Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование ассиметричных шифров

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

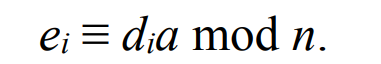
1. **Теоретическая часть**

Асимметричная криптография использует два ключа для шифрования и расшифрования данных: открытый и закрытый ключи, которые составляют пару. Эти ключи принадлежат получателю зашифрованного сообщения. Алгоритмы шифрования с открытым ключом основаны на односторонних математических функциях, таких как вычисление дискретного логарифма.

Шифрование с открытым ключом может использоваться для защиты данных, создания цифровой подписи и распределения секретных ключей для симметричного шифрования. Этот подход обеспечивает безопасность и удобство использования.

Криптоалгоритм на основе задачи об укладке ранца использует рюкзачный вектор и натуральное число в качестве входных данных. Решение этой задачи заключается в нахождении подмножества элементов рюкзачного вектора, сумма которых равна заданному числу.

Открытый ключ, который используется для шифрования, создается из закрытого ключа, который обладает свойством сверхвозрастающей последовательности.



Значения закрытого ключа умножаются на число по модулю n, чтобы получить открытый ключ. Модуль n должен быть больше суммы значений последовательности закрытого ключа, и их наибольший общий делитель должен быть равен 1.

1. **Практическая часть**

Часть кода реализации рюкзака представлена на рисунке 2.1.

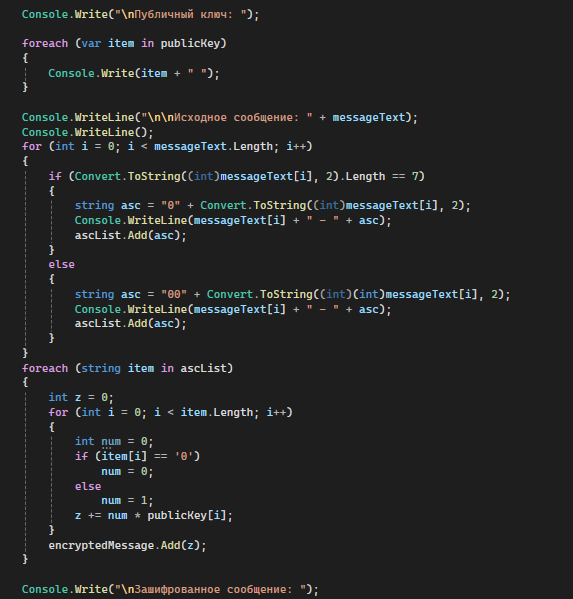


Рисунок 2.1 – реализация рюкзака

Сначала создается сверхвозрастающая последовательность **superSeq**, сумма которой используется для вычисления значений **n** и **a**, которые удовлетворяют условию, что НОД(n, a) равен 1. Используя **a** и **n**, генерируется публичный ключ **publicKey**.

Затем вводится сообщение **messageText**, которое конвертируется в двоичный ASCII-код. Каждый символ сообщения шифруется с использованием публичного ключа, формируя зашифрованное сообщение **encryptedMessage**.

Для дешифрования используется обратное значение **a** по модулю **n**. Процесс дешифрования включает умножение каждого элемента зашифрованного сообщения на это обратное значение и восстановление исходных двоичных символов сообщения с помощью реверсии и проверки значений относительно сверхвозрастающей последовательности.

Расшифрованное двоичное сообщение конвертируется обратно в текст, и выводятся времена выполнения процессов шифрования и дешифрования.

1. **Результат**

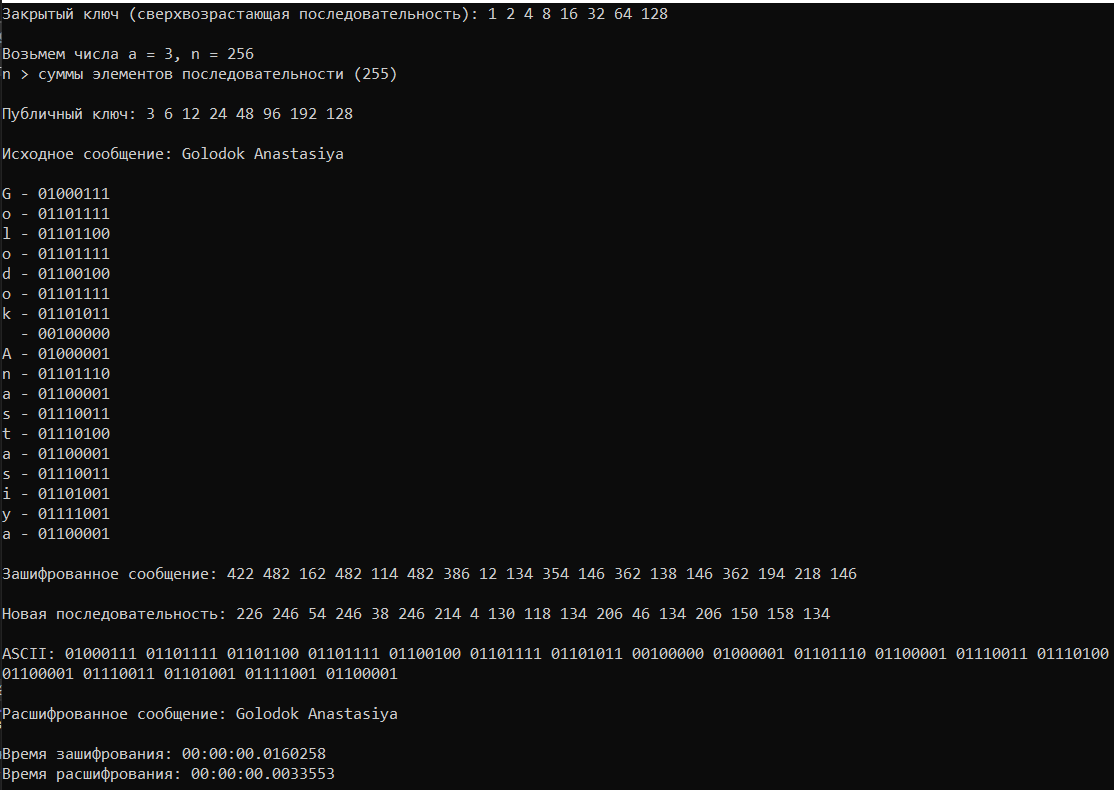


Рисунок 3.1 – результат работы программы