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

доцент, к.т.н., доцент А. В. Окатов

должность, уч. степень, звание подпись, дата инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ № 6

ШИФРЫ С УПРАВЛЯЕМЫМИ ПОДСТАНОВКАМИ

по курсу: ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 5811  Т.С. Климов

подпись, дата инициалы, фамилия

Санкт-Петербург, 2021 г.

# **Цель работы:**

Построить алгоритм шифрования, основанный на управляемых подстановках. На основе этого алгоритма проанализировать основные свойства алгоритма и полученные результаты.

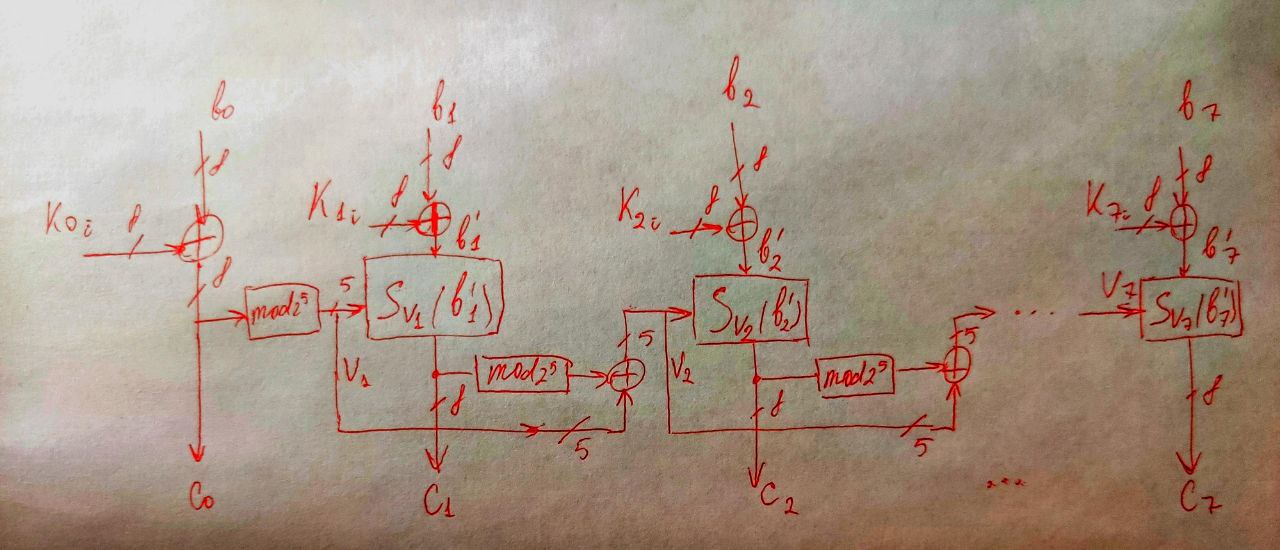
1. **Теоретические сведения:**

Шифр с управляемыми подстановками является еще одной возможностью реализации управляемых операций с целью внесения для противника дополнительной неопределенности в процесс преобразования сообщения при его шифровании. Один из вариантов построения такого шифра заключается в использовании набора из N таблиц подстановки, половина из которых являются таблицами прямой подстановки, а другая - таблицами обратной подстановки. То есть, каждой таблице прямой подстановки соответствует таблица обратной подстановки. Следует отметить, что такое деление довольно условно (которую из таблиц считать таблицей прямой подстановки, а какую обратной подстановки). Важно, чтобы каждая таблица прямой подстановки имела таблицу, взаимно обратную ей. Каждая таблица подстановки содержит 2 строки.

Рассмотрим пример построения шифра с управляемыми подстановками. Положим, что всего имеются N = 32 таблицы подстановки (16 + 16). Положим также, что таблице Т0 соответствует таблица обратной подстановки Т31, таблице Т1 соответствует таблица обратной подстановки Т30, таблице Т2 соответствует таблица Т29 и т.д. симметрично. Используем режим блочного шифрования, для определенности положим, что размер шифруемого блока В равен 64 бита. Каждый блок В разобьем на 8 подблоков (в данном примере на 8 байтов): b0, ... , b1, b7. На каждом i-м раунде шифрования используется свой "набор" из 8-и (байтовых) раундовых секретных подключей: к0i, к1i, ... , к7i. В этом случае в таблицах прямой (и обратной) подстановки должны находиться числа из диапазона от 0 до 255.

В данной таблице в нижней строке присутствуют все возможные числа из верхнего ряда, но расставленные в другом порядке. Очередность расположения чисел в нижней строке определяет конкретный вариант таблицы подстановки, а, следовательно, и конкретный вариант операции подстановки, выполняемой этой таблицей. Выполнение операции подстановки сводится к выбору по значению числа в верхней строке (вход таблицы подстановки - значение входного блока) числа, находящегося под этим числом в нижней строке. Оно и берется в качестве выходного блока.

Структура i-го раунда шифрования с управляемыми подстановками представлена на Рис. 1:



*Рисунок 1. Структура раунда шифрования*

Входные 8-битные подблоки b0, ... , b1, b7 складываются по модулю 2 с секретными раундовыми подключами к0i, ... ,к1i, к7i. Функциональные блоки mod 25 выделяют из 8-разрядных двоичных чисел пять их младших разрядов. Выделенные разряды используются в дальнейшем для (непредсказуемого для противника) формирования номеров, используемых 32-х таблиц подстановки. Порядок расчета номеров таблиц подстановки наглядно показан на рис. 1. Поэтому, если даже противнику известны все используемые в шифре таблицы подстановки, он не может правильно определить номер таблицы, используемой на каждом шаге шифрования в данном раунде. В результате для противника вносится дополнительная неопределенность в процесс шифрования сообщения. На рис. 1 с0, с1, ... , с7 - это подблоки результата i-го раунда шифрования сообщения.

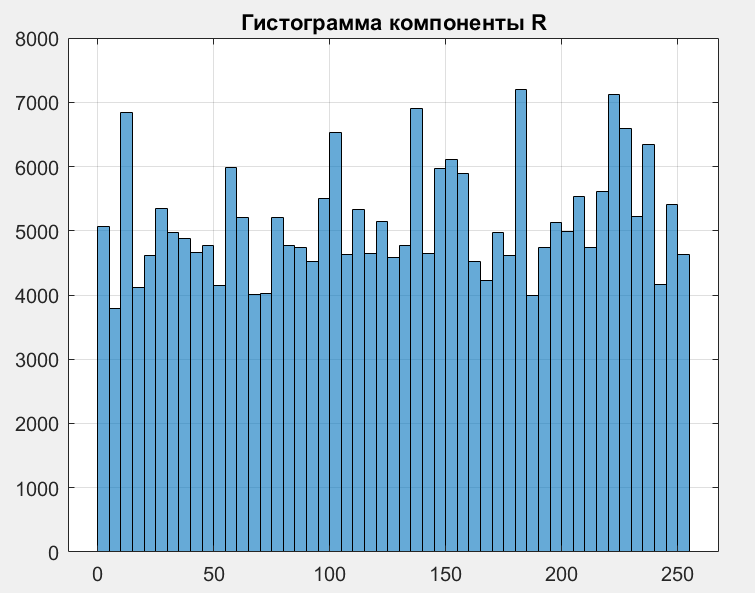
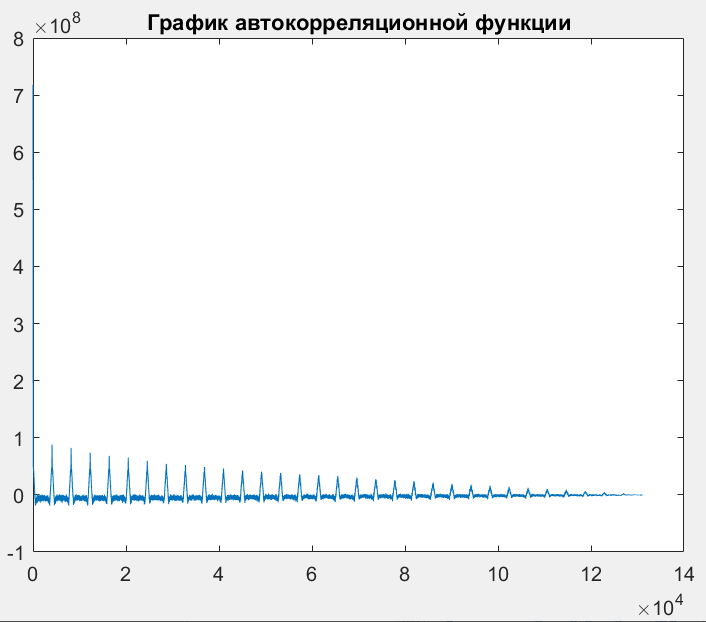
Для расшифрования сообщения надо правильно рассчитать номера таблиц обратной подстановки, в точности соответствующих использованным при шифровании таблицам прямой подстановки. В рассматриваемом примере таблице подстановки Тk (с порядковым номером k) соответствует таблица обратной подстановки с номером 31 - k, где k = 0, 1, ... , 31. Это дает возможность при расшифровании сообщения получить на каждом раунде номера соответствующих таблиц обратной подстановки.

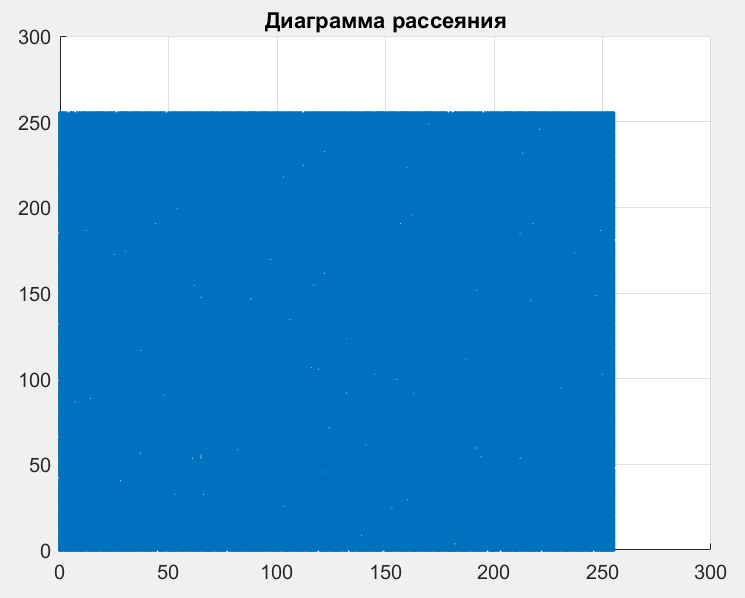
1. **Ход работы:**

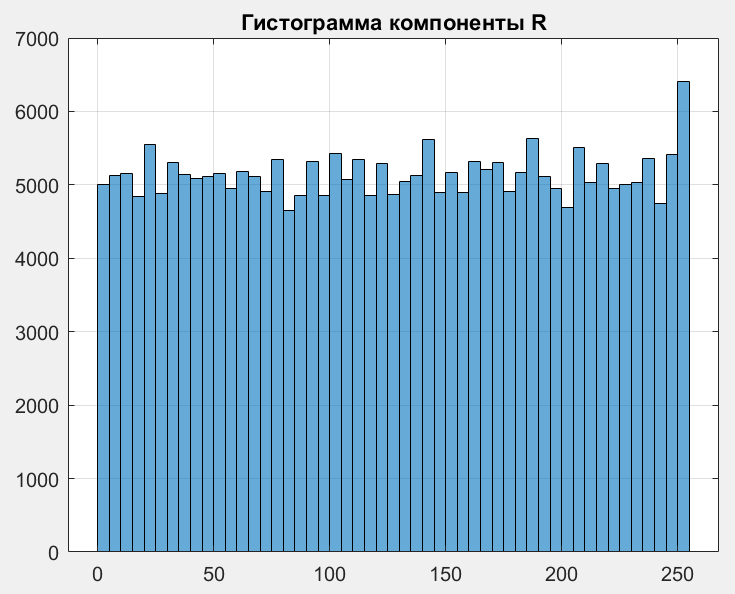
Рисунок 3. График автокорреляционной функции.

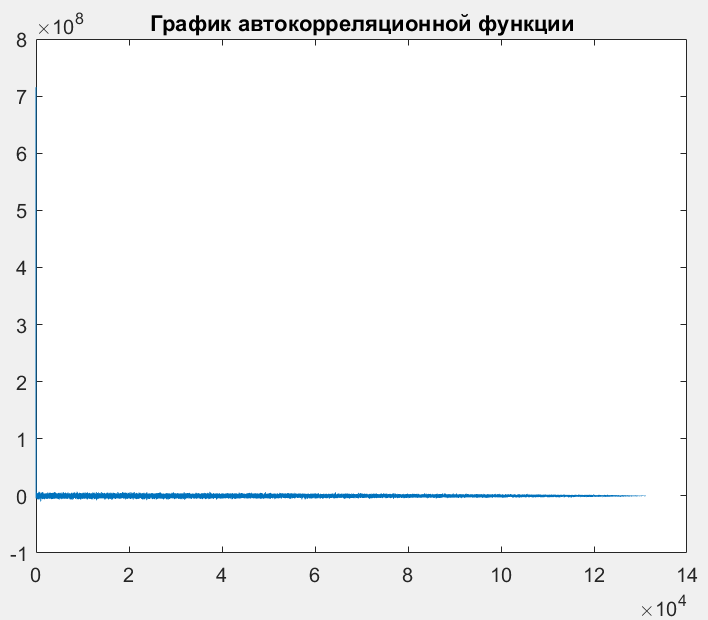
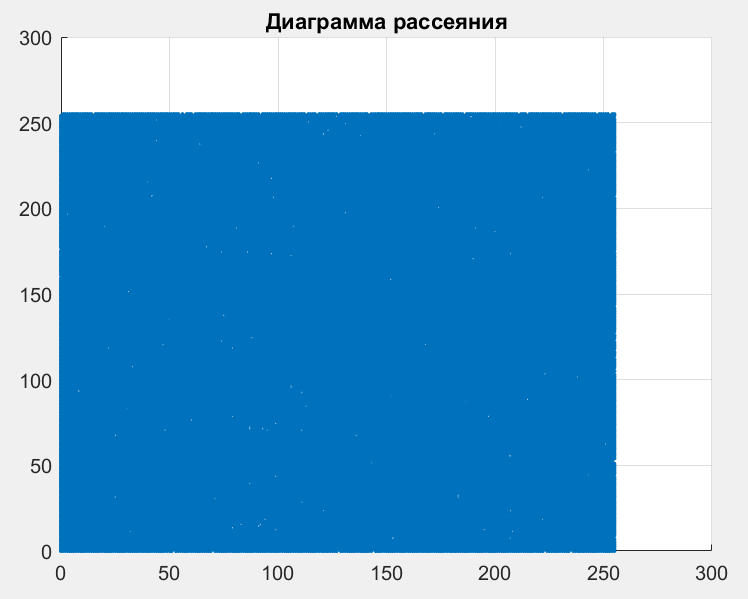
За один проход алгоритма шифрования (при k = 1 раунде шифрования) кодируется 8 байт изображения. Было составлено 32 таблицы подстановки, где i1..16 – таблицы прямой подстановки, i17..32 – таблицы обратной подстановки. Номер таблицы обратной подстановки рассчитывается по правилу:   
 𝑖обр = 𝑖пр + 16 𝑚𝑜𝑑 32,  
 где iобр , iпр – номер таблицы обратной и прямой подстановки.

**Раунд 1:**





Как видим, желаемый результат не был достигнут при первом раунде: неравномерное распределение, периодичность автокорреляционной функции.  
  
**Раунд 2:**



Итого: 2 раунд даёт нам желаемые результаты, все тесты пройдены, силуэт отсутствует на полученном изображении.

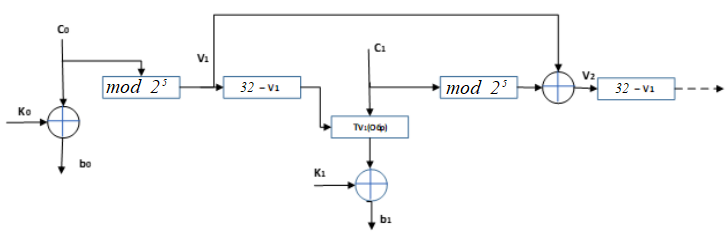


Рисунок 6. Схема дешифрования i-го раунда

Дешифрование происходит в обратном порядке, однако следует учитывать алгоритм высчитывания номера таблицы обратной подстановки. Результат дешифрования:

1. **Выводы:**

В данной лабораторной работе был смоделирован шифр с управляющими подстановками, есследована его работа при разном числе раундов шифрования.   
Чтобы определить оптимальное количество раундов, необходимое для сокрытия информации использовании шифра с управляющими подстановками, к исходному изображению и резльтатам каждого раунда были применены статистические тесты, показывающие наличие зависимостей в изобращении.   
В результате исследования было выяснено, что для того, чтобы исходное изображение превратилось в шум, треюуется 2 раунда шифрования.