Министерство образования Республики Беларусь

Учреждение образования БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

Отчёт по лабораторной работе №6

По теме «Цифровая подпись»

Выполнили: студент гр. 053501 Кривецкий Р. А.

Проверил: ассистент кафедры информатики Лещенко Е. А.

Минск 2023

**СОДЕРЖАНИЕ**

[1 Теоретические сведения 3](#_Toc148061125)

[2 Программная реализация 4](#_Toc148061126)

[Заключение 5](#_Toc148061127)

[Приложение А(обязательное) Листинг программного кода 6](#_Toc148061128)

# 1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Цифровая подпись - это один из ключевых элементов современной криптографии, который обеспечивает аутентификацию и целостность данных в цифровой среде. Она играет важную роль в обеспечении безопасности электронных коммуникаций, электронной коммерции, систем передачи данных и многих других областях. В рамках данной лабораторной работы мы будем исследовать и изучать один из криптографических стандартов, широко применяемых в России - ГОСТ 34.10.

ГОСТ 34.10 является российским стандартом для цифровой подписи, разработанным с целью обеспечения безопасной передачи и хранения данных, а также аутентификации пользователей и защиты информации. Он определяет алгоритмы и процедуры для создания и проверки электронных подписей, которые обеспечивают высокую стойкость к атакам и обеспечивают доверие в цифровом мире.

Блок-схема алгоритма электронно-цифровой подписи представлена на рисунке 1.1.

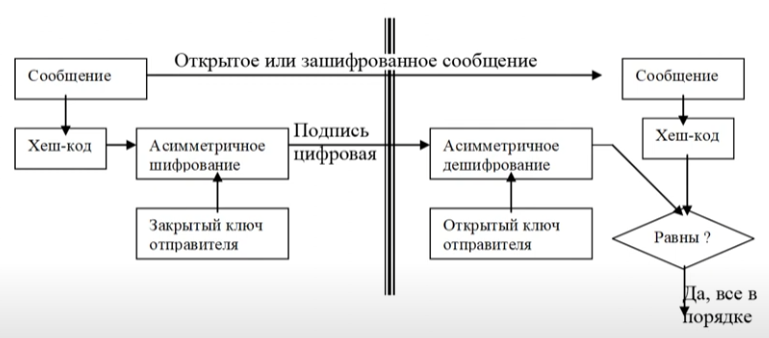


Рисунок 1.1 – Алгоритм электронно-цифровой подписи

Блок-схема алгоритма формирования цифровой подписи представлена на рисунке 1.2.

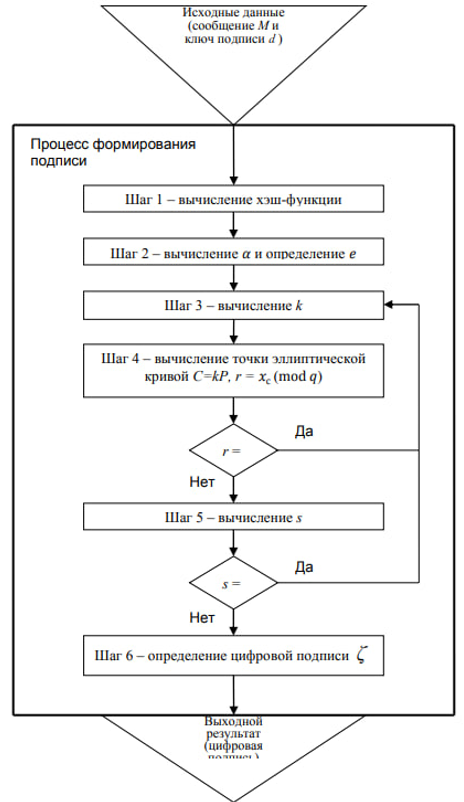


Рисунок 1.2 – Алгоритм формирования цифровой подписи

Блок-схема алгоритма верификации цифровой подписи представлена на рисунке 1.3.

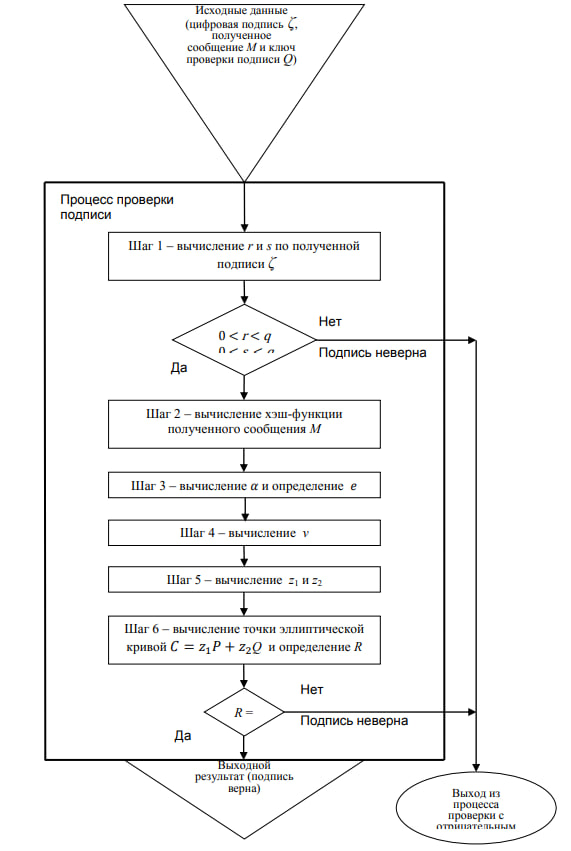
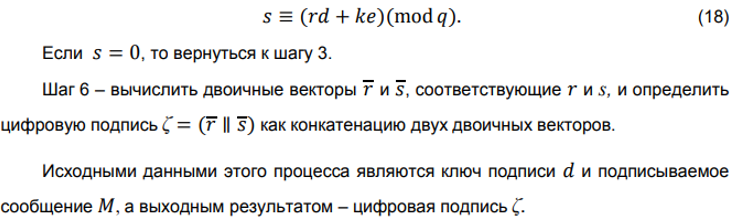
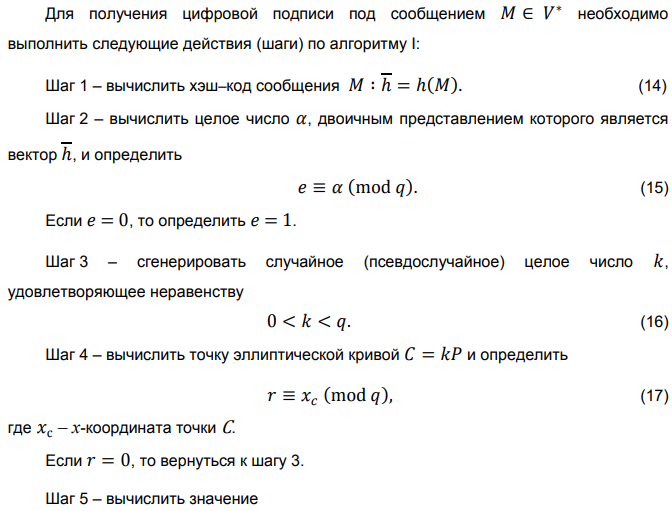
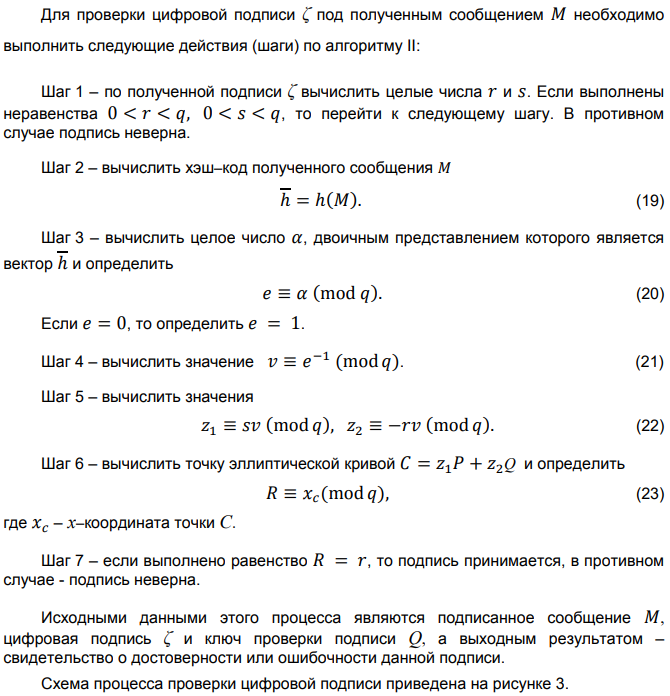


Рисунок 1.3 – Алгоритм верификации цифровой подписи





**2 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ**

Необходимо реализовать программное средство формирования и проверки ЭЦП на базе алгоритма ГОСТ 34.10. Программное средство реализовано на языке программирования Python. Демонстрация работы показана на рисунке 2.1

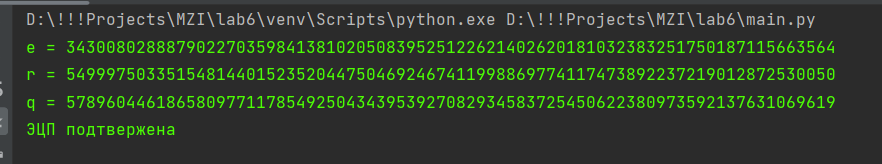


Рисунок 2.1 — Демонстрация работы

# ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы по формированию и проверке ЭЦП (Электронной Цифровой Подписи) на базе алгоритма ГОСТ 34.10 были достигнуты следующие важные результаты и усвоены основные концепции криптографии:

Понимание цифровой подписи: Мы изучили суть цифровой подписи и её значение в современной криптографии. Убедились в том, что она является неотъемлемой частью обеспечения безопасности данных в цифровой эпохе, обеспечивая аутентификацию и целостность информации. Основы ГОСТ 34.10: Изучение алгоритма ГОСТ 34.10 позволило нам понять, как работает этот стандарт, включая основы асимметричной криптографии и эллиптических кривых, используемых в данном алгоритме. Мы создали программное средство для формирования и проверки ЭЦП с использованием алгоритма ГОСТ 34.10. В ходе разработки, мы изучили математические операции, необходимые для создания подписи и её проверки.

# ПРИЛОЖЕНИЕ А

(**обязательное)**

**Листинг программного кода**

Файл main.py

from ec import ECPoint

from gost3410 import DSgost

if \_\_name\_\_ == '\_\_main\_\_':

p = 57896044618658097711785492504343953926634992332820282019728792003956564821041

a = 7

b = 43308876546767276905765904595650931995942111794451039583252968842033849580414

q = 57896044618658097711785492504343953927082934583725450622380973592137631069619

x = 2

y = 4018974056539037503335449422937059775635739389905545080690979365213431566280

message = 207988936744764520171340615615082701306371425153796532899526172526600008872421

gost = DSgost(p, a, b, q, x, y)

key = gost.gen\_keys()

d = key[0]

q\_x = key[1].x

q\_y = key[1].y

r, s = gost.encrypt(message, d)

print(f"r = {r}\nq = {q}")

public\_key = ECPoint(q\_x, q\_y, a, b, p)

is\_verified = gost.verify(message, (r, s), public\_key)

if is\_verified:

print("ЭЦП подтвержена")

else:

print("ЭЦП не подтвержена")