Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №3

За пятый семестр

По дисциплине: «Криптографические методы защиты информации»

**Тема: «Программная реализация ЭЦП»**

Выполнила:

Студент 3 курса

Группы ИИ-23

Макаревич Н.Р.

Проверила:

Хацкевич А. С.

Брест 2024

**Цель:** создать программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.

**Ход работы:**

**Вариант 3** (Цифровая подпись Шнора)

**Задание:**

#include "ShnorDigitalSignature.h"

ShnorDigitalSignature::ShnorDigitalSignature() {

do p = randomInRange(160, 256);

while (!isPrime(p));

do q = randomInRange(3, p - 1);

while (!isPrime(q) || (p - 1) % q != 0);

do a = randomInRange(1, p - 1);

while (modExp(a, q, p) != 1);

s = randomInRange(1, q);

v = modInverse(modExp(a, s, q), q);

std::cout << "p: " << p << "\n";

std::cout << "q: " << q << "\n";

std::cout << "a: " << a << "\n";

std::cout << "s: " << s << "\n";

std::cout << "v: " << v << "\n";

}

std::pair <unsigned long long, unsigned long long> ShnorDigitalSignature::sign(const std::string& message) {

unsigned long long r = randomInRange(1, q);

unsigned long long X = modExp(a, r, p);

unsigned long long e = hashFunction(X, message);

unsigned long long y = (r + s \* e) % q;

std::cout << "Signing: r = " << r << ", X = " << X << ", e = " << e << ", y = " << y << std::endl;

return { e, y };

}

bool ShnorDigitalSignature::verify(std::pair<unsigned long long, unsigned long long> signature, const std::string& message) {

long long exp = signature.second - s \* signature.first;

long long X\_prime = modExp(a, exp, p);

long long e\_prime = hashFunction(X\_prime, message);

std::cout << "Verifying: X' = " << X\_prime << ", e' = " << e\_prime << std::endl;

return signature.first == e\_prime;

}

unsigned long long ShnorDigitalSignature::hashFunction(int r, const std::string& message) {

std::hash<std::string> hasher;

return hasher(std::to\_string(r) + message) % q;

}

**Вывод:** создал программу, которая реализует алгоритм криптографической системы Шнора.