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 №2**  
по дисциплине:

«Защита информации»

Разработал:

Студент группы 8091

Васильев И.В.  
 «\_\_» \_\_\_\_\_2021г

Проверил:

Жгун Т. В. \_\_\_\_\_\_

«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

Разработать программное обеспечения для шифрования текста следующими способами:

1. Парное шифрование
2. С помощью ключа константы
3. С помощью ключа поговорки
4. С помощью ключа псевдослучайной последовательности

**Описание алгоритмов:**

1) Парное шифрование

В этом шифре ключом является фраза, содержащая 15 разных букв. Подписывая под этими буквами буквы в алфавитном порядке, не вошедшие в этот ключ, получаем разбиение 30 основных букв русского алфавита на пары. Чтобы получить из сообщения шифрованный текст, заменяют каждую букву сообщения своим напарником.

**Пример 1.3**

Выбираем в качестве ключа фразу ***“Железный шпиц дома лежит”,*** получим разбиение основных букв русского алфавита на пары, как указано ниже:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 |  | 4 | 5 | б |  | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |  |  |  |  | 15 |
| ж | е | л | е | з | н | ы | и | ш | п | и | ц | д | о | м | а | л | е | ж | и | т |
| б | в | г |  | к | р | с |  | у | ф | х | ч | щ | ь | э | ю |  |  |  |  | я |

Таким образом, получаем отображение букв основного алфавита на последовательность, состоящую из тех же букв

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ж | з | и | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ |
| ю | ж | е | л | щ | в | б | к | х | з | г | э | р | ь | ф | н | ы | я | ш | п | и | ч | ц | у | д |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ь | ы | э | ю | я |
| о | с | м | а | т |

Поэтому сообщение “Встреча отменяется, явка раскрыта”, переходит в следующий шифртекст

ЕЫЯНВ ЦЮЬЯЭ ВРТВЯ ЫТТЕЗ ЮНЮЫЗ НСЯЮ

Очевидно, что в качестве ключа можно использовать любую фразу, в которой имеется не менее 15 разных букв основного алфавита

2) С помощью ключа константы

Алгоритм реализуется следующим образом, берётся некоторая константа, к примеру, она равна четырём, использую алфавит русских символом, мы строим новый алфавит со сдвигом влево всех символов на эту константу. Таким образом, формируется новый алфавит, на основе которого шифруется текст.

3) С помощью ключа поговорки

Алгоритм реализуется следующим образом, берётся некоторая поговорка, к примеру “Железный шпиц дома лежит”, на основе её формируется новый алфавит по следующим правилам:

1) Все последовательные буквы поговорки ключа, записываются в новый алфавит исключая повторения

2) после того, как ключ поговорка закончится, дописываем в наш новый алфавит оставшиеся символы из русского алфавита по порядку идущие.

После формирования нового алфавита, можно кодировать входной текст.

4) С помощью ключа псевдослучайной последовательности

Алгоритм реализуется следующим образом, используя генератор LFSR, генерируем последовательность длинны, равную длине текста, переводим текст и сгенерированную последовательность в двоичное представление и побитово складываем. Полученную битовую последовательность переводим в десятичное представление по 5бит и получаем буквы.

**Реализация**

Поставленная задача решена с помощью языка программирования С++ на фреймворке QT.

**Описание интерфейса**

Программа предоставляет пользовательское окно с полями для ввода входных значений для генераторов.

Пользователю доступны следующие поля для ввода информации:

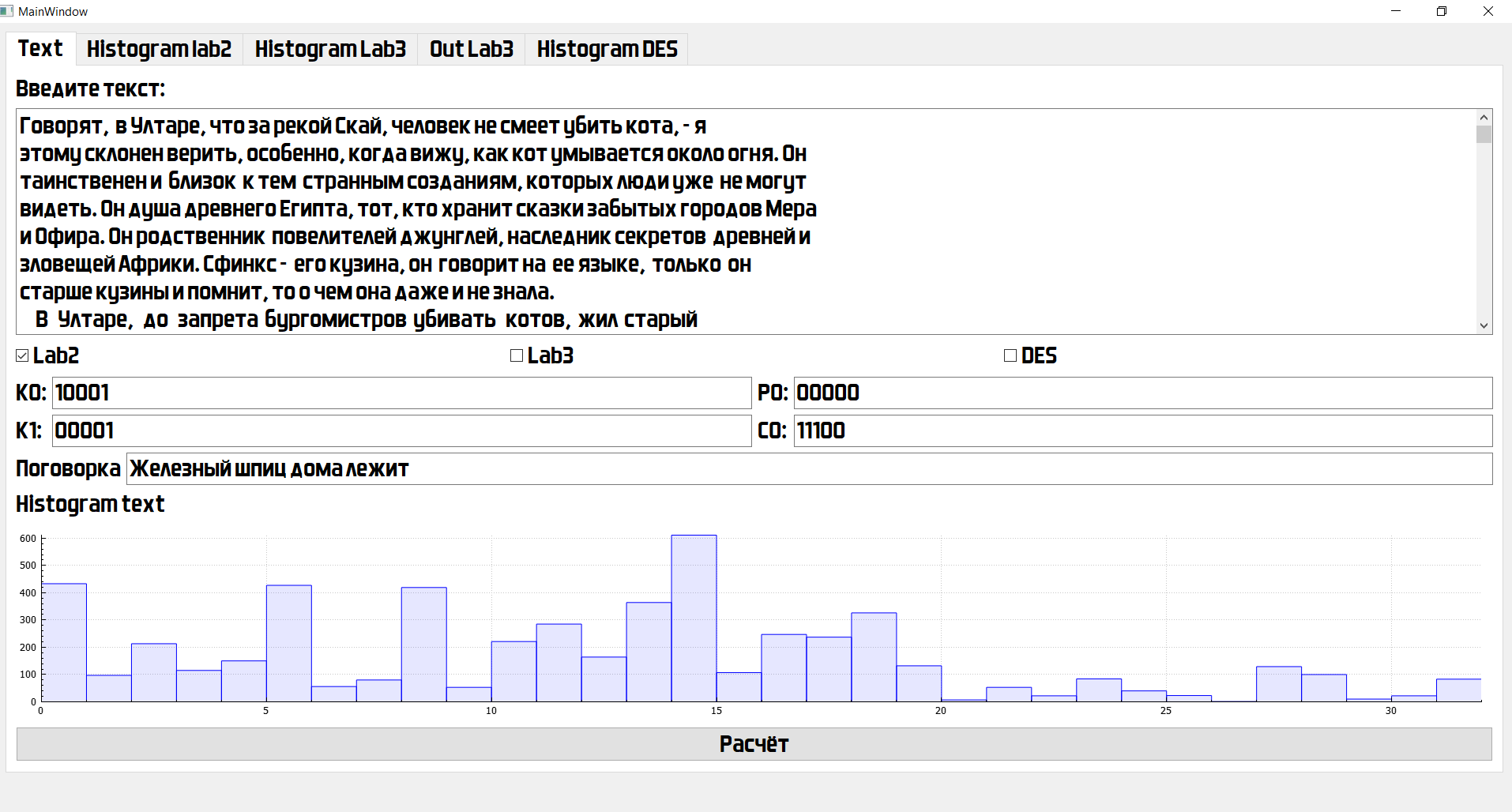
1) Поле для ввода текста

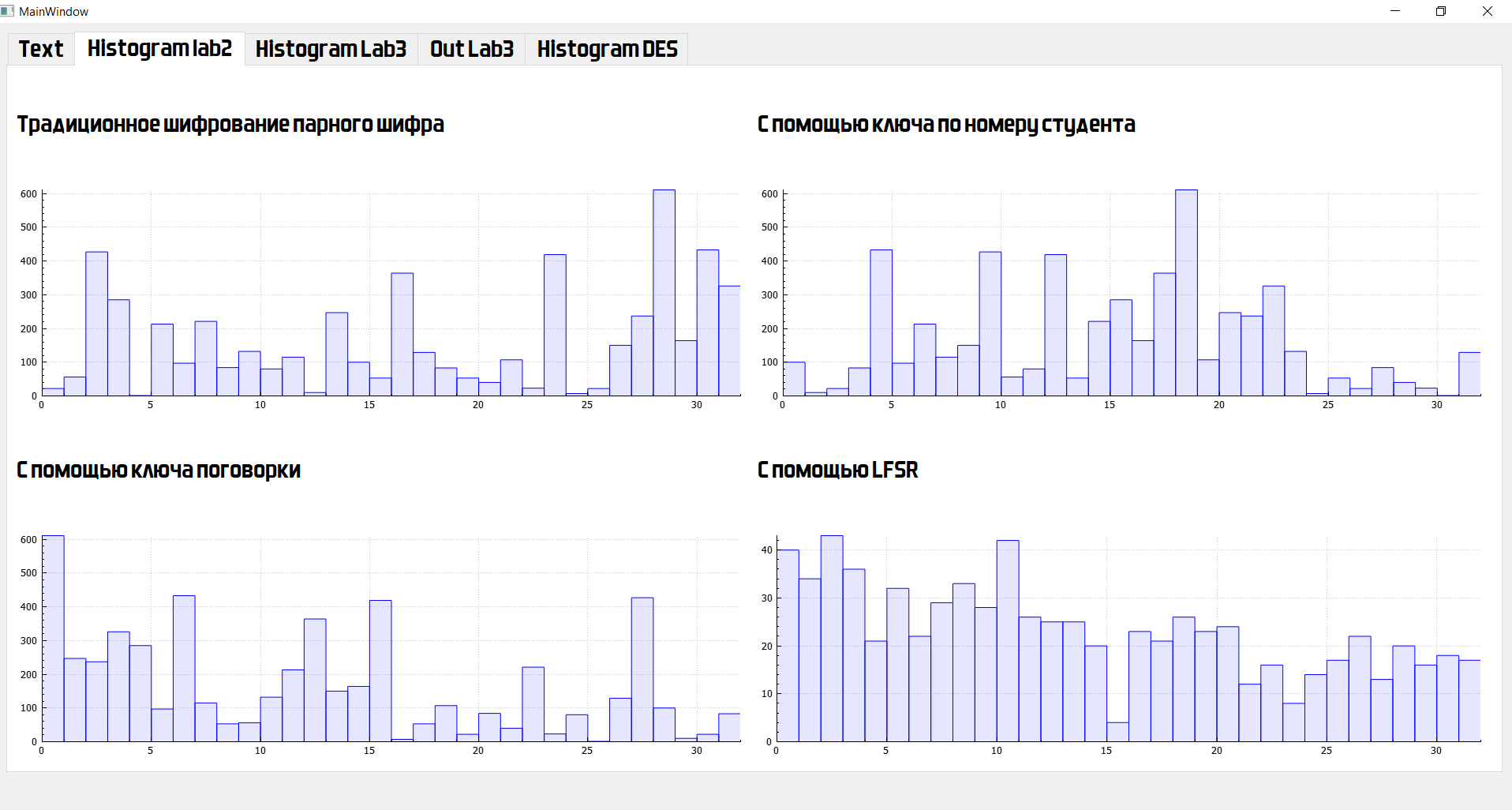
2) Поле для ввода ключа поговорки

В главном окне, пользователь может видеть результат выполнения работы в графическом представлении в виде гистограмм. Программа предоставляет 4 гистограммы для всех предложенных алгоритмов.  
  
Для запуска программы, необходимо нажать на кнопку “Генерировать”

**Результат работы программы**

## Для примера, я взял произведение Говарда Ф. Лавкрафта “Коты Ултара” объёмом в 1013 слов.





**Вывод**

Для выполнения поставленной задачи, была разработана программа, осуществляющая графическое представление алгоритмов.