МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ

ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики и прикладной математики

Кафедра прикладной математики и экономико-математических методов

**КУРСОВАЯ РАБОТА**

по дисциплине:

**«Языки и методы программирования»**

Тема: «Реализация и исследование шифрования Эль-Гамаля»

Направление: 01.03.02 Прикладная математика и информатика

Студент: Карпова Софья

Группа: ПМ1701 Подпись:

Проверил: Фёдоров Дмитрий Юрьевич

Должность: Старший преподаватель

Оценка: Дата:

Подпись:

Санкт-Петербург

2018

**Оглавление**

[**Введение** 3](#_Toc532766945)

[**1.** **Теоретическая часть** 5](#_Toc532766946)

[**1.1.** **Алгоритм** 5](#_Toc532766947)

[**1.1.1.** **Генерация ключей** 5](#_Toc532766948)

[**1.1.2.** **Шифрование** 5](#_Toc532766949)

[**1.1.3.** **Дешифрование** 5](#_Toc532766950)

[**2.** **Реализация** 7](#_Toc532766951)

[**2.1.** **Генерация ключей** 7](#_Toc532766952)

[**2.2.** **Реализация шифрования** 10](#_Toc532766953)

[**2.3.** **Реализация дешифровки** 12](#_Toc532766954)

[**3.** **Исследование алгоритма** 14](#_Toc532766955)

[**3.1.** **Криптографическая стойкость** 14](#_Toc532766956)

[**3.2.** **Недостатки схемы шифрования** 14](#_Toc532766957)

[**4.** **Заключение** 16](#_Toc532766958)

[**Список использованной литературы** 18](#_Toc532766959)

# **Введение**

Защищённое хранение и передача информации. Эта проблема появилась ещё в древние времена, и тогда появилось решение - шифрование. До наших дней дошли упоминания о шифрах в Древнем Египте, Древней Греции и Древнем Риме. С ходом технологического прогресса известные методы шифрования совершенствовались, а также создавались новые. Сегодня шифрование является неотъемлемой частью нашей повседневной жизни. С бурным развитием цифровых технологий значительно возрастает объём информации, которую хочется или необходимо защищать от посторонних лиц, а также методы кражи этой информации. Поэтому шифрование является одной из важнейших задач современной науки, в частности криптографии.

Шифрование с открытым ключом - одно из решений данной проблемы. Строгое определение звучит следующим образом: Криптографическая система с открытым ключом (разновидность асимметричного шифрования) - система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому) каналу и используется для проверки ЭП и шифрования сообщения. Закрытый ключ используется для генерации ЭП и для расшифровки сообщений и строго охраняется. Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уилфреда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Под влиянием работы Ральфа Меркла о распространении открытого ключа, они предложили метод получения секретных ключей, используя открытый канал. Этот метод, известный как метод Диффи-Хеллмана, был первым опубликованным практичным методом для установления разделения секретного ключа между заверенными пользователями канала.

В 1985 году египетский учёный Тахер Эль-Гамаль предложил разработанную им новую схему шифрования, которая является усовершенствованным вариантом схемы Диффи-Хеллмана. Схема Эль-Гамаля основана на трудности вычисления дискретных логарифмов в конечном поле и включает в себя алгоритм шифрования и алгоритм цифровой подписи. В отличие от схемы RSA, схема Эль-Гамаля не была запатентована, поэтому стала более дешёвой альтернативой, так как не требовалась оплата лицензии. Схема Эль-Гамаля лежала в основе бывших стандартов электронной цифровой подписи США (DSA) и России (ГОСТ P.34 10-94).

В рамках данной курсовой работы будет рассмотрена и изучена схема шифрования Эль-Гамаля. Для достижения этой цели будет изучена теоретическая сторона задачи, создан прототип программы для генерации ключей, шифрования и дешифрования информации, а также изучены недостатки данной схемы шифрования.

# **Теоретическая часть**

## **Алгоритм**

Работу алгоритма шифрования можно разделить на несколько этапов:

1. Генерация ключей
2. Шифрование
3. Дешифрование

### **Генерация ключей**

* Генерируется большое случайное простое число
* Выбирается число ***g*** – первообразный корень
* Выбирается случайное целое число , такое что
* Вычисляется
* Тройка чисел – открытый ключ, – закрыты ключ

### **Шифрование**

* ***M*** – сообщение для шифрования. Число ***M*** должно быть меньше числа .
* Вычисляется пара чисел ***(a, b),*** такие что ***, .*** Пара  ***–*** является шифротекстом.
* Число – надёжно удаляется

### **Дешифрование**

***–*** исходное сообщениеНетрудно проверить корректность:

Схематическое изображение схемы шифрования Эль-Гамаля можно увидеть на рисунке 1:

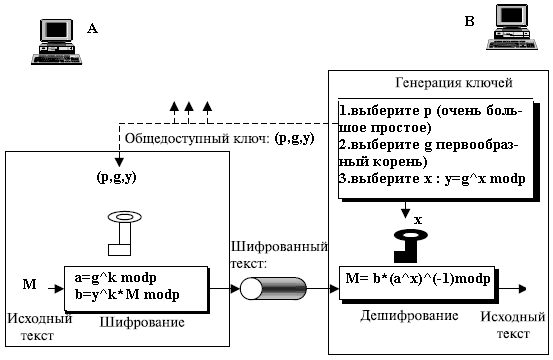


Рисунок 1 – Схема шифрования

# **Реализация**

## **Генерация ключей**

При решении задачи генерации открытого и закрытого ключей возникло несколько важных подзадач, среди которых:

1. Генерация случайных простых чисел
2. Нахождение первообразных корней
3. Возведение больших чисел в степень в поле

Эти подзадачи можно решать стандартными методами, однако в этом случае производительность программы будет низкой.

* + 1. **Генерация случайных простых чисел**

Для решения этой задачи были реализованы такие методы, как решето Эратосфена и решето Аткина. Функции ***eratos()*** и ***atkins()*** принимают в качестве входных данных число ***n***, а в качестве результата выдают ***n***-ое простое число (из-за громоздкости текста кода, в работе он приведён не будет). Для того чтобы понять, кокой из методов эффективнее всего использовать при шифровании, сравним время работы этих функций для ***n*** от 100000 до 750000 (рис. 2) и для ***n*** от 1000000 до 7500000 (рис. 3).

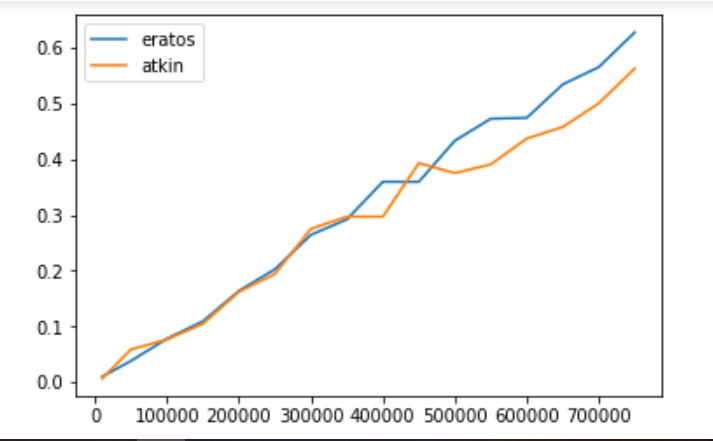


Рисунок 2 – сравнение быстродействия решета Аткина и решета Эратосфена

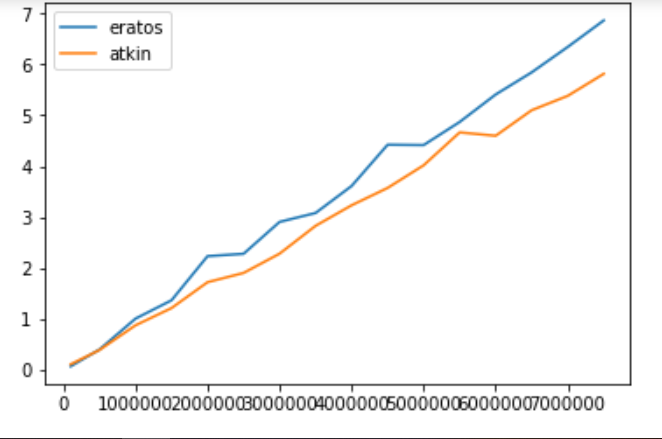


Рисунок 3 – сравнение быстродействия решета Аткина и решета Эратосфена

Функции ***generate\_prime\_atkin()*** и ***generate\_prime\_eratos(),*** которые используют в себе функции ***eratos()*** и ***atkins()*** соответственно***,*** генерируют случайные простые числа в диапазоне от 9973 до 999983 (т.е. от 10000-го простого числа до 1000000-го). На рисунке 4 показано время работы этих функций: по оси абсцисс – номер запуска, по оси ординат – время.

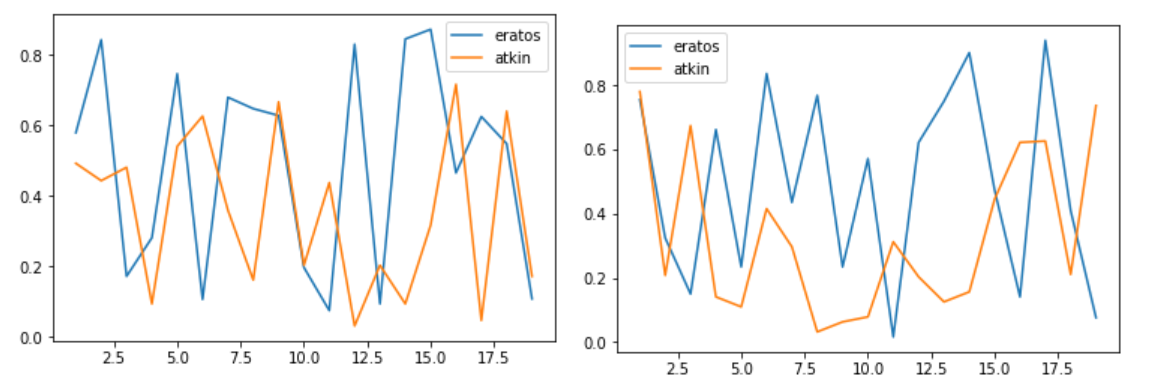


Рисунок 4 – Сравнение быстродействия

Из графиков на рисунках 2,3 и 4 видно, что в большинстве случаев, решето Аткина использовать выгоднее, чем решето Эратосфена

* + 1. **Нахождение первообразных корней**

Для нахождения первообразного корня используется функция ***get\_primitive\_root()***, которая принимает на вход число ***p***, для которого методом полного перебора находит все первообразные корни, а потом среди них выбирает случайное. Возможно усовершенствование данной функции.

* + 1. **Возведение больших чисел в степень в поле**

В рамках этой работы используется базовая функция языка Python - **a%b,** которая находит остаток от деления числа **a** на **b**. Такое решения не является оптимальным, так как затратно по памяти и времени, поэтому требует усовершенствования.

* + 1. **Генерация ключей.**

Функция ***get\_keys()*** по запросу пользователя в соответствии с алгоритмом Эль-Гамаля высчитывает открытый и закрытый ключи, которые записываются в виде списка ***[close\_key, open\_key]***, где ***open\_key*** – список ***[g, p, y].*** Текст функции представлен на рисунке 5.

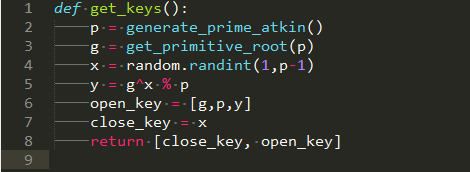


Рисунок 5 - Функция *get\_keys()*

## **Реализация шифрования**

* + 1. **Шифрование числа**

При шифровании числа используется функция ***encrypt(message, open\_k),*** принимающая на вход число ***message***, открытый ключ - ***open\_k,*** и возвращающая в качестве результата список ***cipher***, вида ***[a,b]*** – шифротекст. Числа ***a, b*** высчитываются в соответствии с алгоритмом шифрования Эль-Гамаля, описанном в пункте 1.1.2. Текст функции представлен на рисунке 6.

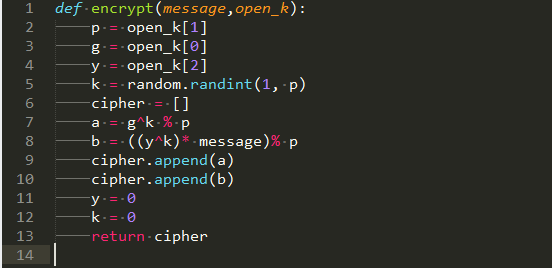


Рисунок 6 - функция *encript()*

* + 1. **Шифрование строки и текстового файла**

Функция ***encrypt\_text(message, open\_k)*** :

* + 1. принимает на вход строку ***message*** и открытый ключ - ***open\_k***
    2. преобразует строку символов в список, где каждый элемент – код символа ASCII
    3. каждый элемент списка преобразуется в шифрограмму вида ***[a,b]*** и записывается в общий список ***cipher.*** Таким образом на выходе получается список вида ***[[a1,b1], [a2,b2], … , [an,bn]]***, где ***n*** – длина строки.

Текст функции представлен на рисунке 7.

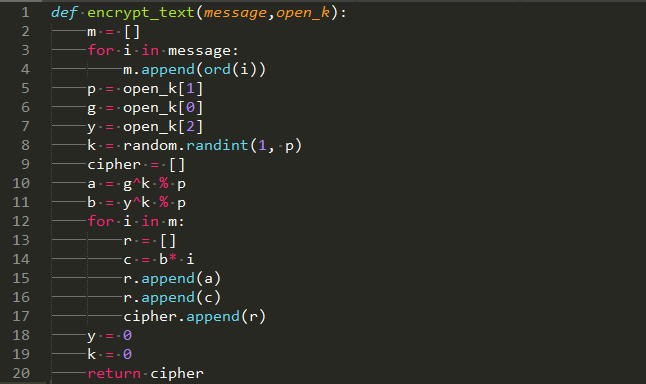


Рисунок 7 - функция *encrypt\_text()*

Для шифрования текстового файла используется функция ***encrypt\_text\_from\_file2newfile(file, newfile, open\_k)*** (рисунок 8):

1. входные параметры ***file, newfile, open\_k,*** где ***file, newfile*** – имена файлов откуда берётся текст для шифрования и куда будет записываться шифрограмма соответственно, а ***, open\_k*** – открытый ключ
2. к каждой строке текстового файла ***file*** применяется функция ***encrypt\_text***() и в новый файл ***newfile*** построчно записывается шифротекст.

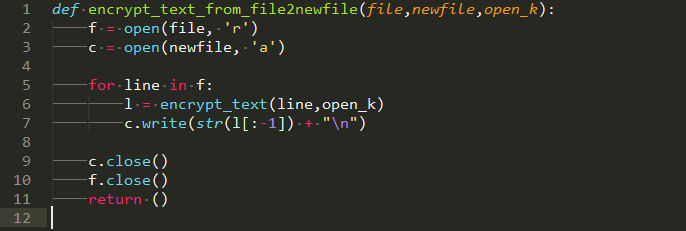


Рисунок 8 - функция *encrypt\_text\_from\_file2newfile()*

## **Реализация дешифровки**

Дешифровка происходит аналогично шифрованию:

1. Функция ***decipher(cipher, open\_key, close\_key)*** дешифрует шифротекст - список вида ***[a,b],*** в число. Рисунок 9.

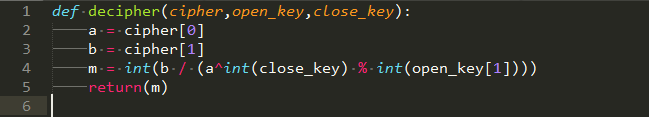


Рисунок 9 - фукция *decipher()*

1. Функция ***decipher\_text(cipher, open\_key, close\_key)*** дешифрует список ***cipher*** вида ***[[a1,b1], [a2,b2], … , [an,bn]]*** – в строку длины ***n***. Реализация функции представлена на рисуноке 10.

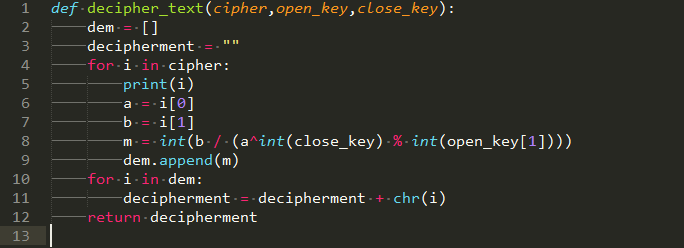


Рисунок 10 - Функция *decipher\_text()*

1. Функция ***decipher\_from\_file2newfile(file, newfile, open\_key, close\_key)*** дешифрует текстовый файл ***file*** с шифротекстом. Построчно считывая из ***file*** строки вида “***[[a1,b1], [a2,b2], … , [an,bn]]***”, функция дешифрует их помощью функции ***decipher\_text()*** и записывается в новый текстовый документ ***newfile***. Реализация функции представлена на рисуноке 11.

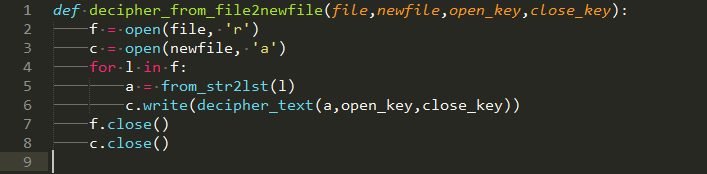


Рисунок 11 - Функция *decipher\_from\_file2newfile()*

Функция ***decipher\_from\_file2newfile()*** построчно считывает шифротекст из файла ***file***. Но функция ***decipher\_text()*** на вход принимает объект типа ***list***, а не ***string***. Поэтому для корректной работы используется функция ***from\_str2lst(st)***, которая переделывает строку ***st*** вида “***[[a1,b1], [a2,b2], … , [an,bn]]*** ” в список. Реализация функции представлена на рисуноке 12.

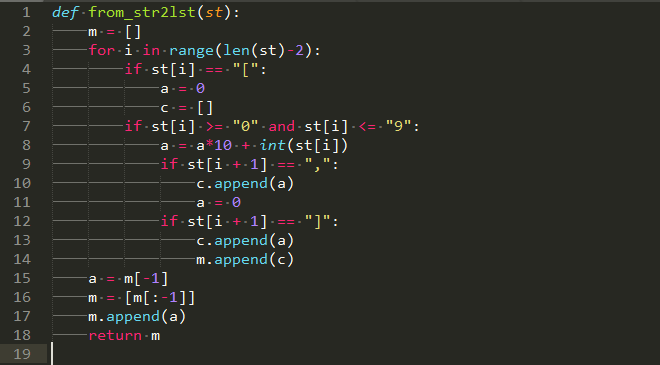


Рисунок 12 - функция *from\_str2lst()*

# **Исследование алгоритма**

## **Криптографическая стойкость**

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится и схема Эль-Гамаля, крипто стойкость которой основана на вычислительной сложности проблемы дискретного логарифмирования, где по известным требуется вычислить ,удовлетворяющий сравнению:**.** Проблема дискретного логарифма состоит в том, что, зная основание степени и получившийся после возведения результат по модулю простого числа, невозможно за обозримое время определить, в какую именно степень было возведено основание.

Так как при шифровании вводится случайная величина ,то шифр Эль-Гамаля можно назвать шифром многозначной замены. Из-за случайности выбора числа такую схему ещё называют схемой вероятностного шифрования. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля, так как у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определённым процессом шифрования.

Криптостойкость схемы Эль-Гамаля сравнима с криптостойкостью схемы RSA и составляет MIPS для ключа 1300 бит, но из-за большой трудоёмкости операции возведения в степень больших чисел быстродействие RSA ниже.

## **Недостатки схемы шифрования**

Одним из недостатком схемы шифрования Эль-Гамаля является удвоение длины зашифрованного текста по сравнению с начальным текстом. Так шифротекстом одного числа (символа) является пара чисел **,** объём передаваемого сообщения увеличивается вдвое.

Другим недостатком схемы является трудность задачи вычисления дискретных логарифмов в поле. Операции возведения в степень больших чисел в конечном поле достаточно трудоёмки даже для современных процессоров, даже если производятся по оптимизированным алгоритмам. Поэтому процесс вычисления новых ключей шифрования занимает достаточно долгое время. Например, в рамках этой курсовой работы среднее вычисление ключей занимает от 10 до 30 секунд, где случайное простое число ***p*** находится в промежутке от 1000-го до 100000-го простого числа (991 и 99991 соответственно). Однако на практике используются ключи большего размера (как правило 768б 1024 и 1536 бит), и время вычисления одного ключа занимает до нескольких минут.

# **Заключение**

В процессе написания курсовой работы была изучен метод шифрования Эль-Гамаля, его теоретическое обоснование, принцип работы и, как результат, создан прототип программы, которая позволяет генерировать открытый и закрытый ключи для шифрования, шифровать и дешифровывать сообщения – числа, строки символов, текстовые сообщения. На данный момент времени криптосистемы с открытым ключом, к которым относится схема шифрования Эль-Гамаля, считаются наиболее перспективными.

Главным преимуществом схемы шифрования является её высокая криптостойкость. Как было показано в работе, это достигается благодаря сложности процесса вычисления степеней больших чисел в конечном поле, а также использованию случайных величин при шифровании. Благодаря этому схема шифрования Эль-Гамаля широко применялась для шифрования данных как в частных, так и в государственных структурах.

Однако сложность вычислительных процессов и, как следствие, большое потребление ресурсов для них (время) является одним из главных недостатков данной схемы шифрования. Так при приблизительно одинаковой криптостойкости, алгоритм шифрования RSA быстродейственнее примерно в тысячу раз. Также в процессе шифрования длина сообщения увеличивается в два раза, что также является большим недостатком схемы шифрования. Как результат, алгоритм шифрования не является оптимальным по затрачиваемым ресурсам, времени шифрования и конечным объёмом зашифрованного сообщения.

Вследствие этих недостатков, схема шифрования Эль-Гамаля не применяется в чистом виде в настоящее время. Сегодня для шифрования больших объёмов данных применяются более быстрые схемы шифрования (обычно симметричные) с использованием сессионного ключа, а этот ключ уже шифруется с помощью ассиметричной схемы шифрования (в частности схема Эль-Гамаля) и уже передаётся получателю. Таким образом схема шифрования Эль-Гамаля применяется в более совершенных современных схемах шифрования. На её основе было разработано и используются большое количество современных алгоритмов. К ним относятся алгоритмы DSA, ECDSA, KCDSA, схема Шнорра.

**Список использованной литературы**

1. Википедия: статья: «Схема Эль-Гамаля» 2018 - Режим доступа: <https://ru.wikipedia.org/wiki/Схема_Эль-Гамаля>, свободный. – Загл. с экрана. – Язык русский.
2. TAHER ELGAMAL, MEMBER, IEEE, «A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms», IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, JULY 1985 - Режим доступа: <https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf>, свободный. – Загл. с экрана. – Язык английский.
3. Википедия: статья: «Криптосистема с открытым ключём» 2018 - Режим доступа: <https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом>, свободный. – Загл. с экрана. – Язык русский.
4. Статья: «Криптосистема Эль-Гамаля» 15.01.2014 - Режим доступа: <https://studopedia.su/10_105628_kriptosistema-el-gamalya.html> свободный. – Загл. с экрана. – Язык русский.
5. Статья: «3.2. Алгоритм шифрования Эль Гамаль» 2006 - Режим доступа: <https://studfiles.net/preview/909637/page:10/> свободный. – Загл. с экрана. – Язык русский.
6. Википедия: статья: «Протокол Диффи-Хелммана» 2018 - Режим доступа: <https://ru.wikipedia.org/wiki/Протокол_Диффи_—_Хеллмана>, свободный. – Загл. с экрана. – Язык русский.
7. Статья «Ещё раз о поиске простых чисел» 21.11.2012 - Режим доступа: <https://habr.com/post/133037/>, свободный. – Загл. с экрана. – Язык русский.
8. Статья: «6.4. Нахождение первообразных корней по простому модулю» 2007 - Режим доступа: <https://studfiles.net/preview/6268704/page:25/> свободный. – Загл. с экрана. – Язык русский.