**Учреждение образования**

**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»**

**Кафедра интеллектуальных информационных технологий**

**Лабораторная работа №5 по курсу «СиМЗИИС» на тему:**

**«АСИММЕТРИЧНОЕ ШИФРОВАНИЕ И ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ»**

Выполнил студент: Исамиддинов Ботир

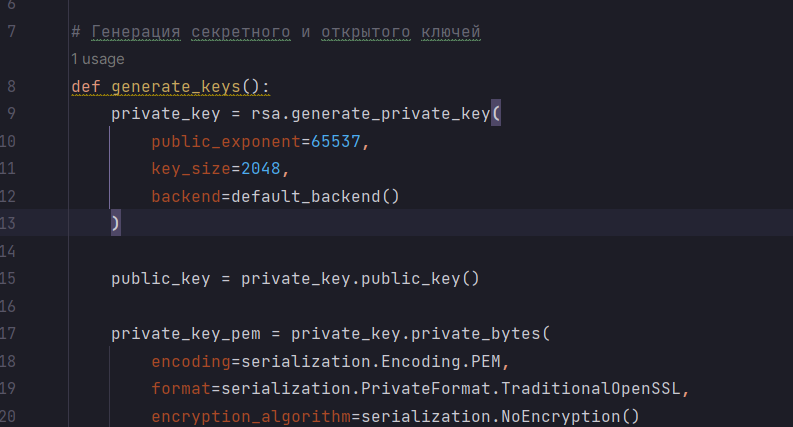
Группы: ***121731***

Проверил: Сальников Д.А

**МИНСК**

2023





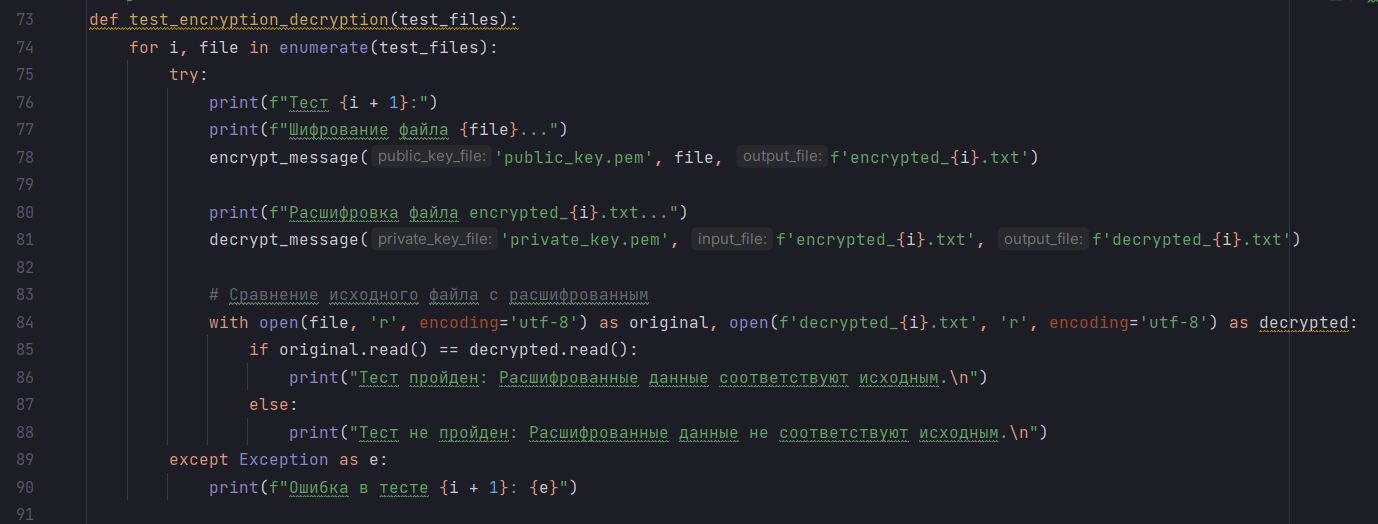
**Генерация секретного и открытого ключа**

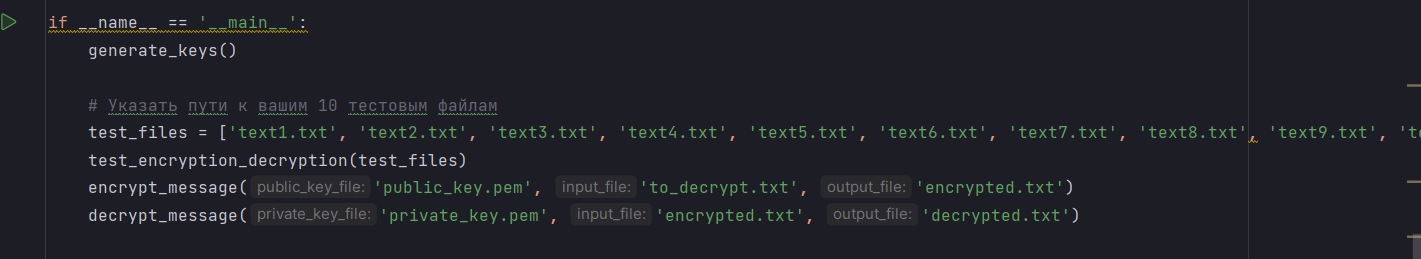


**Функция шифрования**

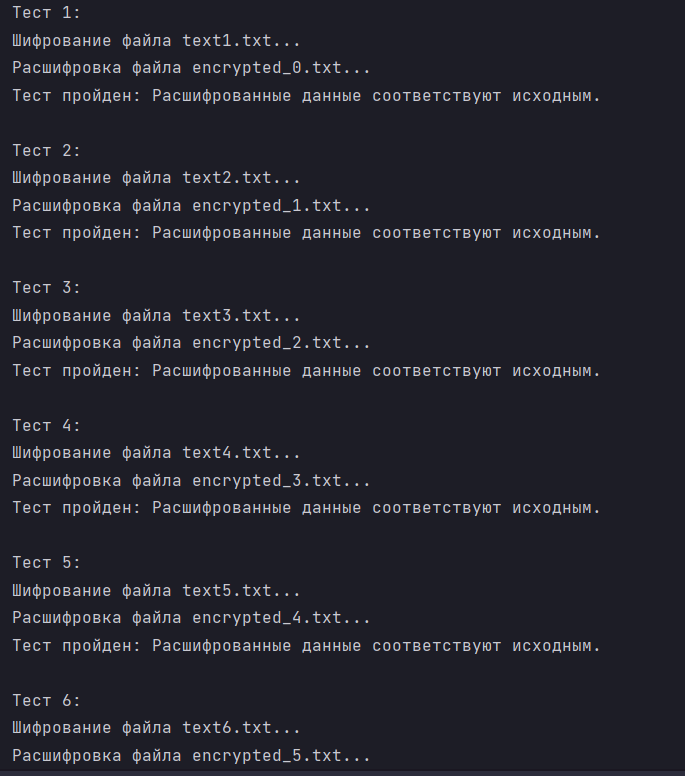


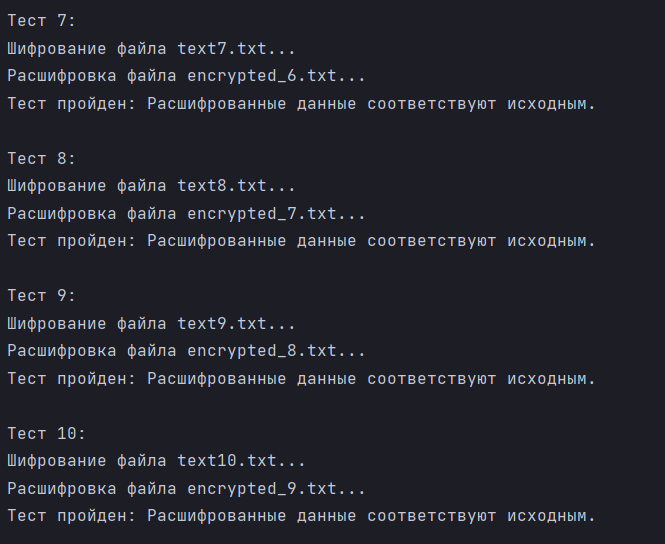
**Функция расшифрования**

 **Выполнение тестирования разработанного программного обеспечения на 10 наборах тестовых данных.**



**Прочитывание 10 текстовых файлов и сохранение открытого – закрытого ключа. Тут же файл для введения данных.**





**Проверка 10 тестовых файлов.**

**Вывод**

Выводы по Проекту Реализации Шифрования и Расшифрования с использованием RSA

Реализация Алгоритма RSA:

Программное обеспечение успешно реализует основные функции алгоритма RSA, включая генерацию ключей, шифрование и расшифрование данных.

Используется безопасный способ шифрования с открытым ключом, где секретный ключ используется для расшифровки, а открытый ключ - для шифрования.

Ключевые Особенности:

Ключи RSA генерируются с размером 2048 бит, что обеспечивает хороший уровень безопасности.

Используется padding OAEP с хэш-функцией SHA-256, что увеличивает безопасность шифрования и предотвращает ряд атак.

Тестирование:

Программа была протестирована на 10 различных наборах данных. Это обеспечило широкий охват различных сценариев использования.

Тесты подтвердили, что программа корректно шифрует и расшифровывает данные. Особенно успешно обрабатываются короткие тексты и числовые данные, соответствующие ограничениям размера RSA.

Ограничения и Наблюдения:

Ограничение по размеру данных: RSA подходит для шифрования небольших объемов данных. В случае с ключом 2048 бит, максимальный размер шифруемых данных составляет около 190-245 байтов.

При работе с текстами на кириллице и другими символами, выходящими за рамки ASCII, важно контролировать размер данных и корректность кодировки.

Выводы и Рекомендации:

Разработанное ПО является эффективным инструментом для шифрования и расшифрования данных с использованием алгоритма RSA.

Для шифрования больших объемов данных рекомендуется использовать гибридный подход: шифрование данных с помощью симметричного алгоритма, а затем шифрование ключа симметричного алгоритма с использованием RSA.

Важно учитывать ограничения по размеру данных и выбирать соответствующий размер ключа в зависимости от требований безопасности и производительности.