Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе

на тему

РАЗРАБОТКА HTTP-СЕРВЕРА

БГУИР КР 1-40 02 01 201 ПЗ

Студент: Д. Г. Альховик

Руководитель: Е. Д. Игнатьев

Минск 2018

Оглавление

[ВВЕДЕНИЕ 5](#_Toc533261487)

[1 ОБЗОР ИСТОЧНИКОВ 6](#_Toc533261488)

[1.1 Обзор использованной литературы 6](#_Toc533261489)

[1.2 Обзор аналогов 6](#_Toc533261490)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 7](#_Toc533261491)

[3 ФУНКЦИОНАЛЬНОЕ ПРОГРАММИРОВАНИЕ 9](#_Toc533261492)

[4 РАЗРАБОТКА ПРОГРАММНЫХ МОДУЛЕЙ 12](#_Toc533261497)

[5 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ 15](#_Toc533261498)

[6 ТЕСТИРОВАНИЕ 20](#_Toc533261499)

[ЗАКЛЮЧЕНИЕ 22](#_Toc533261500)

[ПРИЛОЖЕНИЕ А Схема структурная 25](#_Toc533261501)

[ПРИЛОЖЕНИЕ Б Диаграмма классов 26](#_Toc533261502)

[ПРИЛОЖЕНИЕ В Схема алгоритма 27](#_Toc533261503)

# ВВЕДЕНИЕ

Во все времена информация была и остаётся одним из основных жизненно необходимых ресурсов человека. Она является основным безопасным способом передачи опыта от одного человека другому, а, следовательно, получая и обрабатывая большие объемы информации человек получает знания необходимые ему для жизнедеятельности и самосовершенствования.

С течением времени человечество накопило очень много сведений об окружающем нас мире, но сохранить и осмыслить столько данных человек не способен. Тогда возникает вопрос: как не потерять весь тот опыт, который человечество накапливало веками?

Выходом стало фиксирование полученной информации во всевозможных хранилищах, таких как книги. Однако и книга не всегда удобна для использования из-за объёмных размеров и трудности быстрого поиска необходимых сведений. Тогда на помощь пришли вычислительные машины, которые способны хранить огромные объёмы информации при помощи баз данных.

Хотя работа с базами данных не всегда является удобной напрямую, так как иногда необходим определенный осмысленный поиск среди хранящийся информации, либо же некоторые данные и вовсе не предоставляют ценности без соответствующей обработки и т.д.

Отличным решением для данной проблемы станет использование технологии «клиент-сервер». В данном случае это удобно, так как пользователь может доступным для него образом отправить запрос на сервер, который сумеет грамотно его обработать и выполнить, чтобы удовлетворить потребность клиента. А дабы работа клиента с сервером могла быть оперативной из любой точки земного шара следует использовать «всемирную сеть» как способ передачи запросов.

Целью данного курсового проекта будет разработка сервера, позволяющего сохранять, обрабатывать и возвращать необходимые данные по запросу пользователя и работающего по протоколу http(HyperText Transfer Protocol).

Таким образом в результате должны получить готовый http-сервер, способный работать с несколькими типами клиентов для хранения и обработки их информации на удалённом носителе.

В соответствии с поставленной целью определены следующие задачи:

* Организация обработки запроса пользователя
* Преобразование данных для их хранения
* Запись данных в базу данных
* Чтение данных из базы данных
* Организация работы по протоколу http

# ОБЗОР ИСТОЧНИКОВ

Для решения поставленных задач необходимо определить нужные компоненты для создания http-сервер. Для создания связи между клиентом и сервером нужно использовать соответствующую сетевую архитектуру. Для её реализации и построения корректной работы с базами данных необходимо использовать подходящий для этого язык программирования.

Важно также выбрать базу данных, которая позволила бы хранить различные типы данных для более универсального использования сервера. Связь между протоколом и сервером воспользуемся стандартными http-протоколами.

1.1 Архитектура «Клиент-сервер»

«Клиент-сервер» — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами.

Фактически клиент и сервер — это программное обеспечение. Обычно эти программы расположены на разных вычислительных машинах и взаимодействуют между собой через вычислительную сеть посредством сетевых протоколов, но они могут быть расположены также и на одной машине. Программы-серверы ожидают от клиентских программ запросы и предоставляют им свои ресурсы в виде данных (например, загрузка файлов посредством HTTP, FTP, BitTorrent, потоковое мультимедиа или работа с базами данных) или в виде сервисных функций (например, работа с электронной почтой, общение посредством систем мгновенного обмена сообщениями или просмотр web-страниц во всемирной паутине).

Поскольку одна программа-сервер может выполнять запросы от множества программ-клиентов, её размещают на специально выделенной вычислительной машине, настроенной особым образом, как правило, совместно с другими программами-серверами, поэтому производительность этой машины должна быть высокой. Из-за особой роли такой машины в сети, специфики её оборудования и программного обеспечения, её также называют сервером, а машины, выполняющие клиентские программы, соответственно, клиентами.

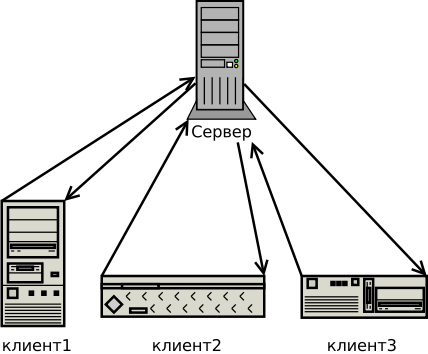


Рисунок 1.1 – Сетевая архитектура «Клиент-сервер»

Преимуществами данного подхода являются:

* Отсутствие дублирования кода программы-сервера программами-клиентами.
* Так как все вычисления выполняются на сервере, то требования к компьютерам, на которых установлен клиент, снижаются.
* Так как все вычисления выполняются на сервере, то требования к компьютерам, на которых установлен клиент, снижаются.

1.2 Обзор протокола HTTP

HyperText Transfer Protocol – это протокол передачи данных прикладного уровня, предназначенный передачи произвольных данных. Основой HTTP является технология «клиент-сервер».

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т. д.

Обмен сообщениями идёт по обыкновенной схеме «запрос-ответ». Для идентификации ресурсов HTTP использует глобальные URI.

1.3 Контейнер сервлетов Apache Tomcat

Tomcat (в старых версиях — Catalina) — контейнер сервлетов с открытым исходным кодом, разрабатываемый Apache Software Foundation. Реализует спецификацию сервлетов, спецификацию JavaServer Pages (JSP) и JavaServer Faces (JSF). Написан на языке Java.

Tomcat используется в качестве самостоятельного веб-сервера, в качестве сервера контента в сочетании с веб-сервером Apache HTTP Server, а также в качестве контейнера сервлетов в серверах приложений JBoss и GlassFish.

Для данного проекта нам подойдёт такой компонент как Coyote, который поддерживает протокол HTTP 1.1 для веб-серверов или контейнера приложений. Coyote прослушивает входящие соединения на определённом TCP порту сервера, пересылает запросы в механизм Tomcat для обработки запросов и отправляет ответ назад запрашивающему клиенту.

1.4 Система управления базами данных MongoDB

MongoDB — документоориентированная система управления базами данных (СУБД) с открытым исходным кодом, не требующая описания схемы таблиц. Классифицирована как NoSQL, использует JSON-подобные документы и схему базы данных. Написана на языке C++.

Система поддерживает ad-hoc-запросы: они могут возвращать конкретные поля документов и пользовательские JavaScript-функции. Поддерживается поиск по регулярным выражениям. Также можно настроить запрос на возвращение случайного набора результатов.

Данная система подходит нам больше всего, так как она не хранит информацию в таблицах, что удобно нам, потому что мы не знаем изначально, в каком виде информация будет поступать нам на сервер. Это даёт нам возможность хранить объекты целиком, не конвертируя содержимое данных.

1.5 Обзор аналогов

Что-то написать про то, что удалённое хранения и доступ с разных устройств из-за использования кроссплатформенного языка. Тип всякие «облака» или «гугл/яндекс диски»

## Обзор использованной литературы

В данной роботе использовалась различная литература для проектирования данного приложения. Ниже приведено их краткое описание.

1. Герберт Шилдт, С++ Базовый курс [1]. В этой книге описаны все основные средства языка С++. Данная книга использовалась для изучения языка и углубления уже имеющихся знаний.
2. Макс Шлее, Профессиональное программирование на С++ [2]. Qt 5.10. Книга посвящена разработке приложений для Windows, Mac OS X, Linux, Android и iOS с использованием библиотеки Qt версии 5.10. Подробно рассмотрены возможности, предоставляемые этой библиотекой, и описаны особенности, выгодно отличающие ее от других библиотек. Описана интегрированная среда разработки Qt Creator и работа с технологией Qt Quick.

## Обзор аналогов

Аналогами разрабатываемого приложения являются приложение PGPTools(Apple) и Secret Space Encryptor(Paranoia Works). Все данные приложения служат для шифрования информации. Однако, приведённые аналоги обладают также рядом свойств, которых не будет в разрабатываемом приложении – это возможность отправки зашифрованного сообщения по электронной почте и шифрования баз данных.

Но, данное приложение будет обладать и рядом преимуществ перед приложениями ведущих компаний:

– Кроссплатформенность, т.е. приложение будет работать на разных операционных системах: Windows, Linux и др.

– Приложение будет предоставляться бесплатно, т.е. не будет необходимости в покупке приложения или в оформлении подписки.

– В приложении можно будет узнавать подробную информации об используемом методе в целях изучения алгоритмов шифрования.

# СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описана структурная схема работы приложения. Сама структурная схема представлена в приложении А.

Работа программы разбита на пять основных блоков: выбор метода шифрования информации, пользовательский интерфейс, обработка введённых параметров, преобразование информации в соответствии с выбранным методом шифрования, вывод полученных данных на экран.

Блок выбора метода шифрования информации содержит функции для преобразования пользовательского интерфейса для удобства работы с данным методом, а также выбирает соответствующие методы для работы с пользовательской информацией в третьем блоке, блоке преобразования информации в соответствии с выбранным методом шифрования, поэтому связь между ними односторонняя.

Блок пользовательского интерфейса служит для получения от пользователя необходимых данных и передачи этой информации в блок обработки введённых параметров.

Блок обработки введённых параметров содержит функции для преобразования полученных данных от пользователя и передачи этой информации в третий блок, блок преобразования информации в соответствии с выбранным методом шифрования, что и обусловило наличие односторонней связи между данными блоками программы.

Блок преобразования информации в соответствии с выбранным методом шифрования содержит функции для изменения введенной информации и записи ее в соответствующее поле для хранения.

Блок вывод полученных данных на экран содержит функции для удобного представления результатов выполнения функций блока преобразования информации. Данный блок получает все необходимые данные и отображает их в диалоговом окне. Необходимость передачи данных для вывода на экран обусловила наличие связей между двумя рассматриваемыми блоками. Также при необходимости пользователь может продолжить работу с программой для чего и сделана связь между блоками пользовательского интерфейса, блоком обработки введённых параметров и блоком выбора метода шифрования информации.

# ФУНКЦИОНАЛЬНОЕ ПРОГРАММИРОВАНИЕ

Поскольку в данной работе используется объектно-ориентрованный подход программирования, то в программе были использованы следующие классы (диаграмма классов представлена в приложении Б):

1. Класс Cipher:

## Поля:

– QString input – необходима для хранения введённой пользователем информации.

– QString output – необходима для хранения преобразованной информации.

Методы:

– Cipher() – конструктор, в котором инициализируются поля класса.

– virtual ~Chipher() – виртуальный деструктор.

– virtual void setInput(QString \_input) – функция для получения доступа к полю класса QString input..

– virtual void setOutput(QString \_output) – функция для получения доступа к полю класса QString output.

– QString getInput() – функция установки значения поля класса QString input.

– QString getOutput() – функция установки значения поля класса QString input.

– virtual void doCipher()=0 – функция, в которой информация из QString input шифруется и записывается в QString output.

– virtual QString descpiption()=0 – функция, которая читает информацию из соответствующего файла и записывает её в строку.

– static Cipher\* createCipher(int name\_ID, QString \_input, QString \_smth) – функция для реализации патерна «Фабрика», в качестве значения int name\_ID ставится номер нужного шифра.

1. Класс CipherCaesar:

## Поля:

– int shift – необходима для хранения «шага».

Методы:

– CipherCaesar() – конструктор, в котором инициализируются поля класса как «тестовые».

– CipherCaesar(QString \_input, QString \_shift=”3”) – конструктор, в котором инициализируются поля класса.

– ~CipherCaesar() – переопределение виртуального деструктора.

– void setShift(int \_shift) – функция установки значения поля класса int shift.

– int getShift() – функция для получения доступа к полю класса int shift.

– void doCipher() – переопределение функции под шифр Цезаря.

– bool isCapitalLetter(char) – функция возвращающая значение true, если предаваемая переменная является заглавной буквой английского алфавита.

– bool isUppercaseLetter(char) – функция возвращающая значение true, если предаваемая переменная является строчной буквой английского алфавита.

– QString description() – переопределение функции под шифр Цезаря.

1. Класс CipherVizhener:

## Поля:

– QString key – необходима для хранения ключа.

Методы:

– CipherVizhener() – конструктор, в котором инициализируются поля класса как «тестовые».

– CipherVizhener(QString \_input, QString \_key=”a”) – конструктор, в котором инициализируются поля класса.

– ~CipherVizhener() – переопределение виртуального деструктора.

– void setKey(QString \_key) – функция установки значения поля класса QString key.

– QString getKey() – функция для получения доступа к полю класса QString key.

– void doCipher() – переопределение функции под шифр Виженера.

– bool isCapitalLetter(char) – функция возвращающая значение true, если предаваемая переменная является заглавной буквой английского алфавита.

– bool isUppercaseLetter(char) – функция возвращающая значение true, если предаваемая переменная является строчной буквой английского алфавита.

– QString description() – переопределение функции под шифр Виженера.

1. Класс TranslationNS:

## Поля:

– QString key – необходима для хранения «шага».

Методы:

– TranslationNS() – конструктор, в котором инициализируются поля класса как «тестовые».

–TranslationNS(QString \_input, QString \_key=”a”) – конструктор, в котором инициализируются поля класса.

– ~TranslationNS() – переопределение виртуального деструктора.

– void seеNS(int \_ns) – функция установки значения поля класса int ns.

– int getKey() – функция для получения доступа к полю класса int ns.

– void doCipher() – переопределение функции для перевода чисел из десятичной системы счисления.

– QString description() – переопределение функции для перевода чисел из десятичной системы счисления.

Для упрощения работы с классами в данной работе используются преобразованные элементы стандартной библиотеки шаблонов (STL), а конкретно контейнер QString.

Также для дальнейшего улучшения программы используется патерн «Фабрика», который позволяет без значительных изменений в коде программы расширять её функционал.

# РАЗРАБОТКА ПРОГРАММНЫХ МОДУЛЕЙ

В данном разделе приведён алгоритм шифрования данных по методу Цезаря. Он построен на принципе посимвольного преобразования входной строки и записи в поле выходной.

После выбора пользователя алгоритма Цезаря, ввода входных данных и нажатия кнопки «DO», программа выполняет функцию, в результате которой создаётся указатель на класс советующего алгоритма.

void MainWindow::on\_doButton\_clicked()

{

QString input=ui->inputLineEdit->text();

QString key=ui->keyLineEdit->text();

…

if(ui->caesarRadioButton->isChecked())

{

Cipher \*p=Cipher::createCipher(1, input, key);

…

}

…

}

Здесь l – это индивидуальный номер(name\_ID), известный разработчику, метода шифрования. Вторые два параметра input и key – это входные данные, т.е. текст для преобразования и «шаг». В ходе работы конструктора вызывается метод void doCipher(), который и создаёт зашифрованную строку и помещает в поле QString output.

void CipherCaesar::doCipher()

{

QString str=getInput(), res;

if(str.isEmpty())

{

setOutput(" ");

return;

}

for (int i=0; i<str.length(); ++i)

{

if(str[i].isLetter())

{

int ch=str[i].cell();

if (isUppercaseLetter(ch))

{

ch+=shift;

while(!isUppercaseLetter(ch))

{

if(ch>'z')

{

ch-=26;

}

else

{

ch+=26;

}

}

res[i]=static\_cast<char>(ch);

continue;

}

ch+=shift;

while(!isCapitalLetter(ch))

{

if(ch>'Z')

{

ch-=26;

}

else

{

ch+=26;

}

}

res[i]=static\_cast<char>(ch);

continue;

}

res[i]=str[i];

}

setOutput(res);

}

Изначально для удобства работы создаются переменные str, в которую помещается исходный текст, а также переменная для записи результата res.

После идёт проверка на существование введенной строки.

Затем осуществляется проход по контейнеру, в который уже занесена вся имеющаяся информация и преобразуются только те значения, которые являются символом английского алфавита. Если символ не является буквой, он записывается в выходную строку без изменений.

Если же символ является буквой, то его Unicode записывается в рабочую переменную int ch с помощью метода QChar::cell(). Далее к полученному Unicode добавляется «шаг», что и является ключевым моментом шифра Цезаря.

Поскольку «шаг» мог быть таким, что в результате изменения Unicode рабочей переменной вышел за пределы английского алфавита, то во избежание изменения регистра введенной буквы и несоответствия её символу английского алфавита выполняются соответствующие проверки.

После записи всего шифра результат заноситься в поле хранения результата QString output, которое будет позже выведено на экран.

Полученную результирующую строку заносим в текстовое поле с помощью функции:

void MainWindow::on\_doButton\_clicked()

{

…

if(ui->caesarRadioButton->isChecked())

{

Cipher \*p=Cipher::createCipher(1, input, key);

QString result=(\*p).getOutput();

ui->resultOutput->setText(result);

}

…

}

После чего производиться вывод на экран строки с результатом работы в соответствующем поле интерфейса.

# РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Для корректной работы разработанного программного средства нужны следующие файлы и папки:

— исполняемый файл;

— необходимые для работы приложения DLL файлы.

При соблюдении требуемых условий дополнительной установки компонентов не требуется.

Разработанное программное средство просто в использовании. Ниже будут даны описания последовательностей действий, необходимых для успешной генерации шифра.

После запуска программы откроется главное рабочее окно.

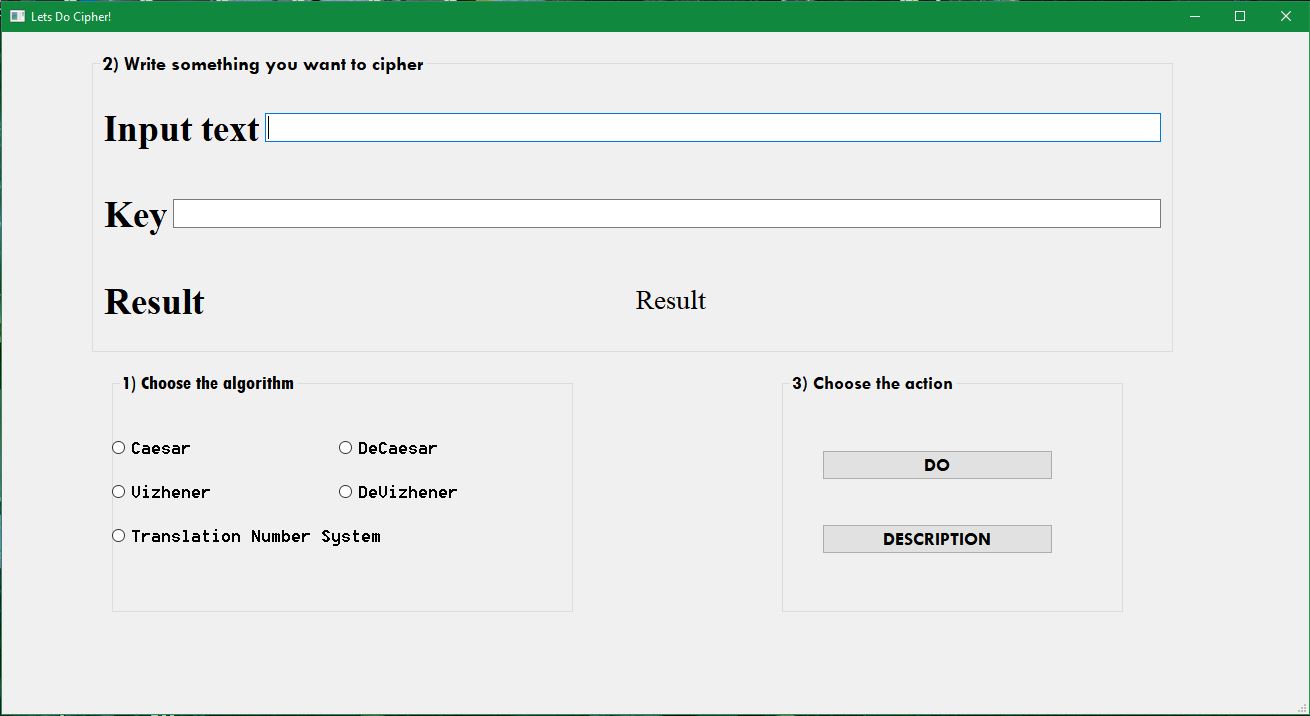


Рисунок 1

Далее в появившемся списке необходимо выбрать один из предложенных алгоритмов кодирования.

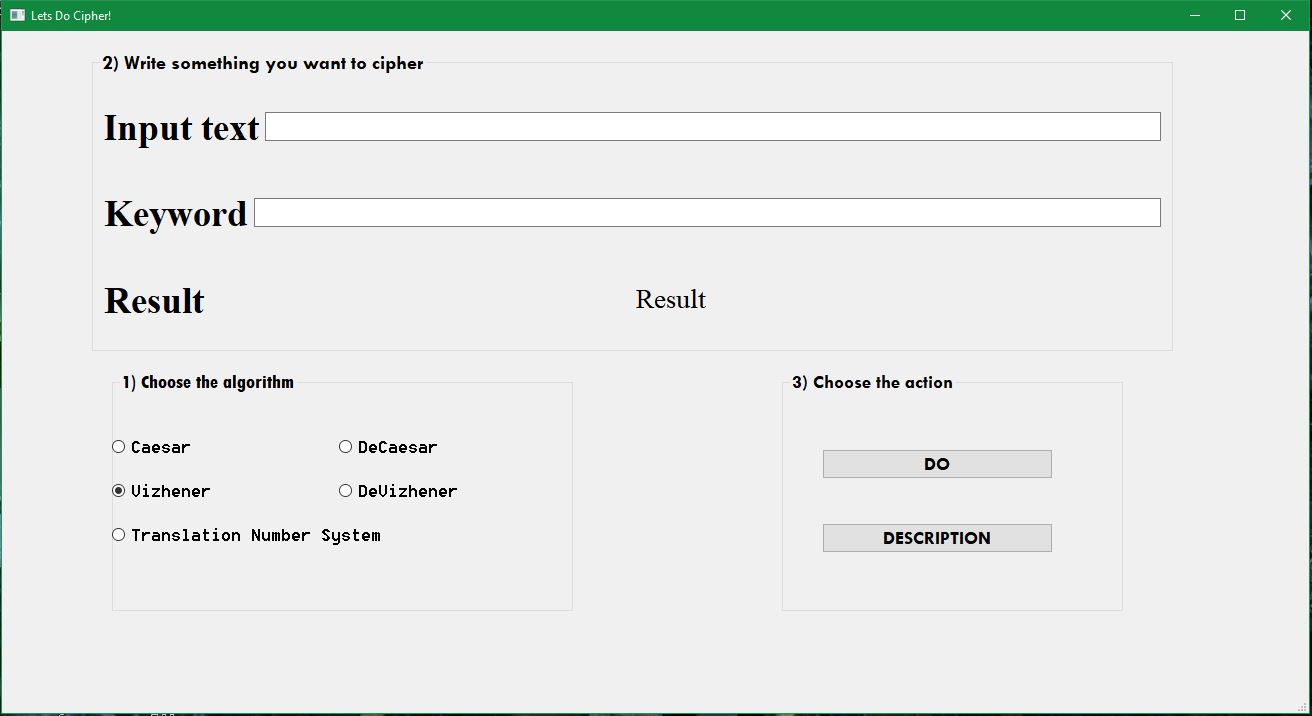


Рисунок 2

После чего необходимо ввести текст для шифрования и ключ.

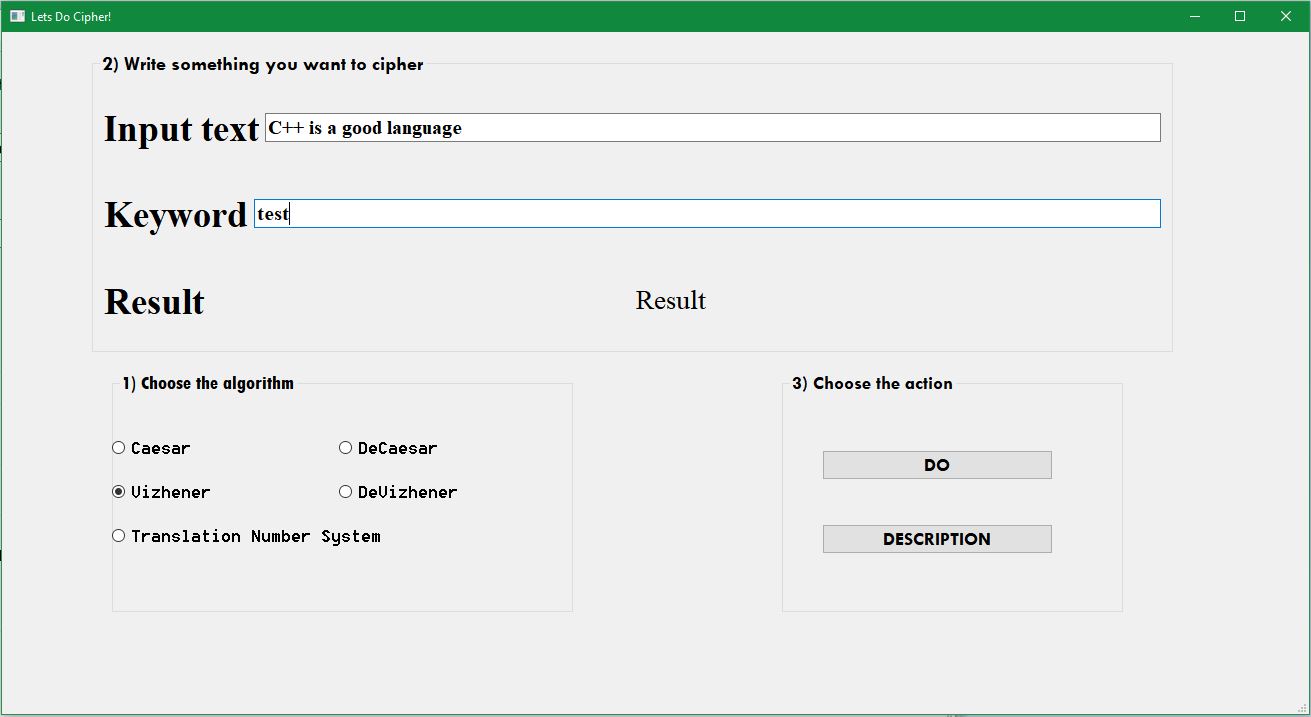


Рисунок 3

Затем для получения зашифрованного текста следует нажать кнопку «DO».

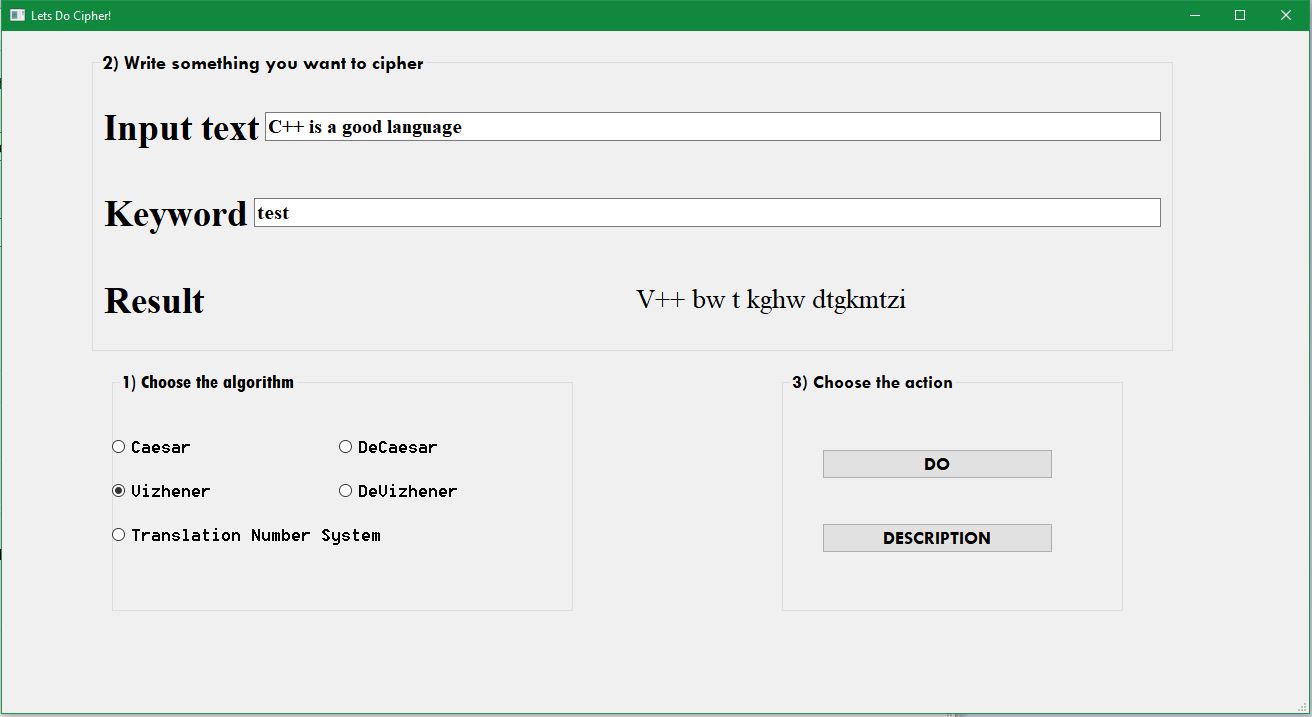


Рисунок 4

Для получения справочной информации о способе кодирования нужно нажать кнопку «DESRIPTION».

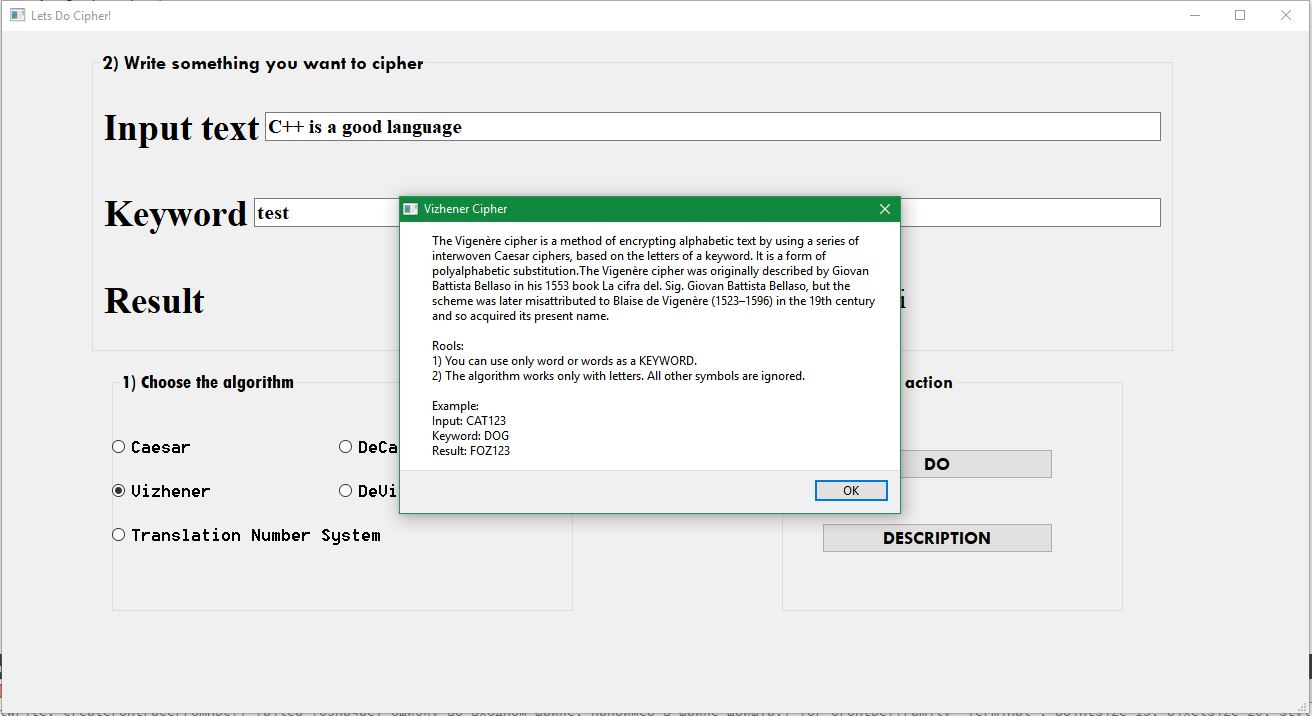


Рисунок 5

Для удобства пользования при наведении на поля ввода либо кнопки «DO» программа подсказывает, какую информацию необходимо ввести для корректной работы программы. При наведении на кнопку «DESCRIPTION» сообщает, что делает данная кнопка.

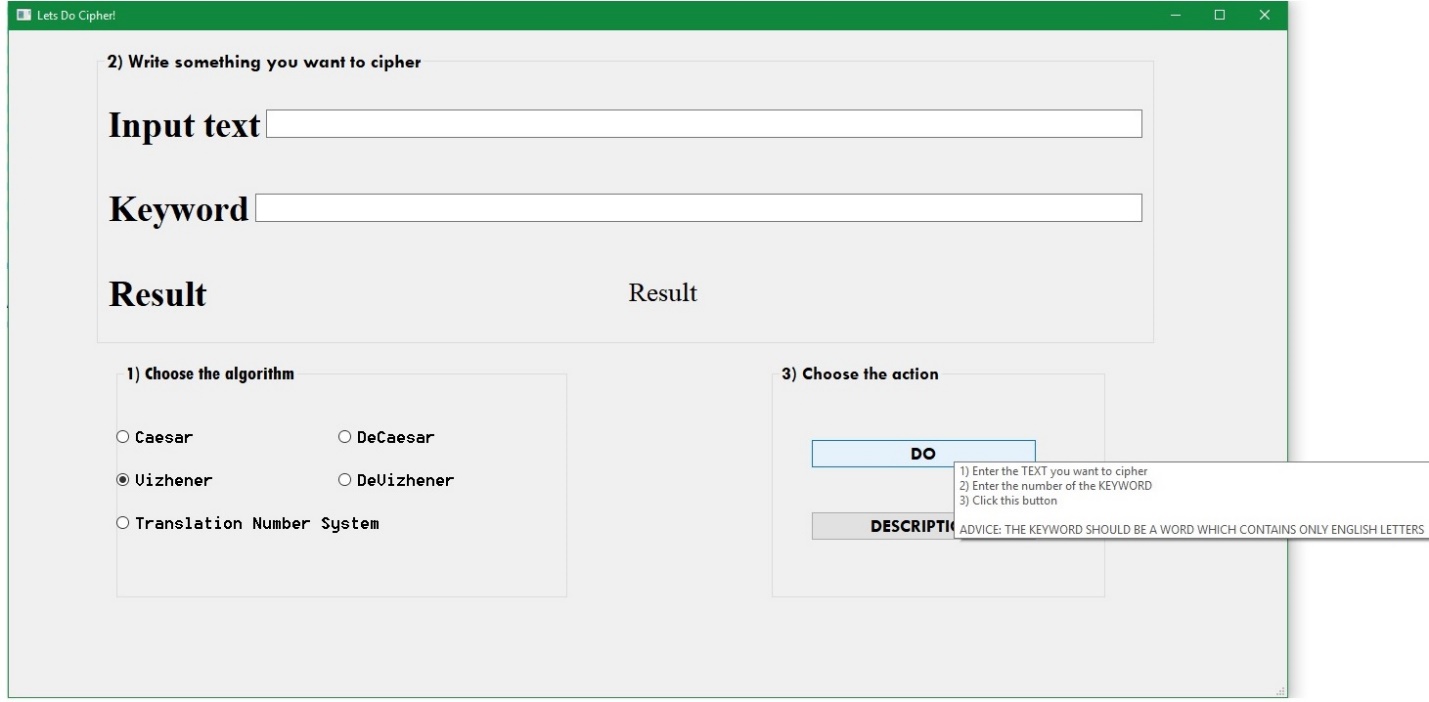


Рисунок 6

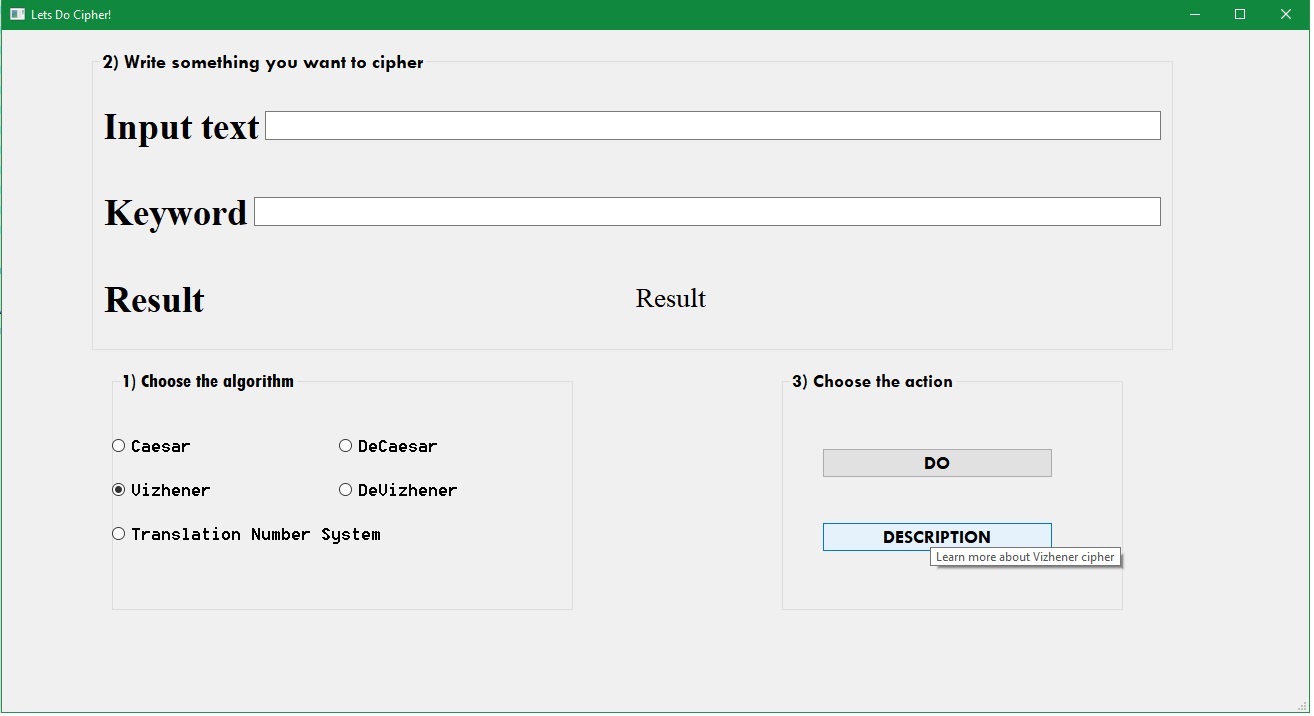


Рисунок 7

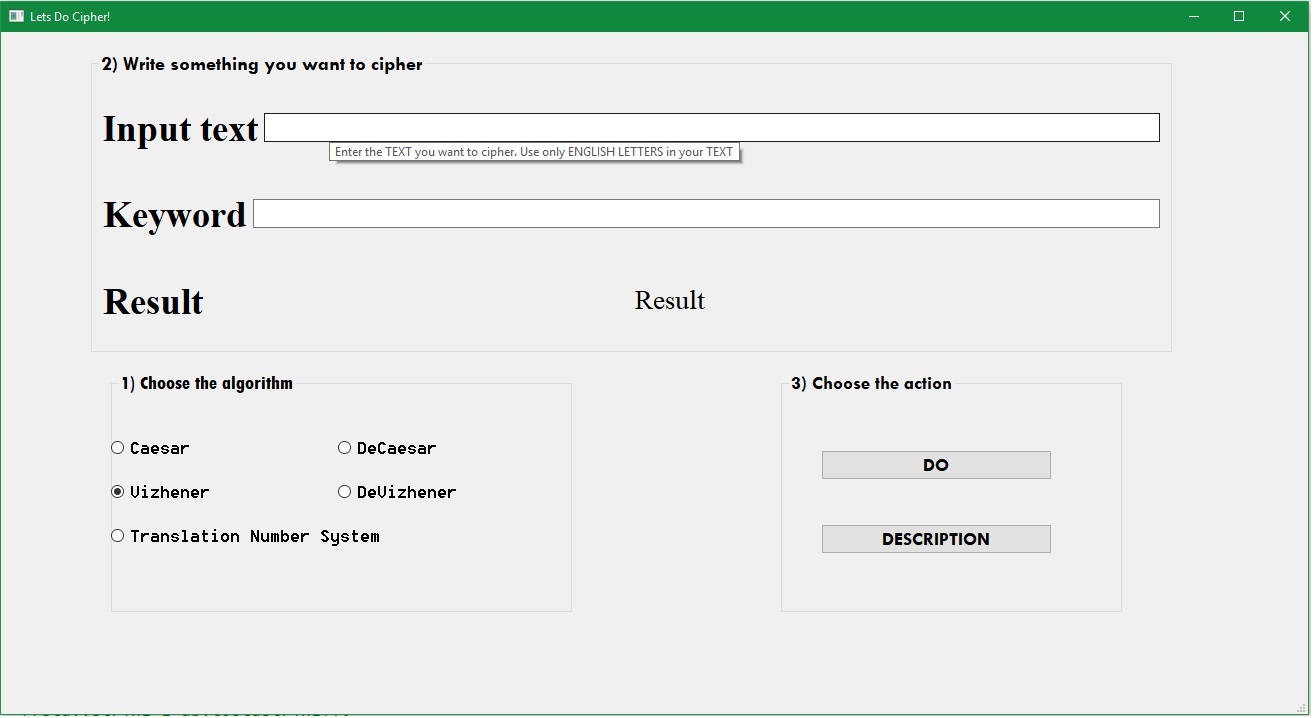


Рисунок 8

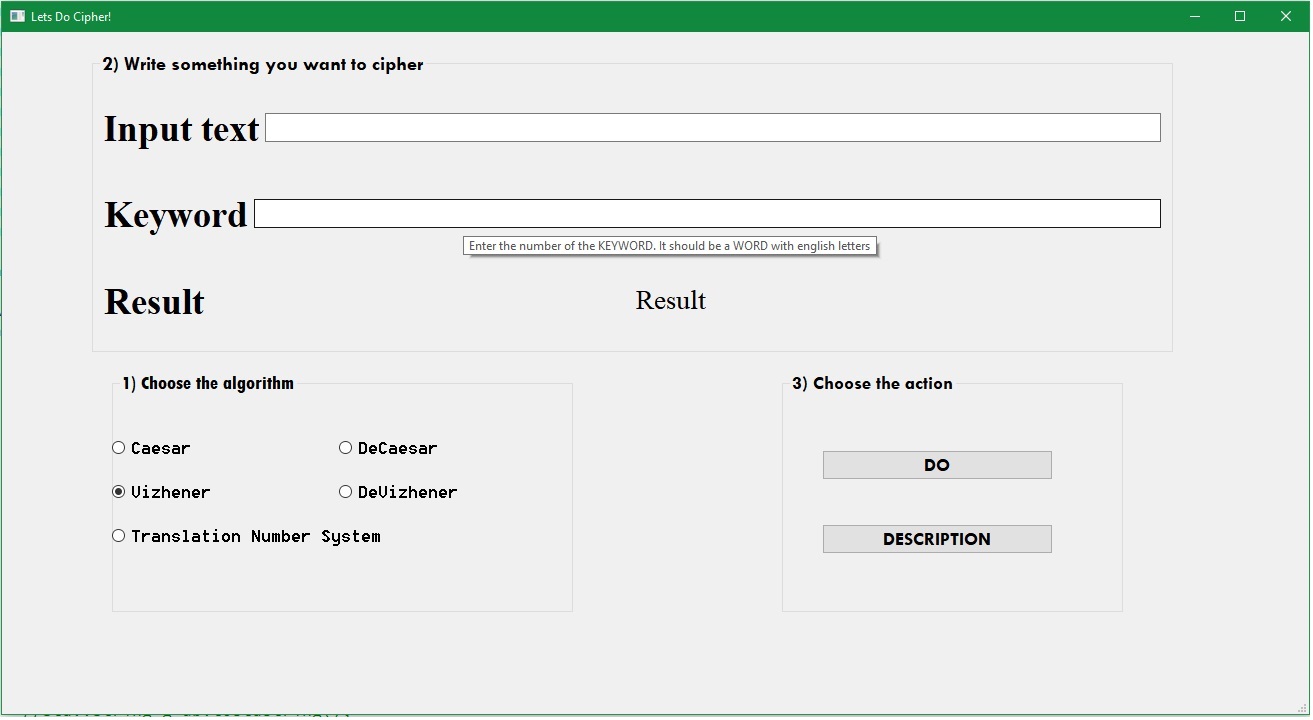


Рисунок 9

# ТЕСТИРОВАНИЕ

Проведём тестирование некоторых кнопок.

|  |  |  |  |
| --- | --- | --- | --- |
| Вид кнопки | Действие | Ожидаемый результат | Успешность тестирования |
| 1 | 2 | 3 | 4 |
| Radio Button | Нажатие на кнопку | Изменение текста некоторых полей, текста подсказок | да |
| Push Botton «DO» | Нажатие на кнопку | Вывод соответствующего шифра | да |
| Line Edit | Наведение мыши на поле | Вывод подсказки | да |
| Push Button  «DESRIPTION» | Нажатие на кнопку | Вывод окна с описанием алгоритма | да |

Результат тестирования Radio Button.

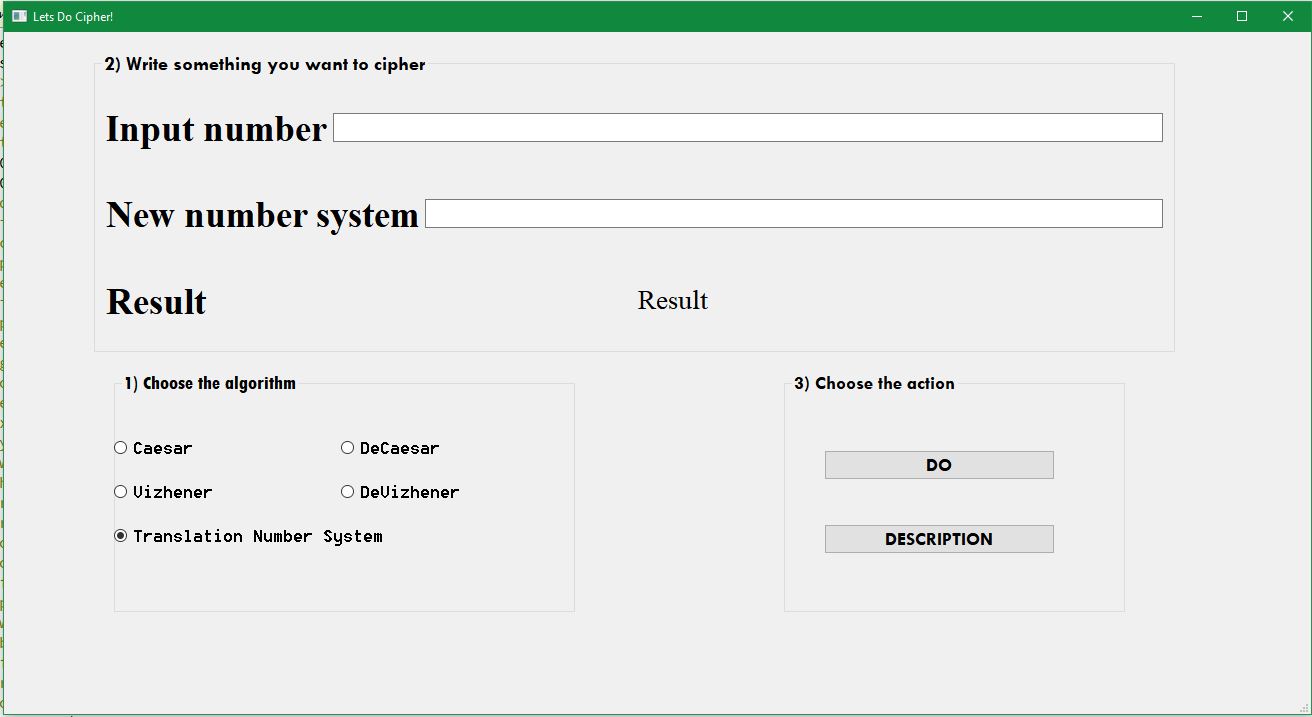


Рисунок 10

Результат тестирования Push Botton «DO».

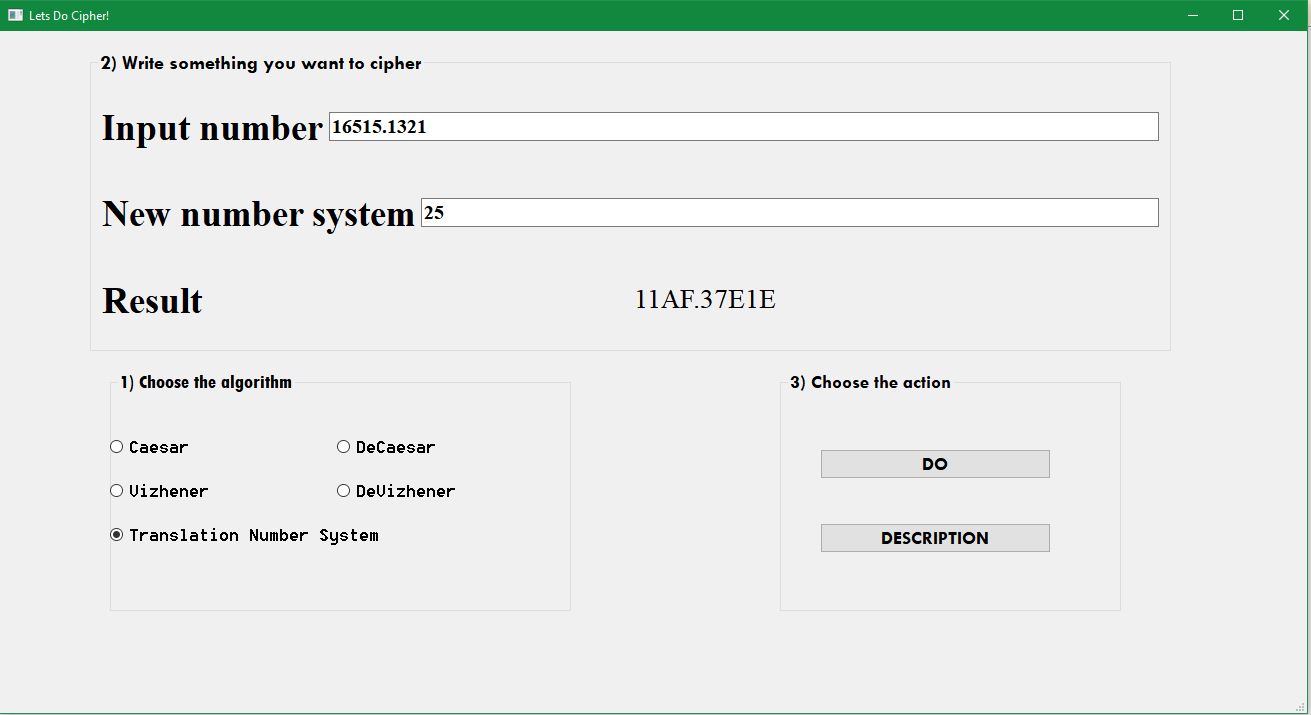


Рисунок 11

Результат тестирования Line Edit.

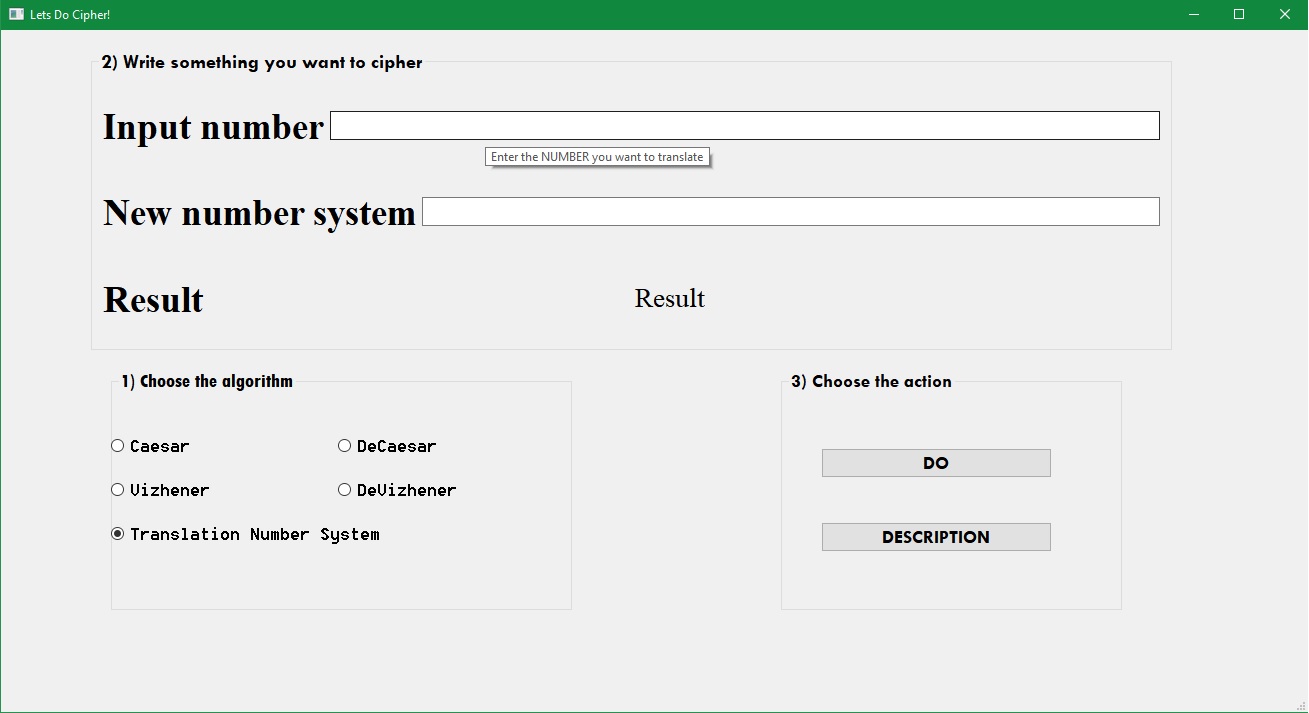


Рисунок 12

Результат тестирования Push Button «DESCRIPTION».

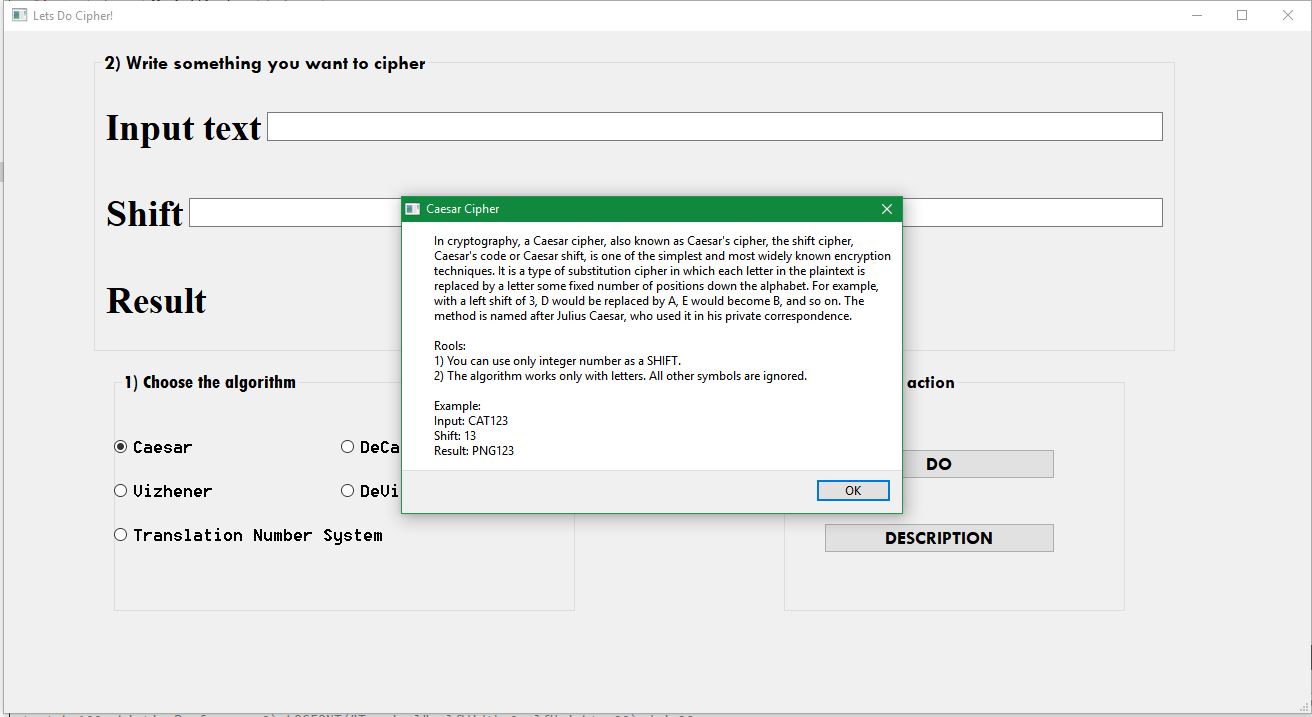


Рисунок 13

# ЗАКЛЮЧЕНИЕ

Во время выполнения курсовой работы были выполнены все поставленные задачи.

Создание программы, которая позволяет не только правильно шифровать переданную ей информацию, но и также помогать пользователю разобраться с использованным методом шифрования, узнать его историю создания и изучить основные принципы его работы.

Использование объектно-ориентированного подхода программирования дало возможность удобной реализации разработки шифратора. Но самым важным преимуществом подхода в данной программе является возможность использования патерна «Фабрика».

Применение патерна «Фабрика» позволяет постоянно усовершенствовать программу без особых изменений в коде проекта. А именно добавлять новые алгоритмы шифрования в функционал программы, и, как следствие, увеличивать её мощности.

Изучение среды разработки Qt Creator позволило создать простое и понятное для использования приложения при помощи стандартных библиотек языка С++. Эта среда является отличным способом создания хорошего фронтенда, так как на её основе уже были написаны такие приложения как Skype, Opera, Google Earth и т.д.

Подводя итог, было создано компьютерное приложение, работающее на разных устройствах, однако несмотря на проделанную работу, данное приложение ещё не раскрыло весь свой потенциал. Более детальная проработка пользовательского интерфейса, добавления новых методов шифрования и адаптация приложения для большего количества языков позволит создать мощное учебно-практическое средство защиты информации, которая играет важную составляющую каждого современного человека.

СПИСОК ЛИТЕРАТУРЫ

[1] Шилдт Г. С++, базовый курс, третье издание – Osborne, 2013.

[2] Макс Шлее: Qt 5.10. Профессиональное программирование на C++ – BHV, 2018 – 1072.

[3] Объектно-ориентированное программирование на языке С++: учеб. пособие по курсу «Объектно-ориентир.программирование» для студентов специальности«Вычислит. машины, системы и сети» всех форм обучения Ю.А.Луцик [и др.]. – Мн.: БГУИР, 2003.

[4] Демидович Е.М. «Конструирование программ и языки программирования» учебное пособие для студентов специальности «Вычислительные машины, системы и сети». – Мн.: БГУИР, 2001.

[5] Луцик Ю.А., Лукьянова И.В., Калабухов Е.В., Ковальчук А.М. Электронный учебно-методический комплекс по дисциплине «Конструирование программ и языки программирования» для студентов специальности I-40 02 01 «Вычислительные машины системы и сети» всех форм обучения, БГУИР, Минск, 2011.

[6] Бушкевич А.В. Конструирование программ и языки программирования: метод. указания по курсовому проектированию для студ. спец. I-40 02 01 «Вычислительные машины, системы и сети» всех форм обуч. / сост. А. В. Бушкевич, А. М. Ковальчук, И. В. Лукьянова. – Минск : БГУИР, 2009.

[7] Шилдт Г. Искусство программирования на C++ / Г. Шилд – СПб.: BHM, 2004.

# **ПРИЛОЖЕНИЕ А**

(обязательное)

Схема структурная

# **ПРИЛОЖЕНИЕ Б**

(обязательное)

Диаграмма классов

# **ПРИЛОЖЕНИЕ В**

(обязательное)

Схема алгоритма