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

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

Проверил:

Жгун Т. В. \_\_\_\_\_\_

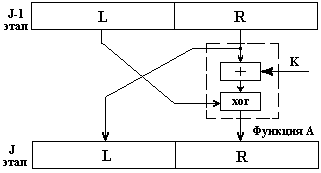
«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

Реализовать работу сети Файстеля для блока 16 бит (шифрование и расшифрование). Число раундов 8.



**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.

**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:

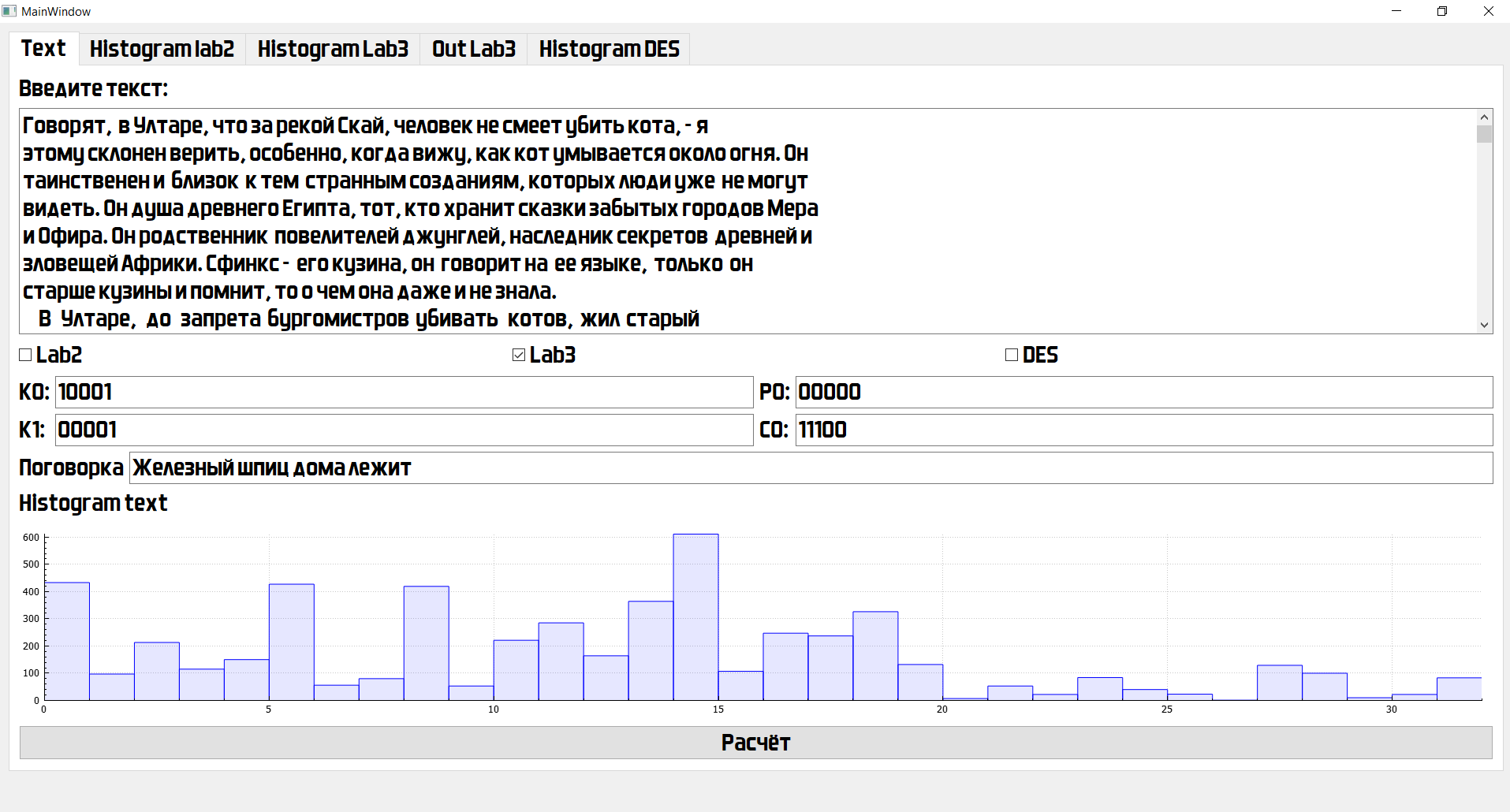
1) Поле для ввода текста

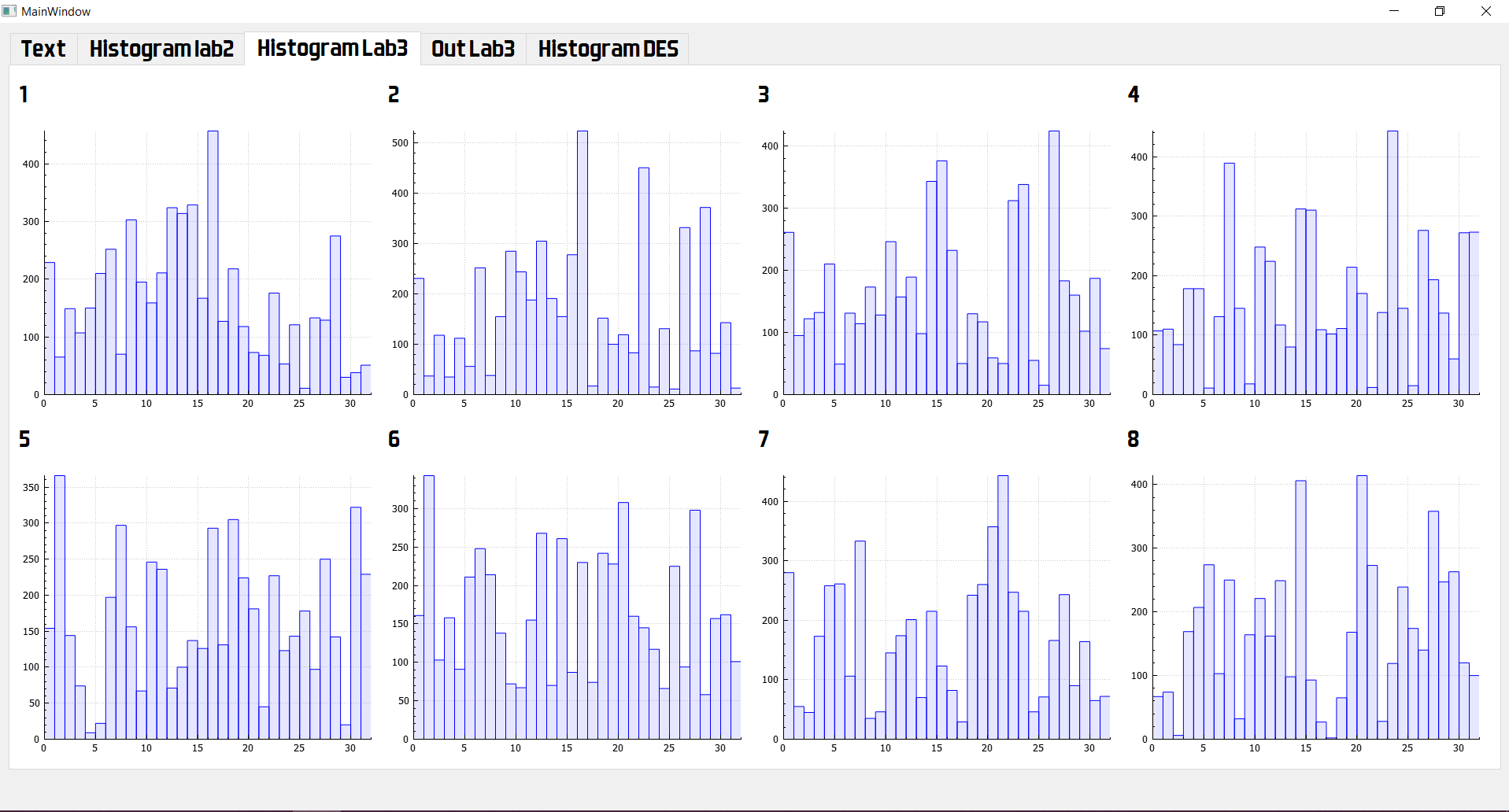
2) Поле для ввода ключа поговорки

В главном окне, пользователь может видеть результат выполнения работы в графическом представлении в виде гистограмм. Программа предоставляет 8 гистограмм и 8 окон с промежуточными результатами.  
  
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 алгоритма сети Файстеля.