Отчет по лабораторной работе №2

по дисциплине «Информационная безопасность»

на тему «Стандарт симметричного шифрования AES RIJNDAEL»

Выполнил:

студент группы БИСТ-20-1

Султыева Ю.В

Проверил:

Бахаров Л.Е.

Москва, 2022

Задание: Изучить на примере обычных текстовых файлов способы шифрования и расшифрования с помощью алгоритма RIJNDAEL

Rijndael представляет собой итеративный блочный шифр, имеющий переменную длину блоков и различные длины ключей. Длина ключа и длина блока могут быть независимо друг от друга 128,192 или 256 бит.

Алгоритм состоит из следующих шагов:

1. Расширение ключа - KeyExpansion;
2. Начальный раунд - сложение state с основным ключом;
3. 9 раундов шифрования, каждый из которых состоит из преобразований:

· SubBytes

· ShiftRows

· MixColumns

· AddRoundKey

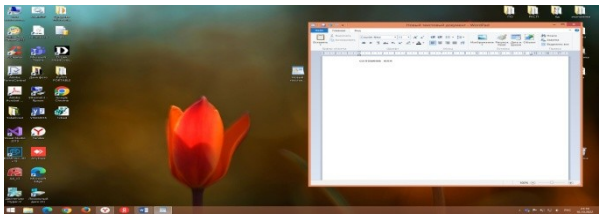
4. Финальный раунд, состоящий из преобразований:

· SubBytes

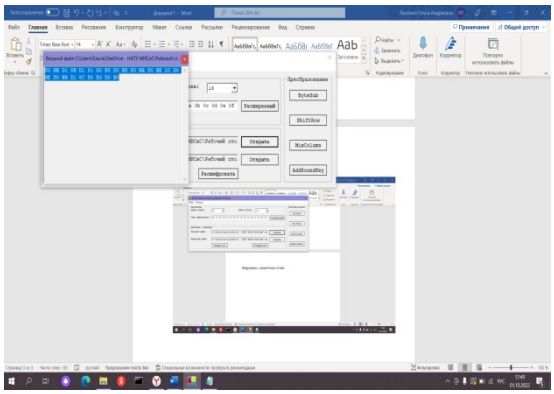
· ShiftRows

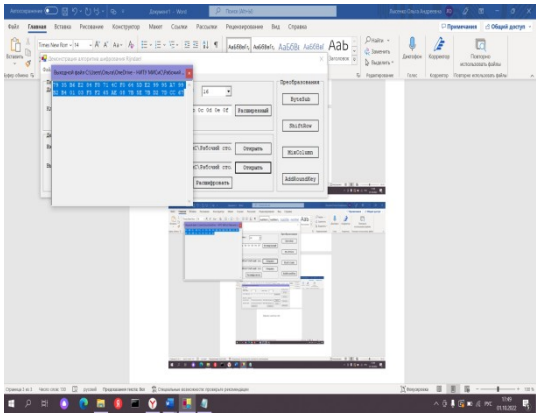
· AddRoundKey

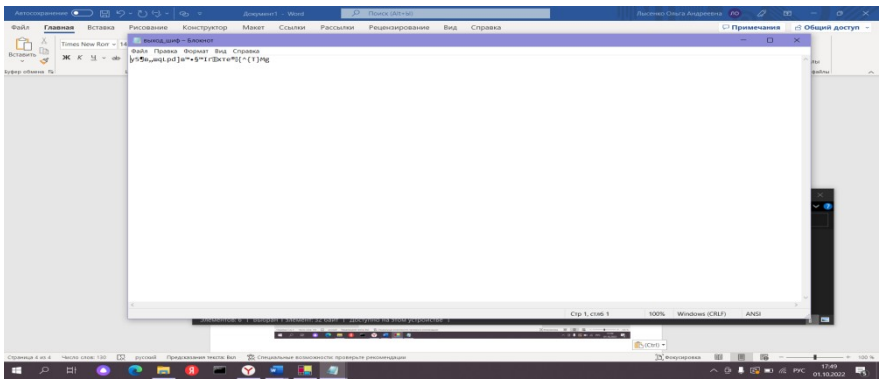
Ход работы:
Исходный текст



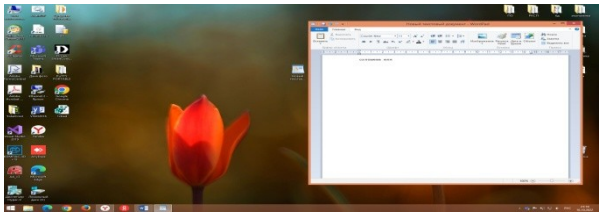
1. Шифрование с длиной блока 16 байт





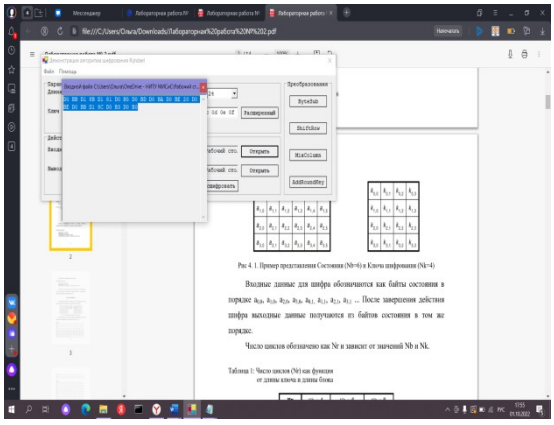


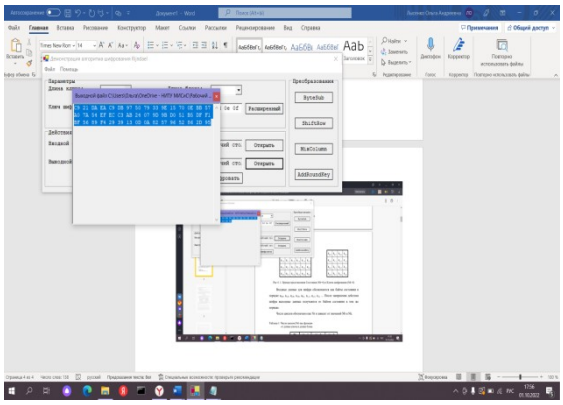
Расшифрование:

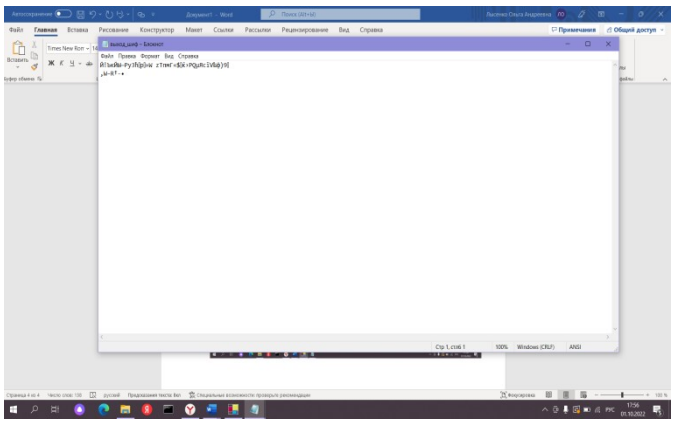


2.

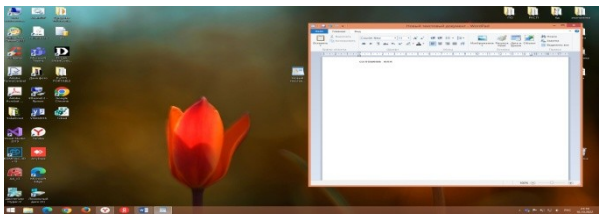
Шифрование с длиной блока 24 байт





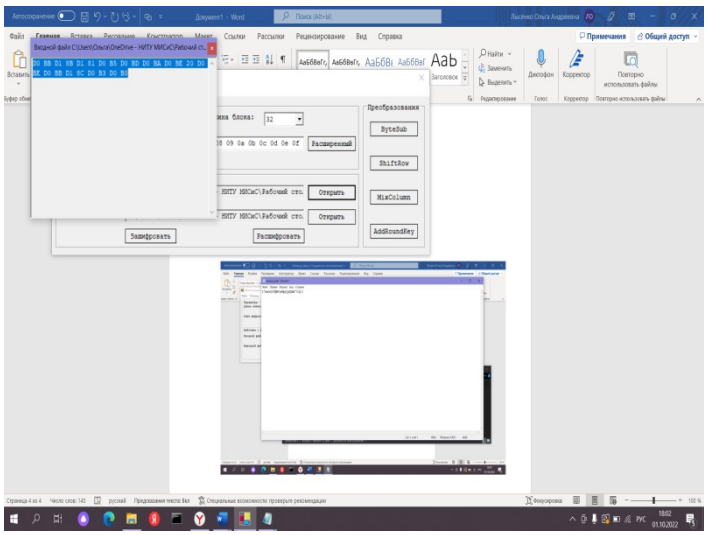


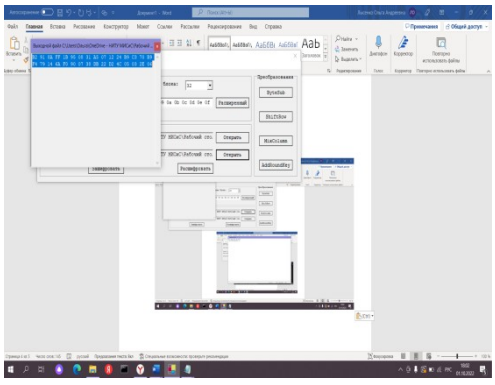
Расшифрование:

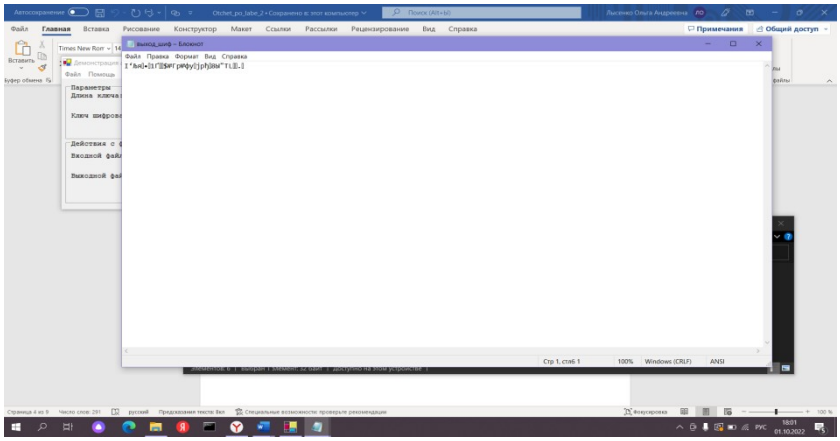


3.

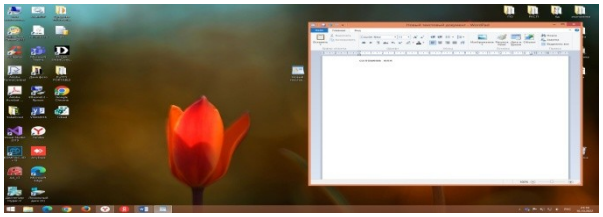
Шифрование с длиной блока 32 байт







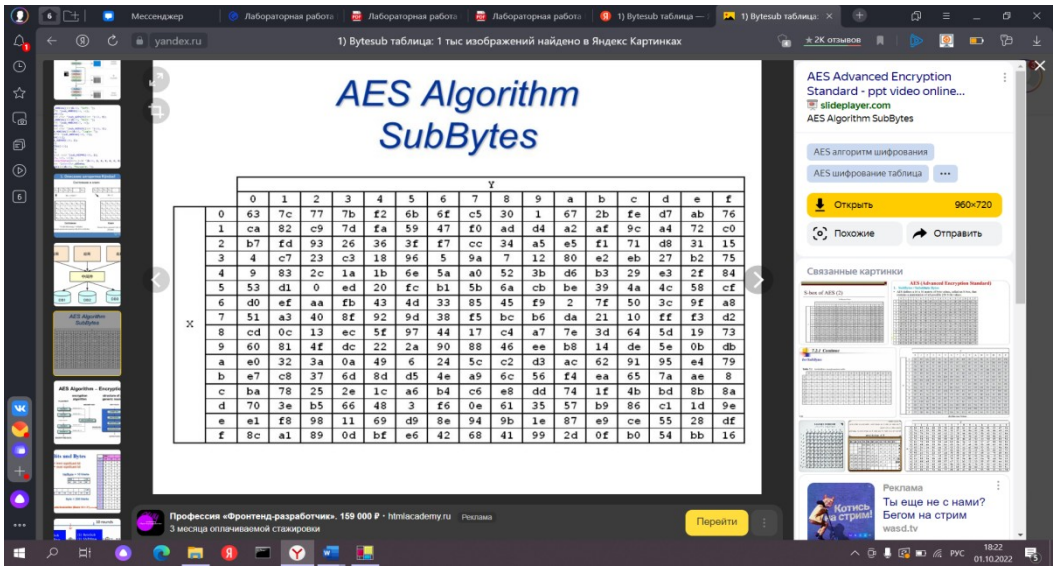
Расшифрование:



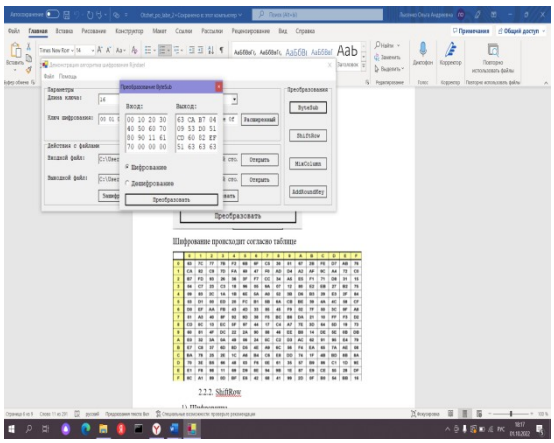
Задание: Подробно рассмотреть действие всех цикловых преобразований (Bytesub, ShiftRow, MixColumn, AddRoundKey)

1. **Bytesub**

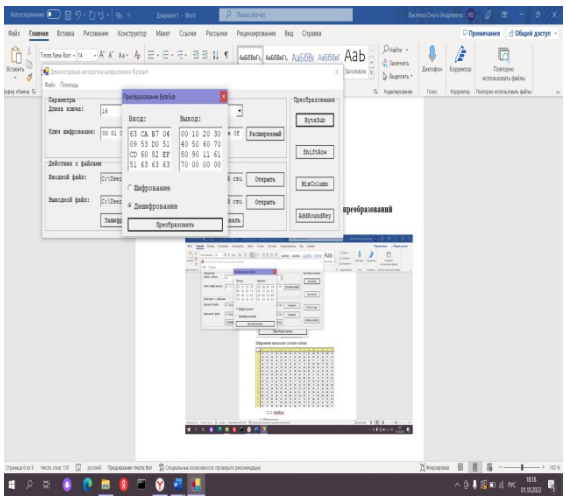
Это преобразование делает шифрование по таблице:



Шифрование:



Дешифрование:



2. **ShiftRow**

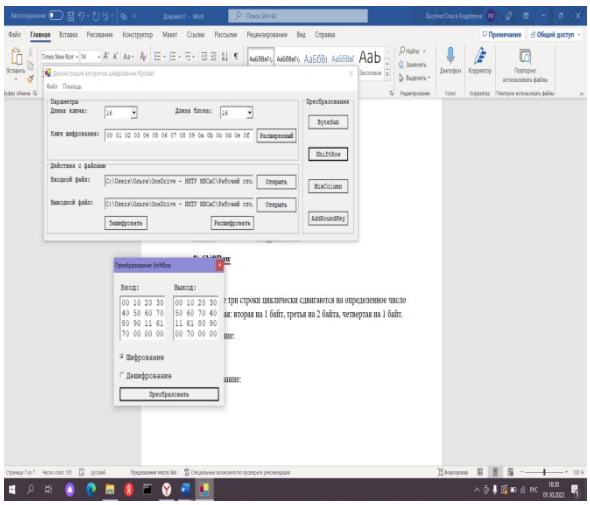
Последние три строки циклически сдвигаются на определенное число байт каждая: вторая на 1 байт, третья на 2 байта, четвертая на 1 байт.

Значения сдвигов зависят от длины блока.

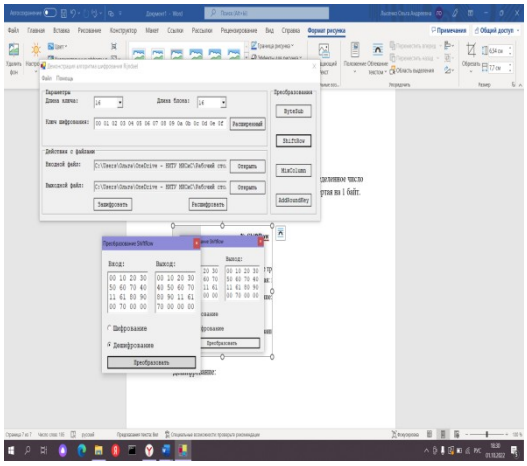
Расшифрование происходит в обратном направление, т.е вправо.

Шифрование:

Сдвиг влево



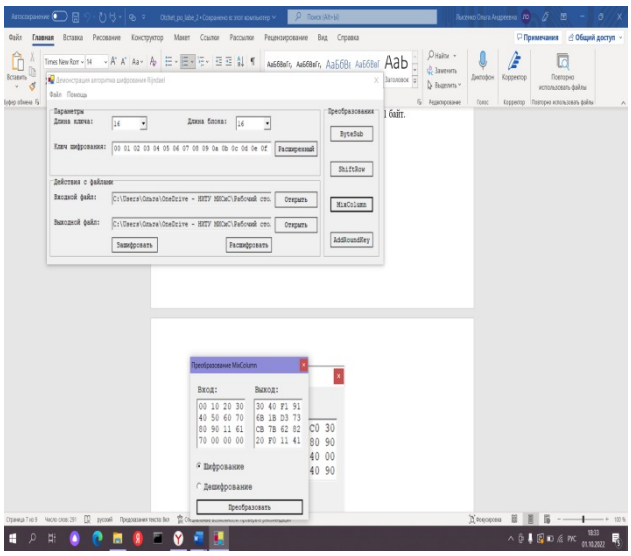
Дешифрование:



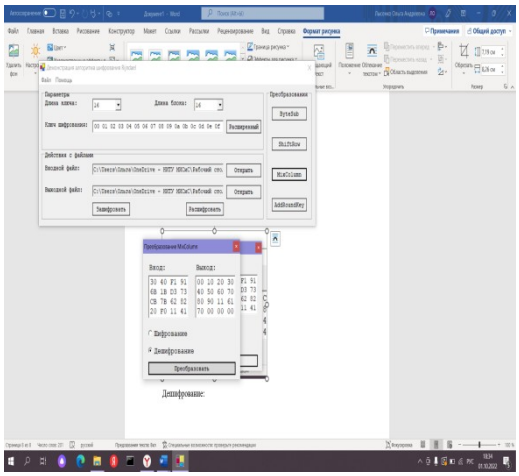
3. **MixColumn**

Умножение каждого столбца на фиксированную матрицу.

Шифрование:



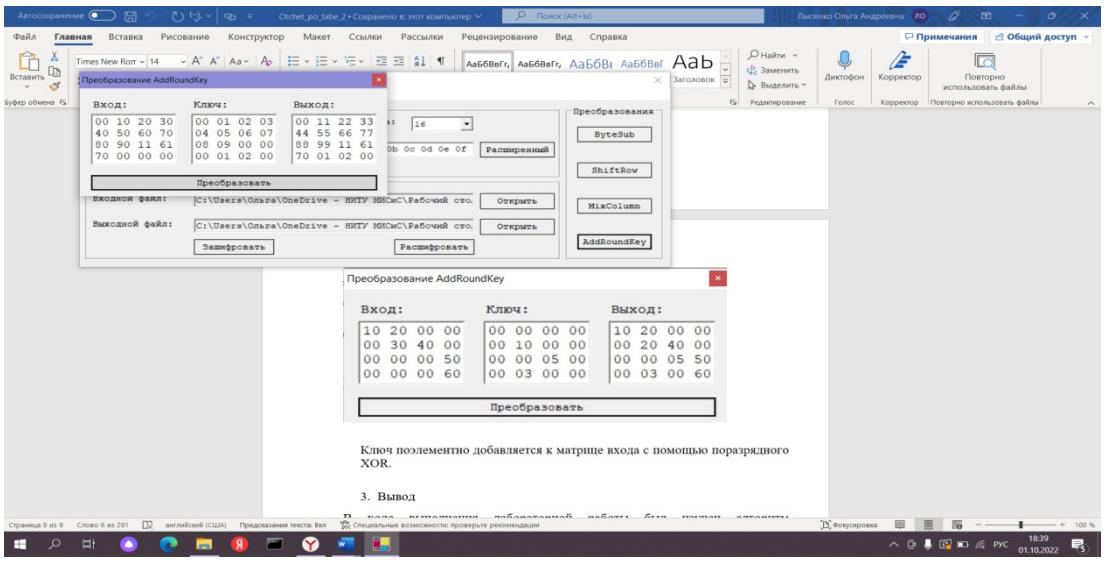
Дешифрование:



4. **AddRoundKey**

Ключ поэлементно добавляется к матрице входа с помощью поразрядного XOR.

При шифровании части расширенного ключа выбираются от начала к концу, при расшифровании – от конца к началу.
Шифрование:



Ключ поэлементно добавляется к матрице входа с помощью поразрядного XOR.

3. Вывод