Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование ассиметричных шифров RSA и Эль-Гамаля**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

1. **Задание**

1. 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: *а* (десятичные числа от 5 до 35; можно взять 1 или 2 числа), *х* (числа, желательно простые, из диапазона от 103 до 10100; для примера взять 5–10 чисел, равномерно распределенных в указанном диапазоне), *n* (для примера взять числа, в двоичном виде состоящие из 1024 и 2048 битов).

2. Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами. В основе вычислений – кодировочные таблицы Base64 и ASCII. Приложение должно реализовывать следующие операции:

• зашифрование и расшифрование текстовых документов на основе алгоритмов RSA и Эль-Гамаля;

• определение времени выполнения операций.

Исходный текст для зашифрования – собственные фамилия, имя, отчество. Для численного представления блоков текста можно в том числе пользоваться указанными выше кодировочными таблицами. Ключевую информацию для обоих алгоритмов можно сгенерировать самостоятельно либо воспользоваться, например, одной из утилит криптографической библиотеки OpenSSL, с помощью которой, в частности, можно сгенерировать ключевую информацию для алгоритма RSA.

3. Используя примерно одинаковый порядок ключевой информации, оценить производительность обоих алгоритмов и относительное изменение объемов криптотекстов (по отношению к объемам открытых текстов).

1. **Ход работы**

Для первого задания в качестве параметров были выбраны следующие значения:

*a* – [5, 15];

*x* – [103, 1000, 5000, 10000, 100000];

*n* – [21024, 22048].

Далее, по формуле *у* ≡ *ax* mod *n* были вычислены значения *y*, а также было оценено время подсчёта этих значений, которое мы можем увидеть на графике 3.1.

Рисунок 3.1 – Графическая форма зависимости времени вычисления параметра *у*

Для второго задания были разработаны классы ElGamal и Rsa для реализации соответствующих алгоритмов шифрования. Их коды представлены на рисунках 3.2 – 3.3.

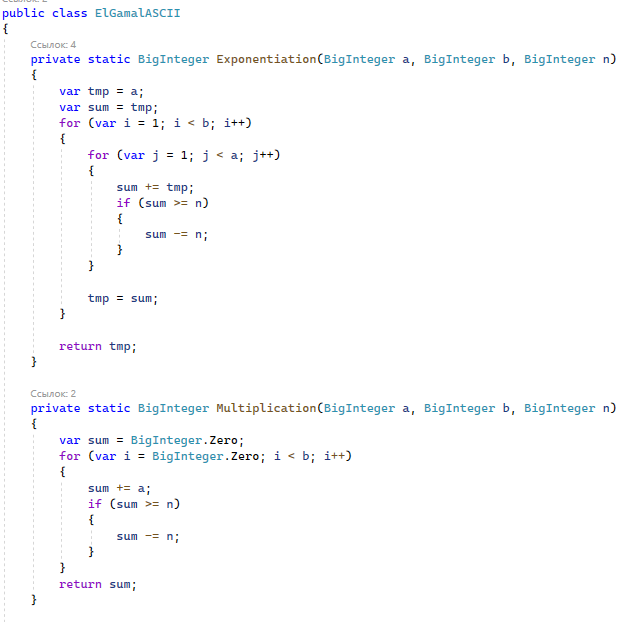


Рисунок 3.2 – Класс ElGamal

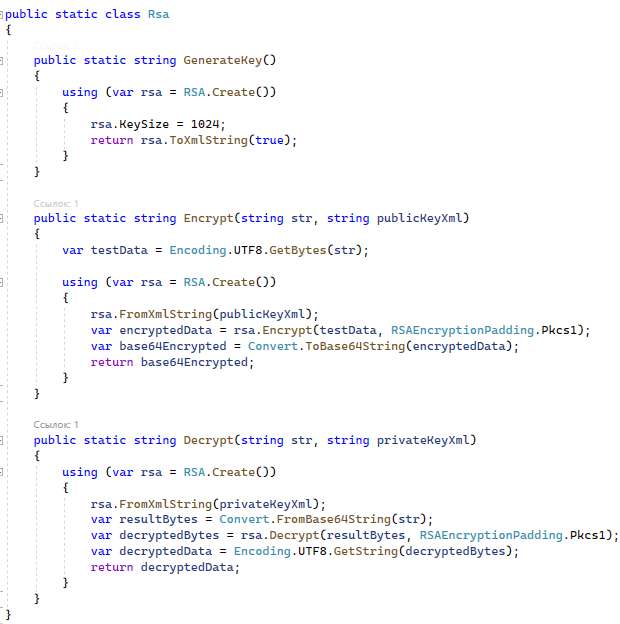


Рисунок 3.3 – Класс Rsa

Шифруемые строки в обоих случаях – «Budanowa Ksenya Andreevna». Тут же была оценена производительность обоих алгоритмов и относительное изменение объемов криптотекстов (по отношению к объемам открытых текстов). В результате при использовании двух шифров получим следующий вывод, представленный на рисунке 3.4.

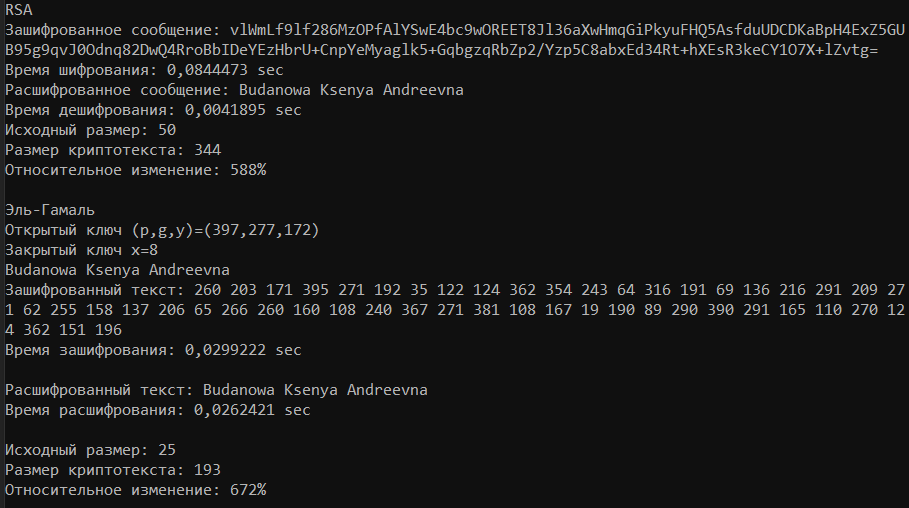
r 

Рисунок 3.4 – Результаты шифрования и расшифрования для Base64

Данный вывод был получен для кодировки Base64. Теперь сравним его с выводом для кодировки ASCII, представленном на рисунке 3.5.

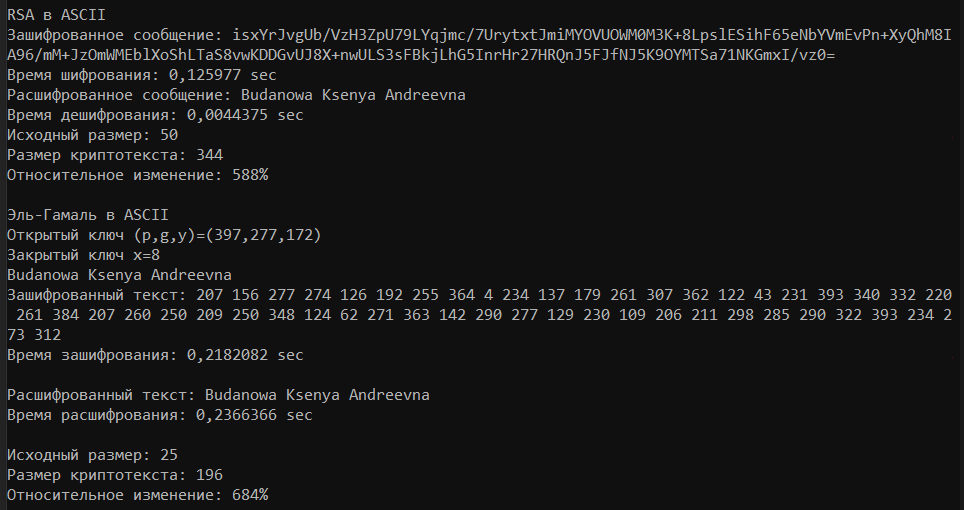


Рисунок 3.5 – Результаты шифрования и расшифрования для ASCII

Исходя из полученных результатов, можно увидеть, что кодировка ASCII справляется быстрее. Это обусловлено тем, что ASCII представляет символы непосредственно в виде однобайтовых значений, тогда как Base64 кодирует данные в последовательность символов, используя шесть битов из каждого байта и добавляя символы заполнения. Расшифровка ASCII-кодированного текста требует простого сопоставления каждого символа с его однобайтовым значением, что делает процесс очень быстрым и эффективным.

Кроме того, посмотрим на графики 3.6 – 3.9, демонстрирующие производительность обоих алгоритмов в разных кодировках:

Рисунок 3.6 – Оценка скорости шифрования и дешифрования для RSA с использованием Base64

Рисунок 3.7 – Оценка скорости шифрования и дешифрования для RSA с использованием Base64

Рисунок 3.8 – Оценка скорости шифрования и дешифрования для RSA с использованием Base64

Рисунок 3.9 – Оценка скорости шифрования и дешифрования для RSA с использованием Base64

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.