Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ

РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

**Колледж информатики и программирования**

ДОПУСКАЮ К ЗАЩИТЕ

заместитель директора колледжа

по учебно-производственной работе

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Л.В. Фокина

« » июня 2019г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

На тему: Разработка программы шифрования файлов

Студент группы 4ПКС-115

Черников Алексей Владимирович « » июня 2019г.

Основная профессиональная образовательная программа по специальности

09.02.03 Программирование в компьютерных системах

Форма обучения очная

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Аксёнова Т.Г.

Председатель предметно-цикловой комиссии \_\_\_\_\_\_\_\_\_Пестов А.И.

Москва

2019

Федеральное государственное образовательное бюджетное

учреждение высшего образования

Финансовый университет при Правительстве Российской Федерации

**КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ**

УТВЕРЖДАЮ

Председателю ПЦК

Программирования и баз данных

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.И. Пестов

«\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г.

ЗАДАНИЕ

на выпускную квалификационную работу

|  |  |  |
| --- | --- | --- |
| Студенту Черникову Алексею Владимировичу | | |
| 1. Тема выпускной квалификационной работы: Разработка программы шифрования файлов. | | |
| 1. Срок сдачи студентом законченной выпускной квалификационной работы | | 07 июня 2019 года |
| 1. Исходные данные: | | |
| 3.1 Файлы, которые необходимо зашифровать или дешифровать. | | |
| 1. Перечень подлежащих разработке задач/вопросов | | |
| 4.1 Предпроектное исследование предметной области | | |
| 4.2 Сравнительный анализ и выбор алгоритмов шифрования | | |
| 4.3 Проектирование программы | | |
| 4.4 Разработка пользовательского интерфейса | | |
| 4.5 Кодирование алгоритмов | | |
| 4.6 Тестирование и отладка программы | | |
| 4.7 Составление руководств по использованию программы | | |
| 1. Перечень графического/иллюстративного /практического материала | | |
| 5.1 Схемы и диаграммы | | |
| 5.2 Программа шифрования файлов | | |
| 5.3 Презентация выпускной квалификационной работы | | |
| 1. Консультант по выпускной квалификационной работе (с указанием относящихся к ним разделов проекта) | | |
|  | | |
| Дата выдачи задания | «\_\_\_» \_\_\_\_\_\_\_\_\_\_2019 | |
| Руководитель ВКР Аксёнова Татьяна Геннадьевна | | |
|  | | |
| Задание принял к исполнению | «\_\_\_» \_\_\_\_\_\_\_\_\_\_2019 | |
| Студент Черников Алексей Владимирович | | |
|  | | |

Содержание

[Введение 5](#_Toc9607034)

[Глава 1 Теоретическая часть 7](#_Toc9607035)

[1.1 Предпроектное обследование 7](#_Toc9607036)

[1.2 Характеристика инструментальных средств разработки 17](#_Toc9607037)

[Глава 2 Практическая часть 22](#_Toc9607038)

[2.1 Постановка задачи 22](#_Toc9607039)

[2.2 Анализ требований и определение спецификаций программного обеспечения 23](#_Toc9607040)

[2.3 Проектирование программного обеспечения 24](#_Toc9607041)

[2.4 Разработка пользовательских интерфейсов 24](#_Toc9607042)

[2.5 Тестирование и отладка программного обеспечения 24](#_Toc9607043)

[2.6 Руководство по использованию программы 25](#_Toc9607044)

[Заключение 29](#_Toc9607045)

[Список литературы 30](#_Toc9607046)

[Приложение А 31](#_Toc9607047)

[Приложение Б 32](#_Toc9607048)

[Приложение В 33](#_Toc9607049)

# Введение

Проблема защиты информации путем её преобразования волновала человечество с давних времен. С распространением письменности появилась потребность в обмене письмами и сообщениями, что вызвало необходимость сокрытия их содержимого от посторонних. Так начала формироваться наука под названием криптография и именно поэтому её можно считать ровесницей истории человеческого языка.

Первые криптосистемы встречаются уже в начале нашей эры. В основном развитию криптографии способствовали войны. Письменные приказы и донесения обязательно шифровались, чтобы пленение курьеров не позволило противнику получить важную информацию. Так, древнеримский политический деятель и полководец Гай Юлий Цезарь в своих переписках активно использовал уже более-менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Почему проблема использования криптографических методов стала в настоящий момент особенно актуальна?

На сегодняшний день криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи. Что уж говорить про важность криптографии в глобальной сети «Интернет», по которой ежедневно передаются колоссальные объемы информации государственного, военного, коммерческого и частного характера, которая нуждается в защите от доступа к ней посторонних лиц.

Переоценить возможности криптографии для человечества сложно. С момента появления она прошла множество модификаций и сейчас представляет собой систему безопасности, которая практически не может быть взломана. Современные методы криптографии применяются практически во всех отраслях, в которых присутствует необходимость безопасной передачи или хранения данных.

Целью данной выпускной квалификационной работы является разработка программы шифрования файлов (и их дешифровки соответственно), которая позволила бы пользователю защитить желаемую информацию наиболее эффективными методами.

Для достижения поставленной цели необходимо выполнить ряд задач:

* детально изучить предметную область;
* провести сравнительный анализ и на его основе выбрать наиболее эффективные алгоритмы шифрования;
* разработать функциональные и нефункциональные требования к программе;
* составить необходимые диаграммы и схемы;
* выбрать подходящие для разработки инструментальные средства;
* реализовать функциональные и нефункциональные требования;
* провести тестирование и отладку программы;
* составить руководства по использованию программы.

Исходя из написанного выше можно сказать что объектом исследования будет являться – криптография, а предметом исследования – математические методы кодирования информации в современной криптографии.

# Теоретическая часть

## Предпроектное обследование

### Описание предметной области

Криптография – это наука, изучающая способы сокрытия данных и обеспечения их конфиденциальности. Это одна из старейших наук и ее история насчитывает четыре тысячелетия. Сам термин «криптография» образовался от двух древнегреческих слов «крипто» – скрытый, «графо» – пишу.

До 1975 года криптография представляла собой шифровальный метод с секретным ключом, который предоставлял доступ к расшифровке данных. Позже начался период ее современного развития и были разработаны методы криптографии с открытым ключом, которые может передаваться по открытым каналам связи и использоваться для проверки данных.

Современная прикладная криптография представляет собой науку, образованную на стыке математики и информатики. Смежной наукой криптографии считается криптоанализ. Криптография и криптоанализ тесно взаимосвязаны между собой, только в последнем случае изучаются способы расшифровки сокрытой информации.

С модификацией до открытого ключа криптография получила более широкое распространение и стала применяться частными лицами и коммерческими организациями, а в 2009 году на ее основе была выпущена первая криптовалюта Биткоин. До этого времени она считалась прерогативой государственных органов правления.

В основе криптографических систем лежат различные виды криптографии. Всего различаю четыре основных криптографических примитива:

* симметричное шифрование – данный метод предотвращает перехват данных третьими лицами и базируется на том, что отправитель и получатель данных имеет одинаковые ключи для разгадки шифра;
* асимметричное шифрование – в этом методе задействованы открытый и секретный ключ. Ключи взаимосвязаны – информация, зашифрованная открытым ключом, может быть раскрыта только связанным с ним секретным ключом. Применять для разгадки ключи из разных пар невозможно, поскольку они связаны между собой математической зависимостью;
* хэширование – метод основывается на преобразовании исходной информации в байты заданного образца. Преобразование информации называется хэш-функцией, а полученный результат хэш-кодом. Все хэш-коды имеют уникальную последовательность символов;
* электронная подпись – это преобразование информации с использованием закрытого ключа, позволяющее подтвердить подлинность документа и отсутствие искажений данных.

Изначально криптография использовалась правительством для безопасного хранения или передачи документов. Современные же асимметричные алгоритмы шифрования получили более широкое применение в сфере IT-безопасности, а симметричные методы сейчас применяются преимущественно для предотвращения несанкционированного доступа к информации во время хранения.

В частности, криптографические методы применяются для: безопасного хранения информации коммерческими и частными лицами, реализации систем цифровой электронной подписи, подтверждения подлинности сертификатов, защищенной передачи данных онлайн по открытым каналам связи.

### Изучение аналогов

На мировом рынке существует множество программ по шифрованию файлов самыми различными способами. При поиске информации о них мне удалось выделить такие программы как:

* Pretty Good Privacy (PGP) Desktop;
* Folder Lock.

Начнём с PGP Desktop. Она представляет собой комплекс программ для шифрования, обеспечивающий гибкое многоуровневое шифрование. От Folder Lock, которая будет описана позднее, она отличается тем, что имеет тесную интеграцию в системную оболочку, а доступ к её функциям осуществляется через контекстное меню проводника. Программа позволяет выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, которая предоставляется в электронном виде, а также шифровать информацию на съёмных носителях.

Шифрование PGP осуществляется последовательно: хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Такой подход позволяет достичь сильной защищённости информации.

К сожалению, PGP Desktop имеет низкую производительность и отсутствие поддержки русского языка.

Программа Folder Lock работает почти по тем же принципам. Заходя в программу сразу же хочется отметить простой и удобный интерфейс, который позволяет быстро начать работу. Используя эту программу можно:

* скрыть конфиденциальные данные в папках, на съёмных носителях и электронике;
* зашифровать конфиденциальные данные в папках, на съёмных носителях и электронике;
* устанавливать пароли;
* хранить важную информацию в «облаке» на сайте производителя;
* создавать виртуальные зашифрованные диски;
* шифрование сообщений электронной почты;
* полное удаление файлов без какой-либо возможности восстановления;
* другое.

Как видно, возможностей у программы предостаточно (особенно для персонального использования). Однако также, как и в PGP Desktop отсутствует поддержка русского языка, поэтому для пользователей не знакомых с английским, могут возникнуть некоторые сложности при работе.

Подводя итоги изучения аналогов можно сказать что в разрабатываемой программе должно в обязательном порядке присутствовать русский язык и разные алгоритмы шифрования файлов, при работе которых программа будет иметь высокую производительность.

### Описание методов шифрования и принципов их работы

#### Транспозиция

Первым методом шифрования рассмотрим транспозицию или как его по-другому называют – шифр перестановки. Он относится к симметричным криптосистемам перестановочного типа. Принцип работы этого метода заключается в том, что элементы открытого текста меняются местами. Элементами текста могут быть как отдельные символы, так и их пары, тройки и так далее, а также комбинирование этих случаев.

Классическая криптография делит шифры перестановки на два класса:

* шифры простой перестановки – когда при шифровании символы открытого текста перемещаются с исходных позиций на новые один раз;
* шифры сложной перестановки – когда при шифровании символы открытого текста перемещаются с исходных позиций на новые несколько раз.

В разрабатываемой программе применяется первый класс подобных шифров – простой.

Как правило, при шифровании и дешифровании текста используется таблица перестановок, для примера, возьмём такую (рисунок 1.1).



Рисунок 1.1 – Таблица перестановок

Первая строка – номера символов в открытом тексте, вторая строка – номера позиций, которые должны занимать символы в шифрограмме (или проще говоря – это наш ключ, который задаёт порядок перестановки символов открытого текста).

Соответственно, для того, чтобы зашифровать исходное сообщение нужно разбить его на блоки, равные длине ключа. Как говорилось выше, кодирование осуществляется перестановкой букв (символов). Таким образом первый символ должен быть переставлен на второе место, второй на четвёртое, третий на пятое, четвёртый на первое, пятый на третье.

Если с помощью таблицы на рисунке 1.1 зашифровать текст «пример маршрутной перестановки» получиться таблица, продемонстрированная на рисунке 1.2.

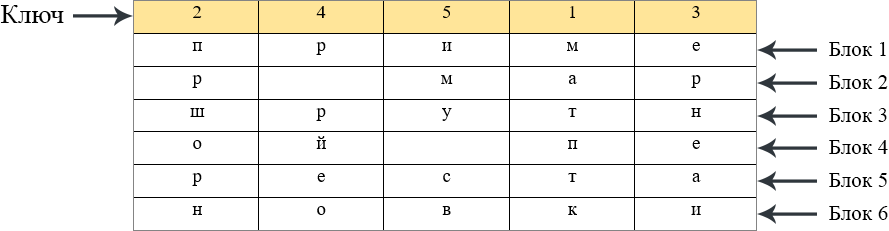


Рисунок 1.2 – Текст, зашифрованный методом транспозиции в табличном виде

В процессе шифрования символы текста переставляются в порядке, соответствующем заданному ключу по блокам (в данном примере по возрастанию) в результате чего получается следующая шифрограмма: «мпериарр мтшнрупоей траескниов».

Дешифрование производится в обратном порядке. На примере указанного ранее ключа: второй символ на первое, четвёртый на второе, третий на пятое и так далее.

Следует отметить, что при использовании любого блочного шифра могут возникать ситуации, когда текст не делиться на равные блоки. В таких случаях длину исходного текста увеличивают до тех пор, пока он не будет делиться на равные блоки длины заданного ключа.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования так как символы всего лишь переставляются на другие позиции.

Минусами этого метода можно считать сохранение частотных характеристик текста и малое количество возможных ключей шифрования, что делает его уязвимым к криптоатакам. Главным недостатком этого и других симметричных алгоритмов шифрования можно считать передачу ключа. Ведь для того, чтобы он не попал в чужие руки для его передачи требуется обеспечить дополнительную безопасность, его также требуется регулярно обновлять, а после его смены опять же возникает нужда в его безопасной передаче.

#### Моноалфавитный шифр

Следующий метод шифрования – моноалфавитный шифр или по-другому – шифр простой замены. Он относится к симметричным криптосистемам подстановочного типа. К этому типу относятся, наверное, самый известный шифр – шифр Цезаря, в котором каждый символ алфавита сдвигается на три позиции правее. Принцип работы подстановочных шифров сводится к созданию таблицы шифрования (по определённому алгоритму), в которой каждой букве открытого текста соответствует единственная сопоставимая ей буква шифротекста. Само же шифрование заключается в замене букв согласно созданной таблице. Как можно заметить, всё очень просто.

Отмечу также, что в шифрах замены не всегда подразумевается замена буквы на какую-то другую букву. Допускается использовать замену на число. Соответственно в создаваемой таблице каждой букве используемого алфавита приравнивается любое число.

В разрабатываемой программе используется вариант замены буквы на букву, поэтому рассмотрим принцип работы на основе шифра Цезаря.

Для упрощения воспользуемся русским алфавитом, состоящим только из заглавных букв. Следуя принципу работы описанному выше создадим таблицу шифрования, где каждая буква алфавита сдвигается на три позиции вправо. Из этого следует, что выбранный нами ключ равен числу три (рисунок 1.3).

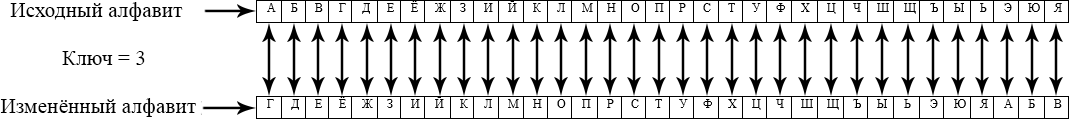


Рисунок 1.3 – Исходный алфавит и алфавит, сдвинутый на три позиции

Теперь, глядя на рисунок мы чётко видим, как будут взаимозаменяться буквы при шифровании и дешифровании текста. При шифровании буква «А» будет заменена на «Г», «Б» на «Д» и так далее, а при дешифровании обратно. Таким образом, зашифровав сообщение «ШИФР ЦЕЗАРЯ» мы получим «ЫЛЧУ ЩЗКГУВ».

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования.

Минусами этого метода можно считать то, что в шифротексте не скрывается частота появления символов открытого текста, что делает его уязвимым к криптоатакам и то, что максимальный количество ключей равно количеству букв в используемом алфавите. Также здесь имеется проблема передачи больших объёмов текста (чем больше текст, тем легче его взломать). Так как алгоритм относится к симметричным опять же требуется дополнительная безопасность при передаче ключа и его регулярное обновление.

#### Полиалфавитный шифр

Рассмотрим метод шифрования – полиалфавитный шифр или по-другому – многоалфавитный шифр.

Как и моноалфавитный шифр он относится к симметричным криптосистемам подстановочного типа принцип работы которых был описан ранее.

Суть работы полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к некоторому количеству букв открытого текста.

Рассмотрим, как это работает на примере. Для упрощения воспользуемся русским алфавитом, состоящим только из заглавных букв. Пусть в качестве ключа будет использоваться слово «КЛЮЧ». Это слово мы можем поделить на четыре отдельных моноалфавита в каждом из которых будет произведён сдвиг на количество символов равное номеру отдельной буквы ключевого слова в алфавите. Сделав это, мы получим следующие моноалфавиты (рисунок 1.4).

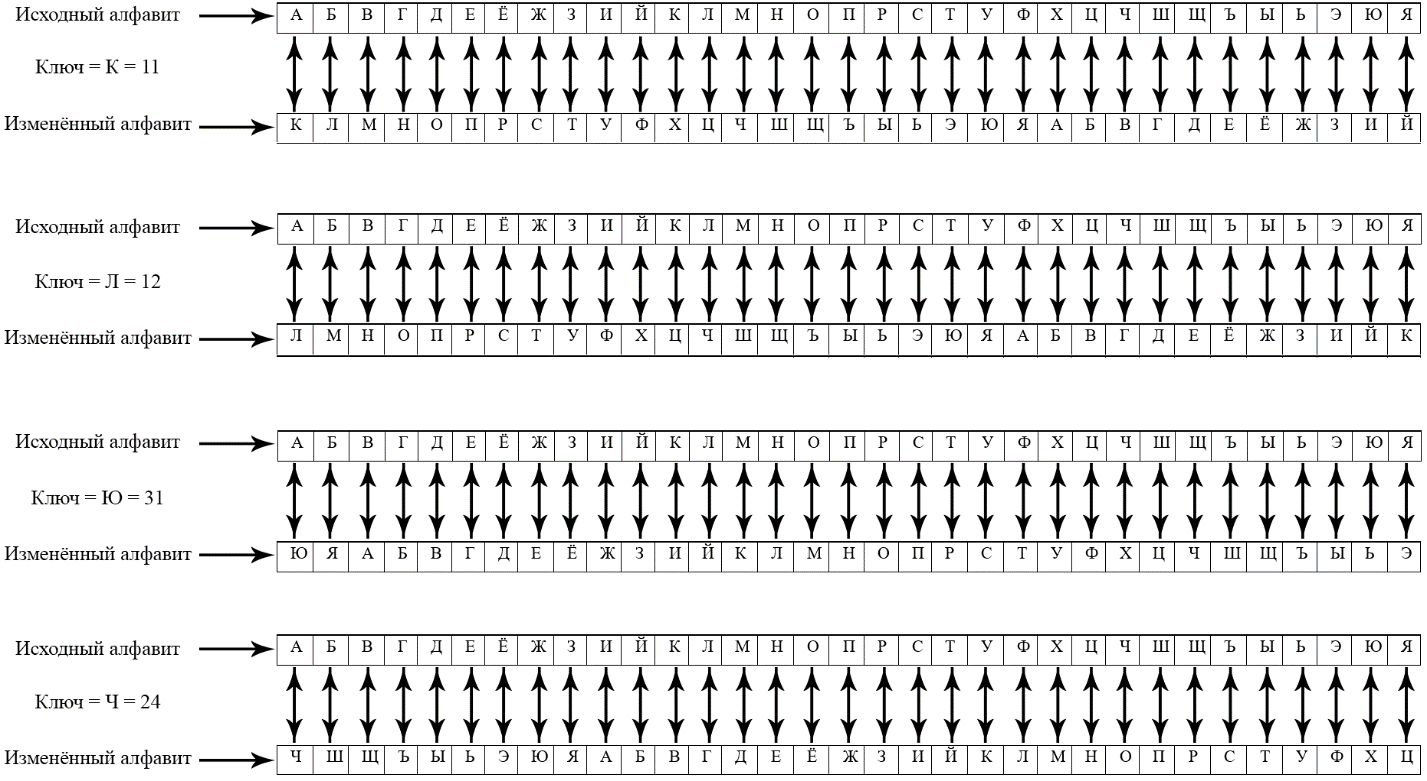


Рисунок 1.4 – Моноалфавиты полученные при использовании ключевого слова «КЛЮЧ»

Теперь, когда у нас алфавиты, изменённые под выбранный ключ можно приступить к шифрованию. Зашифруем сообщение «ПОЛИАЛФАВИТНЫЙ ШИФР». Для этого первую буква открытого текста будем шифровать через моноалфавит буквы «К», вторую через моноалфавит буквы «Л», третью через моноалфавит буквы «Ю», четвёртую через моноалфавит буквы «Ч». Для последующих букв требуется повторять цикл до тех пор, пока весь открытый текст не будет зашифрован. В результате шифрования мы получим «ЪЪЙАКЧТЧМФРЕЁХ ПУАО» (рисунок 1.5).

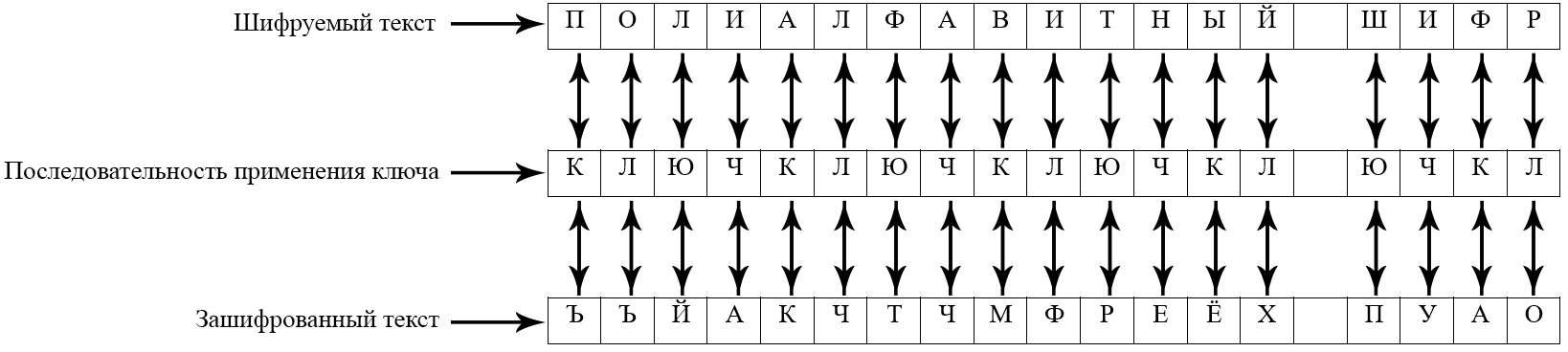


Рисунок 1.5 – Развёртка, как шифруется каждая буква открытого текста

Дешифрование соответственно происходит в обратном порядке.

Обычно, если текст хотят зашифровать или расшифровать этим методом используют таблицу под названием «квадрат Виженера» (рисунок 1.6).

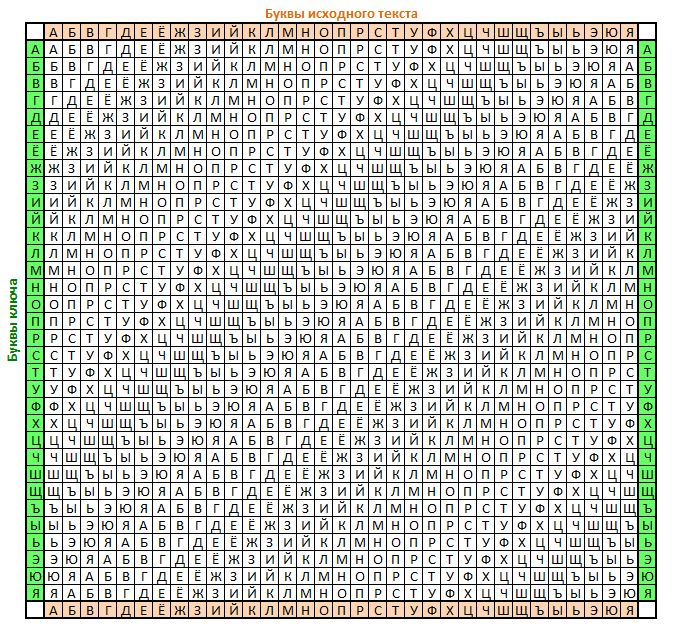


Рисунок 1.6 – Квадрат Виженера для русского алфавита

Пользоваться ей довольно просто, по вертикали выбирается буква ключа, по горизонтали буква текста, на их пересечении и будет шифруемая буква.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также маскировку частот появления тех или иных букв в тексте.

Минусами этого метода можно считать передачу больших объёмов текста, а также распространение ключей и их обновление.

#### Исключающее ИЛИ (XOR)

Метод исключающего ИЛИ (XOR) относится к симметричным криптосистемам типа гаммирование. Принцип работы этого типа шифров заключается в «наложении» последовательности, состоящей из случайных чисел на открытый текст. То есть генератор случайных чисел выдаёт последовательность битов (гамму), которая накладывается на открытый текст с помощью побитовой операции исключающего ИЛИ, в результате чего получается шифротекст.

Метод является достаточно простым. Давайте представим русский алфавит (для упрощения без буквы «Ё») в двоичном виде (таблица 1.1).

Таблица 1.1 – Русский алфавит в двоичном представлении

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Символ | Код | Символ | Код | Символ | Код | Символ | Код |
| А | 00000 | И | 01000 | Р | 10000 | Ш | 11000 |
| Б | 00001 | Й | 01001 | С | 10001 | Щ | 11001 |
| В | 00010 | К | 01010 | Т | 10010 | Ъ | 11010 |
| Г | 00011 | Л | 01011 | У | 10011 | Ы | 11011 |
| Д | 00100 | М | 01100 | Ф | 10100 | Ь | 11100 |
| Е | 00101 | Н | 01101 | Х | 10101 | Э | 11101 |
| Ж | 00110 | О | 01110 | Ц | 10110 | Ю | 11110 |
| З | 00111 | П | 01111 | Ч | 10111 | Я | 11111 |

Как мы знаем из булевой алгебры, операция логического сложения имеет следующую семантику (рисунок 1.7).

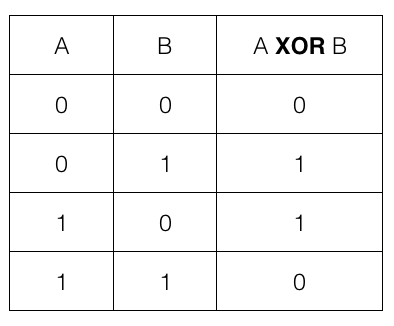


Рисунок 1.7 – Таблица истинности для операции исключающего ИЛИ (XOR)

Соответственно, если мы к примеру, захотим зашифровать букву «Х» (10101) используя в качестве ключа букву «У» (01011) результатом операции логического сложения будет буква «Ю» (11110). Для дешифровки нужно проделать те же самые действия, с тем же самым ключом, но уже над буквой «Ю». Отсюда вытекает свойство обратимости результата.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также его стойкость, определяющаяся гаммой (длительностью периода и равномерностью статических характеристик).

Минусами являются: распространение ключей и их обновление.

#### Одноразовый блокнот

Шифр Вернама или одноразовый блокнот – представляет собой систему симметричного шифрования типа гаммирование, так как использует булеву функцию «исключающее ИЛИ». Этот метод был изобретён в 1917 году Гилбертом Вернамом. При правильном использовании этого метода, текст, который был им зашифрован невозможно взломать. Этот метод является примером системы с абсолютной криптографической стойкостью при этом считаясь одной из простейших криптосистем.

Так как работает этот метод основываясь на XOR, алгоритм шифрования такой же, как был описан выше. Единственная разница в том, что длина ключа обязательно должна быть равна длине открытого текста.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также его абсолютную криптографическую стойкость при правильном использовании.

Минусами являются: существенный размер ключа, а также распространение ключей и их регулярное обновление (настолько регулярное, что ни один ключ не должен использоваться более одного раза).

#### Rivest, Shamir, Adleman (RSA)

Последний метод, который мы рассмотрим называется RSA (аббревиатура от фамилий его создателей Rivest, Shamir, Adleman). Он относится к асимметричным криптосистемам.

Эта криптосистема стала первой системой, пригодной как для шифрования, так и для цифровой подписи. Принцип её работы можно разделить на три шага: первый – создание открытого (публичного) и закрытого (секретного) ключей на основе взаимно простых чисел (тех, которые делятся только на единицу или сами на себя), второй шаг – шифрование сообщения и третий шаг – расшифровка.

Как же создать эти самые ключи? Для создания открытого ключа нужно: выбрать два простых числа, вычислить модуль их произведения, вычислить функцию Эйлера, выбрать открытую экспоненту, которая также будет являться простым числом, при этом будет меньше числа, полученного при вычислении функции Эйлера и наконец будет взаимно простым для этой функции. В результате этих манипуляций с формулами мы получим пару чисел, это и есть наш публичный ключ. Закрытый ключ создаётся вычислением обратной открытой экспоненты по модулю функции Эйлера, при этом модуль должен быть равен единице.

Теперь нужно отдать полученный открытый ключ человеку, который с помощью него планирует отправлять вам зашифрованные сообщения. Допустим, что, выполнив все предыдущие операции мы получили числа 5 и 21 – это публичный ключ и числа 17 и 21 – это секретный ключ. Теперь допустим, что вы хотите зашифровать букву «С», в русском алфавите она располагается на 19 позиции. Для того чтобы зашифровать эту букву нужно возвести позицию нашей буквы в 5 степень и от полученного числа взять остаток от деления на 21. В результате получиться число 10 или буква «И» это и будут наши закодированные данные.

Шифрованные данные передаются владельцу секретного ключа. Тут следует обратить внимание на то, что открытый ключ не может расшифровать сообщение, а закрытый находится только у владельца (если он никому его не говорил), так что передача может осуществляться по открытому каналу. Итак, чтобы дешифровать сообщение нужно провести те же действия, что и при шифровании сообщения только используя закрытый ключ. Возьмём нашу зашифрованную букву «И» расположенную на позиции 10, возведём её в 17 степень и от полученного числа возьмём остаток от деления на 21. Результатом вычислений будет число 19 или буква «С».

Подводя итоги, если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить у него открытый ключ, зашифровать своё сообщение и передать его владельцу. При этом расшифровать сообщение не может никто, кроме владельца секретного ключа. Весь этот процесс представлен на рисунке 1.8.

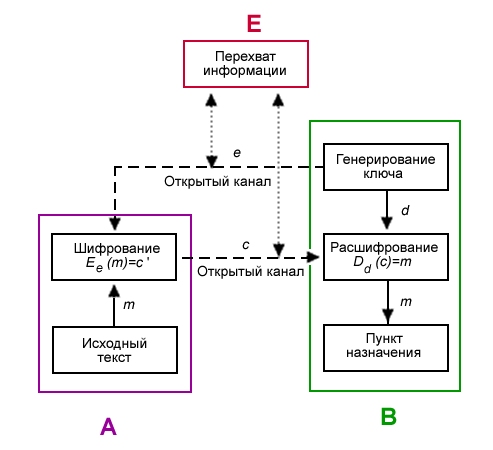


Рисунок 1.8 – Процесс шифрования при помощи алгоритмы RSA

Надёжность такого шифрования обеспечивается тем, что третьему лицу очень трудно вычислить закрытый ключ по открытому. Хотя ключи вычисляются из одной пары чисел и по сути связаны между собой, установить их связь очень сложно, а чем большие числа были взяты, тем длиннее становится процесс вскрытия.

Плюсами такого шифрования можно считать

Плюсами этого метода можно считать удобство распространения ключей и высокую безопасность при передаче небольших сообщений.

Минусами являются: существенный размер ключа, низкая скорость шифрования, а также то, что шифрование происходит по буквам, то есть одна и та же буква будет шифроваться одним и тем же числом, если злоумышленник перехватит достаточно большое сообщение расшифровать его не составит никакого труда.

## Характеристика инструментальных средств разработки

### Характеристика среды программирования

Для написания программы использовалась среда программирования Microsoft Visual Studio 2017, представляющая собой полный набор средств разработки для создания веб-приложений Active Server Pages (ASP), eXtensible Markup Language (XML), настольных приложений и мобильных приложений. Visual Studio использует единую интегрированную среду разработки Integrated Development Environment (IDE), которая позволяет совместно использовать средства и упрощает создание решений на базе нескольких языков. Кроме того, в этих языках используются функциональные возможности платформы .NET Framework, которая позволяет получить доступ к ключевым технологиям, упрощающим разработку веб-приложений ASP и XML.

Microsoft Visual Studio объединяет в себе огромное количество функций, позволяющих осуществлять разработки для Windows всех версий, Интернета, SharePoint, различных мобильных устройств и облачных технологий. В Visual Studio реализуется новая среда разработчика, благодаря которой создавать приложения стало проще.

### Описание системы Windows Presentation Foundation (WPF)

В качестве системы для построения клиентских приложений была выбрана WPF.

WPF – это платформа пользовательского интерфейса для создания клиентских приложений для настольных систем. Платформа разработки WPF поддерживает широкий набор компонентов для разработки приложений, включая модель приложения, ресурсы, элементы управления, графику, макет, привязки данных, документы и безопасность.

В основе WPF лежит независимый от разрешения векторный модуль визуализации, использующий возможности современного графического оборудования. Возможности этого модуля расширяются с помощью комплексного набора функций разработки приложений, которые включают в себя язык eXtensible Application Markup Language (XAML), элементы управления, привязку к данным, макет, двумерную и трехмерную графику, анимацию, стили, шаблоны, документы, мультимедиа, текст и типографические функции. WPF входит в состав .NET Framework, поэтому вы можете создавать приложения, включающие другие элементы библиотеки классов .NET Framework.

При разработке поведения приложения главной задачей является обеспечение реакции на действия пользователя, включая обработку событий (таких как выбор пункта меню или нажатие на кнопку), и вызов в ответ бизнес-логики и логики доступа к данным. В WPF такое поведение реализуется в коде, связанном с разметкой. Этот код называется кодом программной части.

Возможности взаимодействия с пользователем, обеспечиваемые моделью приложения, реализуются с помощью сконструированных элементов управления. В WPF элемент управления – это общий термин, который относится к категории классов WPF, размещаемых в окне или на странице, имеющих пользовательский интерфейс и реализующих некоторое поведение.

### Описание языка программирования

В качестве языка программирования был выбран язык С# версии 7.0. NET Framework 4.7.1.

**Язык C#** появился на свет в июне 2000 г., в результате кропотливой работы большой группы разработчиков компании Microsoft, возглавляемой Андерсом Хейлсбергом.

Создание инструментария для разработчиков с их полноценной поддержкой является одной из главных задач нового языка C#.

**Авторы C#** стремились создать язык, сочетающий простоту и выразительность современных объектно-ориентированных языков c богатством возможностей и мощью C++.

Особенности С#:

* полная поддержка классов и объектно-ориентированного программирования, включая наследование интерфейсов и реализаций, виртуальных функций и перегрузки операторов;
* полный и хорошо определенный набор основных типов;
* встроенная поддержка автоматической генерации XML-документации;
* возможность отметки классов и методов атрибутами, определяемыми пользователем. Это может быть полезно при документировании и способно воздействовать на процесс компиляции;
* автоматическое освобождение динамически распределенной памяти;
* полный доступ к библиотеке базовых классов .NET, а также легкий доступ к Windows Application Programming Interface;
* указатели и прямой доступ к памяти, если они необходимы. Однако язык разработан таким образом, что практически во всех случаях можно обойтись и без этого;
* поддержка свойств и событий в стиле Visual Basic;
* простое изменение ключей компиляции. Позволяет получать исполняемые файлы или библиотеки компонентов .NET, которые могут быть вызваны другим кодом так же, как элементы управления ActiveX;
* поддержка как Framework Class Library (FCL), так и Common Language Runtime (CLR);
* возможность использования С# для написания динамических web-страниц ASP.NET.

В настоящее время C# является одним из самых популярных языков программирования. Он применяется в разработке компьютерных, мобильных и веб-приложений. Также язык регулярно обновляется и имеет огромное количество документации, которая сильно упрощает и ускоряет процесс разработки программ на нём.

### Другие средства разработки

При разработке программы использовалось пространство имён System.Security.Cryptography.

System.Security.Cryptography предоставляет криптографические службы, включающие безопасное кодирование и декодирование данных, а также целый ряд других функций, таких как хэширование, генерация случайных чисел и проверка подлинности сообщений.

Для создания контекстной справки использовалась программа «Htm2chm». Она представляет собой [проприетарный](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D0%B5%D1%82%D0%B0%D1%80%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) [формат файлов](https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82_%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2) контекстной справки, разработанный корпорацией [Microsoft](https://ru.wikipedia.org/wiki/Microsoft" \o "Microsoft) и выпущенный в [1997 году](https://ru.wikipedia.org/wiki/1997_%D0%B3%D0%BE%D0%B4) в качестве замены формата [WinHelp](https://ru.wikipedia.org/wiki/WinHelp" \o "WinHelp). Содержит в себе набор HTML-страниц, может также включать в себя содержание со ссылками на страницы, предметный указатель, а также базу для [полнотекстового поиска](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BF%D0%BE%D0%B8%D1%81%D0%BA) по содержимому страниц.

Преимуществами программы можно считать:

* размер файла меньше, чем у обычного [HTML](https://ru.wikipedia.org/wiki/HTML);
* используются все возможности форматирования, имеющиеся в HTML и [CSS](https://ru.wikipedia.org/wiki/Cascading_Style_Sheets);
* возможность [полнотекстового поиска](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BF%D0%BE%D0%B8%D1%81%D0%BA);
* возможность просмотра множества .chm-файлов как один, с общим содержанием и предметным указателем.

Для построения схем и диаграмм при составлении технического задания и сопровождающей документации было решено использовать Draw.io. Draw.io – это сервис, предназначенный для формирования диаграмм и схем. Сервис разделён на три части – меню, панель объектов и сам документ.

С помощью веб-сервиса Draw.io можно создавать:

* диаграммы;
* UML-модели;
* вставка в диаграмму изображений;
* графики;
* блок-схемы;
* формы;
* другое.

Также доступен экспорт готовых схем в изображение и синхронизация полученных документов с Google Диском.

# Практическая часть

## Постановка задачи

### Описание входных данных

Описание входной информации включает в себя описание входных документов и/или входных данных задачи. Формы входных документов рекомендуется оформлять в виде приложения к пояснительной записке. Входных документов в задаче может не быть, например, при разработке компьютерных игр. В этом случае следует ограничиться описанием входных данных задачи. Описание входных данных рекомендуется оформлять в виде таблицы с полями: Наименование, Идентификатор, Тип данных, Размер.

### Описание выходных данных

Описание выходной информации включает в себя описание выходных документов и/или выходных данных задачи. Формы выходных документов рекомендуется оформлять в виде приложения к пояснительной записке. Выходных документов в задаче также может не быть, в этом случае следует ограничиться описанием выходных данных задачи. Описание выходных данных рекомендуется оформлять в виде таблицы с полями: Наименование, Идентификатор, Тип данных, Размер.

### Математическая модель задачи

Математическая модель задачи включается в пояснительную записку только для задач вычислительного типа и содержит все формулы и уравнения, используемые при написании программного кода, с подробным описанием коэффициентов, входящих в их состав.

### Требования к программному обеспечению

#### Функциональные требования

Что должна делать программа

#### Нефункциональные требования

Требования к интерфейсу, требования к реализации и требования к надежности. В требованиях к надежности необходимо указать способы защиты информации в программе

## Анализ требований и определение спецификаций программного обеспечения

содержит определенный набор моделей и диаграмм (в зависимости от используемого подхода к разработке ПО):

- функциональную диаграмму;

- диаграмму потоков данных;

- диаграмму «сущность-связь» (при наличии подключаемой к программе базы данных);

- модели данных;

- диаграмму вариантов использования;

- диаграмму классов и другие.

Перечисленные выше диаграммы и модели оформляются в виде рисунков и могут выноситься в приложения пояснительной записки.

### Диаграмма вариантов использования

### Диаграмма потоков данных

### Функциональная диаграмма

### Диаграмма классов

## Проектирование программного обеспечения

### Структурная схема

### Функциональная схема

## Разработка пользовательских интерфейсов

представляет собой скриншоты интерфейсов всех составных частей программы (подсистем) с отображением диалоговых окон, управляющих элементов и полей ввода информации.

## Тестирование и отладка программного обеспечения

содержит примеры ввода в программу как верных, так и ошибочных входных данных с указанием реакции программы. Реакцию программы необходимо оформлять в виде скриншотов. Тестовые данные рекомендуется оформлять в виде таблицы с полями: № операции, Входные данные, Вводимое значение, Реакция программы. Также данный подраздел должен содержать краткий анализ приведенных в таблице тестовых данных, а также выводы о соответствии работы программного средства функциональным и нефункциональным требованиям, заявленным в предпроектном обследовании.

## Руководство по использованию программы

### Руководство системного программиста

#### Общие сведения о программе

В пункте «Общие сведения о программе» должны быть указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих выполнение данной программы.

#### Структура программы

В пункте «Структура программы» должны быть приведены сведения о структуре программы, ее составных частях, о связях между составными частями и связях с другими программами.

#### Настройка программы

В пункте «Настройка программы» должно быть приведено описание действий по настройке программы на условия конкретного применения.

#### Проверка программы

В пункте «Проверка программы» должны быть приведено описание способов проверки, позволяющих дать общее заключение о работоспособности программы (контрольные примеры, методы прогона, результаты).

#### Дополнительные возможности

В пункте «Дополнительные возможности» должно быть приведено описание дополнительных разделов функциональных возможностей программы и способов их выбора.

#### Сообщения системному программисту

В пункте «Сообщения системному программисту» должны быть указаны тексты сообщений, выдаваемых в ходе выполнения настройки, проверки программы, а также в ходе выполнения программы, описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

### Руководство программиста

#### Назначение и условия применения программы

В пункте «Назначение и условия применения программы» должны быть указаны назначение и функции, выполняемые программой, условия, необходимые для выполнения программы (системные требования).

#### Характеристики программы

В пункте «Характеристики программы» должно быть приведено описание основных характеристик и особенностей программы.

#### Обращение к программе

В пункте «Обращение к программе» должно быть приведено описание процедур вызова программы.

#### Входные и выходные данные

В пункте «Входные и выходные данные» должно быть приведено описание организации, используемой входной и выходной информации.

#### Сообщения

В пункте «Сообщения» должны быть указаны тексты сообщений, выдаваемых программисту или пользователю в ходе выполнения программы, описание их содержания и действия, которые необходимо предпринять по этим сообщениям.

### Руководство пользователя

#### Назначение программы

В пункте «Назначение программы» должны быть указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации.

#### Условия выполнения программы

В пункте «Условия выполнения программ» должны быть указаны условия, необходимые для выполнения программы (системные требования).

#### Выполнение программы

В пункте «Выполнение программы» должна быть указана последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, должно быть приведено описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы, а также описание реакции программы.

#### Сообщения пользователю

В пункте «Сообщения пользователю» должны быть приведены тексты сообщений, выдаваемых в ходе выполнения программы, описание их содержания и соответствующие действия пользователя.

# Заключение

//заключение

# Список литературы

//список литературы в алфавитном порядке

# Приложение А

# Приложение Б

# Приложение В