Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №12**

по дисциплине Информационная безопасность

Тема: Исследование алгоритмов генерации и верификации электронной цифровой подписи

Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №12**

**Цель:** изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП).

2. Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра, а также DSA.

3. Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.

4. Оценить скорость генерации и верификации ЭЦП.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

# Теоретические сведения

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

Таким образом, ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

• аутентифицирование лица, подписавшего сообщение;

• контроль целостности подписанного сообщения;

• защита сообщения от подделок;

• доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшие отличительные особенности ЭЦП:

• ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);

• указанная бинарная последовательность зависит от содержания подписываемого сообщения.

Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

ЭЦП на основе RSA. Здесь можно рассматривать две ситуации:

• сообщение Мo подписывается и передается в открытом (незашифрованном) виде;

• сообщение Мo подписывается и передается в зашифрованном виде.

При этом подпись S вычисляется на основе соотношения:

S ≡ (H(Mo))dо modno.

Передаваемое сообщение М' = Мo||S. Соответственно, операция расшифрования на приемной стороне (получатель анализирует Мп||S) производистя с известной модификацией ключей:

H(Mo) ≡ (S) ео modno.

Далее вычисляется Н(Mп). Если H(Mo) = H(Mп), подпись верифицирована.

Если подписываемое сообщение М(М') также должно передаваться в зашифрованном виде, то обычно М' шифруется на стороне отправителя стандартным образом: с помощью открытого ключа получателя (еп и nп), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: dп и nп. Далее осуществляются вычисления и анализ, как и в первом случае.

Основное отличие в применении расчетов в алгоритме Эль-Гамаля состоит в том, что результатом зашифрования является только одна пара чисел, а не пара для каждого блока исходного сообщения. Причем в рассматриваемом случае таким сообщением является хеш подписываемого документа: Н(Mо).

Алгоритм ЭЦП К. Шнорра (К. Schnorr) является вариантом алгоритма ЭЦП Эль-Гамаля. Одной из особенностей ЭЦП Эль-Гамаля является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуемая длина p должна составлять по крайней мере 1024 бита. Чтобы уменьшить размер подписи, Шнорр предложил новую схему, но с уменьшенным размером подписи.

Ключевая информация: p – простое число в диапазоне от 512 до 1024 битов; q –160-битное простое число, делитель (p – 1); любое число g (g ≠ 1) такое, что

gq ≡ 1 mod p.

Числа p, g, q являются открытыми и могут применяться группой пользователей. Выбирается число х < q (х является тайным ключом) и вычисляется последний элемент открытого ключа:

y ≡ g–х mod p.

Секретный ключ имеет длину не менее 160 битов.

# Ход работы

Было необходимо разработать приложение, выполняющее генерацию и верификацию ЭЦП с помощью алгоритмов RSA, Эль-Гамаля и Шнорра.

Метод createDigitalSignature класса RSA принимает на вход оригинальный текст и подписывает его с помощью алгоритма RSA. Код метода представлен на рисунке 2.1.



Рисунок 2.1 – Метод генерации ЭЦП алгоритмом RSA

Метод verifyDigitalSignature класса RSA принимает на вход полученный от отправителя текст, электронную подпись и осуществляет верификацию подписи с помощью алгоритма RSA. Код метода представлен на рисунке 2.2.

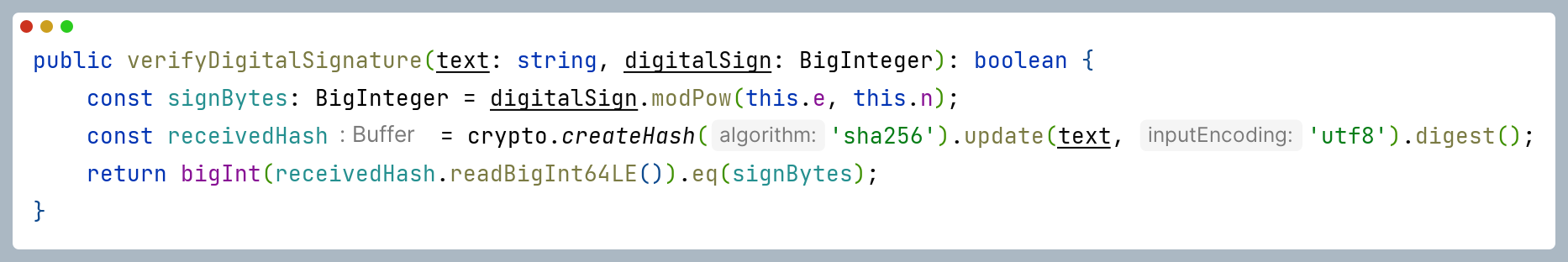


Рисунок 2.2 – Метод верификации ЭЦП алгоритмом RSA

Результат работы приложения с исходным текстом «Ivanov Ivan Ivanovich» представлен на рисунке 2.3.

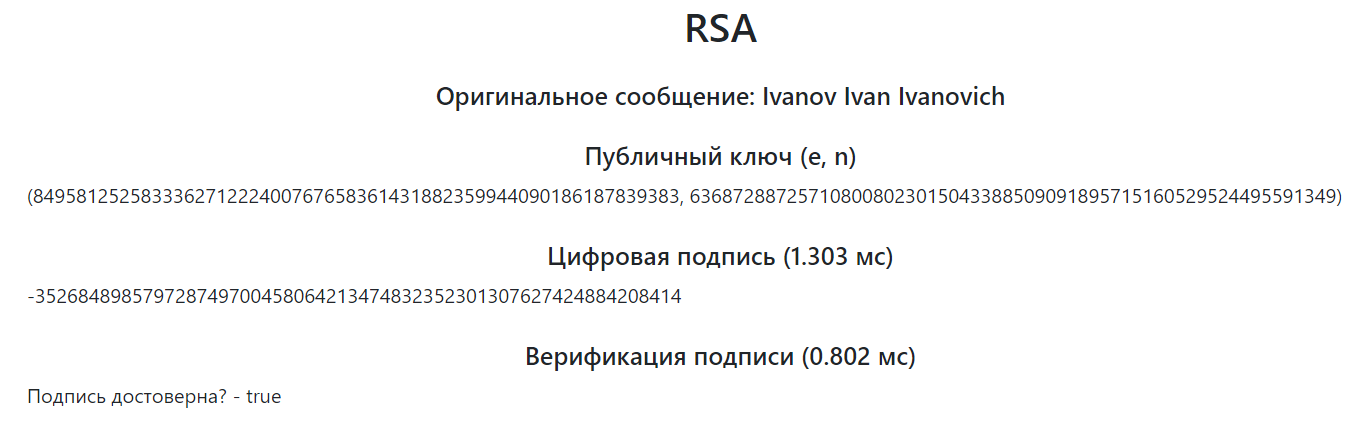


Рисунок 2.3 – Результат работы приложения

Время генерации подписи – около 1.3 мс. Время верификации подписи – около 0.8 мс.

Метод createDigitalSignature класса ElGamal принимает на вход оригинальный текст и подписывает его с помощью алгоритма Эль-Гамаля. Подписью являются два числа а и b (S = {a, b}). Число а вычисляется по формуле: a ≡ gk mod p. При вычислении параметра b, решается уравнение Н(Mо) ≡ (x\*a + k\*b) mod (p – 1). Код метода представлен на рисунке 2.4.



Рисунок 2.4 – Метод генерации ЭЦП алгоритмом Эль-Гамаля

Метод verifyDigitalSignature класса ElGamal принимает на вход полученный от отправителя текст, электронную подпись (массив из двух параметров: а и b) и осуществляет верификацию подписи с помощью алгоритма Эль-Гамаля. Для верификации подписи вычисляется хеш полученного сообщения Н(Мп) = h. Далее нужно убедиться, что выполняется равенство yaab ≡ ghmod p. Код метода представлен на рисунке 2.5.



Рисунок 2.5 – Метод верификации ЭЦП алгоритмом Эль-Гамаля

Результат работы приложения с исходным текстом «Ivanov Ivan Ivanovich» представлен на рисунке 2.6.

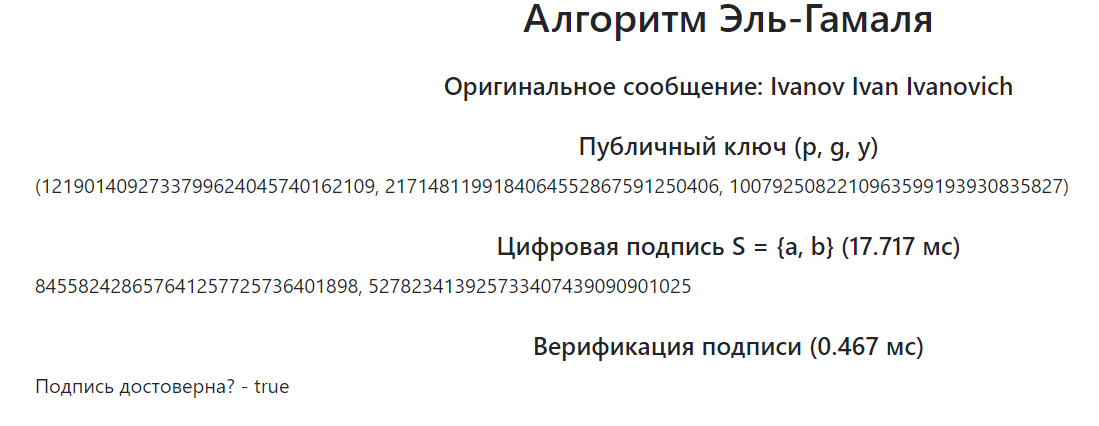


Рисунок 2.6 – Результат работы приложения

Время генерации подписи – около 18 мс. Верификация с помощью алгоритма Эль-Гамаля заняла немного меньше времени по сравнению с алгоритмом RSA и составило 0.5 мс.

Метод createDigitalSignature класса Schorr принимает на вход оригинальный текст и подписывает его с помощью алгоритма Шнорра. Ключевой информацией в алгоритме Шнорра являются числа p, g, q, y. p – простое число в диапазоне от 512 до 1024 битов; q –160-битное простое число, делитель (p – 1); любое число g (g ≠ 1) такое, что gq ≡ 1 mod p, число y ≡ g–х mod p. Для подписи сообщения Мо выбирается случайное число k (1 < k < q) и вычисляет параметр а: а ≡ gk mod p. Далее вычисляется хеш от канкатенации сообщения Мо и числа а: h = H(Mo||a). Далее вычисляется значение b: b ≡ (k + x\*h) mod q. Получателю отправляются М' = Мо||S; S = {h, b}.

Код метода представлен на рисунке 2.7.



Рисунок 2.7 – Метод генерации ЭЦП алгоритмом Шнорра

Метод verifyDigitalSignature класса Schorr принимает на вход полученный от отправителя текст, электронную подпись и осуществляет верификацию подписи с помощью алгоритма Шнорра. Для проверки подписи вычисляется Х ≡ gbyh (mod p). Затем он проверяет выполнение равенства: h = Н(Mп||Х). Подпись достоверна, если равенство выполняется. Код метода представлен на рисунке 2.8.



Рисунок 2.8 – Метод верификации ЭЦП алгоритмом Шнорра

Результат работы приложения с исходным текстом «Ivanov Ivan Ivanovich» представлен на рисунке 2.9.

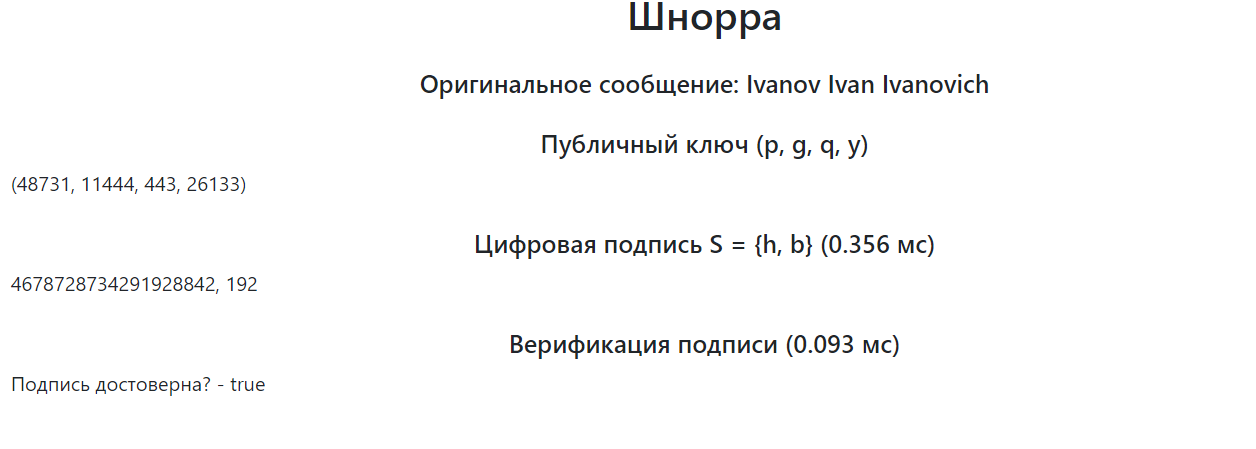


Рисунок 2.9 – Результат работы приложения

Время генерации подписи – около 0.35 мс. Время верификации подписи – около 0.09 мс.

**Вывод:** в ходе выполнения лабораторной работы был изучен принцип генерации и верификации ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра. Также было разработано приложение, выполняющее генерацию и верификацию ЭЦП на основе данных алгоритмов. Была оценена скорость генерации и верификации подписи.