МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №7**

**″ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ″**

Выполнил:

Cтудент 3 курса 3 группы

Шедько Е.А.

Проверил:

Копыток Д.В.

**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.

Выполнение работы:

Сообщение для шифрования представлено на Рис. 1.



Рисунок 1 – Сообщение для шифрования

Зашифрованное сообщение на Рис. 2.



Рисунок 2 – Зашифрованное сообщение

Расшифрованное сообщение на Рис. 3.



Рисунок 3 – Расшифрованное сообщение

**Вывод:** в результате данной лабораторной работы было разработано приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.