Dokumentacja końcowa projektu
Algorytm DSA

Jakub Turek

Podstawy teoretyczne

FIPS[1] jest zbiorem, w którym opisane są publiczne standardy bezpieczeństwa używane przez federalny rząd Stanów Zjednoczonych. Oficjalnym standardem podpisywania wiadomości cyfrowych zamieszczonym w FIPS jest DSS (ang. Digital Signature Standard). DSS opiera się o algorytm DSA (ang. Digital Signature Algorithm).

Standard DSS (wraz z algorytmem DSA) został opisany w dokumencie FIPS PUB 186[2]. Na potrzeby projektu zaimplementowany został oryginalny algorytm opublikowany w 1994 roku, który wykorzystuje funkcję skrótu SHA.

Algorytm

Generacja kluczy Wybierz parametry:

- Liczba pierwsza p w pierścieniu reszt modulo a, gdzie $2^{L-1} < p < 2^L$ oraz $512 \leqslant L \leqslant 1024$ i L jest wielokrotnością 64.
- Liczba pierwsza q będąca dzielnikiem liczby $p-1$ w pierścieniu reszt modulo a, gdzie $2^{159} < q < 2^{160}$.
- Liczba $g = h^{\frac{p-1}{q}} \pmod p$, gdzie h jest dowolną liczbą naturalną spełniającą warunek $1 < h < p-1$ taką, że $h^{\frac{p-1}{q}} \pmod p > 1$ (czyli g ma rząd $q \pmod p$).
- Losowo wygenerowana liczba x z przedziału $0 < x < q$.
- Liczba $y = g^x \pmod p$.
- Losowo wygenerowana liczba k z przedziału $0 < k < q$.

Liczby p, q oraz g są publiczne. Klucz prywatny użytkownika to x, natomiast klucz publiczny użytkownika to y. Parametr k musi być obliczany dla każdego nowego podpisu. Klucze są wielokrotnego użytku.

Podpisywanie wiadomości Podpisem wiadomości M jest para liczb (r, s) obliczanych według poniższego wzoru:

$$\begin{aligned} r &= (g^k \mod p) \mod q \\ s &= (k^{-1}(SHA(M) + xr)) \mod q \end{aligned}$$

gdzie k^{-1} jest odwrotnością liczby k w pierścieniu reszt modulo q (czyt. $k \cdot k^{-1} \equiv 1 \pmod q$).

Opcjonalnie można zweryfikować, czy $r \neq 0$ i $s \neq 0$. Jeżeli jeden z warunków nie jest spełniony, należy wygenerować podpis od nowa. Sytuacja taka nie powinna się jednak zdarzyć dla prawidłowo wygenerowanych kluczy.

[1] Skrót od **F**ederal **I**nformation **P**rocessing **S**tandard (ang. federalny standard przetwarzania informacji).
[2] `http://www.itl.nist.gov/fipspubs/fip186.htm`.