МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		Исаева М.Н.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

БЛОКОВЫЕ ШИФРЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912		Нам Д.О.
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

1. Цель

Вариант 34.

Реализовать алгоритм шифрования RC6, предусмотреть возможность работы алгоритма в режиме OFB.

Исследовать процесс распространения ошибок в реализуемом режиме шифрования, привести пример распространения ошибок. По результатам анализа сделать выводы о качестве реализованных систем шифрования.

Вычислить коэффициент корреляции для входного и выходного потока алгоритма шифрования, оценить распределение «0» и «1» в выходном потоке.

2. Описание алгоритма

Алгоритм шифрования RC6

RC6 — итеративный блоковый алгоритм с переменной длиной информационного блока, переменным числом циклов и переменной длиной ключа. Алгоритм построен по классической схеме сетей Файстела. В общем случае авторы обозначили свой алгоритм как RC6- w/r/b, где w — размер обрабатываемых алгоритмом блоков, r—число циклов, b — длина ключа.

Алгоритм RC6 – с w = 32, r = 20, b = 128/192/256 бит обозначается просто как RC6

На рисунке 1 изображена схема одного раунда (цикла) алгоритма RC6.

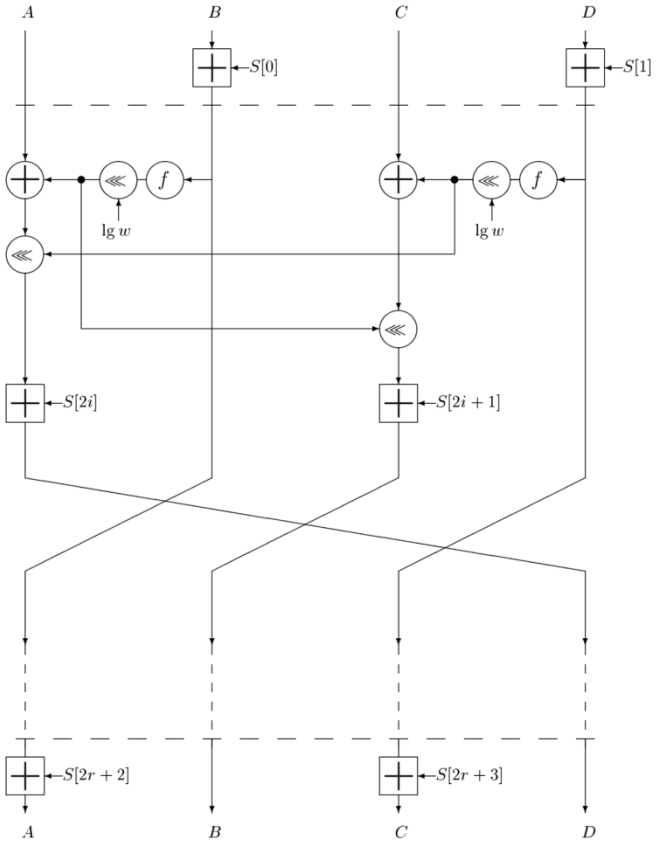

Рисунок 1 – раунд алгоритма RC6

Режим шифрования OFB

Режим OFB — режим обратной связи вывода, превращающий блочный шифр в синхронный шифр потока. OFB генерирует ключевые блоки, которые являются результатом сложения с блоками открытого текста, чтобы получить зашифрованный текст.

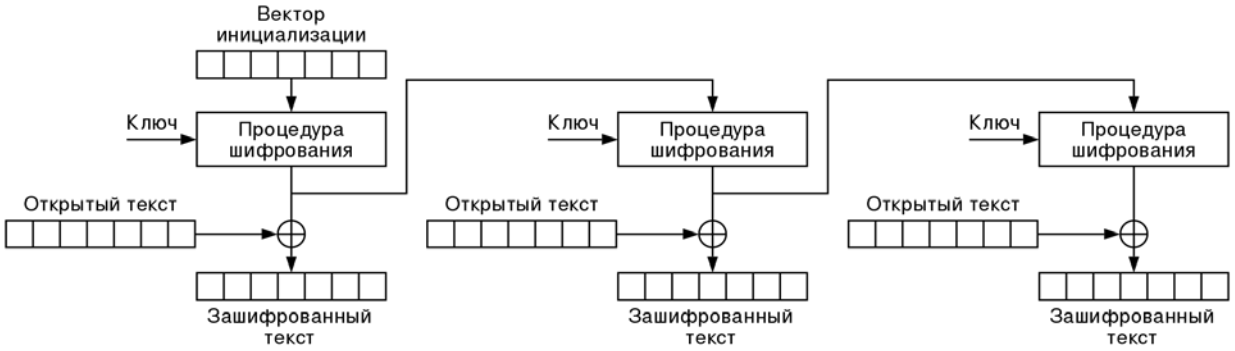

Рисунок 2 – шифрование в режиме OFB

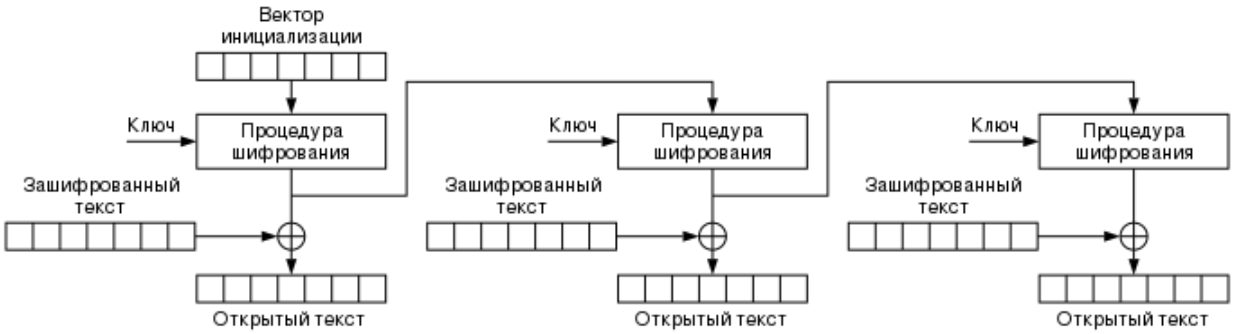

Рисунок 3 – дешифрование в режиме OFB

3. Описание реализации

При запуске программа в начале записывает информацию о входном изображении в массив байт, а также составляет ключ, длиной 128 бит.

После чего программа шифрует входной массив байт с помощью алгоритма RC6, и составляет из них новое изображение.

Когда зашифрованное изображение готово, программа дешифрует его и составляет третье изображение, равное исходному

Также доступен режим шифрования OFB. Его включение регулируется пользователем с помощью переменной OFB, которая может принимать значения true или false.

4. Примеры

Для проверки работы программы используется стандартное изображение Лены (рисунок 4)

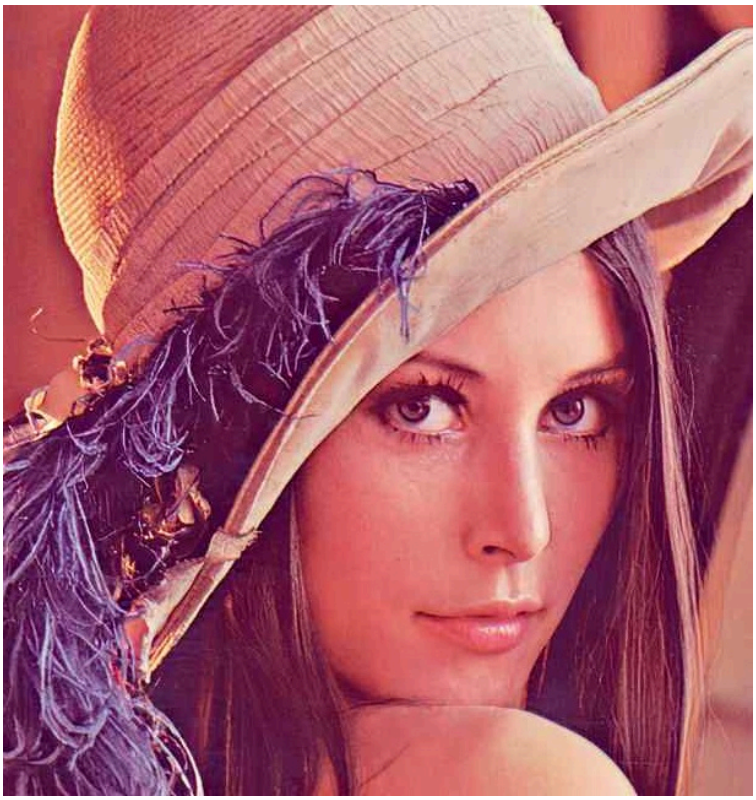

Рисунок 4

Проведем шифрование, используя режим OFB. Результат шифрования представлен на рисунке 5

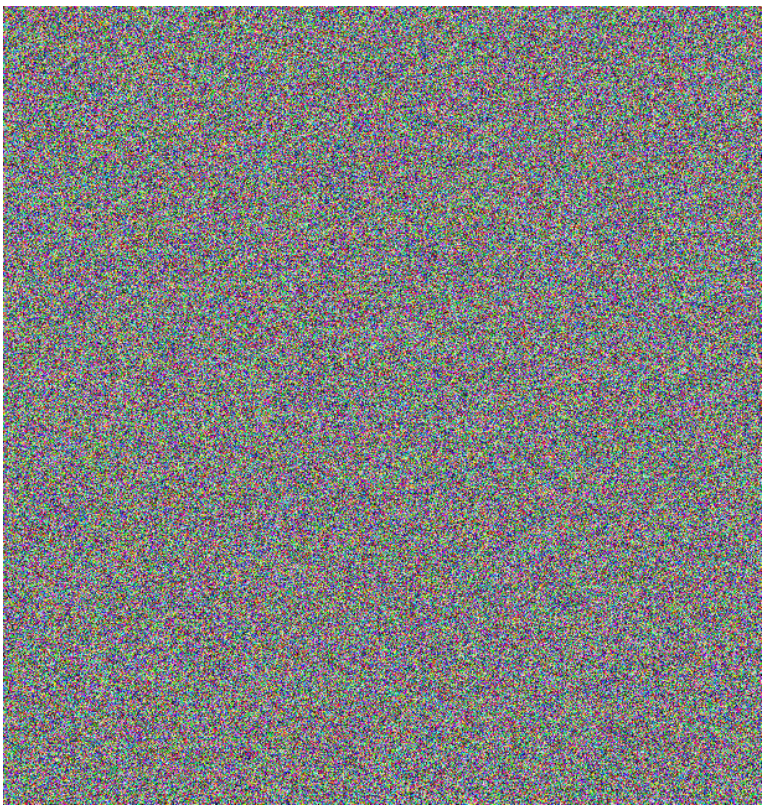

Рисунок 5

Результат дешифрования представлен на рисунке 6. Как можно заметить, он идентичен входному изображению.

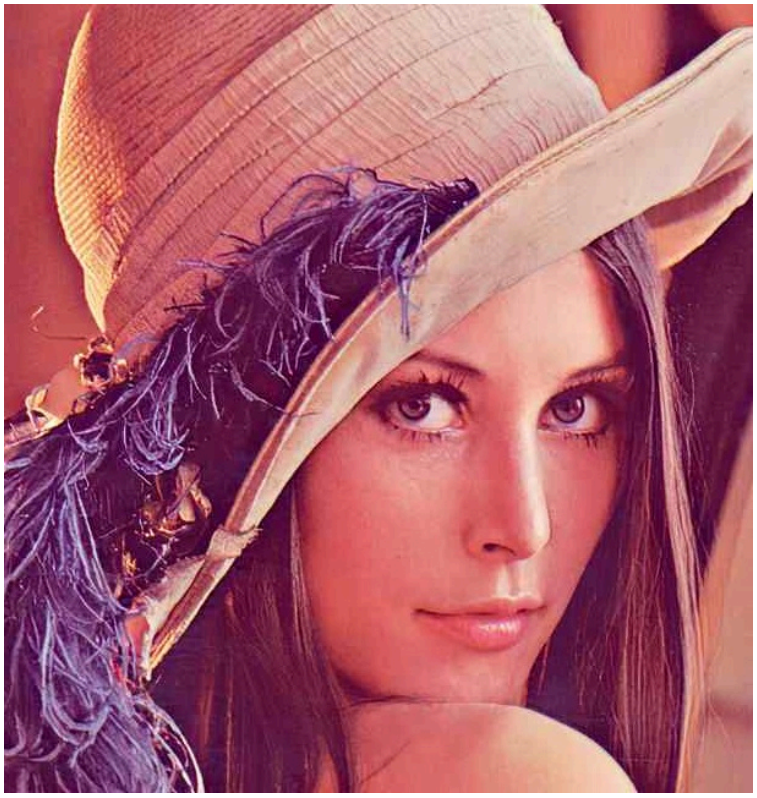

Рисунок 6

Если зашифрованный файл будет как-либо повреждён (рисунок 7), то и дешифрованный файл будет отличаться от исходного (рисунок 8)

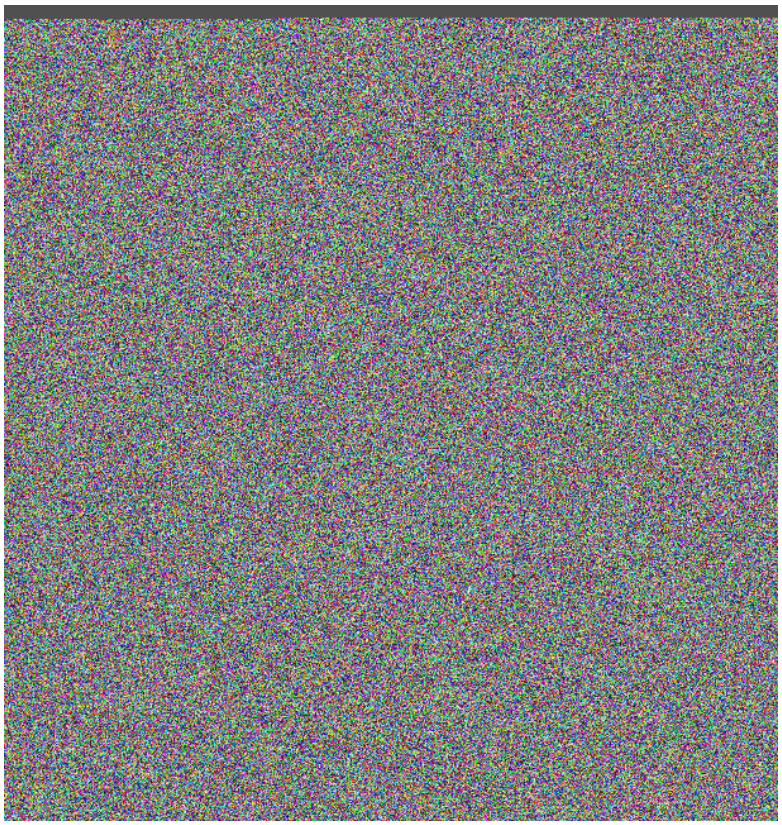

Рисунок 7

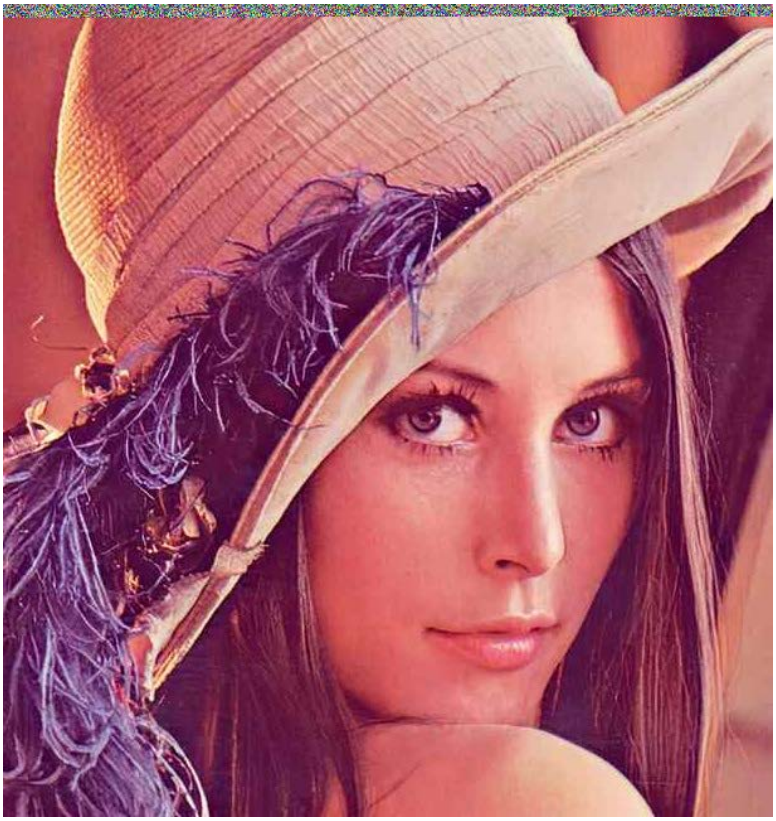

Рисунок 8

Коэффициент корреляции отличается от одного запуска программы к другому, т.к. 128-битный всегда генерируется заново. Тем не менее, значение коэффициента корреляции для данной реализации никогда не превышает значение в «0.002254455483527771».

5. Вывод

Реализовал алгоритм шифрования RC6, а также режим шифрования OFB. Исследовал процесс распространения ошибок в реализуемом режиме шифрования. Вычислил коэффициент корреляции.

6. Список литературы

[1] С.В. Беззатеев, Е.А. Крук, А.А. Овчинников, Блоковые Шифры. Учебное пособие, Санкт-Петербург : Издательство Нестор, 2003.

[2] А.Л. Чмора Современная прикладная криптография, Гелиос АРВ, 2002.