Kochajmy RSA!

SEKCJA 1 - “Dlaczego RSA jest nam potrzebne?”

Algorytm RSA jest jednym z najpopularniejszych asymetrycznych algorytmów kryptograficznych. Jest stosowany w szyfrowaniu wiadomości, w operacjach między bankami oraz w komunikatorach internetowych. To w głównej mierze on dba o nasze Internetowe bezpieczeństwo!

SEKCJA 2 - “Przykład działania RSA”

To tak, jakby rozdawać kłódki wszystkim swoim znajomym, każdy może zamknąć pudełko i wysłać je do ciebie, ale to ty jesteś jedyną osobą, która może otworzyć pudełka. Gdy znajomy zamknie pudełko, nawet on sam nie będzie mógł go otworzyć. Dystrybucja kłódek jest bardzo łatwa. Klucze publiczne są takie same - możesz je bezpiecznie upublicznić.

SEKCJA 3 - “Co składa się na algorytm RSA?”

Możemy wyróżnić 3 główne fazy algorytmu:

1. Generowanie kluczy. Ten publiczny przekazujemy do wszystkich zainteresowanych, a prywatny zatrzymujemy tylko dla siebie. To on w przyszłości umożliwi nam rozszyfrowanie danych.
2. Szyfrowanie danych za pomocą klucza publicznego. Tak otrzymany szyfrogram przekazujemy zainteresowanym instytucjom. Nie musimy się martwić o jego bezpieczeństwo, ponieważ algorytm jest nieodwracalny.
3. Adresat po otrzymaniu wiadomości rozszyfrowuje ją za pomocą tajnego klucza.

SEKCJA 4 - “Tworzenie publicznego klucza RSA”

Wygeneruj swój przykładowy klucz publiczny.

[tu się wyświetli klucz]

SEKCJA 5 - “Tworzenie prywatnego klucza RSA”

Teraz musimy wygenerować dla Ciebie klucz prywatny! W normalnych warunkach, nie powinien go zobaczyć nikt poza Tobą.

[tu się wygeneruje klucz]

SEKCJA 6 - “Szyfrowanie danych za pomocą klucza”

Możesz teraz zaszyfrować dowolną wiadomość!

[klucz publiczny] - [tekst do zaszyfrowania]
Oto twój szyfrogram: [szyfrogram]

SEKCJA 7 - “Deszyfrowanie danych za pomocą klucza”

Teraz spróbujmy to rozszyfrować!

[klucz prywatny] - [szyfrogram]
Czy to twoja wiadomość? [rozszyfrowana wiadomość]

SEKCJA 8 - “Podsumowanie”

I co? Już rozumiesz?
My też nie. A tak swoją drogą… w trakcie twojej nauki, złamano właśnie **x[to sie jakoś policzy]%** szyfru RSA o wielkości 128 bitów!

Chcesz jeszcze coś zaszyfrować? Wejdź na [/playground]!

ŹRÓDŁA:

- https://home.agh.edu.pl/~zobmat/2021/rzepka_radoslaw/zastosowania.html
- https://eduinf.waw.pl/inf/alg/001_search/0067.php
- https://bezkomputera.wmi.amu.edu.pl/ppi/chapters/coding-encryption.html
- https://www.doyler.net/security-not-included/cracking-256-bit-rsa-keys