Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №9**

ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ

Вариант №6

Выполнил:

Студент 3 курса 4 группы ФИТ

Левша Марк Сергеевич

Минск 2023

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

**Задачи**:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.

3. Выполнить анализ криптостойкости асимметричных шифров.

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.

**Практическое задание**

Было разработано приложение, шифрующее и расшифровывающее сообщения, используя сверхвозрастающюю последовательность. Исходное сообщение преобразуется в набор чисел с помощью кодировки ASCII, с которыми в свою очередь и происходит работа.

Вывод программы представлен на рисунке 1.

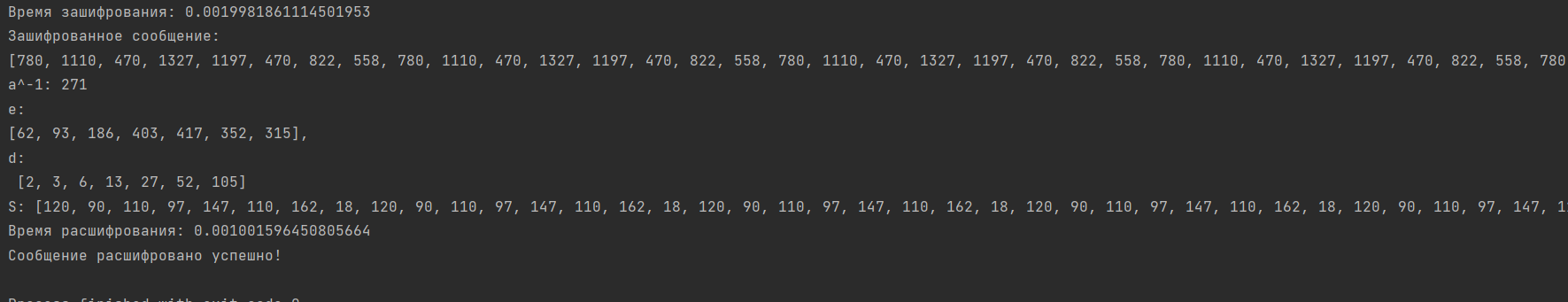


Рис. 1 – вывод консоли программы

Для выполнения всех операций мы должны передать сообщение и свехвозрастающюю последовательность *d*, которая будет использоваться для расшифрования сообщения и будет являться закрытым ключом.

Так же мы должны выбрать *n*, которое будет больше суммы всех элементов закрытого ключа, и *а*, которое должно быть взаимно простым с *n.*

На основе закрытого ключа, *а* и *n* вычисляется открытый ключ, который будет представлять собой обычную последовательность чисел.

*ei* ≡ *di*×*a* mod *n*.

Так же было оценено время выполнения зашифрования и расшифрования. Операция зашифрования длится дольше, чем операция расшифрования. График зависимости времени зашифрования и расшифрования от количества символов в исходном сообщении при использовании разных кодировок представлено на рисунке 2.

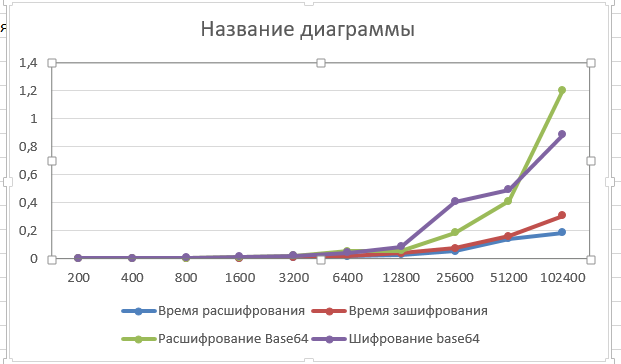


Рис. 2 – График зависимости времени зашифрования и расшифрования от количества символов в исходном сообщении

Хоть Base64 имеет меньшую длину битов в символе по сравнению с ASCII, но время преобразования символов в биты Base64 занимает больше времени, что приводит к большему времени шифрования и расшифрования.

**Вывод**: в ходе лабораторной работы было разработано приложение для шифрования сообщения с помощью асимметричного шифра и использованием кодировок Base64 и ASCII.