyli maksymalną potęgę dwójki dzielącą n-1
4. Podstawiamy d = n/2s
5. W pętli k razy powtarzamy czynności
    1. Losujemy a>1 i jednocześnie a<n
    2. Sprawdzamy czy ad mod n nie równa się 1
    3. Jeżeli tak, to sprawdzamy czy ad*2r mod n nie równa się n-1 dla wszystkich r (dla $0 \leqq r \leqq s-1$)
    4. Jeśli tak, to kończymy test. Liczba nie jest liczbą pierwszą.
6. Jeśli nie przerwano testu, oznacza to że liczba prawdopodobnie jest pierwsza