Kryptografia z kluczem publicznym.

Mariusz Strzelecki (szczeles@mat.umk.pl)
Na podstawie notatek dra Bobińskiego

7 lipca 2009

1 Podstawowe definicje

Celem *kryptografii* jest opracowanie metod przekazywania wiadomości, które uniemożliwią jej odczytanie osobom niepowołanym w przypadku jej przechwycenia.

Definicja 1.1. *Systemem kryptograficznym* nazywamy trójkę (P, C, f), gdzie
P - zbiór symboli używanych do zapisu tekstu jawnego
C - zbiór symboli używanych do zapisu tekstu zakodowanego
$f : P \to C$ - bijekcja, zwana *funkcją szyfrującą*
Funkcję odwrotną (czyli $f^{-1} : C \to P$) nazywamy *funkcją deszyfrującą*.

Szyfr asymetryczny, czyli inaczej *system z kluczem publicznym* to taki, gdzie znajomość klucza szyfrującego nie wystarcza do odczytania wiadomości. Przykładem takiego szyfru jest RSA.

2 R(ivest)S(hamir)A(dleman)

Niech p, q będą różnymi (i dużymi! - dla prawdziwych zastosowań) liczbami pierwszymi, niech $n := pq$ oraz wybierzmy (losowo) liczbę $e \in [2, \varphi(n) - 1]$ taką, że $(e, \varphi(n)) = 1$. Definiujemy $P := [0, n - 1] := C$ oraz $f : P \to C$ zadaną wzorem $f(a) = a^e \bmod n$. Parę (n, e) nazywamy *kluczem szyfrującym*. Parę (n, d) nazywamy *kluczem deszyfrującym*, gdzie $d \in [2, \varphi(n) - 1]$ jest rozwiązaniem kongruencji $de \equiv 1 \pmod{\varphi(n)}$.

Lemat 2.1 (O działaniu RSA)**.** *Jeśli p i q są różnymi liczbami pierwszymi oraz $n = pq$ i $d, e \in [2, \varphi(n) - 1]$ i jednocześnie $de \equiv 1 \ (mod\ \varphi(n))$ to $a^{de} \equiv a \ (mod\ \varphi(n))$ dla dowolnego $a \in \mathbb{Z}$.*

Dowód. Z twierdzenie Eulera wiemy, że jeśli $(a, p) = 1$ to $a^{\varphi(p)} \equiv 1 \pmod{p}$. Ponieważ $\varphi(n) = \varphi(p)\varphi(q)$ (z własności tej funkcji), to również mamy $a^{\varphi(n)} \equiv 1 \pmod{p}$. W dodatku wiemy, że $\varphi(n) | de - 1$, skąd $a^{de-1} \equiv 1 \pmod{p}$. Pomnóżmy obie strony przez a i już mamy $a^{de} \equiv a \pmod{p}$. Analogicznie liczymy dla q. Ponieważ $n = pq$, więc $a^{de} \equiv a \pmod{n}$. □

Uwaga 2.2. Dowód nie jest do końca prawdziwy ☺. Na początku założyliśmy, że $(a, p) = 1$, a przecież w lemacie mamy $a \in \mathbb{Z}$, więc wcale nie muszą być względnie pierwsze. W dowodzie dra Bobińskiego jest sobie zdanie „ta kongruencja jest również prawdziwa, gdy $(a, p) \neq 1$". Niestety nie potrafię tego pokazać, więc w dobrym tonie byłoby napisać w lemacie $a \in \mathbb{Z} \cap [0, min(p, q) - 1]$, stąd niniejsza uwaga.

Uwaga 2.3. Wyliczenie d wymaga znajomości $\varphi(n)$, czyli znajomości rozkładu $n = pq$. O ile wylosowanie dwóch liczb pierwszych i ich wymnożenie jest prostą operacją arytmetyczną, to rozkład liczby na dwa duże czynniki pierwsze jest niebanalny. Dzięki temu RSA jest bezpieczny, nie występuje problem dystrybucji kluczy.

Są jeszcze inne systemy kryptograficzne z kluczem publicznym, ale ten jest raczej najprostszy ☺