МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра защиты информации



**РАСЧЕТНО-ГРАФИЧЕСКАЯ РАБОТА**

Разработка криптографического программного обеспечения «Шифровка и дешифровка текста».

**по дисциплине:** «Программирование»

Выполнили:Проверил:

Студенты гр. АБ-121, АВТФ доцент каф. ЗИ

Вобликов В.Е., Втюрин А.Р.Архипова А. Б.

«\_\_» \_\_\_\_\_\_\_\_\_ 2022 г.«\_\_\_» \_\_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

(подпись)

Новосибирск 2022

Оглавление

[**ВВЕДЕНИЕ** 3](#_Toc106436333)

[**1.ТЕОРЕТИЧЕСКАЯ ЧАСТЬ** 4](#_Toc106436334)

[**1.1 Алгоритм работы RSA** 4](#_Toc106436335)

[**1.2 Шифр Виженера** 6](#_Toc106436336)

[**1.3 Алгоритм работы шифрующей таблицы Трисемуса** 9](#_Toc106436337)

[**1.4 Алгоритм работы шифра Гронсфельда** 11](#_Toc106436338)

[**1.5 Алгорим работы шифра Вернама** 13](#_Toc106436339)

[**1.6 Алгоритм работы Тарабарской грамоты** 15](#_Toc106436340)

[**2. ПРАКТИЧЕСКАЯ ЧАСТЬ** 16](#_Toc106436341)

[**2.1. Постановка задачи** 16](#_Toc106436342)

[**2.2. Характеристика задачи** 16](#_Toc106436343)

[**2.4 Руководство пользователя** 17](#_Toc106436344)

[**2.4.1 Введение** 17](#_Toc106436345)

[**2.4.2 Описание операций** 17](#_Toc106436346)

[**2.4.3 Сообщения пользователю** 19](#_Toc106436347)

[**2.5 Руководство системного программиста** 20](#_Toc106436348)

[**2.6 Контрольный пример** 22](#_Toc106436349)

[**СИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ** 29](#_Toc106436350)

# **ВВЕДЕНИЕ**

Несомненно, шифрование текста является главным союзником при преобразовании обычного текста в нечитаемый секретный формат. Шифрование несет в себе как конфиденциальность сообщения, так и дает сто процентную вероятность неизменности данных во время передачи различного рода сообщений. Данные привилегии могут быть получены при помощи любого метода шифровки. Различного рода механизмы шифрования информациивсе время совершенствуются, для того, чтобы не случалось утечек секретной информации, в результате чего тема шифрования становится все более актуальной.

**Целью работы** является разработка криптографического программного обеспечения «Шифровка и дешифровка текста».

**Для реализации** поставленной цели необходимо решить ряд задач:

-изучить методику шифрования и дешифрования текста путем шифра Трисемуса, RSA, шифра Виженера, шифра Гронсфельда, шифра Вермана, Тарабарской грамоты.

-проанализировать теоретическую информацию и алгоритм шифрованиятекста.

# **1.ТЕОРЕТИЧЕСКАЯ ЧАСТЬ**

В программе используется 6 методов шифрования: RSA, шифр Виженера, шифр Трисемуса, Шифрующие таблицы Трисемуса, шифр Гронсфельда, шифр Вернама, Тарабарская Грамота.

## **1.1 Алгоритм работы RSA**

Идея асимметричной криптосистемы с открытым и закрытым ключом приписывается Уитфилду Диффи и Мартину Хеллману, которые опубликовали эту концепцию в 1976 году. Они также ввели цифровые подписи и попытались применить теорию чисел. В их формулировке использовался секретный ключ с общим доступом, созданный путем экспоненциализации некоторого числа по модулю простого числа. Однако они оставили открытой проблему реализации односторонней функции, возможно, потому что сложность факторизации в то время не была хорошо изучена.

Рон Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института в течение года предприняли несколько попыток создать одностороннюю функцию, которую было бы трудно инвертировать. Ривест и Шамир, будучи компьютерными учеными, предложили множество потенциальных функций, а Адлеман, будучи математиком, отвечал за поиск их слабых мест. Они опробовали множество подходов, включая "ранцевый" и "перестановочные полиномы". Какое-то время они думали, что то, чего они хотели достичь, невозможно из-за противоречивых требований. В апреле 1977 года они провели Песах в доме одного из студентов и выпили много манишевицкого вина, а затем вернулись к себе домой около полуночи. Ривест, не в силах заснуть, лег на диван с учебником математики и начал думать о своей односторонней функции. Остаток ночи он провел, формализуя свою идею, и к рассвету большая часть статьи была готова. Алгоритм теперь известен как RSA - инициалы их фамилий в том же порядке, что и в их статье.

Для генерации двух ключей используется два больших случайных простых числа, p и q. Для максимальной безопасности выбирайте p и q равной длинны.

n = p q

Затем случайным образом выбирается ключ шифрования e, такой что e и (p-1) (q-1) является взаимно простыми числами. Наконец расширенный алгоритм Эвклида используется для вычисления ключа дешифрования d, такой что

ed = 1 (mod (p-1)(q-1))

или

d = e-1 mod ((p-1)(q-1))

d и n взаимно простые числа. e и n – открытые ключи, d – закрытый ключ

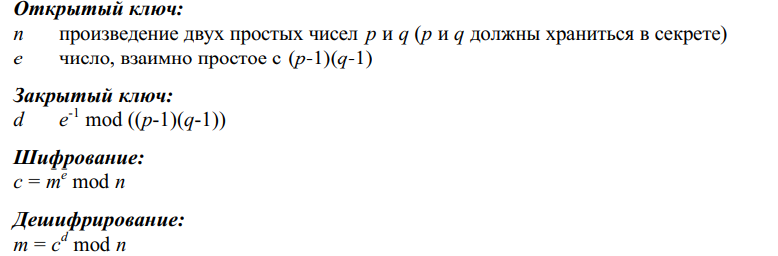
Для шифровки используется формула:

ci =mie mod n

Для дешифровки сообщения применяется формула:

mi = cid mod n

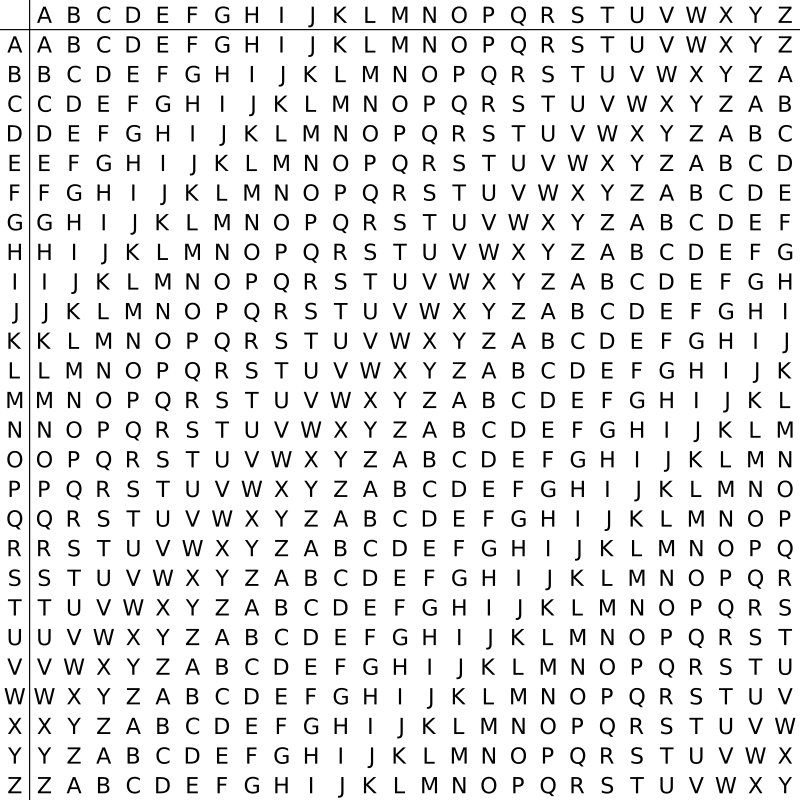
Так как

cid  mod n (mie)d mod n = mied mod n = mik(p-1)(q-1)+1 mod n = mi mik(p-1)(q-1) mod n

## **1.2 Шифр Виженера**

Первое его описание можно найти еще в XVI веке в «Трактате о шифрах» Леона Баттиста Альберти, более известного тем, что он впервые изложил математические основы перспективы в живописи. Идея была довольно простой, однако все равно означала выход криптографии на новый уровень — полиалфавитные шифры.

Полиалфавитный шифр использует множество разных алфавитов подстановки циклически. На примере шифра Виженера это выглядит следующим образом: берем за основу шифр Цезаря и составляем таблицу, содержащую все возможные смещения:



В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Человек, посылающий сообщение, записывает ключевое слово циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

Шифровка производится посредствам сопоставления буквы исходного текста с буквой ключ слова. Зашифрованный символ находится на пересечении столбца с номером буквы исходного текста и строки с номером буквы ключ слова

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если {\displaystyle n}количество букв в алфавите, {\displaystyle m\_{j}}номер буквы открытого текста, {\displaystyle k\_{j}}номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:

cj = (mj + kj) mod n{\displaystyle c\_{j}=(m\_{j}+k\_{j})\mod {n}}

И расшифровывание:

mj = (cj – kj) mod n{\displaystyle m\_{j}=(c\_{j}-k\_{j})\mod {n}}

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание.

## **1.3 Алгоритм работы шифрующей таблицы Трисемуса**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже неё в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самая верхнюю букву из того же столбца**.**

***Задача 9****.* Зашифровать таблицей Трисемуса сообщение:

Вылетаем пятого

Решение. Для русского алфавита шифрующая таблица может иметь размер 4×8. Выберем ключевое слово**БАНДЕРОЛЬ**. Заполним шифрующую таблицу. Построчно записываются буквы ключевого слова, затем оставшиеся буквы алфавита, которых нет в ключевом слове. Шифрующая таблица выглядит так:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Б | А | Н | Д | Е | Р | О | Л |
| Ь | В | Г | Ж | З | И | Й | К |
| М | П | С | Т | У | Ф | Х | Ц |
| Ч | Ш | Щ | Ъ | Ы | Э | Ю | Я |

Рисунок 5 - Шифрующая таблица Трисемуса с ключевым словом **БАНДЕРОЛЬ**

Используя эту таблицу, получим шифртекст: букве **В** исходного текста соответствует буква **П** шифртекста, стоящая в шифрующей таблице Трисемуса на одну позицию ниже в том же столбце. Букве **Ы** соответствует буква **Е**– самая верхняя в данном столбце, т. к. **Ы**– самая нижняя в этом же столбце. По этому принципу зашифруем оставшиеся буквы исходного текста и получим:

Пекзъвзчшлъйсй.

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются *биграммными.*

**1.4 Алгоритм работы шифра Гронсфельда**  
  
Шифр Гронсфельда -  
Длина ключа (K) должна быть равной длине исходного текста. Для этого циклически записывают ключ до тех пор, пока его длина не будет соответствовать длине исходного текста.  
полиалфавитный подстановочный шифр создан графом Гронсвельдом (руководителем первой дешифровальной службы Германии) в XVII веке.  
  
Генерация ключей:  
Вводится ключ с клавиатуры  
Шифрование/дешифрование  
Каждый символ Mi открытого текста M нужно на Ki (соответствующий символ ключа K) шагов сдвинуть вправо.  
Или пользуясь таблицей Гронсфельда (Tx y, где x — номер строки, а y — номер столбца и отсчет ведется с нуля):

Каждый символ Ci шифротекста C находится на пересечении столбца y, первый (заголовочный) символ которого равен соответствующему символу открытого текста Mi, и Ki-й (соответствующей цифры ключа) строки — (TKi y) Каждый символ (Ci) зашифрованного текста C нужно на Ki (соответствующий символ ключа K) шагов сдвинуть влево.

Или пользуясь таблицей Гронсфельда (Tx y, где x — номер строки, а y — номер столбца и отсчет ведется с нуля):  
нужно в Ki (i-ая цифра ключа K) строке найти символ, который равен соответствующему символу шифротекста (TKi y = Ci), и первый (заголовочный) элемент столбца будет i-ый символ открытого текста. Допустим, мы хотим зашифровать слово «ТАЙНЫ», используя ключ «103». Записываем циклически под словом ТАЙНЫ наш ключ, после чего сдвигаем по алфавиту каждую букву на столько букв вперед, сколько указано ниже, получим:  
Т А Й Н А  
1 0 3 1 0  
У А М О А  
Соответственно для дешифровки, сдвиг по алфавиту происходит в обратную сторону.

## **1.5 Алгорим работы шифра Вернама**

Шифр Вернама представляет собой шифр, который зашифровывается с помощью ключа. Ключ k должен быть той же длины что и передаваемое сообщение m. Зашифровка действует таким образом: m1 ⊕ k1, m2 ⊕ k2, …, mi ⊕ ki .

⊕ - эта операция называется XOR.

Такое шифрование является надёжным, так как из текста m можно получить подходящий ключом любой другой текст той же самой длины.

Дешифрование текста происходит таким же образом что и шифрование.

Например:

Шифрованный текст = mi ⊕ ki, i=1,2,…, идёт до длины сообщения.

Расшифрованный текст = (шифрованный текст)i ⊕ ki , i=1,2,…, идёт до длины сообщения.

Распишем mi ⊕ ki, i=1,2,…, идёт до длины сообщения.:

mi ⊕ ki = mi + ki (mod n) , i=1,2,…, идёт до длины сообщения.

Как мы уже говорили, данный шифр является довольно надёжным, но у него есть недостатки. Проблемой является передача последовательности ключа и сохранение её в тайне. Если существует надёжно защищённый от перехвата канал передачи сообщений, шифры вообще не нужны: секретный сообщение можно передавать по этому каналу. Если же передавать ключ с помощью другого шифра, то шифр Вернама окажется защищённым ровно настолько, насколько защищён другой шифр. Поскольку длина ключа та же, что и длина сообщения, передать его не проще, чем сообщение.

Проведем ручную шифровку

Текст: Тайна

Ключ: RPH^G

Т ⊕ R=А

а ⊕ P=р

й ⊕ H=б

н ⊕ ^=у

а ⊕ G=з

Полученное зашифрованное сообщение Арбуз

**1.6 Алгоритм работы Тарабарской грамоты**  
Тарабарская грамота (простая литорея) - древнерусский шифр, в частности, применявшийся в рукописях, а также дипломатами.

Суть тарабарской грамоты довольно прост. Нам всего лишь нужно иметь при себе такую таблицу:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| б | в | г | д | ж | з | к | л | м | н |
| щ | ш | ч | ц | х | ф | т | с | р | п |

Алгоритм:

Символ сообщения ищется в таблице.

Ищется пара этого символа. Пара этого символа в другой строке, но в том же столбце, то есть пара символа б будет символ щ, а пара символа ш будет символ в.

Затем как мы определили пару для символа, мы просто заменяем символ на его пару.

Если мы не нашли пару для символа, то он остаётся таким же.

Например:

Есть слово АЗБУКА.

Зашифрованный текст будет: АФЩУТА.

У данного шифра есть минусы. Он не заменяет гласные и пробелы.

Так как он не заменяет пробелы легко, то можно узнать сколько слов в тексте.

И так как он не заменяет гласные, то нам не подойдут слова у которых гласных букв больше чем согласных, так как эти слова очень легко отгадать. Например:

АУЦИКОМИЯ – АУДИТОРИЯ.

ЛОЕЦИПЕПИЕ – СОЕДИНЕНИЕ.

Если в шифрованном тексте много таких слов, то при вскрытии вручную можно легко понять, что гласные не заменяются, а затем раскрыть, как заменяются согласные.

# **2. ПРАКТИЧЕСКАЯ ЧАСТЬ**

## **2.1. Постановка задачи**

Необходимо разработать программу, которая должна шифровать и дешифровать текст. Программа должна выполнять следующие основные действия:

- ввод исходного текста и запись его в файл;

- шифровка, то есть кодировка, текста из указанного файла; перед кодировкой пользователь вводит пароль;

- дешифровка текста из указанного файла; перед дешифровкой пользователь должен ввести пароль;

- печать файла на экране.

## **2.2. Характеристика задачи**

1. Программа RGRпредназначена для автоматизации процесса шифрования текста и защиты паролем от использования алгоритмов сторонними лицами.

2. Программа используется пользователем для защиты персональной информации.

3Периодичность решения задачи по запросу пользователя.

4 Прекращение автоматизированного решения задачи происходит при отключении источника электропитания ЭВМ.

5 Связь с другими задачами отсутствует.

6 Специальных ограничений на временные характеристики решения задачи не налагается

7 Специальных требований на уровень подготовки пользователя не налагается. Но лицо, работающее с программой, должно иметь минимальное представление о компьютере (знание необходимых операций)

## **2.4 Руководство пользователя**

### **2.4.1 Введение**

#### 2.4.1.1 Программа «RGR\_AB-121\_Vtyurin-A.\_Voblikov-V.» предназначена для шифровки\дешифровки английских текстов.

#### 2.4.1.2 Программа представляет пользователю следующие возможности:

- Возможность ручного ввода текста для шифровки\дешифровки.

- Возможность автоматической генерации текста для шифровки.

- Возможность считывания текста из файла.

- Возможность автоматической генерации ключа шифрования.

- Возможность ручного ввода ключа шифрования.

- Возможность записи шифрованного\дешифрованного текста в файл.

#### 2.4.1.3 Программа реализована на языке программирования C++. Работает в любой среде совместимой с «Windows 10». Дисковой памяти для запуска требуется не менее 2 Gb. Оперативной памяти для нормальной работы программы требуется не менее 2 Mb.

### **2.4.2 Описание операций**

Основные функции программы «RGR\_AB-121\_Vtyurin-A.\_Voblikov-V.» соответствуют . Для удобства пользователя и более легкого изучения системы большинство форм и диалогов имеют идентичный интерфейс. Далее описаны все функции системы, а также формы и диалоги для ввода и вывода информации. Для каждой формы приведены основные компоненты и их назначение.

После входа в систему на экран выводится главное окно программы. Вид окна приведен на рисунке 2.1. Для начала работы с программой необходимо ввести правильный пароль (в данном случае «1111»)

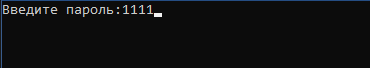


Рисунок 2.1.1 – Главное окно программы

В случае неверного ввода пароля (рисунок 2.1.2):

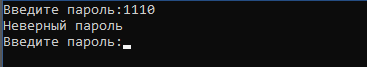


Рисунок 2.1.2 – Главное окно программы, неверный пароль

Далее программа предлагает пользователю на выбор один из трёх вариантов ввода текста (рисунок 2.2):

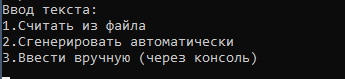


Рисунок 2.2 – Вывод меню ввода текста

После выбора варианта ввода текста программа предлагает пользователю выбрать вариант шифровки\дешифровки текста (рисунок 2.3):

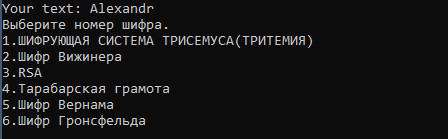


Рисунок 2.3 – Вывод меню выбора варианта шифровки\дешифровки

После выбора метода шифровки\дешифровки (рисунок 2.3) программа предлагает выбрать пользователю выбрать: хочет он зашифровать или расшифровать текст (рисунок 2.4):



Рисунок 2.4 – Вывод меню выбора шифровка\дешифровка

Далее программа предлагает выбрать пользователю сгенерировать ключ автоматически или ввести его вручную (для всех шифров, кроме RSA) (рисунок 2.5):



Рисунок 2.5 – Вывод меню варианта генерации ключа

В конце программа выводит шифрованный\дешифрованный текст в файл в папке с проектом (рисунок 2.6):



Рисунок 2.6 – Вывод шифрованного\дешифрованного текста

### **2.4.3 Сообщения пользователю**

При работе с программой могут появиться следующие сообщения, представленные в таблице 2.1.

Таблица 2.1 – Сообщения пользователю

|  |  |
| --- | --- |
| Текст сообщения программы | Ответ пользователя |
| Неверный пароль | Введён неверный пароль |
| Некорректный выбор | Введён неверный номер шифра |
| Ошибка. Кол - во символов в слове не совпадает с кол-вом символов в ключе. | Введён неверный ключ для шифра Вернама |
| Вы можете написать либо 1, либо 2 | Введён неверный номер для выбора шифровка\дешифровка /Введён неверный номер для выбора варианта генерации ключа |

## **2.5 Руководство системного программиста**

Программа реализована на языке C++ в среде Eclipse, основанном на визуальном построении приложений (помещение компонентов на формы и изменение их свойств и методов), поэтому некоторые функции формирования окон и отчетов невозможно описать в списке функций и листинге программы.

Модули программы:

shifri.h – заголовочный файл, содержит объявления всех функций и библиотек, использованных в данной программе;

gronsfeld\_NEW\_voblikov.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

void gronsf(string s) - шифровка текста при помощи шифра Гронсфельда

rsa.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

void rsa(string s) – шифровка текста при помощи RSA

trisem.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

int trit(string s) – Шифровка текста при помощи шифра Трисемуса

vizh.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

void vizh(string s) - шифровка текста при помощи шифра Виженера

voblikov\_tarabar\_gramota.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

void tarab() - шифровка текста при помощи Тарабарской Грамоты

voblikov\_vernam.cpp – файл содержит определение функций, объявленных в заголовочном файле shifri.h

void vern(string s) - шифровка текста при помощи шифра Вернама

Main.cpp - содержит функцию main, представляющую функционал по вводу пароля, выводу меню выбора шифров, с соответствующим вызовом функций.

Программа содержит ряд сообщений, предназначенных для сигнализации ошибок:

1. «Неверный пароль» - введён неверный пароль; программа не выдаст меню выбора алгоритмов шифрования и даст повторно ввести пароль.
2. «Некорректный выбор» - введён неверный номер шифра; программа не вызовет шифр и попросит повторно ввести номер шифра.
3. «Ошибка. Кол - во символов в слове не совпадает с кол-вом символов в ключе.» - Введён неверный ключ для шифра Вернама.
4. «Вы можете написать либо 1, либо 2» - Введён неверный номер для выбора шифровка\дешифровка /Введён неверный номер для выбора варианта генерации ключа.

Связь модулей программы между собой представлена на рисунке 2.7.

gronsfeld\_NEW\_voblikov.cpp

Main.cpp

voblikov\_vernam.cpp

voblikov\_tarabar\_gramota.cpp

rsa.cpp

vizh.cpp

trisem.cpp

Рисунок 2.7 – Связь модулей программы

### **2.6 Контрольный пример**

После входа в систему на экран выводится главное окно программы. Вид окна приведен на рисунке 2.8.1. Для начала работы с программой необходимо ввести правильный пароль (в данном случае «1111»)

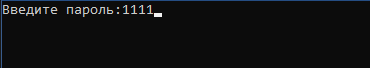


Рисунок 2.8.1 – Главное окно программы

В случае неверного ввода пароля (рисунок 2.8.2):

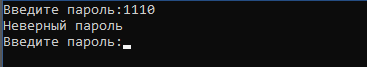


Рисунок 2.8.2 – Главное окно программы, неверный пароль

Далее программа предлагает пользователю на выбор один из трёх вариантов ввода текста (рисунок 2.9):

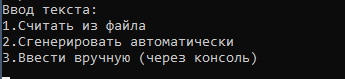


Рисунок 2.9 – Вывод меню ввода текста

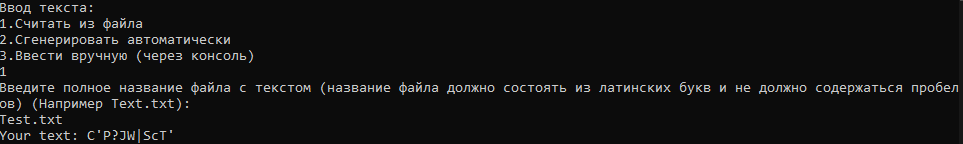


Рисунок 2.9.1 – Ввод текста из файла

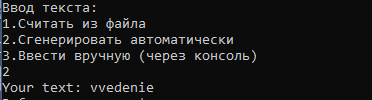


Рисунок 2.9.2 – Случайная генерация текста

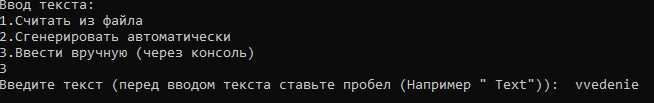


Рисунок 2.9.3 – Ввод текста через консоль

После выбора варианта ввода текста программа предлагает пользователю выбрать вариант шифровки\дешифровки текста (рисунок 2.10):

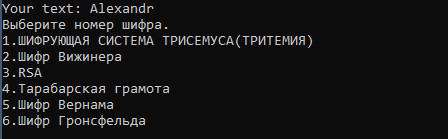
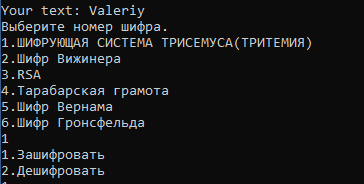
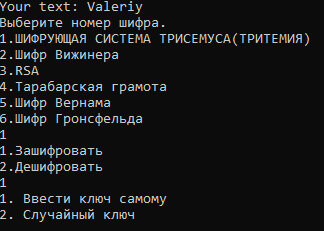
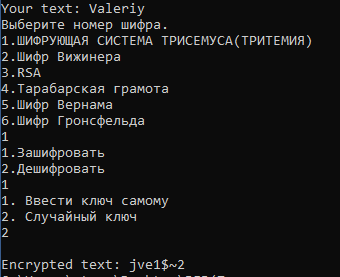
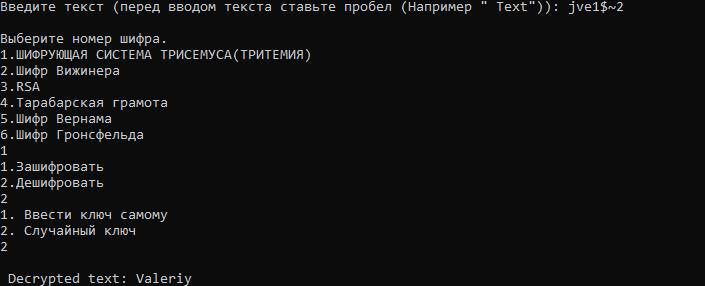


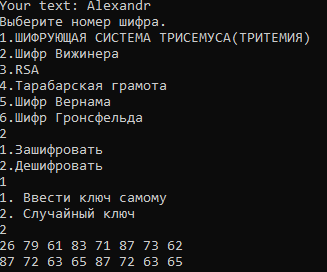
Рисунок 2.10 – Вывод меню выбора варианта шифровки\дешифровки



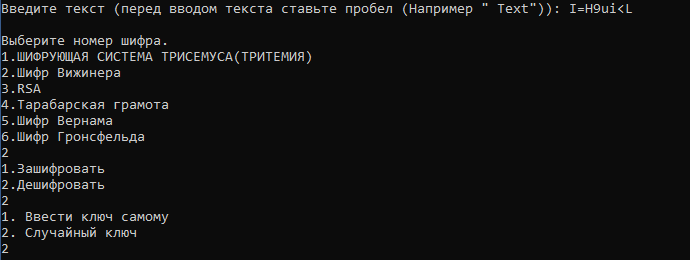




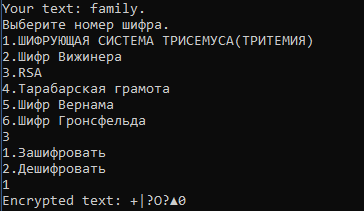


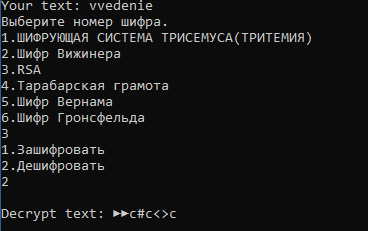


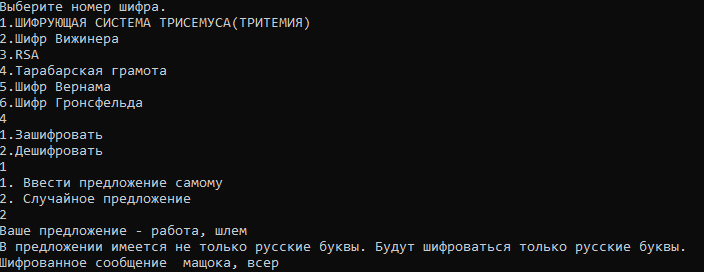


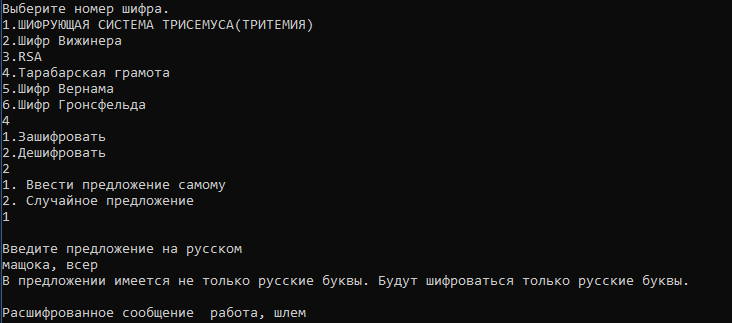


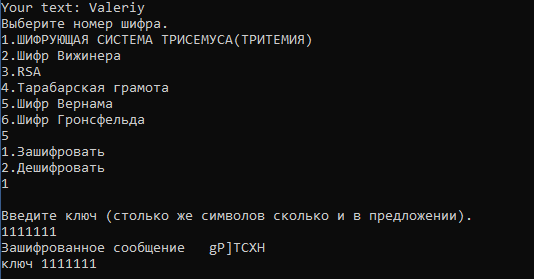


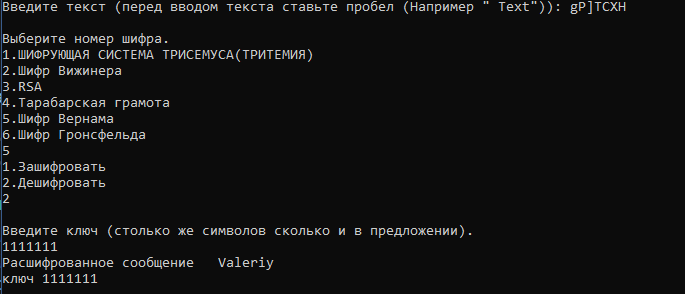


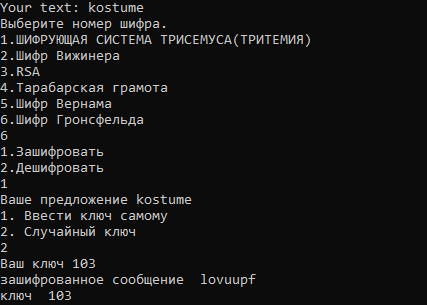


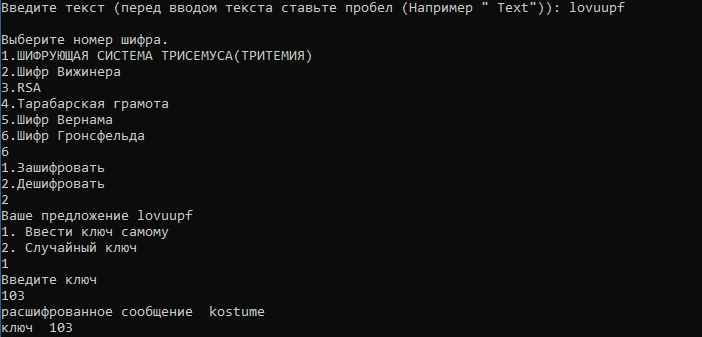












# **СИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. Прикладная криптография : Протоколы, алгоритмы, исход. тексты на яз. Си / Б. Шнайер. - М. : Триумф, 2002. - 815 с. : ил.; 24 см. - (Знания и опыт экспертов).; ISBN 5-89392-055-4
2. Кpиптогpафия с откpытым ключом: Пеp. с англ. — М.: Миp, 1995. — 318 с., ил. ISBN 5–03–001991–X
3. Введение в криптографию. Курс лекций / В.А. Романьков. М. : ФОРУМ, 2012. - 240 с. - (Высшее образование). ISBN 978-5-91134-573-0
4. *Романьков В.А* Введение в криптографию: курс лекций, 2009. — 238 с. — [ISBN 5777909825](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/5777909825).
5. Окулов С.М. Основы программирования [Электронный ресурс]/ Окулов С.М.— Электрон. текстовые данные.— Москва: Лаборатория знаний, 2020.— 337 c.— Режим доступа: http://www.iprbookshop.ru/6449.html.— ЭБС «IPRbooks» (дата обращения 20.05.20222 г.).
6. https://docs.yandex.ru/docs/view?tm=1654950142&tld=ru&lang=ru&name=Lec-04.pdf&text=%D0%9F%D0%B0%D0%BD%D1%84%D0%B8%D0%BB%D0%BE%D0%B2%20%D0%AD.%D0%9A.%20%C2%AB%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%C2%BB.%20%D0%92%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B2%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8E&url=http%3A%2F%2Fvoloshin-sb.ru%2FPortals%2F16%2Fdoc%2FLec-04.pdf&lr=65&mime=pdf&l10n=ru&sign=c3a359d6fa4b7a411b94ab296583f4a9&keyno=0&nosw=1&serpParams=tm%3D1654950142%26tld%3Dru%26lang%3Dru%26name%3DLec-04.pdf%26text%3D%25D0%259F%25D0%25B0%25D0%25BD%25D1%2584%25D0%25B8%25D0%25BB%25D0%25BE%25D0%25B2%2B%25D0%25AD.%25D0%259A.%2B%25C2%25AB%25D0%259A%25D1%2580%25D0%25B8%25D0%25BF%25D1%2582%25D0%25BE%25D0%25B3%25D1%2580%25D0%25B0%25D1%2584%25D0%25B8%25D1%258F%25C2%25BB.%2B%25D0%2592%25D0%25B2%25D0%25B5%25D0%25B4%25D0%25B5%25D0%25BD%25D0%25B8%25D0%25B5%2B%25D0%25B2%2B%25D0%25BA%25D1%2580%25D0%25B8%25D0%25BF%25D1%2582%25D0%25BE%25D0%25B3%25D1%2580%25D0%25B0%25D1%2584%25D0%25B8%25D1%258E%26url%3Dhttp%253A%2F%2Fvoloshin-sb.ru%2FPortals%2F16%2Fdoc%2FLec-04.pdf%26lr%3D65%26mime%3Dpdf%26l10n%3Dru%26sign%3Dc3a359d6fa4b7a411b94ab296583f4a9%26keyno%3D0%26nosw%3D1
7. <https://studfile.net/preview/3827591/page:4/>
8. https://docs.yandex.ru/docs/view?tm=1654951231&tld=ru&lang=ru&name=Salomaa\_Kriptografiya-s-otkrytym-klyuchom\_RuLit\_Me\_677221.pdf&text=%D0%A1%D0%B0%D0%BB%D0%BE%D0%BC%D0%B0%D0%B0%20%D0%90.%20%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%20%D1%81%20%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC%20%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC%3A%20%D0%9F%D0%B5%D1%80.%20%D1%81%20%D0%B0%D0%BD%D0%B3%D0%BB.%20-%20%D0%9C.%3A%20%D0%9C%D0%B8%D1%80%2C%201996%20-%20304%20%D1%81.&url=https%3A%2F%2Fwww.rulit.me%2Fdata%2Fprograms%2Fresources%2Fpdf%2FSalomaa\_Kriptografiya-s-otkrytym-klyuchom\_RuLit\_Me\_677221.pdf&lr=65&mime=pdf&l10n=ru&sign=f6c0ccc9aa0a575487c9a48d04ea1b50&keyno=0&nosw=1&serpParams=tm%3D1654951231%26tld%3Dru%26lang%3Dru%26name%3DSalomaa\_Kriptografiya-s-otkrytym-klyuchom\_RuLit\_Me\_677221.pdf%26text%3D%25D0%25A1%25D0%25B0%25D0%25BB%25D0%25BE%25D0%25BC%25D0%25B0%25D0%25B0%2B%25D0%2590.%2B%25D0%259A%25D1%2580%25D0%25B8%25D0%25BF%25D1%2582%25D0%25BE%25D0%25B3%25D1%2580%25D0%25B0%25D1%2584%25D0%25B8%25D1%258F%2B%25D1%2581%2B%25D0%25BE%25D1%2582%25D0%25BA%25D1%2580%25D1%258B%25D1%2582%25D1%258B%25D0%25BC%2B%25D0%25BA%25D0%25BB%25D1%258E%25D1%2587%25D0%25BE%25D0%25BC%253A%2B%25D0%259F%25D0%25B5%25D1%2580.%2B%25D1%2581%2B%25D0%25B0%25D0%25BD%25D0%25B3%25D0%25BB.%2B-%2B%25D0%259C.%253A%2B%25D0%259C%25D0%25B8%25D1%2580%252C%2B1996%2B-%2B304%2B%25D1%2581.%26url%3Dhttps%253A%2F%2Fwww.rulit.me%2Fdata%2Fprograms%2Fresources%2Fpdf%2FSalomaa\_Kriptografiya-s-otkrytym-klyuchom\_RuLit\_Me\_677221.pdf%26lr%3D65%26mime%3Dpdf%26l10n%3Dru%26sign%3Df6c0ccc9aa0a575487c9a48d04ea1b50%26keyno%3D0%26nosw%3D1
9. Хакинг: искусство эксплойта. 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2010. – 512 с., ил. ISBN 978-5-93286-158-5
10. Язык программирования C++ / Бьерн Страуструп; Пер. с англ. С. Анисимова и М. Кононова под ред. Ф. Андреева, А. Ушакова. - Спец. изд. - М. : Binom Pablishers ; СПб. : Нев. диалект, 2001. - 1098 с. : ил.; 24 см.; ISBN 5-7989-0223-4 (Бином)