Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

ОТЧЁТ

к лабораторной работе №6

на тему

**ЦИФРОВАЯ ПОДПИСЬ**

Выполнил: студент гр.253505 Ющук И.А.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[Введение 3](#_Toc207721845)

[1 Ход работы 4](#_Toc207721846)

[Заключение 5](#_Toc207721847)

[Приложение А (обязательное) Листинг программного кода 6](#_Toc207721848)

# ВВЕДЕНИЕ

Современный этап развития информационных технологий характеризуется повсеместным обменом цифровыми документами и острой необходимостью обеспечения их подлинности и юридической значимости. Под аутентичностью понимается гарантия того, что электронный документ был создан конкретным отправителем и не подвергался изменениям после подписания. Для решения этой фундаментальной задачи информационной безопасности используются механизмы электронной цифровой подписи (ЭЦП).

В отличие от алгоритмов симметричного шифрования, ЭЦП основана на принципах асимметричной криптографии и представляет собой математическую схему, обеспечивающую проверку подлинности электронных документов. Она преобразует произвольный массив данных в уникальную цифровую подпись фиксированной длины с использованием закрытого ключа подписанта. Ключевыми свойствами ЭЦП являются невозможность подделки (стойкость к созданию подписи без знания закрытого ключа), неотрекаемость (невозможность отказа от факта подписания) и гарантия целостности (любые изменения документа делают подпись недействительной).

Одним из таких стандартов является российский алгоритм ГОСТ Р 34.10-2012, который существует в двух вариантах: на эллиптических кривых и на основе дискретного логарифмирования. Его основное преимущество заключается в соответствии требованиям безопасности Российской Федерации и использовании современных криптографических преобразований. Алгоритм работает в связке с хеш-функцией ГОСТ Р 34.11-2012 («Стрибог»), что обеспечивает высокий уровень криптостойкости.

Целью данной лабораторной работы является теоретическое и практическое изучение принципов работы электронной цифровой подписи и реализация программного средства формирования и проверки ЭЦП. В рамках работы будет проведена реализация и анализ отечественного стандарта ГОСТ 34.10-2012. Это позволит на практике оценить математические основы алгоритма, этапы формирования и проверки подписи, а также особенности криптографических преобразований.

Программное средство будет включать модуль генерации ключевой пары, модуль формирования цифровой подписи с использованием закрытого ключа и модуль проверки подписи с использованием открытого ключа. Реализация позволит продемонстрировать практическое применение криптографических принципов и обеспечить понимание механизмов работы современных систем цифровой подписи.

# **1 ХОД РАБОТЫ**

В рамках выполнения лабораторной работы была реализована система электронной цифровой подписи на базе алгоритма ГОСТ Р 34.10-2012 на языке Python.

На первом этапе проведено изучение математических основ и структуры алгоритма цифровой подписи. Особое внимание уделено изучению теории эллиптических кривых, генерации ключевых пар и механизмов формирования и проверки подписи. Для ГОСТ 34.10-2012 изучены принципы работы с закрытым и открытым ключом, процесс хеширования по ГОСТ 34.11-2012 и математические преобразования при создании подписи.

После освоения теоретического материала приступили к практической реализации. Были написаны функции для генерации параметров эллиптической кривой, создания ключевой пары и обработки входных сообщений. Для ГОСТ 34.10-2012 реализованы алгоритмы формирования цифровой подписи с использованием закрытого ключа и проверки подписи с использованием открытого ключа.

Для проверки корректности работы алгоритма проведено тестирование на стандартных тестовых векторах из документации. Реализована функция визуализации подписи и ключей в шестнадцатеричном представлении.

Исходные данные представлены на рисунке 1.1.



Рисунок 1.1 – Входные данные

Программа была в результате появился текст. Процесс работы программы представлен на рисунке 1.2.

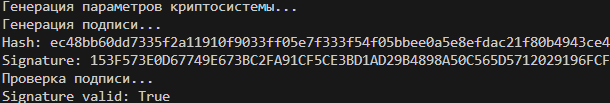


Рисунок 1.2 – Результат работы программы

# ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы была успешно реализована система электронной цифровой подписи на базе алгоритма ГОСТ Р 34.10-2012. Практическая реализация охватила все ключевые этапы работы с ЭЦП: генерацию параметров эллиптической кривой, создание ключевой пары, формирование цифровой подписи с использованием закрытого ключа и верификацию подписи с помощью открытого ключа. Основным достижением работы стало создание работоспособного программного средства формирования и проверки ЭЦП, наглядно демонстрирующего принципы работы современной криптографической системы.

Реализация подтвердила теоретические положения алгоритма, в частности, важность корректного выполнения математических операций на эллиптической кривой и строгого соблюдения процедуры формирования подписи. Особое значение имела точная реализация взаимодействия с хеш-функцией ГОСТ Р 34.11-2012 и преобразования хеш-значения в число для вычислений. Разработанная система продемонстрировала способность надежно подписывать электронные документы и детектировать любые попытки их изменения после подписания.

Практическая ценность работы заключается в создании инструмента для изучения принципов работы электронной цифровой подписи. Реализованная система может использоваться для демонстрации механизмов обеспечения аутентичности и целостности данных, изучения математических основ эллиптической криптографии, а также для понимания особенностей отечественного криптографического стандарта. В процессе реализации были приобретены навыки работы с большими числами, освоены методы криптографических преобразований и отработаны приемы тестирования систем цифровой подписи.

Перспективы развития работы включают оптимизацию алгоритмов для работы с большими объемами данных, реализацию поддержки различных форматов ключей и сертификатов, а также исследование стойкости реализованного алгоритма к различным типам криптоатак. Дальнейшее развитие может включать интеграцию с системами защищенного электронного документооборота.

Таким образом, реализованная система электронной цифровой подписи представляет собой законченное решение, которое демонстрирует принципы построения криптографических средств аутентификации и служит основой для дальнейшего изучения современных методов обеспечения информационной безопасности.

# ПРИЛОЖЕНИЕ А (обязательное) Листинг программного кода

def generate\_signature(message, p, q, g, d):

# Шаг 1 - Вычисление хэш-кода

h = hash\_message(message)

# Шаг 2 - Преобразование хэша в число e

a = int.from\_bytes(h, byteorder='big')

e = a % q

if e == 0:

e = 1

while True:

# Шаг 3 - Генерация k

k = random.randint(1, q - 1)

# Шаг 4 - Вычисление точки C = kP и r = x\_c mod q

r = pow(g, k, p) % q

if r == 0:

continue

# Шаг 5 - Вычисление s = (r\*d + k\*e) mod q

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

if s == 0:

continue

return r, s, h

def verify\_signature(message, p, q, g, Q, r, s):

# Шаг 1 - Проверка границ r и s

if not (0 < r < q and 0 < s < q):

return False

# Шаг 2 - Вычисление хэш-кода

h = hash\_message(message)

# Шаг 3 - Преобразование хэша в число e

a = int.from\_bytes(h, byteorder='big')

e = a % q

if e == 0:

e = 1

# Шаг 4 - Вычисление v = e^{-1} mod q

v = pow(e, -1, q)

# Шаг 5 - Вычисление z1 = s\*v mod q, z2 = -r\*v mod q

z1 = (s \* v) % q

z2 = (-r \* v) % q

# Шаг 6 - Вычисление точки C = z1\*P + z2\*Q и R = x\_c mod q

C = (pow(g, z1, p) \* pow(Q, z2, p)) % p

R = C % q

# Шаг 7 - Проверка R == r

return R == r

if \_\_name\_\_ == "\_\_main\_\_":

message = "Calm. Kindness. Kinship. Love."

q = generate\_q()