Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование ассиметричных шифров RSA и Эль-Гамаля

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

Безопасность RSA основана на проблеме факторизации. Открытый и закрытый ключи являются функциями двух больших простых чисел. Предполагается, что восстановление открытого текста по шифртексту и открытому ключу эквивалентно разложению на множители двух больших чисел.

Для генерации тайного и открытого ключа используются два больших числа p и q, n=pq. Ключ состоит из n, e, d. e – случайное число, такое что *e* и

(*p* – 1)(*q* – 1) являются взаимно простыми числами.

Затем находим *d*:





Шифруется сообщение *М*, состоящее из r блоков: , , …, , …, , шифртекст С будет состоять из такого же числа (*r*) блоков, представляемых числами:



Расшифрование RSA:



Безопасность алгоритма Эль-Гамаля основана на трудности вычисления дискретных логарифмов. Предназначен он для шифрования сообщения и создания цифровой подписи.

Выбирается простое число *р* и *g* (*g* < *p*), являющееся первообразным корнем числа *р*.

Далее выбирается число *х* (*х* < *p*) и вычисляется последний компонент ключевой информации:



Отправка сообщения, зашифрованного ключами *p*, *g*, *y*. Расшифровка сообщения ключами *p*, *g*, *x*. Тайным является только *x*.

1. **Практическая часть**

**2.1 RSA**

Ниже, на рисунке 2.1 представлена часть реализации RSA (шифрование).

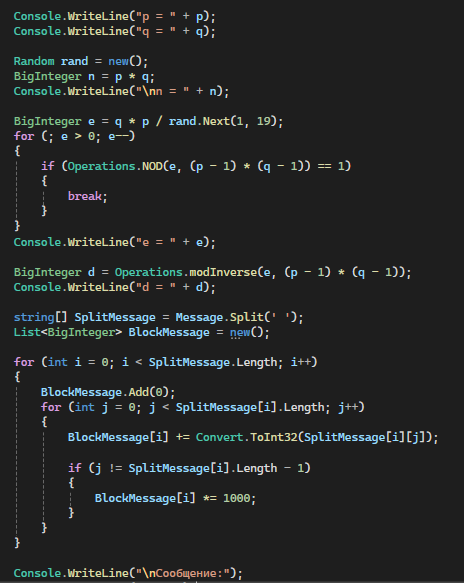


Рисунок 2.1 – реализация RSA алгоритма

Сначала выбираются два простых числа p и q, затем вычисляется их произведение n = p \* q, которое является частью открытого ключа. Случайным образом выбирается значение e, которая должна быть взаимно простой с (p - 1) \* (q - 1). Далее вычисляется секретная d с помощью функции modInverse, находящей модулярную инверсию e по модулю (p - 1) \* (q - 1). Входное сообщение разбивается на слова, каждое слово кодируется в числовой формат путем суммирования ASCII кодов его символов и умножения результата на 1000 между символами. Затем каждый числовой блок сообщения шифруется с использованием операции возведения в степень по модулю n с открытой e, и результаты шифрования выводятся в консоль.

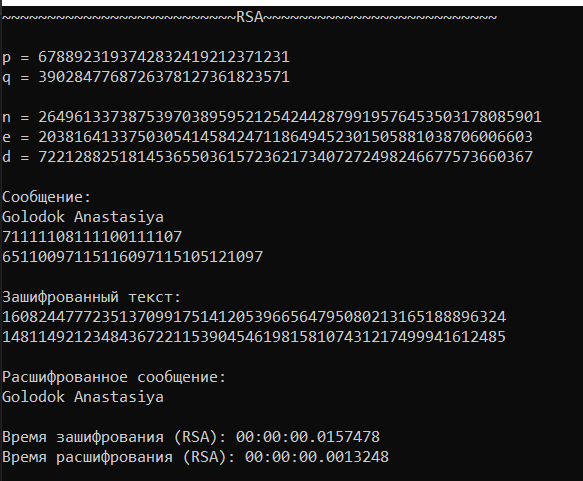


Рисунок 2.2 – вывод работы RSA алгоритма

**2.2 Эль-Гамаля**

Часть кода для шифрования алгоритмом Эль-Гамаля представлена на рисунке 2.3.

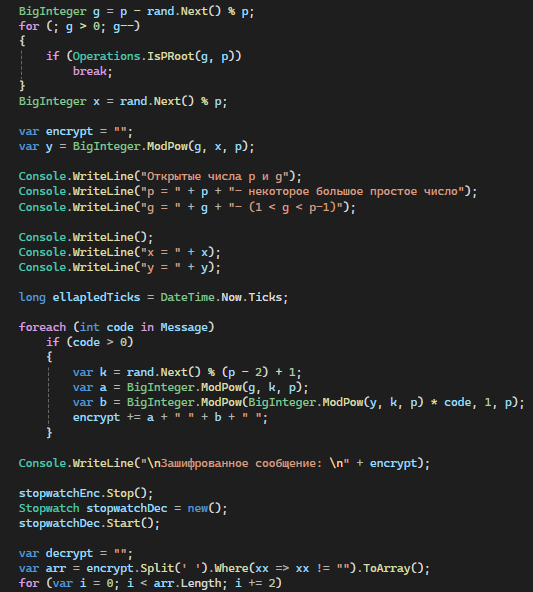


Рисунок 2.3 – Реализация алгоритма Эль-Гамаля

Сначала генерируется случайное число **g**, которое является первообразным корнем по модулю **p**. Затем выбирается случайное число **x**, служащее секретным ключом, и вычисляется **y**, являющееся частью открытого ключа. Открытые ключи **p**, **g** и **y**, а также секретный ключ **x** выводятся на консоль. Для шифрования каждого символа сообщения генерируется случайное число **k**, и вычисляются **a** и **b**, которые составляют зашифрованные пары для каждого символа. Эти пары объединяются в строку и выводятся как зашифрованное сообщение. Для расшифровки сообщения каждая пара **a** и **b** используется для восстановления исходного символа **m** с помощью секретного ключа **x**, и результирующая строка выводится как расшифрованное сообщение.

