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.

[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`.