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 №4**  
по дисциплине:

«Защита информации»

Разработал:

Студент группы 8091

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

Проверил преподаватель:

Жгун Т. В. \_\_\_\_\_

«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

Реализовать режимы шифрования DES для имеющейся процедуры шифрования (работа 3 )

* ECB, Electronic Coding Book
* CBC, Cipher Block Chaining
* CFB, Cipher Feedback
* OFB, Output Feedback

Исходный текст тот же. В качестве ключа шифрования выступает пароль из работы 1. Раундовые ключи являются последовательными отрезками ключа шифрования.

Построить гистограммы для получаемых зашифрованных текстов. Проанализировать результат.

**Описание алгоритмов:**

**Режим простой замены (ECB, Electronic Coding Book)**

Это самый простой режим, в котором 64-битовые блоки шифротекста получают путем зашифрования 64-битовых блоков открытого текста (см. рисунок 4). При этом из одинаковых блоков открытого текста получаются одинаковые блоки шифротекста. Данный режим применяется очень редко, в основном для шифрования ключевых данных, в которых невелика вероятность появления повторяющихся 64-битовых блоков.

**Режим сцепления блоков шифротекста (CBC, Cipher Block Chaining)**

Шифруемое сообщение разделяется на блоки по 64 бита. Первый блок исходного сообщения складывается по модулю 2 с 64-битным блоком, называемым "вектором инициализации". Полученный после этой операции блок подвергается основному циклу преобразования DES. Блок на выходе преобразования DES является первым блоком шифротекста (см. рисунок 5). Далее этот блок шифротекста складывается по модулю 2 со вторым блоком открытого текста, подвергается циклу преобразования DES и становится вторым блоком шифротекста.

При расшифровании первый блок шифротекста расшифровывается алгоритмом DES и побитово складывается по модулю 2 с вектором инициализации. Результирующий блок является первым блоком открытого текста.

**Режим обратной связи по шифротексту (CFB, Cipher Feedback)**

Этот режим был создан для того, чтобы сделать возможным шифрование блоков с размером менее 64 бит и обеспечить зависимость блока шифротекста от его номера. Исходное сообщение разбивается на равные блоки длиной от K=1,2... 64 бит. В режимах за- и расшифрования используется вектор инициализации длиной L. В случае L<64, вектор инициализации располагают в младших разрядах входного блока DES, а оставшиеся биты устанавливают в "0". И при шифровании и расшифровании используют основной цикл преобразования DES в режиме зашифрования.

При зашифровании К-битовый блок шифротекста получают побитовой операцией "исключающее ИЛИ" К-битового блока открытого текста со старшими К битами выхода DES. При расшифровании К бит открытого текста получают операцией "исключающее ИЛИ" К-битового блока шифротекста со старшими К битами выхода DES. В обоих случаях следующий входной блок DES получают, отбрасывая старшие К бит предыдущего входного блока, сдвигая оставшиеся биты на К позиций влево и вставляя в младшие разряды К бит только что полученного шифротекста.

**Режим обратной связи по выходу (OFB, Output Feedback)**

Этот режим отличается от режима с обратной связью по шифротексту только тем, что младшие К бит входного блока DES занимают старшие К бит выходного блока DES, полученного при зашифровании предыдущего блока данных

**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.

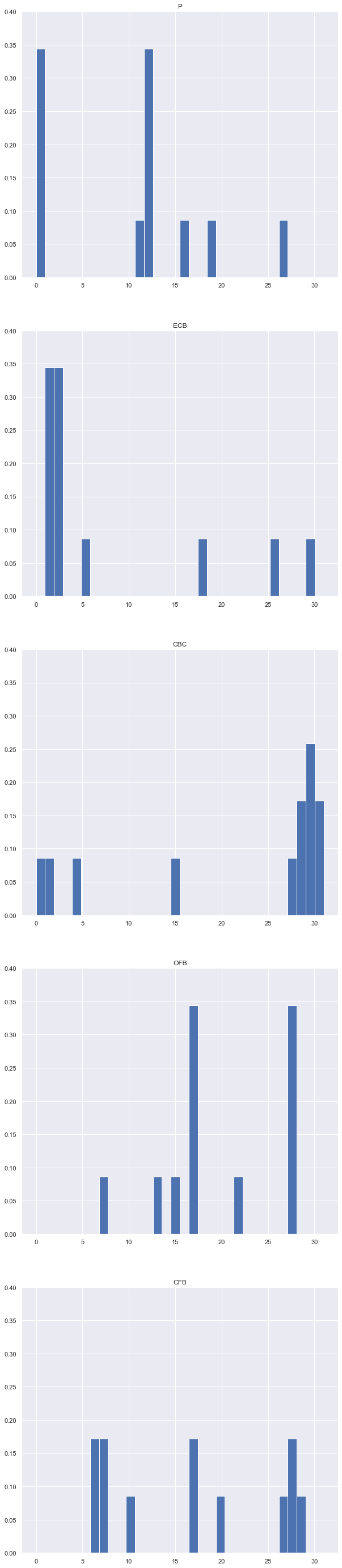
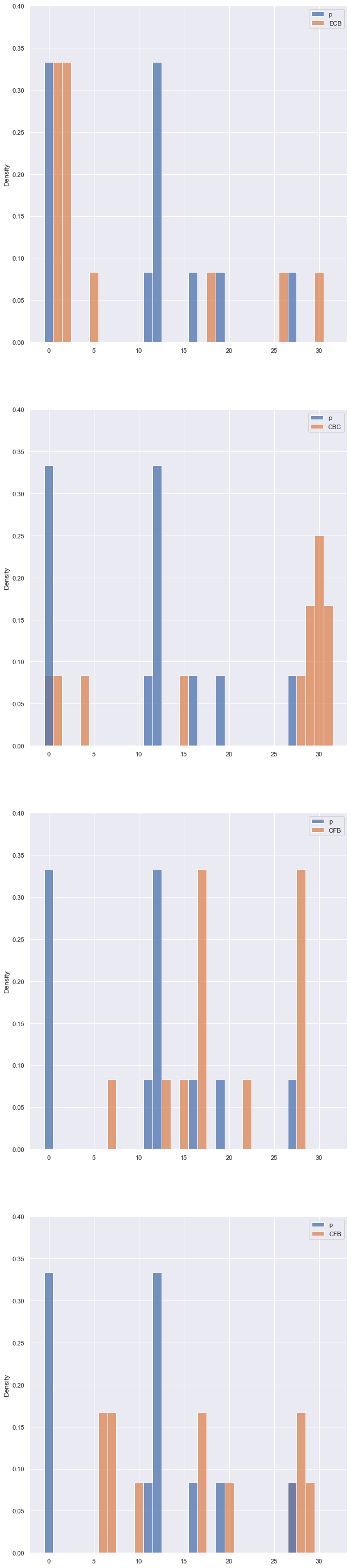
**Описание интерфейса**

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 DES (так же код с возможностью запуска онлайн доступен по адресу <https://mybinder.org/v2/gh/sevskii111/infosec_reports/HEAD?filepath=lab04%2FDES.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 исходную частоту встречаемости символов лучше всего маскируют процедуры CBC и OFB.