Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное учреждение высшего образования

«Новгородский государственный университет имени Ярослава Мудрого»

Кафедра «Информационных технологий и систем»

**Лабораторная работа №3**  
по дисциплине:

«Защита информации»

Разработал:

Студент группы 8091

Шаклеин В. В. \_\_\_\_\_\_  
 «\_\_» \_\_\_\_\_2021г

Проверил преподаватель:

Жгун Т. В. \_\_\_\_\_

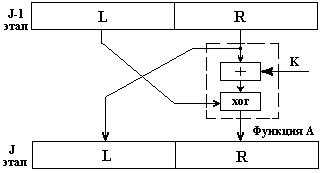
«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

Реализовать работу сети Фейстеля для блока 16 бит (шифрование и расшифрование). Число раундов 8. Исходный текст тот же. В качестве ключа шифрования выступает пароль из работы 1. Раундовые ключи являются последовательными отрезками ключа шифрования.



**Рис. 1** Идея архитектуры "сети Файстеля (Feistel`s NetWork)

Основной шаг криптопреобразования - наложение раундового ключа и сдвиг влево на 1 бит.

Реализуемая программа должна предусмотреть возможности вывода промежуточных результатов на каждом шаге.

2. Построить гистограммы для получаемых на каждом раунде зашифрованных текстов. Проанализировать результат.

**Описание алгоритмов:**

* Блок открытого текста делится на две равные части:
* В каждом раунде вычисляются:

Результатом выполнения N раундов является . В N-м раунде перестановка не производится, чтобы была возможность использовать ту же процедуру и для расшифрования, просто инвертировав порядок использования ключей

Небольшим изменением можно добиться и полной идентичности процедур шифрования и расшифрования.

**Реализация**

Задача решена с помощью языка программирования Python, используются следующие дополнительные модули: numpy, matplotlib, seaborn, они необходимы для упрощения использования математических операций над массивами чисел и построения гистограмм.

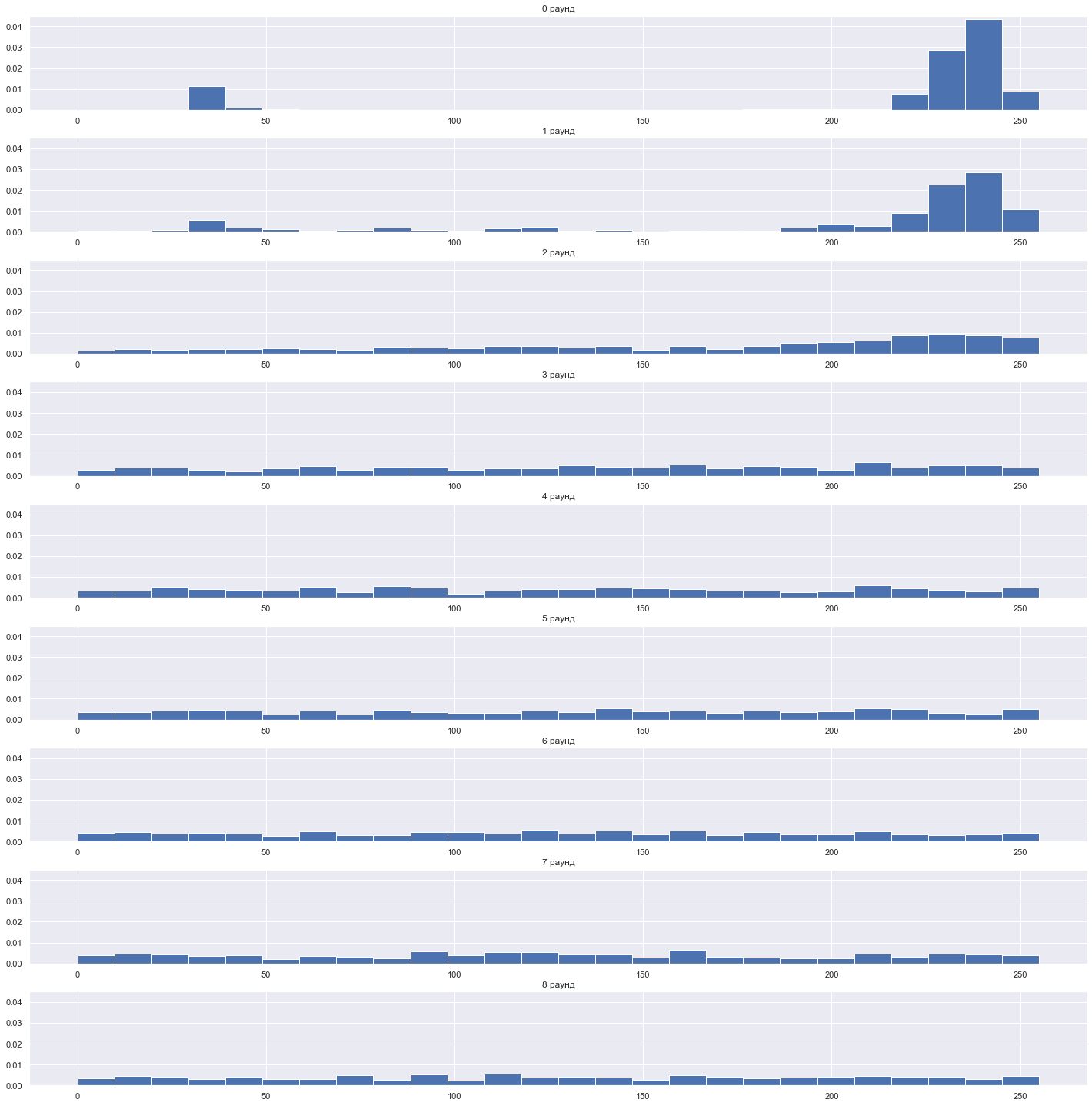
**Описание интерфейса**

Все входные значения жёстко задаются в коде, так что программа не имеет пользовательского интерфейса в привычном понимании.

**Код программы**

Код программы находится в папке с отчетом в файле feistel\_cypher*.ipynb* (так же код с возможностью запуска онлайн доступен по адресу <https://mybinder.org/v2/gh/sevskii111/infosec_reports/HEAD?filepath=lab03%2Ffeistel_cypher.ipynb>).

**Результат работы программы**



**Вывод**Для решения поставленных задач был выбран ЯП Python, также были построены гистограммы.

Рассмотрев полученные гистограммы, можно сделать вывод о том, что уже после 4-его раунда частота встречаемости символов зашифрованного текста визуально ничем не имеет никакой связи с частотой встречаемости символов в исходном тексте.