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 №10**

по дисциплине Информационная безопасность

Тема: Исследование ассиметричных шифров RSA и Эль-Гамаля

        Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №10**

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости ассиметричных шифров RSA и Эль-Гамаля.

2. Разработать приложение для реализации асимметричного зашифрования/ расшифрования на основе алгоритмов RSA и Эль-Гамаля.

3. Выполнить анализ криптостойкости ассиметричных шифров RSA и Эль-Гамаля.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

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

# Теоретические сведения

Асимметричная криптография основана на сложности решения некоторых математических задач. По существу, таких задач две:

• разложение больших чисел на простые сомножители (задача факторизации);

• вычисление дискретного логарифма в конечном поле, а также вычислительные операции над точками эллиптической кривой.

Задача дискретного логарифмирования формулируется так: для данных целых чисел а и b, 1 < а, b < n, найти логарифм – такое целое число х, что

ax ≡ b (mod n),

если такое число существует.

Китайская теорема об остатках. В общем случае если разложение числа N на простые множители представляет собой p1p2…pt (некоторые простые числа могут встречаться несколько раз), то система уравнений

(x mod pi) ≡ ai,

где i = 1, 2, …, t, имеет единственное решение: x, меньшее N.

Алгоритм RSA. Для генерации двух ключей: тайного и открытого (а по сути –двух взаимосвязанных частей одного ключа, т. е. ключа, принадлежащего одному физическому лицу (или группе лиц), либо одному юридическому лицу), используются два больших случайных простых числа p и q. Для максимальной большей криптостойкости нужно выбирать p и q равной длины. Рассчитывается произведение: n = pq. Это есть один из трех компонент ключа, состоящего из чисел n, e, d.

Затем случайным образом выбирается второй компонент ключа: открытый ключ или ключ зашифрования, e, такой что e и (p – 1)(q – 1) являются взаимно простыми числами; (p – 1)(q – 1) = φ(n) – функция Эйлера.

Наконец, расширенный алгоритм Евклида используется для вычисления третьего компонента ключа: ключа расшифрования d такого, что выполняется условие:

ed ≡ 1 (mod φ(n)).

Зашифрование. Если шифруется сообщение М, состоящее из r блоков: m1, m2, …, mi, …, mr, то шифртекст С будет состоять из такого же числа (r) блоков, представляемых числами:

ci ≡ (mi)e mod n.

Расшифрование. Для расшифрования каждого зашифрованного блока производится вычисление вида:

mi ≡ (ci)dmod n.

Алгоритм Эль-Гамаля. Безопасность алгоритма Эль-Гамаля, как и безопасность алгоритма Диффи – Хеллмана, основана на трудности вычисления дискретных логарифмов. Алгоритм Эль-Гамаля фактически использует схему Диффи – Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

# Ход работы

В начале, с помощью простого консольного приложения составить табличную или графическую форму зависимости времени вычисления параметра у, функционально заданного выражением вида:

у ≡ ax mod n,

от параметров a, x, n.

Код приложения представлен на рисунке 2.1.



Рисунок 2.1 – Код приложения

Результат работы приложения приведен на рисунке 2.2.

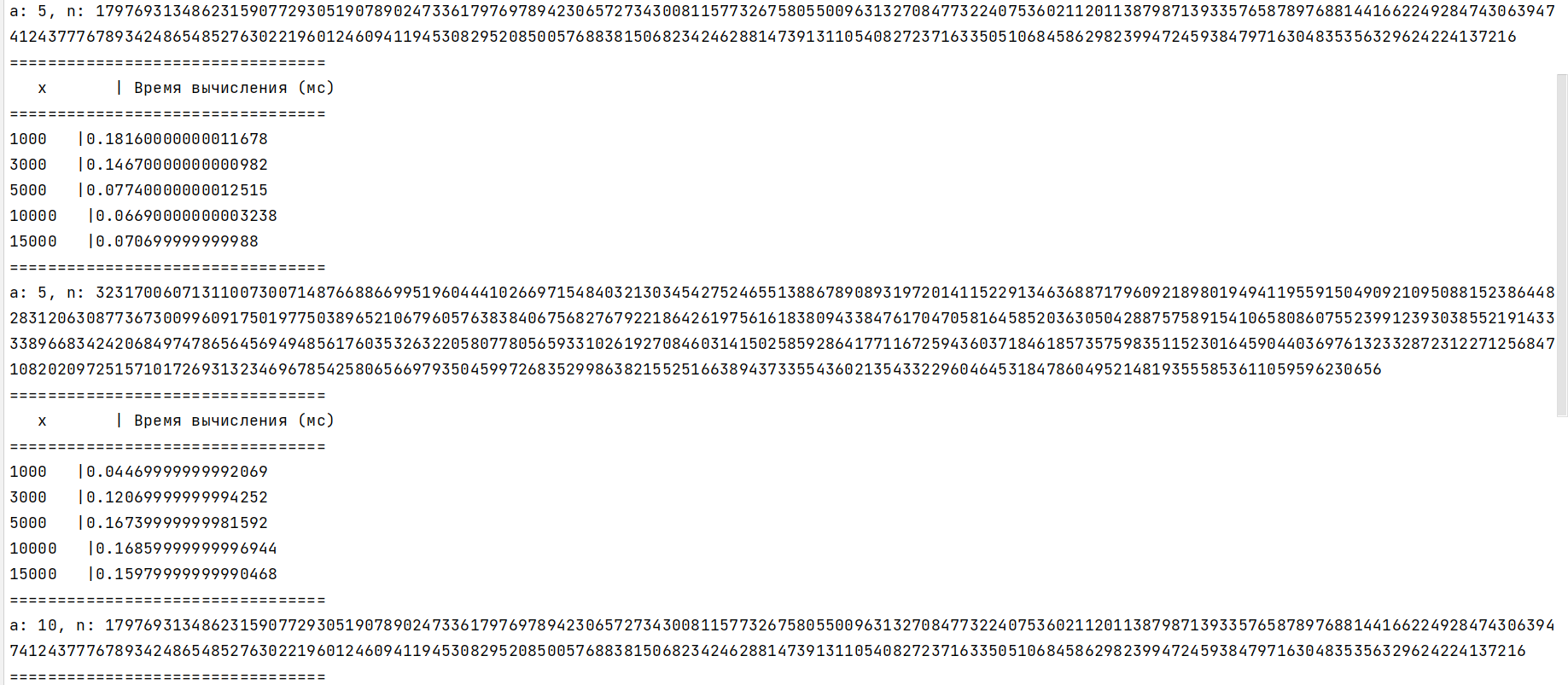


Рисунок 2.2 – Результат работы приложения

Далее было необходимо разработать приложение, выполняющее шифрование и расшифрование с помощью алгоритмов RSA и Эль-Гамаля.

Функция rsaEncrypt принимает на вход оригинальный текст и публичный ключ и осуществляет зашифрование с помощью алгоритма RSA. Код функции представлен на рисунке 2.3.

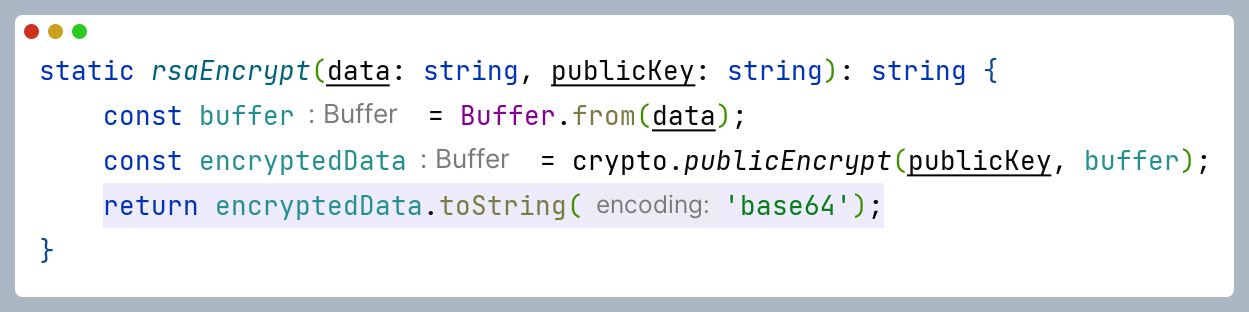


Рисунок 2.3 – Функция шифрования алгоритмом RSA

Функция rsaDecrypt принимает на вход зашифрованный текст и приватный ключ и осуществляет расшифрование с помощью алгоритма RSA. Код функции представлен на рисунке 2.4.

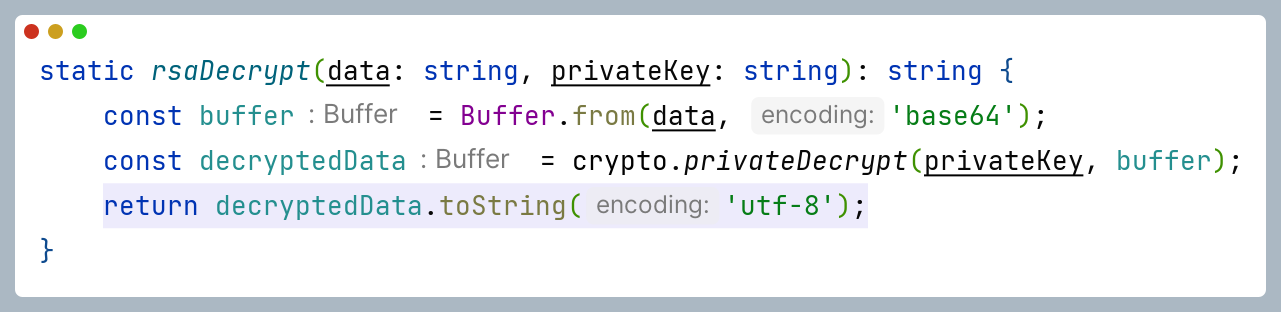


Рисунок 2.4 – Функция расшифрования алгоритмом RSA

Результат работы приложения с исходным текстом «Ivanov Ivan Ivanovich» представлен на рисунке 2.5.

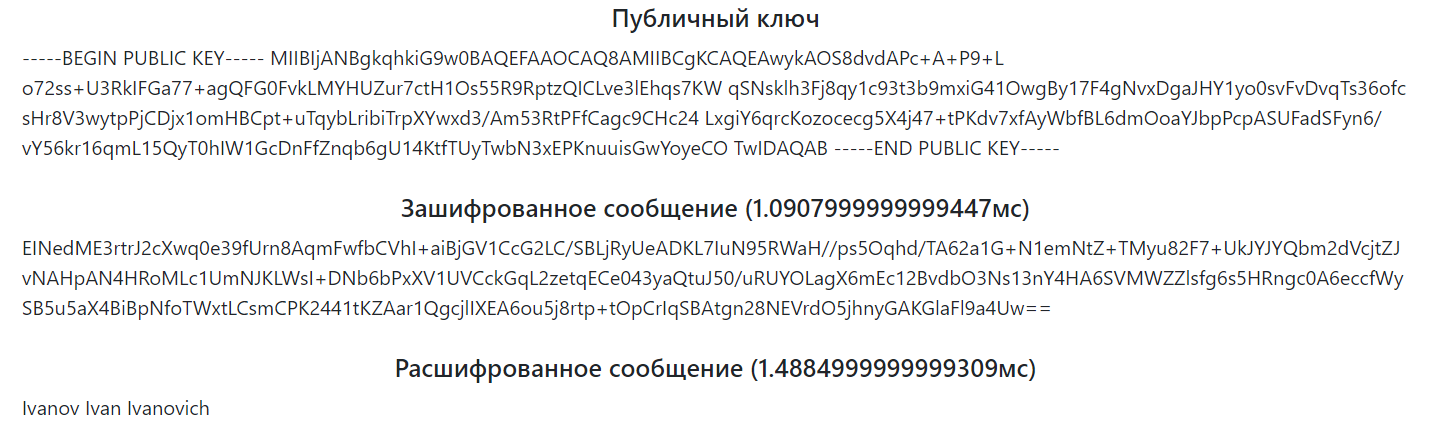


Рисунок 2.5 – Результат работы приложения

Время зашифрования сообщения – около 1 мс. Расшифрование заняло немного больше времени – около 1.5 мс.

Функция encryptElGamal принимает на вход оригинальный текст и параметры публичного ключа и осуществляет зашифрование с помощью алгоритма Эль-Гамаля. Код функции представлен на рисунке 2.6.

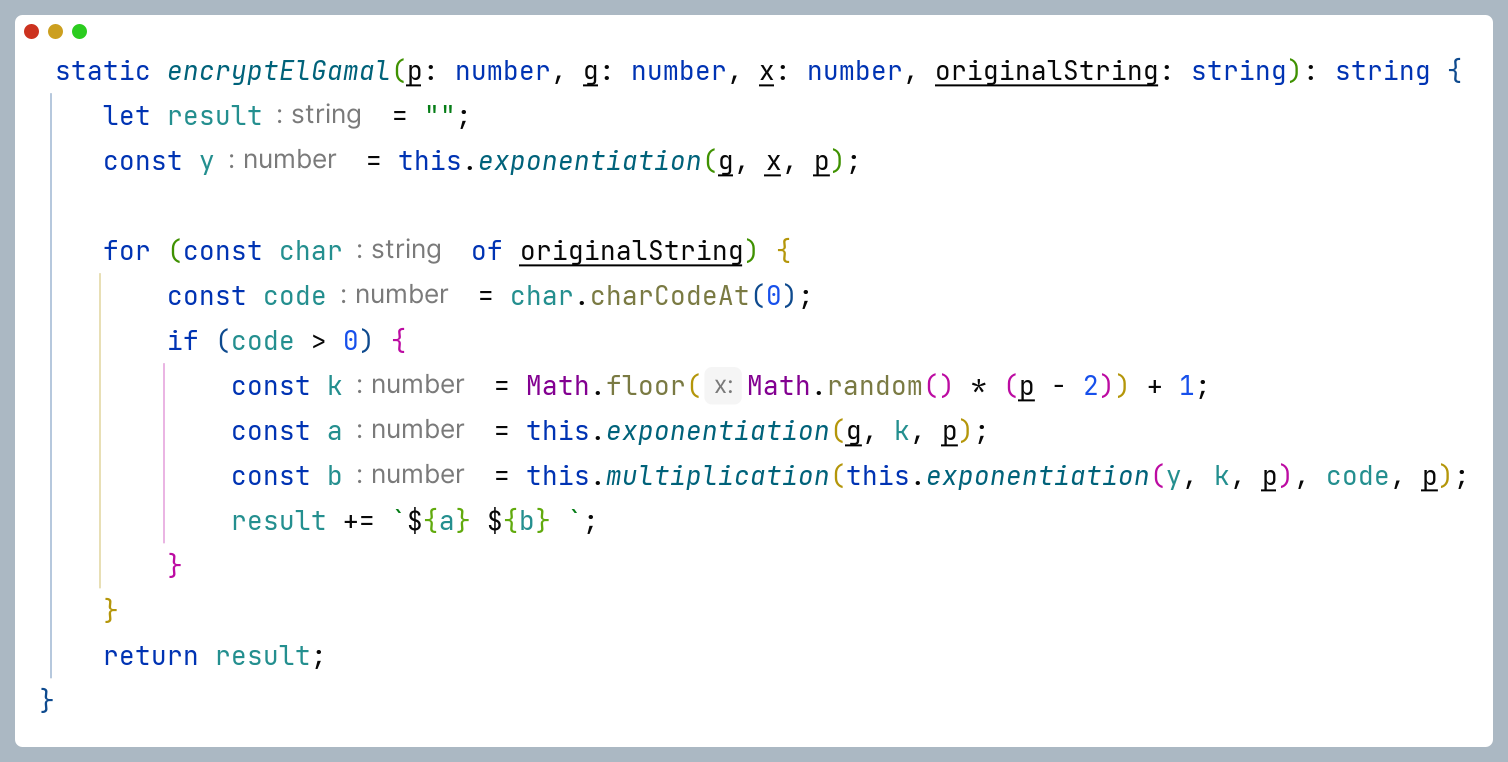


Рисунок 2.6 – Функция шифрования алгоритмом Эль-Гамаля

Функция decryptElGamal принимает на вход зашифрованный текст и приватный параметр x и осуществляет расшифрование с помощью алгоритма Эль-Гамаля. Код функции представлен на рисунке 2.7.

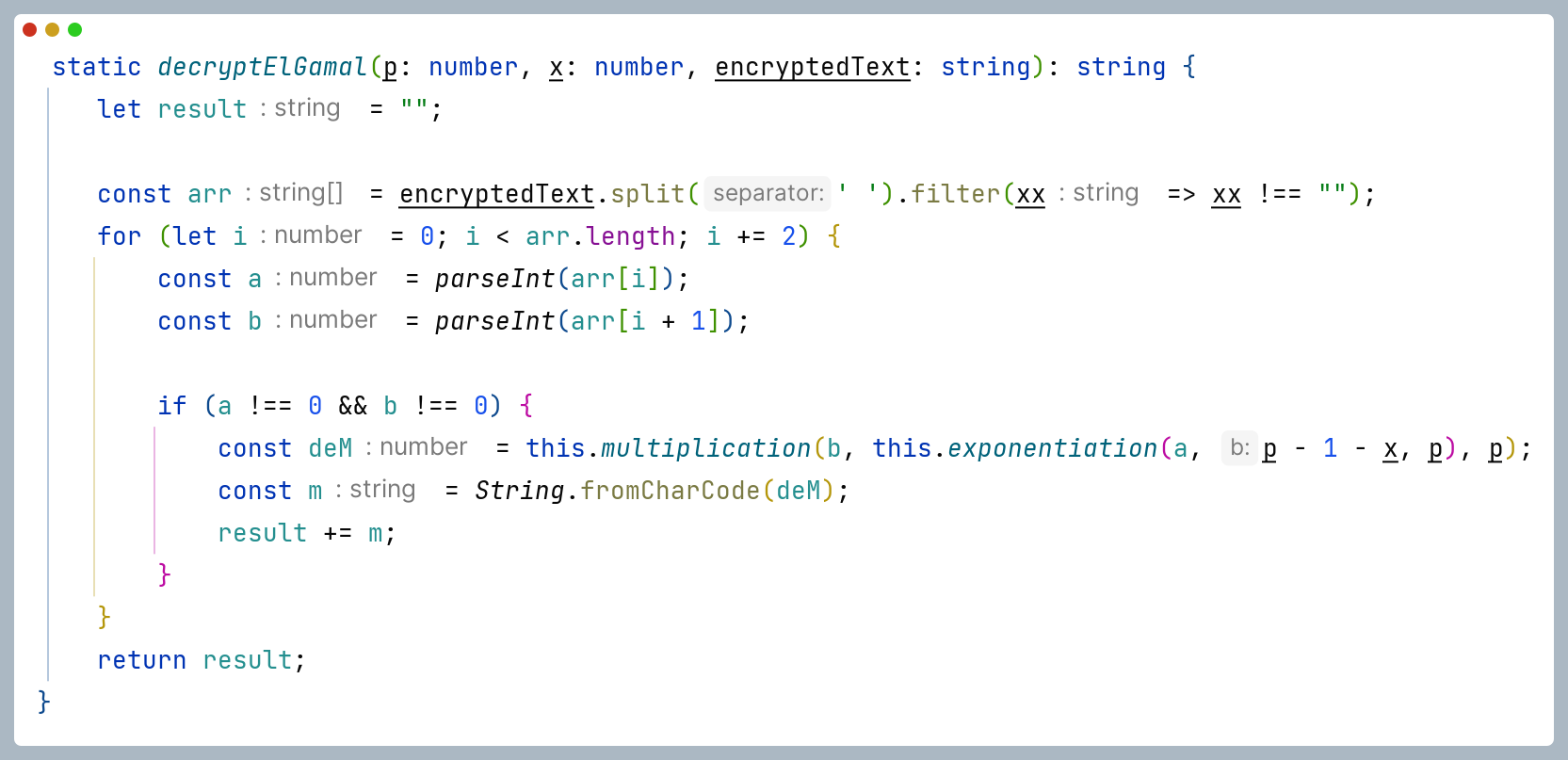


Рисунок 2.7 – Функция расшифрования алгоритмом Эль-Гамаля

Алгоритм Эль-Гамаля использует несколько параметров, которые являются ключевыми. Для начало было выбрано просто число p = 241. Далее было выбрано число g = 56, меньшее числа p и являющееся первообразным корнем числа p. Затем было выбрано число x = 9. Число x должно быть меньше, чем число p. Компонент y вычисляется внутри функции шифрования. Результат работы приложения с исходным текстом «Ivanov Ivan Ivanovich» представлен на рисунке 2.8.

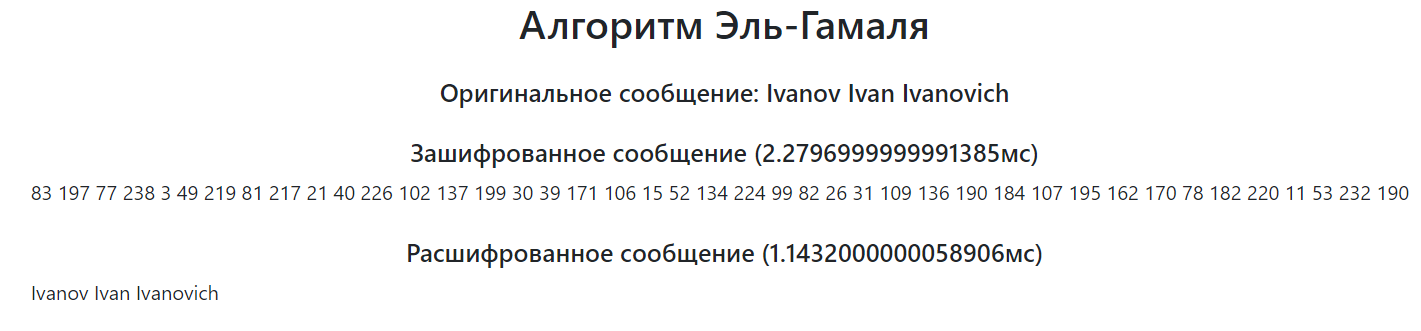


Рисунок 2.8 – Результат работы приложения

Время зашифрования сообщения – около 4 мс. Расшифрование с помощью алгоритма Эль-Гамаля заняло меньше времени по сравнению с алгоритмом RSA и составило 1.6 мс.

**Вывод:** в ходе выполнения лабораторной работы был изучен принцип реализации асимметричных шифров RSA и Эль-Гамаля. Также было разработано приложение, выполняющее шифрование и расшифрование с помощью шифра, основанного на алгоритме об укладке ранца. Была оценена скорость шифрования и дешифрования сообщений.