Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОССУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОННИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №6

По дисциплине «Методы защиты информации»

По теме «Цифровая подпись»

Выполнил:

студент гр. 653502

Максименко П.В.

Проверил:

Артемьев В. С.

Минск 2019

1. Постановка зада4и

Написать программу, реализующую алгоритм цифровой подписи ГОСТ 34.10-2018, используя для хеш-функции ГОСТ Р 34.11-2012.

2. Теорети4еская 4асть

ГОСТ 34.10-2018 (полное название: «ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», англ. «Information technology. Cryptographic data security. Signature and verification processes of electronic digital signature») — действующий [межгосударственный](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D0%B3%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) [криптографический](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) [стандарт](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82), описывающий алгоритмы формирования и проверки [электронной цифровой подписи](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C) реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем. Стандарт разработан на основе национального стандарта Российской Федерации ГОСТ Р 34.10-2012 и введен в действие с [1 июня](https://ru.wikipedia.org/wiki/1_%D0%B8%D1%8E%D0%BD%D1%8F) [2019 года](https://ru.wikipedia.org/wiki/2019_%D0%B3%D0%BE%D0%B4) приказом [Росстандарта](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B0%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BF%D0%BE_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%BC%D1%83_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8E_%D0%B8_%D0%BC%D0%B5%D1%82%D1%80%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8) № 1059-ст от [4 декабря](https://ru.wikipedia.org/wiki/4_%D0%B4%D0%B5%D0%BA%D0%B0%D0%B1%D1%80%D1%8F) [2018 года](https://ru.wikipedia.org/wiki/2018_%D0%B3%D0%BE%D0%B4).

«Стрибог» — [криптографический](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) алгоритм вычисления [хеш-функции](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) с размером блока входных данных 512 [бит](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) и размером [хеш-кода](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D0%BA%D0%BE%D0%B4) — 256 или 512 [бит](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). Разработан Центром защиты информации и специальной связи [ФСБ России](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) с участием [ОАО «ИнфоТеКС»](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D0%A2%D0%B5%D0%9A%D0%A1) на основе национального стандарта Российской Федерации ГОСТ Р 34.11-2012 и введен в действие с [1 июня](https://ru.wikipedia.org/wiki/1_%D0%B8%D1%8E%D0%BD%D1%8F) [2019 года](https://ru.wikipedia.org/wiki/2019_%D0%B3%D0%BE%D0%B4) приказом [Росстандарта](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B0%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BF%D0%BE_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%BC%D1%83_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8E_%D0%B8_%D0%BC%D0%B5%D1%82%D1%80%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8) № 1060-ст от [4 декабря](https://ru.wikipedia.org/wiki/4_%D0%B4%D0%B5%D0%BA%D0%B0%D0%B1%D1%80%D1%8F) [2018 года](https://ru.wikipedia.org/wiki/2018_%D0%B3%D0%BE%D0%B4). Стандарт ГОСТ Р 34.11-2012 разработан и введён в качестве замены устаревшему стандарту [ГОСТ Р 34.11-94](https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_34.11-94).

3. Блок-схема

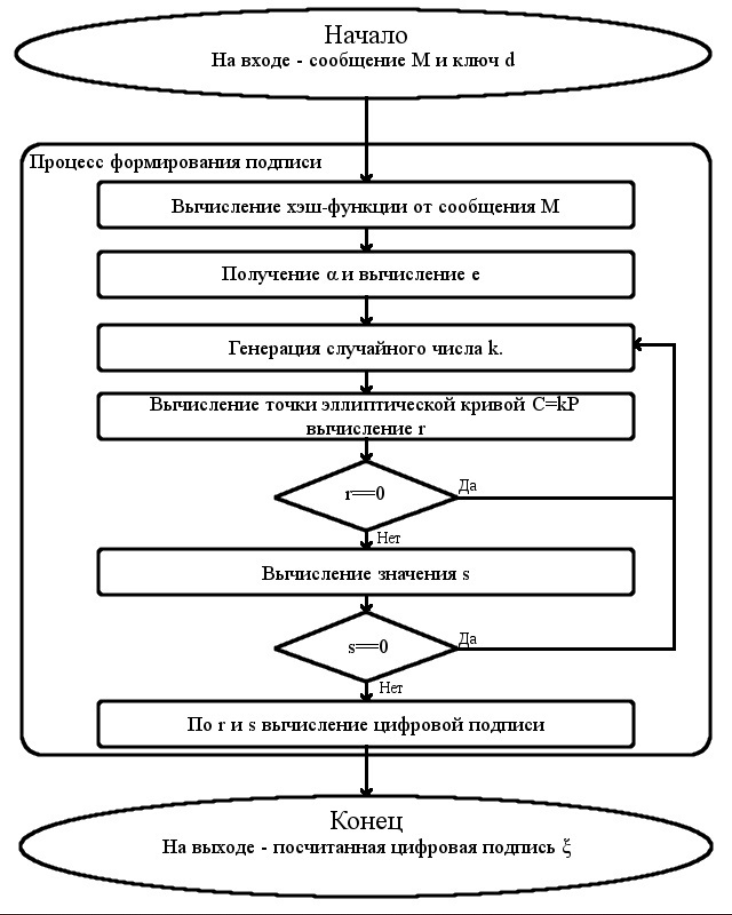


Рис 3.1. Схема работы алгоритма.

4. Ход программы



Рис 4.1. Данные, поступающие на вход



Рис 4.2. Хеширование данных



Рис 4.3. Вы4исление “e” и то4ки эллипти4еской кривой



Рис 4.4. Формирование вектора цифровой подписи

5. Код программы

#include <Windows.h>

#include <iostream>

#include <fstream>

#include <string>

#include <vector>

using namespace std;

std::string Hash\_Stribog(string inp\_data)

{

int n = 8;

string data = inp\_data;

if (data.length() > n)

{

for (int i = n; i < inp\_data.length(); i++) {

if (i % 8 == 0)

{

data.insert(n + i, "-");

}

}

}

while (data.length() % n != 0)

{

data = data + "0";

}

return data;

}

std::vector<float> EDS(string inp\_data)

{

std::cout << "inp\_data = " << inp\_data << std::endl;

int p = 13;

// elliptic curve

int a = 2;

int b = 3;

float J = int(1728 \* (4 \* pow(a, 3) / (4 \* pow(a, 3) + 27 \* pow(b, 2)))) % p;

int m = 5;

int q = 11;

float P[2] = {1, 2};

int d = 10; // 0 < d < q

// encrypt data

string data = Hash\_Stribog(inp\_data);

std::cout << "hashed data = " << data << std::endl;

float e = data.length() % q;

if (e == 0) { e = 1; }

int k = 9; // 0 < k < q

int C[2];

C[0] = k \* P[0];

C[1] = k \* P[1];

float r = C[0] % q;

float s = int(r \* d + k \* e) % q;

std::vector<float> DS(2);

DS.push\_back(r);

DS.push\_back(s);

return DS;

}

int main()

{

SetConsoleCP(1251);

SetConsoleOutputCP(1251);

// lab6

// EDS

string data = "00001110001011000001111000001110110001111";

EDS(data);

return 0;

}

6. Вывод

В ходе выполнения лабораторной работы был успешно реализован алгоритм создания электронной цифровой подписи. Были выявлены его сильные и слабые стороны, а также возможности улу4шения.

Криптостойкость цифровой подписи опирается на две компоненты — на стойкость хеш-функции и на стойкость самого алгоритма шифрования.

Вероятность взлома хеш-функции по ГОСТ 34.11-94 составляет {\displaystyle 1{,}73\times {10}^{-77}}1.73\*10^-77 при подборе коллизии на фиксированное сообщение и {\displaystyle 2{,}94\times {10}^{-39}}2.94\*10^-39 при подборе любой коллизии. Стойкость алгоритма шифрования основывается на проблеме дискретного логарифмирования в группе точек эллиптической кривой. На данный момент нет метода решения данной проблемы хотя бы с субэкспоненциальной сложностью.