Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина «Методы защиты информации»

**ОТЧЕТ**

к лабораторной работе

на тему:

**«Цифровая подпись»**

|  |  |
| --- | --- |
|  | Выполнил:  Слуцкий Никита Сергеевич,  студент группы 053505 |
|  | Проверил: Лещенко Евгений Александрович, ассистент каф. Информатики |

Минск 2023

СОДЕРЖАНИЕ

[Введение 3](#_Toc149242799)

[1 Краткие теоретические сведения 4](#_Toc149242800)

[2 Ход выполнения работы 5](#_Toc149242801)

[Заключение 6](#_Toc149242802)

[Приложение А 7](#_Toc149242803)

# Введение

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 будет реализован один из криптографических стандартов – ГОСТ 34.10.

Целью данной лабораторной работы является реализовать программное средство работы с алгоритмом ГОСТ 34.10. А также оформить отчёт в соответствии со стандартом предприятия БГУИР.

# 1 Краткие теоретические сведения

Электронная цифровая подпись позволяет подтвердить авторство электронного документа. Подпись связана как с автором, так и с самим документом с помощью криптографических методов и не может быть подделана с помощью обычного копирования.

ЭЦП – это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Широко применяемая в настоящее время технология электронной подписи основана на асимметричном шифровании с открытым ключом и опирается на следующие принципы:

1 Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. Механизм генерации ключей строго определён и является общеизвестным. При этом каждому открытому ключу соответствует определённый закрытый ключ. Если, например, Иван Иванов публикует свой открытый ключ, то можно быть уверенным, что соответствующий закрытый ключ есть только у него.

2 Имеются надёжные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.

3 Если электронный документ поддается расшифровке с помощью открытого ключ, то можно быть уверенным, что он был зашифрован с помощью уникального закрытого ключа. Если документ расшифрован с помощью открытого ключа Ивана Иванова, то это подтверждает его авторство: зашифровать данный документ мог только Иванов, т.к. он является единственным обладателем закрытого ключа.

Однако шифровать весь документ было бы неудобно, поэтому шифруется только его хеш – небольшой объём данных, жёстко привязанный к документу с помощью математических преобразований и идентифицирующий его. Механизм хеширования строго определён и является общеизвестным. Шифрованный хеш и является электронной подписью.

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.

# 2 Ход выполнения работы

В рамках лабораторной работы были созданы два проекта на языке программирования C++ и языке программирования Python. Ввиду требований работы с крайней большими числами целесообразным для дальнейшего развития оказался вариант на втором упомянутом языке программирования, потому что он поддерживает работу с длинной арифметикой из коробки.

В приложении с листингом кода предоставлена вырезка кода с классом Gost3410 без инициализации полей класса. Реализованное программное средство имеет возможность зашифровать сообщение, а затем проверить цифровую подпись.

# Заключение

В ходе выполнения данной работы было произведено ознакомление с теорией об алгоритме электронно-цифровой подписи ГОСТ 34.10, реализовано программное средство для верификации на языке программирования Python и языке программирования C++. Цель лабораторной работы, поставленная во введении настоящего отчёта, можно считать достигнутой.

# Приложение А

(Листинг кода)

class Gost3410:

def generate\_keys(self):

d = random.randint(1, self.q - 1)

q\_point = d \* self.p\_point

return d, q\_point

def encrypt(self, message, private\_key):

e = message % self.q

print(f'e = {e}')

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

r, s = 0, 0

while r == 0 or s == 0:

c\_point = k \* self.p\_point

r = c\_point.x % self.q

s = (r \* private\_key + k \* e) % self.q

return r, s

def verify\_signature(self, message, encrypt, public\_key):

if not (0 < encrypt[0] < self.q) or not (0 < encrypt[0] < self.q):

return False

e = message % self.q

if e == 0:

e = 1

nu = ECPoint.\_mod\_inverse(e, self.q)

z1 = (encrypt[1] \* nu) % self.q

z2 = (-encrypt[0] \* nu) % self.q

c\_point = z1 \* self.p\_point + z2 \* public\_key

r = c\_point.x % self.q

if r == encrypt[0]:

return True

return False