|  |
| --- |
|  |
|

|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования**«МИРЭА– Российский технологический университет»****РТУ МИРЭА****Филиал РТУ МИРЭА в г. Ставрополе** |

 |
|  |

**Методические указания к лабораторным работам**

**и самостоятельной работе по дисциплине**

**«Информационная безопасность»**

**для студентов направления подготовки**

**09.03.01 «Информатика и вычислительная техника»**

**Квалификация: бакалавр**

**Ставрополь**

Методические указания составлены в соответствии с Федеральным государственным образовательным стандартом высшего образования для студентов направления подготовки 09.03.01 Информатика и вычислительная техника и программой дисциплины «Информационная безопасность».

Составитель: А.И. Сосин, доцент, канд. экон. наук

**Оглавление**

[Указания по технике безопасности 5](#_Toc85816157)

[Лабораторная работа 1. Исследование шифра гаммирования 6](#_Toc85816158)

[Лабораторная работа 2. Исследование шифра Вижинера 11](#_Toc85816159)

[Лабораторная работа 3. Исследование шифра перестановки 17](#_Toc85816160)

[Лабораторная работа 4. Исследование классических криптоалгоритмов подстановки и перестановки для защиты информации 23](#_Toc85816161)

[Лабораторная работа 5. Исследование различных методов защиты информации и их стойкости на основе подбора ключей, ч.1 33](#_Toc85816162)

[Лабораторная работа 6. Исследование различных методов защиты информации и их стойкости на основе подбора ключей, ч.2 40](#_Toc85816163)

[Лабораторная работа 7. Генерация простых чисел, используемых в асимметричных системах шифрования, ч.1 47](#_Toc85816164)

[Лабораторная работа 8. Генерация простых чисел, используемых в асимметричных системах шифрования, ч.2 52](#_Toc85816165)

[Лабораторная работа 9. Исследование шифра RSA, ч.1 57](#_Toc85816166)

[Лабораторная работа 10. Исследование шифра RSA, ч.2 62](#_Toc85816167)

[Лабораторная работа 11. Исследование принципов хеширования сообщений, ч.1 67](#_Toc85816168)

[Лабораторная работа 12. Исследование принципов хеширования сообщений, ч.2 70](#_Toc85816169)

[Лабораторная работа 13. Исследование процедур формирования и проверки электронной подписи, ч.1 73](#_Toc85816170)

[Лабораторная работа 14. Исследование процедур формирования и проверки электронной подписи, ч.2 80](#_Toc85816171)

[Лабораторная работа 15. Исследование принципов формирования общего секретного ключа на основе схемы Диффи-Хеллмана, ч.1 87](#_Toc85816172)

[Лабораторная работа 16. Исследование принципов формирования общего секретного ключа на основе схемы Диффи-Хеллмана, ч.2 93](#_Toc85816173)

[Список рекомендуемой литературы 99](#_Toc85816174)

# Указания по технике безопасности

Перед началом занятия необходимо:

1. Проверить правильность установки стола, стула, угол наклона экрана монитора, положение клавиатуры и, при необходимости, произвести корректировку их установки в целях исключения неудобных поз и длительных напряжений тела. Дисплей должен находиться на расстоянии 60 – 70 см от глаз, плоскость его экрана должна быть перпендикулярна направлению взгляда и центр экрана должен быть ниже или на уровне глаз.
2. Подготовить к работе рабочее место, разместив необходимые принадлежности таким образом, чтобы исключить их падение и опрокидывание.
3. Проверить работу компьютера, обо всех замеченных нарушениях, неисправностях и поломках немедленно доложить преподавателю или лаборанту.

Запрещается приступать к работе в случае обнаружения несоответствия рабочего места установленным в данном разделе требованиям, а также при невозможности выполнить указанные в данном разделе действия.

Обо всех неполадках в работе оборудования необходимо ставить в известность преподавателя или лаборанта. Запрещается самостоятельное устранение любых неисправностей используемого оборудования.

При обнаружении неисправности в работе оборудования (нагревании, появлении искрения, запаха горелой изоляции, появлении посторонних звуков и т.п.) немедленно прекратить работу и сообщить об этом лицу, проводящему занятия или лаборанту и действовать по его указаниям.

По окончании занятия следует:

1. Произвести закрытие всех выполняемых задач.
2. Привести в порядок рабочее место.
3. При обнаружении неисправности мебели, оборудования проинформировать об этом преподавателя и лаборанта.
4. С разрешения преподавателя организованно покинуть кабинет.

# Лабораторная работа 1. Исследование шифра гаммирования

**Цель:** сформировать практические умения по исследованию порядка формирования криптограмм (шифрования) методами алфавитного и двоичного гаммирования.

**Содержание:** Изучить алгоритм метода гаммирования «Шифрование с помощью датчика псевдослучайных чисел», зашифровать текст методом гаммирования согласно варианта, исследовать свойства шифра гаммирования.

**1. Теоретическая часть**

Принцип шифрования заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на открытые данные обратимым образом (например, при использовании логической операции «Исключающее ИЛИ»).

Расшифрование данных сводится к повторной генерации гаммы шифра при известном ключе и наложению этой гаммы на зашифрованные данные.

Зашифрованное сообщение достаточно трудно для несанкционированного расшифрования (раскрытия) в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей или если период гаммы превышает длину всего зашифрованного сообщения и неизвестна никакая часть исходного текста. Шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых сообщений, используются генераторы ПСЧ.

Различают методы конечной гаммы и бесконечной гаммы. В качестве конечной гаммы может использоваться фраза, в качестве бесконечной - последовательность, вырабатываемая датчиком псевдослучайных чисел.

**Пример 1**. Открытый текст: «ПРИКАЗ» («16 17 09 11 01 08» согласно табл. .1).

Таблица 1 – Нумерация букв алфавита



Пример 1.

Шифрующая гамма: «ГАММА» («04 01 13 13 01»).

Операция, сложение по mod 33.

Y1=l6+4(mod33) = 20;

Y2=17+1(mod33) = 18;

Y3=9+13(mod33) = 22;

Y4=11+13(mod33) = 24;

Y5=1+1(mod33) = 2;

Y6=8+4(mod.33) = 12;

Шифртекст: «УСХЧБЛ» («20 18 22 24 02 12»).

Пример 2.

Открытый текст: «ПРИКАЗ» («16 17 09 11 01 08» согласно табл. 1).

Первые значения датчика: «2 1 7 9 4 5 6 7».

Операция: сложение по mod 2.

0⊕0=0 0⊕1=1 1⊕0=1 1⊕1=0.

Запишем код каждой буквы открытого текста в двоичном виде, используя пять разрядов, а каждую цифру гаммы – используя четыре разряда:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1000 | 1000 | 0100 | 0101 | 0000 | 0100 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 0001 | 0000 | 0011 | 0100 | 0010 | 0010 |
| 0 | 1 | 1 | 1 | 0 | 1 |
| 1001 | 1000 | 0111 | 0001 | 0010 | 0110 |
| 0 | 0 | 0 | 0 | 1 | 1 |

Шифртекст: «СПНБДК».

**2. Задания к лабораторной работе**

**Задание 1**. Зашифруйте предложенный текст (табл. 2) методом гаммирования, используя, в качестве шифрующей гаммы соответствующие слова. Номера вариантов получите у преподавателя (по 2 варианта – каждому студенту).

Таблица 2 – Варианты текста и шифрующей гаммы

|  |  |  |
| --- | --- | --- |
| Номер варианта | Текст | Шифрующая гамма |
| 1 | Школа | Лодка |
| 2 | Ведро | Папка |
| 3 | Окунь  | Халва |
| 4 | Клика  | Зубры |
| 5 | Гроза | Хурма |
| 6 | Слива | Шорты |
| 7 | Крупа | Гости |
| 8 | Труба | Тыква |
| 9 | Круги | Вишня |
| 10 | Глина  | Капля |
| 11 | Трава | Масло |
| 12 | Спина | Сахар |
| 13 | Крыло | Карта  |
| 14 | Грибы | Санки |
| 15 | Марка | Озеро |
| 16 | Посол | Проем |
| 17 | Опрос | Мосол |
| 18 | Просо | Полоз |
| 19 | Семен | Мохер |
| 20 | Посох | Паром |

**Задание 2**.Зашифруйте предложенный текст методом гаммирования, используя значения датчика псевдослучайных чисел, представленные в табл. 3 (по 2 варианта – каждому студенту).

Таблица 3 – Варианты текста и значения датчика ПСП

|  |  |  |
| --- | --- | --- |
| Вариант  | Текст | Первые значения датчика ПСЧ |
| 1 | Хеш\_функция | 3126543821 |
| 2 | База\_данных | 2718521329 |
| 3 | Иллюстрация | 1270346755 |
| 4 | Строка таблицы | 5414327016 |
| 5 | Программа | 4569874324 |
| 6 | Криптостойкость | 3536378918 |
| 7 | Эквивалент | 5290421459 |
| 8 | Реализация | 9495627413 |
| 9 | Вероятность | 2701654143 |
| 10 | Синхронизация | 3417067525 |
| 11 | Турбулентность | 6987429749 |
| 12 | Вариативность | 8521370165 |
| 13 | Защищенность | 4340512167 |
| 14 | Безопасность | 1675203479 |
| 15 | Землетрясение | 8455721907 |
| 16 | Организация | 4971056328 |
| 17 | Космический | 8997856421 |
| 18 | Доверенный | 6547834290 |
| 19 | Аналитический | 4315327896 |
| 20 | Двоичный\_код | 7685943208 |

**Задания для самостоятельной работы**

1. Укажите в письменной форме, в каком случае шифр гаммирования является теоретически абсолютно стойким.

2. Укажите в письменной форме, какая последовательность может быть использована в качестве гаммы.

3. Укажите в письменной форме, в чем заключается операция сложения по модулю 2.

4. Укажите в письменной форме, как определяется стойкость шифрования методом алфавитного гаммирования.

5. Укажите в письменной форме, как определяется стойкость шифрования методом гаммирования с использованием генератора ПСЧ.

6. Укажите в письменной форме, чем определяется стойкость засекречивания методом гаммирования.

7. Укажите в письменной форме, при засекречивании способом гаммирования происходит или не происходит размножения ошибок при передаче криптограммы по каналу связи и почему.

**Вопросы к лабораторной работе**

1. В чем заключается метод гаммирования?

2. Какие операции можно использовать в процедуре наложения гаммы?

3. Каким выражением определяется стойкость шифрования методом двоичного гаммирования?

# Лабораторная работа 2. Исследование шифра Вижинера

**Цель и содержание**: провести исследование алгоритма шифрования методом Вижинера, научится пользоваться таблице Вижинера для шифрования текстовых сообщений.

**1. Теоретическая часть**

Наиболее известными являются шифры замены, или подстановки, особенностью которых является замена символов (или слов, или других частей сообщения) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста. Различают одноалфавитную и многоалфавитную замену. Вскрытие одноалфавитных шифров основано на учете частоты появления отдельных букв или их сочетаний (биграмм, триграмм и т. п.) в данном языке.

Примером многоалфавитного шифра замены является так называемая система Виженера. Шифрование осуществляется по таблице, представляющей собой квадратную матрицу размерностью n\*n, где n - число символов используемого алфавита. На рисунке показана таблица Виженера для русского языка (алфавит 32 буквы и пробел). Первая строка содержит все символы алфавита. Каждая следующая строка получается из предыдущей циклическим сдвигом последней на символ влево.



Выбирается ключ или ключевая фраза. После чего процесс шифрования осуществляется следующим образом. Под каждой буквой исходного сообщения последовательно записываются буквы ключа; если ключ оказался короче сообщения, его используют несколько раз. Каждая буква шифртекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пусть, например, требуется зашифровать сообщение:

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ

с помощью ключа ВЕНТИЛЬ.

Запишем строку исходного текста с расположенной над ней строкой с циклически повторяемым ключом:



Составляем вспомогательную матрицу, выбрав из таблицы Вижинера первую строку и строки, которые начинаются на буквы ключа.

Далее производим шифрование по следующей схеме:

По букве шифруемого текста входим в рабочую матрицу и выбираем букву, расположенную в строке, соответствующей букве ключа.



По букве шифруемого текста входим в рабочую матрицу и выбираем букву, расположенную в строке, соответствующей букве ключа.

В результате шифрования, начальный этап которого показан на рисунке, получим шифртекст:



Дешифрование осуществляется следующим образом. Под буквами шифртекста последовательно записываются буквы ключа; в строке таблицы, соответствующей очередной букве ключа, происходит поиск соответствующей буквы шифртекста. Находящаяся над ней в первой строке таблицы буква является соответствующей буквой исходного текста.

 Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем некоторые из них:

1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке;

2) в качестве ключа используются случайные последовательности чисел. Из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе. Известны и другие модификации метода.

Вариант системы подстановок Вижинера при M = 2 называется системой Вернама (1917 год). В то время ключ k=(k0, k1 … , kK–1) записывался на бумажной ленте. Каждая буква исходного текста переводилась с использованием кода Бодо в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования использовался корпусом связи армии США. Общий принцип шифрования подстановкой может быть представлен следующей формулой:

R[i]= S[i] + W mod(k – 1),

где R[i] – символ зашифрованного текста; S[i] – символ исходного текста; W – целое число в диапазоне 0-(к- 1); к – число символов используемого алфавита.

Если W фиксировано, то формула описывает моноалфавитную подстановку, если W выбирается из последовательности w1 w2, … wn, то получается полиалфавитная подстановка с периодом n.

Если в полиалфавитной подстановке n > M (где M – число знаков шифруемого текста) и любая последовательность w1 w2, … wn, используется только один раз, то такой шифр является теоретически не раскрываемым, если, конечно, злоумышленник не имеет доступа к исходному тексту. Такой шифр получил название шифра Вернама.

**2.Задания к лабораторной работе**

**Задание 1**. Зашифруйте и расшифруйте сообщение методом Вижинера.



Каждому студенту преподавателем выдается по 2 варианта сообщения.

**Задания для самостоятельной работы**

* 1. Укажите в письменной форме, можно ли шифр Цезаря назвать частным случаем шифра Вижинера.
	2. Укажите в письменной форме, что из себя представляет шифр Вернама.
	3. Укажите в письменной форме, шифр Вернама блочный или поточный.
	4. Укажите в письменной форме, какова стойкость шифра Вижинера.
	5. Укажите в письменной форме, как аппаратно может быть реализован шифр Вижинера.

**Вопросы к лабораторной работе**

1. В чем преимущество шифров многоалфавитной замены?
2. Что из себя представляет множество алфавитов в шифре Вижинера?
3. Какой формулой описывается алгоритм Вижинера?

# Лабораторная работа 3. Исследование шифра перестановки

**Цель**: Исследовать алгоритм шифрования методом перестановки и его свойства при шифровании и дешифровании текстовых сообщений.

**Содержание:** Изучить алгоритм шифрования методом перестановки, выполнить шифрование заданного текста методом перестановки по ключу, дешифровать тексты, зашифрованные методом перестановки и пояснить алгоритмы дешифрования.

**1. Теоретическая часть**

Шифрование методом перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка - написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявятся серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).



После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Вариант этого шифра: сначала исходную фразу записать в столбики:



Потом разбить строки на пятерки букв:

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-решетка, в который можно записывать исходный текст. Но тут уже требуются предварительные договоренности между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины и высоты, записывать в нее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и по диагоналям, а для шифрования можно брать тоже различные направления.

Для примера возьмем решетку 6x6 (причем количество строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам:



Если шифровать по стрелкам (диагоналям) сверху вниз с левого верхнего угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБМ АМЕВЛ ЫЛГК ИДИ ЕЗ Ж

Для окончательного оформления шифротекст может быть разбит на, группы по 6 символов:

ПУУСДК ТЕКХЬТ АОАБТК ТБМАМЕ ВЛЫЛГК ИДИЕЗЖ

Весьма часто используют **перестановки с ключом**. Тогда правила заполнения решетки и шифрования из нее упрощаются, становятся стандартными. Единственное, что надо помнить и знать, - это **ключ**, которым может быть любое слово, например РАДИАТОР. В соответствии с расположением букв в алфавите буква А получает номер 1, вторая буква А - 2, следующая по алфавиту буква Д - 3, потом И - 4, О - 5, первая буква Р - 6, вторая Р - 7 и буква Т - 8.

Заполняем решетку:



Записываем столбики в соответствии с номерами букв ключа: УТЫ ЬКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ Затем последовательность опять разбивается на пятерки: УТЫЬК ТСТХТ АОУАЛ ПЕМОД КИБКЕ

Таким шифром простой перестановки колонок пользовались немецкие секретные агенты во время Второй мировой войны. В качестве ключа они использовали первые буквы строк на определенной странице какой-нибудь обыкновенной книги.

Развитием этого шифра является шифр **перестановки колонок с пропусками**, которые располагаются в решетке тоже в соответствии с ключом (в нашем случае через 6-1-3-4-2-8-5-7 ... символов):





Шифрограмма будет такой:

УДК Ь СЕХЛ ТТОМ АЕП ПКИ УКЛР БТТО

Из рассмотренных примеров очевидно, что все процедуры шифрования и расшифровки по методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

**2. Задания к лабораторной работе**

**Задание 1.** Зашифровать следующий текст методом перестановки по ключу Текст для шифрования: **Не обещайте деве юной любови вечной на земле.**

Варианты ключа:



**Задание 2**. Дешифровать следующие тексты, зашифрованные методом перестановки. Пояснить алгоритмы дешифрования текстов:

1. Изречение немецкого философа Фридриха Ницше: ОЬТСОНЙАЧУ ЛСВТЯ РЕВЕН ИЛЕТИДЕБОП
2. Изречение немецкого ученого-гуманиста Эразма Роттердамского: ЙЫТЫР КСТНА ЛАТЕН ТЕАДЗ ОСИИЦ АТУПЕРОООО
3. Изречение чешского писателя Карела Чапека: ЕЛЙГС АМОЛТ ЕМИЬР УНСЕО ЕАПОМ МОООП МОЖОЕ ОЕКШО ШРАОЬ АЙОСЙ ДОДНДР ОЕЕУО
4. Изречение польского писателя-фантаста Станислава Лема: ТОУМА МЕЖЕЧ ЫАООО ОММГЗ ЕСНМЕ ДЕООО ЧЫАОД НЛОТМ УМООО ТДЕРО ЕОЧОММОООО
5. Изречение датского ученого-физика Нильса Бора: ТПРРО УСЕБД ООДИН ОБЖВЛ ООЕЕУ ИОЧОЕ НАДТО ЩНЬЕУОТДБУ
6. Изречение французского философа Жана-Поля Сартра: ИНККО ОТСОЧ ЯЧПОТ ЕАРЕЯ ОЛНЕА АЕМТКОНСТШ
7. Изречение американского писателя Джона Стейнбека: АРЕНОЫЕТМО ЕЖОИБ ЕДДЖЙ ЯПТВС ОДОКМ ПСИОЖ ОЙЛГООИЕНТ

**Задания для самостоятельной работы**

* 1. Укажите в письменной форме, каковы особенности использования этого метода.
	2. Укажите в письменной форме, в чем заключается метод перестановки с ключом.
	3. Укажите в письменной форме, в чем заключается метод перестановки колонок с пропусками.
	4. Укажите в письменной форме, каковы возможности использования метода перестановки.
	5. Укажите в письменной форме, какова стойкость шифра перестановки.
	6. Укажите в письменной форме, к какому классу относится шифр перестановки.

**Вопросы к лабораторной работе**

1. В чем заключается метод перестановки?
2. Какой шифр использовался во время гражданской войны в США?
3. Как можно шифровать текст при помощи решетки?

# Лабораторная работа 4. Исследование классических криптоалгоритмов подстановки и перестановки для защиты информации

**Цель и содержание**: Исследование свойств классических криптографических алгоритмов многоалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование в исследовании гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

**1. Теоретическая часть**

Метод подстановки, пожалуй, самый древний из всех известных методов. В его основе лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смещении букв относительно их обычного местоположения в алфавите. Например, для кириллицы, если смещение равно 1, то “А” соответствует букве “Б”, “Б” – “В”, и так далее, а когда алфавит подходит к концу, то начинают брать буквы из начала списка. И выходит, например, следующее: из слова “КОДИРОВАНИЕ” получается“ ЛПЕЙСПГБОЙЖ”.

Частным случаем данного метода является шифр Цезаря. В I в.н.э. Ю.Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита *(А)* на четвертую *(D)*, вторую *(B)* – на пятую *(E)*, наконец последнюю – на третью. Шифр Цезаря относится к так называемому классу *одноалфавитных подстановок* и имеет множество модификаций.

Очевидно, что произвольный шифр из класса одноалфавитных методов не является шифром Цезаря (если мощность алфавита текста равна *n*, то число шифров Цезаря равно *n*, а число всех одноалфавитных шифров равно *n!*). Однако и для таких методов легко предложить способы дешифрования, основанные на статистических свойствах шифрованных текстов поскольку открытый и закрытый тексты имеют одинаковые статистические характеристики.

Суть этого перестановки заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного)текста.

Перестановки в классической криптографии обычно получаются в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.

Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы.

Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Таким образом, для матрицы размером 8\*8 (длина блока 64 символа) возможно 1.6\*109 ключей, что позволяет на современных компьютерах путем перебора дешифровать заданный текст. Однако для матрицы размером 16\*16 (длина блока 256 символов) имеется 1.4\*1026 ключей, и перебор их с помощью современных вычислительных средств весьма затруднителен.

Примером применения метода перестановки может быть также восьмиэлементная таблица, обладающая совокупностью маршрутов, носящих название маршрутов Гамильтона. Последовательность заполнения таблицы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом.

Для методов перестановки характерны простота алгоритма, возможность программной реализации и низкий уровень защиты, так как при большой длине исходного текста в его зашифрованном варианте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть. Другой недостаток этих методов – легкое раскрытие, если удается направить в систему для шифрования несколько специально подобранных сообщений. Так, если длина блока в исходном тексте равна *К* символам, то для раскрытия ключа достаточно пропустить через шифровальную систему *К-1* блоков исходного текста, в которых все символы, кроме одного, одинаковы.

Одним из наиболее известных методов криптоанализа является изучение статистических характеристик шифрованных текстов. Графическое отображение совокупности частот встречаемости символов в тексте называют гистограммой этого текста.

Предположим, что мы имеем дело с методом одноалфавитного шифрования. Зная частоту встречаемости букв в алфавите, можно предположить, какая буква была заменена на данную. Например, часто встречаемая буква “О” заменена на редко встречающуюся букву “Щ”.

Следует иметь в виду, что вид гистограммы для стандартного распределения зависит от вида исходного текста следующим образом: если исходный текст содержит символы кириллицы и латинского алфавита, то выводится статистическое распределение для кириллицы и латиницы, если только кириллицы (латиницы) то выводится статистическое распределение для кириллицы (латиницы).

**2. Задания к лабораторной работе**

Для выполнения лабораторной работы необходимо запустить программу L\_LUX (выдает преподаватель). На экране дисплея появится окно с размещенным в его центре текстовым редактором. В верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие. Чуть ниже основного меню расположена панель инструментов, а в самом низу окна, под текстовым редактором находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов для удобства снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, не обходимо нажать клавишу F10. Передвижение по главному меню осуществляется мышью.

Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, вернуться в главное меню или вовсе выйти из него – “ESC”.

А теперь более подробно рассмотрим каждый из пунктов главного меню.

**Редактор**

Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы.

Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню (кроме создания документа, открытия файла, выхода из программы, информации о программе) и большая часть клавиш панели управления (за исключением создания документа, открытия файла и выхода из программы).

**Создать документ (Ctrl+N) –** данный подпункт делает доступным для работы тестовый редактор (пользователь получает право создать свой текстовый файл, который впоследствии можно будет использовать при работе с программой), также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

**Открыть файл (Ctrl+L**) **–** при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в окне редактора текстов.

Аналогично пункту “Создать документ” доступным для работы становится текстовый редактор с отображаемым текстом, а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

**Сохранить файл (Ctrl+S) -** при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое редактора текстов.

**Выход из программы (Ctrl+X) -** при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

**Гистограмма**

Вывод на экран двух гистограмм, отображающих частоту встречаемости символов в тексте.

Имеется возможность просмотра следующих сочетаний гистограмм:

* гистограммы исходного и зашифрованного файла,
* гистограммы зашифрованного и расшифрованного файла,
* гистограммы стандартного распределения и зашифрованного текста,
* гистограммы стандартного распределения и расшифрованного текста.

В гистограммах с целью масштабирования используются левая и правая клавиши мыши.

Например, после шифрования текста большого объема пользователь хочет посмотреть гистограммы исходного и зашифрованного файла. Поскольку размеры текста достаточно большие, то на экран будут выведены две гистограммы с большим количеством столбцов в каждой (столбец соответствует одному символу текста), однако трудно будет сказать, какой из этих столбцов соответствует тому или иному символу текста, и какова частота встречаемости данного символа. Поэтому у пользователя есть возможность увеличить масштаб любой из двух гистограмм с целью более точного определения требуемого значения частоты встречаемости конкретного символа. Для этого необходимо навести указатель мыши на левую границу того участка гистограммы, который требуется увеличить, затем нажать левую клавишу мыши, и не отпуская ее растянуть прямоугольник так, чтобы его нижний правый угол совпал с правой границей увеличиваемого участка гистограммы. После этого следует отпустить левую клавишу мыши и на экране появится увеличенное изображение нужного участка.

Причем, нажав и не отпуская правую клавишу мыши, можно перемещать гистограмму в любом направлении с целью изучения всего полученного распределения в увеличенном масштабе.

Для того, чтобы от увеличенного масштаба вернуться к исходному виду, нужно навести указатель мыши на гистограмму, затем нажать левую клавишу мыши, и, не отпуская ее, снизу вверх растянуть небольшой по размерам прямоугольник, после этого следует отпустить левую клавишу мыши и на экране появится исходное изображение гистограммы.

**Шифрование**

Выполнение шифрования текстового файла осуществляется одним из семи методов, рассматриваемых в лабораторной работе.

1. Одноалфавитный метод (с фиксированным смещением).
2. Одноалфавитный метод с задаваемым смещением (от 2 до20).
3. Перестановка символов.
4. По дополнению до 255 (инверсный метод).
5. Многоалфавитный метод (с фиксированным ключом).
6. Многоалфавитный метод с ключом фиксированной длины.
7. Многоалфавитный метод с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей “ENTER”.

Затем появляется окно в котором в зависимости от метода шифрования требуется указать те или иные параметры, и либо подтвердить процесс кодировки, либо отказаться от него. После этого в окне редактора будет выдан зашифрованный текст.

**Дешифрование**

Аналогично предыдущему пункту выбирается метод дешифрования (должен соответствовать методу, которым был зашифрован файл).

Снова появляется окно, в котором в зависимости от метода дешифрования требуется указать те или иные параметры, и либо подтвердить процесс дешифрования, либо отказаться от него.

После этого в окно редактора будет выдан дешифрованный текст.

При правильном дешифровании, полученный текст совпадает с исходным.

**Дополнительная информация**

Программа предусматривает возможность посмотреть дополнительную информацию ('Помощь Ctrl+F9'), справочную информацию об используемых методах шифрования ('О методах Ctrl+F10'), сведения о программе ('О программеCtrl+F11').

***Пример работы с программой.*** Рассмотрим одноалфавитное шифрование с фиксированным ключом.

Загрузите в окно редактора исходный текст (любой) длиной от 10 до 15 предложений. Сохраните его, это необходимо для последующей работы с этим файлом. Затем вызовите пункт меню ШИФРОВАНИЕ, выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу ЗАШИФРОВАТЬ. После того как шифрование выполнено, можно в редакторе просмотреть зашифрованный текст.

Перейдите к пункту меню ГИСТОГРАММА. Выберите тип гистограмм, отображающий гистораммы исходного и шифрованного текста. Проанализируйте гистограммы. Они должны иметь примерно одинаковый вид.

Чтобы узнать ключ шифра (смещение второго алфавита относительно первого), необходимо по гистограммам найти символы, имеющие одинаковую частоту встречаемости. Например, самый частый символ в первой гистограмме при шифровании должен перейти в самый частый символ во второй гистограмме. Таким образом, найдя два самых часто встречаемых символа в обеих гистограммах, можно по стандартной таблице ASCII-кодов вычислить смещение. Зная смещение и таблицу кодировки символов, текст можно легко дешифровать. Вызвав меню ДЕШИФРОВАНИЕ, можно провести те же действия в автоматическом режиме.

**Примечание.** При шифровании и дешифровании из таблицы кодировки не используются символы с кодами 176-223 и 240-255, то есть при ручной расшифровке эти символы следует пропускать и считать, что, например, символ Я имеет код 159, а 223, аналогично П не 175, а 239.

Иногда в гистограммах под столбцами, показывающими частоту встречаемых символов, изображены не сами символы, а их табличные коды в квадратных скобках.

**Задание 1.** Ознакомиться с описанием лабораторной работы и заданиями.

**Задание 2.** Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;

- выполнить для этого файла шифрование;

- просмотреть в редакторе зашифрованный файл;

- просмотреть гистограммы исходного и зашифрованного текстов;

- описать гистограммы (в чем похожи, в чем отличаются) и определить, с каким смещением было выполнено шифрование;

- расшифровать зашифрованный текст:

С помощью гистограммы, после чего проверить в редакторе правильность расшифрования;

Вручную с помощью гистограмм, описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

В отчет предоставить ход проделанной работе и все использованные и созданные файлы.

**Задание 3.** Для одноалфавитного метода с заданным смещением (шифр Цезаря) следует:

- выполнить шифрование с произвольным смещением для своего исходного текста;

- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;

- расшифровать текст с помощью программы;

- дешифровать зашифрованный шифром Цезаря текст с помощью программы методом перебора смещения; указать в отчете с каким смещением был зашифрован файл.

**Задание 4.** Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько символов с известным вам текстом, зашифруйте его. Посмотрите гистограммы, опишите их, ответьте можно ли извлечь из них полезную для дешифрования информацию. Сравните с помощью редактора ваш исходный текст и зашифрованный текст и определите закон перестановки символов.

Дешифруйте файл:

- вручную и объясните ваши действия;

- с помощью программы.

**Задание 5.** Для инверсного кодирования (по дополнению до 255)

- выполните шифрование для своего произвольного файла;

- посмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;

- дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

**Задание 6.** Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

**Задание 7**. Для многоалфавитного шифрования с ключом фиксированной длины:

- выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;

- выполните шифрование и расшифрование для файла произвольно текста;

- просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

**Задание 8.** Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7.

Отчет должен содержать:

- наименование работы;

- цель работы;

- рабочие схемы, основные соотношения и расчетные формулы, таблицы;

- выводы по работе.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, какова стойкость шифра перестановки.
2. Укажите в письменной форме, какова стойкость шифра подстановки.
3. Укажите в письменной форме, какую информацию можно получить из гистограмм.

**Вопросы к лабораторной работе**

1. В чем преимущества и недостатки одноалфавитных методов?
2. Если необходимо зашифровать текст, содержащий важную информацию, какой метод вы выберете?
3. Целесообразно ли повторно применять для уже зашифрованного текста: а) метод много алфавитного шифрования; б) метод Цезаря?

# Лабораторная работа 5. Исследование различных методов защиты информации и их стойкости на основе подбора ключей, ч.1

**Цель работы:**  исследование и сравнение стойкости шифров перестановки, подстановки, гаммирования, Виженера на основе атак путем перебора всех возможных ключей.

**Содержание работы:**

1. Исследование способа вскрытия шифра, основанного на переборе всех вариантов ключа.

2. Дешифрование текста на найденных ключах.

**1. Теоретическая часть**

Для выполнения лабораторной работы необходимо запустить программу *LAB\_RAB.exe* (выдает преподаватель), используемую для шифрования/расшифрования, а также дешифрования (методом протяжки вероятного слова)файлов.

Система реализует следующие функции:

* ввод, удаление и селекция ключей пользователя;
* поддержка списка ключей;
* шифрование и расшифрование текста;
* дешифрование текста путем подбора ключей, методом протяжки вероятного слова.

Система поддерживает следующие методы криптографического преобразования информации:

* шифр замены;
* шифр перестановки;
* шифр гаммирования;
* шифр Виженера.

При запуске утилит шифрования и расшифрования у пользователя запрашивается подтверждение на правильность выбранного метода для работы и соответствия заданного ключа целям пользователя (также всегда при изменении файла в текстовом редакторе выдается запрос на сохранение изменений при каждом шаге, дальнейшее развитие которого приведет к необратимым изменениям в файле и потере изначальной информации).

*Описание интерфейса.*

* + Окно текстового редактора с широким набором дополнительных функций.
	+ Таблица всех ключей, введенных в систему с быстрым доступом для ввода, удаления или выбора текущего ключа.
	+ Список всех методов шифрования для быстрого и удобного переключения между ними.
	+ Основное меню (вверху экрана).
	+ Дополнительное меню (вызывается нажатием правой кнопки мыши).
	+ Набор вспомогательных кнопок для быстрого и удобного интерфейса.
	+ Поля вывода текущего состояния системы:
		- Текущий ключ;
		- Вероятное слово;
		- сила ключа для протяжки.

***Внимание!*** *Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся. После запуска программы абсолютно все рабочие поля пустые и необходимо провести первоначальные настройки для работоспособности системы.*

***Пример работы с программой***

1. Вводится список ключей.
2. Вводится вероятное слово (необязательно вначале, до его ввода все меню запуска протяжки все равно недоступны).
3. Выбирается необходимый метод шифрования.
4. Загружается исходный или зашифрованный файл (открываются соответствующие меню для шифрования и расшифрования).
5. Запускается необходимый процесс:
	* шифрование;
	* расшифрование;
	* протяжка вероятного слова;
	* конвертация текста.
6. Продолжение работы в любом порядке в соответствии с описанными пунктами.
7. При завершении работы не забудьте сохранить необходимые результаты (при закрытии и загрузке новых файлов система автоматически запрашивает подтверждение на запись).

**Шифрование**

1. Открыть файл.
2. Внести необходимые изменения.
3. Настроить соответствующие параметры:
	* тип шифрования;
	* ключ;
	* прочие.
4. Запустить процесс шифрования через пункт меню УТИЛИТЫ \ ЗАШИФРОВАТЬ F5.

**Внимание!** При шифровании файла все внесенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

**Дешифрование**

1. Открыть файл.
2. Произвести необходимые изменения.
3. Настроить соответствующие параметры:
	* тип шифрования;
	* прочие.
4. Запустить процесс расшифрования через пункт меню УТИЛИТЫ \ РАСШИФРОВАТЬF6.

**Внимание!** При дешифровании файла все проведенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

**Протяжка вероятного слова (дешифрование)**

**Внимание!** Мощность ключа задастся заранее в опции "сила ключа".

Длина ключа значительно влияет на время протяжки вероятного слова (в худшем случае имеем дело с логарифмическим алгоритмом).

1. Вводится вероятное слово (длинной от 1(3) до9)
2. Для отделения вновь найденных ключей от предыдущих между ними добавляется надпись "подбор".
3. Перебор ключей.
4. Расшифровывается первая вся строка текста по текущему ключу.
5. Порциями, равными длине вероятного слова, сравнивается содержимое этой строки со значением вероятного слова.
6. Если найдено хоть одно совпадение, запоминаем ключ.
7. Переходим к новому ключу.
8. Переходим к следующей строке.
9. Результаты должны содержаться в списке ключей. Если совпадений не найдено, в список ключей ничего не добавляется.

**Операции с ключами**

С базой ключей могут осуществляться следующие действия:

* добавить новый ключ;
* удалить одну запись;
* изменить активную запись;
* очистить всю таблицу введенных ключей.

**Примечание**. Под словами "работа с таблицей ключей" имеются в виду ключи, введенные для использования в двух методах (гаммирования и Виженера).

**Ключи для перестановки**

В каждый момент времени в системе может быть только один текущий ключ для перестановки.

Правила ввода ключа для перестановки:

1. При переключении в списке поддерживаемых системой методов шифрования на пункт "Перестановка" вызывается окно ввода ключа перестановки. Окно состоит из двух кнопок (Отмены и Выхода без изменений и кнопки Enter – подтверждение установленной длины ключа) и окна задания длины ключа для перестановки.
2. В окне задания длины ключа необходимо выбрать необходимую длину (параметры заменяются в пределах 1 … 9), и подтвердить желание использовать ключ именно такой длины.
3. После подтверждения в окне высветятся кнопки с цифрами на лицевой стороне (в количестве, равном длине ключа), при нажатии на кнопку происходит фиксация кнопки (ее обесцвечивание) для невозможности ее дальнейшего использования (так как все цифры в ключе перестановки должны быть неповторяющимися).
4. После перебора всех кнопок система запоминает введенный ключ, выводит его в поле ввода ключей и выходит из окна ввода ключа перестановки в окно основной программы.

**2. Задания к лабораторному занятию**

**Задание 1.** Ознакомиться с описанием лабораторной работы и заданием.

**Задание 2.** Выполнить настройку программы: выбрать метод шифрования; ввести ключи для всех методов; ввести вероятное слово; осуществить все остальные системные настройки.

**Задание 3.** Для метода замены (одноалфавитного метода):

* выбрать данный алгоритм в списке доступных методов шифрования;
* установить необходимое смещение;
* открыть произвольный файл;
* просмотреть содержимое исходного файла;
* выполнить для этого файла шифрование (при необходимости можно задать имя зашифрованного файла);
* просмотреть в редакторе зашифрованный файл;
* ввести вероятное слово;
* ввести вероятную длину ключа (кроме метода замены);
* подобрать ключ;
* выполнить расшифрование со всеми найденными ключами;
* найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
* расшифровать файл исходным ключом;
* проверить результат.

**Задание 4.** Для метода перестановки:

* выбрать метод перестановки;
* в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
* далее действия полностью соответствуют изложенным в предыдущем пункте задания.

**Задание 5.** Для метода гаммирования:

* + - выбрать метод гаммирования;
		- ввести ключ гаммирования;
		- полностью повторить п. 3.

**Задание 6.** Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, в чем недостатки метода дешифрования с использованием протяжки вероятного слова.

2. Дайте письменно все определения: шифра гаммирования, шифра подстановки, шифра Виженера, шифра перестановки, шифра многоалфавитной подстановки.

**Вопросы к лабораторной работе**

1. Чем отличается “псевдооткрытый” текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?

2. Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины “вероятного” слова?

3. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?

# Лабораторная работа 6. Исследование различных методов защиты информации и их стойкости на основе подбора ключей, ч.2

**Цель работы:**  исследование и сравнение стойкости шифров перестановки, подстановки, гаммирования, Виженера. на основе атак путем перебора всех возможных ключей.

**Содержание работы:**

1. Исследование способа вскрытия шифра, основанного на переборе всех вариантов ключа.

2. Дешифрование текста на найденных ключах.

**1. Теоретическая часть**

Для выполнения лабораторной работы необходимо запустить программу *LAB\_RAB.exe* (выдает преподаватель), используемую для шифрования/расшифрования, а также дешифрования (методом протяжки вероятного слова)файлов.

Система реализует следующие функции:

* ввод, удаление и селекция ключей пользователя;
* поддержка списка ключей;
* шифрование и расшифрование текста;
* дешифрование текста путем подбора ключей, методом протяжки вероятного слова.

Система поддерживает следующие методы криптографического преобразования информации:

* шифр замены;
* шифр перестановки;
* шифр гаммирования;
* шифр Виженера.

При запуске утилит шифрования и расшифрования у пользователя запрашивается подтверждение на правильность выбранного метода для работы и соответствия заданного ключа целям пользователя (также всегда при изменении файла в текстовом редакторе выдается запрос на сохранение изменений при каждом шаге, дальнейшее развитие которого приведет к необратимым изменениям в файле и потере изначальной информации).

*Описание интерфейса.*

* + Окно текстового редактора с широким набором дополнительных функций.
	+ Таблица всех ключей, введенных в систему с быстрым доступом для ввода, удаления или выбора текущего ключа.
	+ Список всех методов шифрования для быстрого и удобного переключения между ними.
	+ Основное меню (вверху экрана).
	+ Дополнительное меню (вызывается нажатием правой кнопки мыши).
	+ Набор вспомогательных кнопок для быстрого и удобного интерфейса.
	+ Поля вывода текущего состояния системы:
		- Текущий ключ;
		- Вероятное слово;
		- сила ключа для протяжки.

***Внимание!*** *Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся. После запуска программы абсолютно все рабочие поля пустые и необходимо провести первоначальные настройки для работоспособности системы.*

***Пример работы с программой***

1. Вводится список ключей.
2. Вводится вероятное слово (необязательно вначале, до его ввода все меню запуска протяжки все равно недоступны).
3. Выбирается необходимый метод шифрования.
4. Загружается исходный или зашифрованный файл (открываются соответствующие меню для шифрования и расшифрования).
5. Запускается необходимый процесс:
	* шифрование;
	* расшифрование;
	* протяжка вероятного слова;
	* конвертация текста.
6. Продолжение работы в любом порядке в соответствии с описанными пунктами.
7. При завершении работы не забудьте сохранить необходимые результаты (при закрытии и загрузке новых файлов система автоматически запрашивает подтверждение на запись).

**Шифрование**

1. Открыть файл.
2. Внести необходимые изменения.
3. Настроить соответствующие параметры:
	* тип шифрования;
	* ключ;
	* прочие.
4. Запустить процесс шифрования через пункт меню УТИЛИТЫ \ ЗАШИФРОВАТЬF5.

**Внимание!** При шифровании файла все внесенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

**Дешифрование**

1. Открыть файл.
2. Произвести необходимые изменения.
3. Настроить соответствующие параметры:
	* тип шифрования;
	* прочие.
4. Запустить процесс расшифрования через пункт меню УТИЛИТЫ \ РАСШИФРОВАТЬ F6.

**Внимание!** При дешифровании файла все проведенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

**Протяжка вероятного слова (дешифрование)**

**Внимание!** Мощность ключа задастся заранее в опции "сила ключа".

Длина ключа значительно влияет на время протяжки вероятного слова (в худшем случае имеем дело с логарифмическим алгоритмом).

1. Вводится вероятное слово (длинной от 1(3) до9)
2. Для отделения вновь найденных ключей от предыдущих между ними добавляется надпись "подбор".
3. Перебор ключей.
4. Расшифровывается первая вся строка текста по текущему ключу.
5. Порциями, равными длине вероятного слова, сравнивается содержимое этой строки со значением вероятного слова.
6. Если найдено хоть одно совпадение, запоминаем ключ.
7. Переходим к новому ключу.
8. Переходим к следующей строке.
9. Результаты должны содержаться в списке ключей. Если совпадений не найдено, в список ключей ничего не добавляется.

**Операции с ключами**

С базой ключей могут осуществляться следующие действия:

* добавить новый ключ;
* удалить одну запись;
* изменить активную запись;
* очистить всю таблицу введенных ключей.

**Примечание**. Под словами "работа с таблицей ключей" имеются ввиду ключи, введенные для использования в двух методах (гаммирования и Виженера).

**Ключи для перестановки**

В каждый момент времени в системе может быть только один текущий ключ для перестановки.

Правила ввода ключа для перестановки:

1. При переключении в списке поддерживаемых системой методов шифрования на пункт "Перестановка" вызывается окно ввода ключа перестановки. Окно состоит из двух кнопок (Отмены и Выхода без изменений и кнопки Enter – подтверждение установленной длины ключа) и окна задания длины ключа для перестановки.
2. В окне задания длины ключа необходимо выбрать необходимую длину (параметры заменяются в пределах 1 … 9), и подтвердить желание использовать ключ именно такой длины.
3. После подтверждения в окне высветятся кнопки с цифрами на лицевой стороне (в количестве, равном длине ключа), при нажатии на кнопку происходит фиксация кнопки (ее обесцвечивание) для невозможности ее дальнейшего использования (так как все цифры в ключе перестановки должны быть неповторяющимися).
4. После перебора всех кнопок система запоминает введенный ключ, выводит его в поле ввода ключей и выходит из окна ввода ключа перестановки в окно основной программы.

**2. Задания к лабораторному занятию**

**Задание 1.** Ознакомиться с описанием лабораторной работы и заданием.

**Задание 2.** Выполнить настройку программы: выбрать метод шифрования; ввести ключи для всех методов; ввести вероятное слово; осуществить все остальные системные настройки.

**Задание 3.** Для метода замены (одноалфавитного метода):

* выбрать данный алгоритм в списке доступных методов шифрования;
* установить необходимое смещение;
* открыть произвольный файл;
* просмотреть содержимое исходного файла;
* выполнить для этого файла шифрование (при необходимости можно задать имя зашифрованного файла);
* просмотреть в редакторе зашифрованный файл;
* ввести вероятное слово;
* ввести вероятную длину ключа (кроме метода замены);
* подобрать ключ;
* выполнить расшифрование со всеми найденными ключами;
* найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
* расшифровать файл исходным ключом;
* проверить результат.

**Задание 4.** Для метода перестановки:

* выбрать метод перестановки;
* в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
* далее действия полностью соответствуют изложенным в предыдущем пункте задания.

**Задание 5.** Для метода гаммирования:

* + - выбрать метод гаммирования;
		- ввести ключ гаммирования;
		- полностью повторить п. 3.

**Задание 6.** Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, в чем недостатки метода дешифрования с использованием протяжки вероятного слова.

2. Дайте письменно все определения: шифра гаммирования, шифра подстановки, шифра Виженера, шифра перестановки, шифра многоалфавитной подстановки.

**Вопросы к лабораторной работе**

1. Чем отличается “псевдооткрытый” текст (текст, полученный при расшифровке по ложному ключу) от настоя-щего открытого текста?

2. Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины “вероятного” слова?

3. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?

# Лабораторная работа 7. Генерация простых чисел, используемых в асимметричных системах шифрования, ч.1

**Цель**: Изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

**Содержание:**

1.Проверить на простоту два произвольных целых числа, разрядностью не менее 5.

2. Генерация простых чисел.

**1. Теоретическая часть**

Для выполнения лабораторной работы необходимо запустить программу *L\_PROST.EXE* (выдается преподавателем).На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения информации об осуществленных программой действиях), в верхней строке окна расположено главное меню, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под тестовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, “ESC” – выход из основного меню.

Для удобства в программе предусмотрена работа с мышью. В этом случае указатель подводится к нужному пункту главного меню или к нужной кнопке на панели инструментов и нажимается левая клавиша мыши, для отказа достаточно нажать клавишу “ESC”.

Кроме основных функций главного меню (“Генерация простого P”, “Поиск в интервале”, “Проверка на простоту” и так далее) панель инструментов содержит клавишу, при нажатии которой выводится информация о программе.

**Генерация простого P**

Возможность генерации простого числа; количество разрядов генерируемого числа задается пользователем (от 1 до 5).

**Поиск в интервале**

Возможность поиска простых чисел в заданном интервале. Пользователем задается: начало интервала – значение *x*, затем длина интервала – значение *L*. Поиск будет осуществляться в интервале *(x, x+L).*

При проверке на простоту каждого числа интервала сначала выполняется тест пробных делений на первые по порядку простые числа, а затем проверка по тесту Ферма. Для задания способов проверки на простоту необходимо левой клавишей мыши отметить флажок рядом с названием нужного метода, а затем указать все необходимые данные для начала поиска.

В методе пробных делений исходные данные – количество первых простых чисел для деления, а в тесте Ферма надо указать количество оснований и их значения.

По окончании расчета на экран выведутся найденные простые числа и их количество. Полную картину результатов работы можно просмотреть в пункте меню “Вывод результатов“.

**Проверка на простоту**

Возможность проверки на простоту любого числа. Необходимо ввести число и параметры расчета аналогично поиску в интервале.

**Вывод результатов**

Возможность просмотра всех результатов последней обработки. При входе в программу, когда никаких расчетов еще не производилось,

предоставляется возможность просмотра исходного файла первых простых чисел, используемых для теста пробных делений.

**Дополнительные сведения о программе**

1. При запуске утилит генерации простого числа, поиска в интервале и проверки на простоту у пользователя запрашивается подтверждение на правильность выбранного метода для работы.
2. Во время работы длительных по исполнению процедур запускается прогресс процесса и гасится окно текстового редактора. По полоске прогресса можно наблюдать и оценивать примерную скорость работы алгоритма и время окончания текущего процесса.
3. Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся.
4. Описание "горячих клавиш":

Ctrl+F1 - ‘Генерация простого P’

Ctrl+F2 - ‘Поиск в интервале’

Ctrl+F3 - ‘Проверка на простоту’

Ctrl+F4 - ‘Вывод результатов’

Ctrl+X - ‘Выход из программы’

1. В лабораторной работе из-за большого времени счета рекомендуется использовать числа не более пяти разрядов и длину интервала выбирать не более 500, количество оснований для теста Ферма – не более 5.
2. Для правильного функционирования программы, в рабочей директории (вместе с файлом *l\_prost.exe*) обязательно должны находиться файлы *prost.txt* и *work.txt.* Не рекомендуется вносить какие-либо изменения в эти текстовые файлы иначе последствия могут быть непредсказуемые.

**2. Задания к лабораторному занятию**

**Задание 1.** Проверить на простоту два произвольных целых числа, разрядностью не менее 5.

**Задание 2.** Распределение простых чисел.

2.1 Задан интервал вида *[х, x+L]*. Вычислить количество *П(х, L)* простых чисел в интервале и сравнить с величиной *L/ln(x)*. При каких условиях *П(x,L)/L* близко к*1/ln(x)*?

*х*=2000, *L*=500,

* + - * количество простых чисел для деления:5-15,
			* количество оснований:1-2.

2.2 Найти в заданном интервале все простые числа. Пусть *L(i)* – разность между двумя соседними простыми числами. Построить гистограмму для *L(i).* Вычислить выборочное среднее *L*сред. . Сравнить с величиной *ln(x)*, где *х* – середина интервала.

Интервал: (1000, 1000+300):

* + - * количество простых чисел для деления:5-20,
			* количество оснований:1-3.

2.3 Для заданного набора чисел {*k*} оценить относительную погрешность формулы для *k* -го простого числа:

*p(k)=k/ln(k), k*={10, 15, 20, 30, 35}.

**Задание 3.** Методы генерации простых чисел.

3.1 В заданном интервале построить график относительного количества натуральных чисел, проходящих “решето Эратосфена”(т. е. не делящихся на первые *k* простых).

Интервал: (500, 500+200).

Расчет производится для всех *k*<=10.

3.2 Для заданного интервала:

а) рассчитать точное количество *Р0*простых чисел в интервале, т.е. при проверке задать только тест на делимость.

Количество первых простых чисел для деления определяется из расчета: максимальное число для деления равно квадратному корню из максимального значения интервала.

б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество *Р1*вероятно простых чисел, удовлетворяющих этому тесту.

в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основаниями в тесте Ферма. Вычислить количество *Р2*вероятно простых чисел, удовлетворяющих этому тесту.

Интервал: (1500,1500 + 300).

Проанализировать полученные данные.

3.3 Известно, что в заданном интервале имеются числа Кармайкла. Найти их.

Варианты интервалов: (1050, 1050 + 100)

(1700, 1700 +100)

(2400, 2400 +100)

**Задания для самостоятельной работы**

1. Вычислить: 1812 (mod 13).

2. Вычислить: 127 (mod7).

3. Укажите в письменной форме, почему в асимметричных системах необходимо использовать простые числа.

4. Укажите в письменной форме, понятие чисел Кармайкла.

5. Укажите в письменной форме, в каких еще криптосистемах еще используются простые числа.

**Вопросы к лабораторной работе**

1. Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2?

2. Какова вероятность Р(х) того, что наугад взятое нечетное очень большое число, не превосходящее х, окажется простым?

3. Почему в асимметричных системах необходимо использовать простые числа?

# Лабораторная работа 8. Генерация простых чисел, используемых в асимметричных системах шифрования, ч.2

**Цель**: Изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

**Содержание:**

1.Проверить на простоту два произвольных целых числа, разрядностью не менее 5.

2. Генерация простых чисел.

**1. Теоретическая часть**

Для выполнения лабораторной работы необходимо запустить программу *L\_PROST.EXE* (выдается преподавателем).На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения информации об осуществленных программой действиях), в верхней строке окна расположено главное меню, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под тестовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, “ESC” – выход из основного меню.

Для удобства в программе предусмотрена работа с мышью. В этом случае указатель подводится к нужному пункту главного меню или к нужной кнопке на панели инструментов и нажимается левая клавиша мыши, для отказа достаточно нажать клавишу “ESC”.

Кроме основных функций главного меню (“Генерация простого P”, “Поиск в интервале”, “Проверка на простоту” и так далее) панель инструментов содержит клавишу, при нажатии которой выводится информация о программе.

**Генерация простого P**

Возможность генерации простого числа; количество разрядов генерируемого числа задается пользователем (от 1 до 5).

**Поиск в интервале**

Возможность поиска простых чисел в заданном интервале. Пользователем задается: начало интервала – значение *x*, затем длина интервала – значение *L*. Поиск будет осуществляться в интервале *(x, x+L).*

При проверке на простоту каждого числа интервала сначала выполняется тест пробных делений на первые по порядку простые числа, а затем проверка по тесту Ферма. Для задания способов проверки на простоту необходимо левой клавишей мыши отметить флажок рядом с названием нужного метода, а затем указать все необходимые данные для начала поиска.

В методе пробных делений исходные данные – количество первых простых чисел для деления, а в тесте Ферма надо указать количество оснований и их значения.

По окончании расчета на экран выведутся найденные простые числа и их количество. Полную картину результатов работы можно просмотреть в пункте меню “Вывод результатов“.

**Проверка на простоту**

Возможность проверки на простоту любого числа. Необходимо ввести число и параметры расчета аналогично поиску в интервале.

**Вывод результатов**

Возможность просмотра всех результатов последней обработки. При входе в программу, когда никаких расчетов еще не производилось,

предоставляется возможность просмотра исходного файла первых простых чисел, используемых для теста пробных делений.

**Дополнительные сведения о программе**

1. При запуске утилит генерации простого числа, поиска в интервале и проверки на простоту у пользователя запрашивается подтверждение на правильность выбранного метода для работы.
2. Во время работы длительных по исполнению процедур запускается прогресс процесса и гасится окно текстового редактора. По полоске прогресса можно наблюдать и оценивать примерную скорость работы алгоритма и время окончания текущего процесса.
3. Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся.
4. Описание "горячих клавиш":

Ctrl+F1 - ‘Генерация простого P’

Ctrl+F2 - ‘Поиск в интервале’

Ctrl+F3 - ‘Проверка на простоту’

Ctrl+F4 - ‘Вывод результатов’

Ctrl+X - ‘Выход из программы’

1. В лабораторной работе из-за большого времени счета рекомендуется использовать числа не более пяти разрядов и длину интервала выбирать не более 500, количество оснований для теста Ферма – не более 5.
2. Для правильного функционирования программы, в рабочей директории (вместе с файлом *l\_prost.exe*) обязательно должны находиться файлы *prost.txt* и *work.txt.* Не рекомендуется вносить какие-либо изменения в эти текстовые файлы иначе последствия могут быть непредсказуемые.

**2. Задания к лабораторному занятию**

**Задание 1.** Проверить на простоту два произвольных целых числа, разрядностью не менее 5.

**Задание 2.** Распределение простых чисел.

2.1 Задан интервал вида *[х, x+L]*. Вычислить количество *П(х, L)* простых чисел в интервале и сравнить с величиной *L/ln(x)*. При каких условиях *П(x,L)/L* близко к*1/ln(x)*?

*х*=2000, *L*=500,

* + - * количество простых чисел для деления:5-15,
			* количество оснований:1-2.

2.2 Найти в заданном интервале все простые числа. Пусть *L(i)* – разность между двумя соседними простыми числами. Построить гистограмму для *L(i).* Вычислить выборочное среднее *L*сред. . Сравнить с величиной *ln(x)*, где *х* – середина интервала.

Интервал: (1000, 1000+300):

* + - * количество простых чисел для деления:5-20,
			* количество оснований:1-3.

2.3 Для заданного набора чисел {*k*} оценить относительную погрешность формулы для *k* -го простого числа:

*p(k)=k/ln(k), k*={10, 15, 20, 30, 35}.

**Задание 3.** Методы генерации простых чисел.

3.1 В заданном интервале построить график относительного количества натуральных чисел, проходящих “решето Эратосфена”(т. е. не делящихся на первые *k* простых).

Интервал: (500, 500+200).

Расчет производится для всех *k*<=10.

3.2 Для заданного интервала:

а) рассчитать точное количество *Р0*простых чисел в интервале, т.е. при проверке задать только тест на делимость.

Количество первых простых чисел для деления определяется из расчета: максимальное число для деления равно квадратному корню из максимального значения интервала.

б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество *Р1*вероятно простых чисел, удовлетворяющих этому тесту.

в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основаниями в тесте Ферма. Вычислить количество *Р2*вероятно простых чисел, удовлетворяющих этому тесту.

Интервал: (1500,1500 + 300).

Проанализировать полученные данные.

3.3 Известно, что в заданном интервале имеются числа Кармайкла. Найти их.

Варианты интервалов: (1050, 1050 + 100)

(1700, 1700 +100)

(2400, 2400 +100)

**Задания для самостоятельной работы**

1. Вычислить: 1812 (mod 13).

2. Сформулируйте суть теста на простоту с использованием пробных делений.

3. Вычислить: 127 (mod7).

4. Укажите в письменной форме, понятие чисел Кармайкла.

5. Укажите в письменной форме, в каких еще криптосистемах еще используются простые числа.

**Вопросы к лабораторной работе**

1. Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2?

2. Какова вероятность Р(х) того, что наугад взятое нечетное очень большое число, не превосходящее х, окажется простым?

3. Почему в асимметричных системах необходимо использовать простые числа?

# Лабораторная работа 9. Исследование шифра RSA, ч.1

**Цель и содержание**: Исследовать алгоритмические основы шифрования и дешифрования шифром с открытым ключом RSA. Выполнить шифрование и расшифрование сообщения методом RSA согласно варианта.

**1. Теоретическая часть**

Суть системы с открытым ключом их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Расшифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

Криптографические системы с открытым ключом используют так называемые необратимые, или односторонние, функции.

Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

* разложение больших чисел на простые множители;
* вычисление логарифма в конечном поле;
* вычисление корней алгебраических уравнений.

Алгоритмы криптосистемы с открытым ключом можно использовать в трех назначениях:

1. как самостоятельные средства защиты передаваемых и хранимых данных;
2. как средства для распределения ключей;
3. средства аутентификации пользователей (электронная подпись).

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Название системы RSA происходит из первых букв фамилий авторов Рона Ривеста, Ади Шамира и Леонарда Эйдельмана.

Она основана на использовании того факта, что легко перемножить два больших простых числа, но в то же время крайне сложно разложить на множители их произведение.

В результате произведение может быть использовано в качестве элемента открытого ключа. Исходные простые числа необходимы для расшифрования, при этом задача их восстановления является вычислительно очень сложной.

Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению на множители. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин его популярности. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм RSA используется во многих стандартах, среди которых SSL, S-HHTP, S-MIME, S/WAN, STT и РСТ.

Под простым числом понимают такое число, которое делится только на 1 и на само себя. Взаимно простыми числами называют такие числа, которые не имеют ни одного общего делителя, кроме 1». Под результатом операции **i mod j** понимают остаток от целочисленного деления i на j.

Чтобы использовать алгоритм RSA, надо сначала:

**1. Сгенерировать открытый и секретный ключи**, выполнив следующие шаги:

- выбрать два очень больших простых числа **p** и **q**

- определить **n** как результат умножения p на q (n =р•q).,

- выбрать большое случайное число **d**. Оно должно быть взаимно простым с результатом умножения (р - l) • (q - 1).

- определить такое число **е,** для которого является истинным следующее соотношение**:** e•d mod((p - l) • (q - 1)) =1.

- назвать открытым ключом числа **е и n,** а секретным ключом -числа **d и n**.

**2. Зашифровать данные по известному открытому ключу{е,n}.**

Для этого необходимо**:**

- разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа М(i) =0,1,..n-1;

- зашифровать текст, рассматриваемый как последовательность чисел M(i) по формуле C(i) = M(i)emod(n).

**3. Расшифровать данные, используя секретный ключ *{d, n}*.**

Для этого необходимо:

- M(i) = С (i)dmod(n).

- в результате будет получено множество чисел M(i), которое представляет собой исходный текст.

**Пример использования метода RSA**

Для шифрования сообщения «ЕДА». Для простоты будем использовать очень маленькие числа (на практике используются намного большие числа),

1. Выберем р = 3 и *q=*11.
2. Определим *п=* 3 • 11 =33.
3. Найдем (р- l) • (q- 1) = 20. Следовательно, в качестве *d* выберем любое число, которое является взаимно простым с 20, например *d =*3.
4. Выберем число *е.* В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение e • 3 mod(20) = 1. например *е* =7,
5. Представим шифруемое сообщение как последовательность целых чисел в диапазоне 0... 32. Пусть буква Е изображается числом 6, буква Д - числом 5, а буква А - числом 1. Тогда сообщение можно представить в виде последовательности чисел651.
6. Зашифруем сообщение, используя ключ {7, 33}. С1 = 67 mod(33) = 279936 mod(33) =30;

С2= 57 mod(33) = 78125 mod(33) = 14;

С3= l7mod(33) = 1 mod(33)= 1;

1. Попытаемся расшифровать сообщение (30,14,1), полученное в результате зашифрования по известному ключу, на основе секретного ключа {3,33}:

М, = 303 mod(33) = 27000 mod(33) - 6;

М2 = 143 mod(33) = 2744 mod(33) = 5;

М3 = 13 mod (33) = 1 mod(33) = 1;

1. Таким образом, в результате расшифрования сообщения получено исходное сообщение «ЕДА».

**2. Задания для лабораторной работы**

Зашифровать информацию по методу **RSA** для последующей передачи, а затем расшифровать его. Для шифрования (дешифрования) использовать таблицу 1. Каждому студенту выдать по 2 варианта.



**Задания для самостоятельной работы**

1. Укажите в письменной форме, можно ли по известному ключу получить секретный ключ.
2. Укажите в письменной форме, для решения каких задач используются криптосистемы с открытым ключом.
3. Укажите в письменной форме, где используется алгоритм RSA.

**Вопросы к лабораторной работе**

1. Какова особенность методов криптографической защиты с открытым ключом?
2. Какой ключ используется для зашифрования?
3. Какой ключ используется для расшифрования?

# Лабораторная работа 10. Исследование шифра RSA, ч.2

**Цель и содержание**: Исследовать алгоритмические основы шифрования и дешифрования шифром с открытым ключом RSA. Выполнить шифрование и расшифрование сообщения методом RSA согласно варианта.

**1. Теоретическая часть**

Суть системы с открытым ключом их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Расшифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

Криптографические системы с открытым ключом используют так называемые необратимые, или односторонние, функции.

Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

* разложение больших чисел на простыемножители;
* вычисление логарифма в конечномполе;
* вычисление корней алгебраическихуравнений.

Алгоритмы криптосистемы с открытым ключом можно использовать в трех назначениях:

1. как самостоятельные средства защиты передаваемых и хранимых данных;
2. как средства для распределения ключей;
3. средства аутентификации пользователей (электронная подпись).

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Название системы RSA происходит из первых букв фамилий авторов Рона Ривеста, Ади Шамира и Леонарда Эйдельмана.

Она основана на использовании того факта, что легко перемножить два больших простых числа, но в то же время крайне сложно разложить на множители их произведение.

В результате произведение может быть использовано в качестве элемента открытого ключа. Исходные простые числа необходимы для расшифрования, при этом задача их восстановления является вычислительно очень сложной.

Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению на множители. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин его популярности. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм RSA используется во многих стандартах, среди которых SSL, S-HHTP, S-MIME, S/WAN, STT и РСТ.

Под простым числом понимают такое число, которое делится только на 1 и на само себя. Взаимно простыми числами называют такие числа, которые не имеют ни одного общего делителя, кроме 1». Под результатом операции **i mod j** понимают остаток от целочисленного деления i на j.

Чтобы использовать алгоритм RSA, надо сначала:

**1. Сгенерировать открытый и секретный ключи**, выполнив следующие шаги:

- выбрать два очень больших простых числа **p** и **q**

- определить **n** как результат умножения p на q (n =р•q).,

- выбрать большое случайное число **d**. Оно должно быть взаимно простым с результатом умножения (р - l) • (q - 1).

- определить такое число **е,** для которого является истинным следующее соотношение**:** e•d mod((p - l) • (q - 1)) =1.

- назвать открытым ключом числа **е и n,** а секретным ключом -числа **d и n**.

**2. Зашифровать данные по известному открытому ключу{е,n}.**

Для этого необходимо**:**

- разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа М(i) =0,1,..n-1;

- зашифровать текст, рассматриваемый как последовательность чисел M(i) по формуле C(i) = M(i)emod(n).

**3. Расшифровать данные, используя секретный ключ *{d, n}*.**

Для этого необходимо:

- M(i) = С (i)dmod(n).

- в результате будет получено множество чисел M(i), которое представляет собой исходный текст.

**Пример использования метода RSA**

Для шифрования сообщения «ЕДА». Для простоты будем использовать очень маленькие числа (на практике используются намного большие числа),

1. Выберем р = 3 и *q=*11.
2. Определим *п=* 3 • 11 =33.
3. Найдем (р- l) • (q- 1) = 20. Следовательно, в качестве *d* выберем любое число, которое является взаимно простым с 20, например *d =*3.
4. Выберем число *е.* В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение e • 3 mod(20) = 1. например *е* =7,
5. Представим шифруемое сообщение как последовательность целых чисел в диапазоне 0... 32. Пусть буква Е изображается числом 6, буква Д - числом 5, а буква А - числом 1. Тогда сообщение можно представить в виде последовательности чисел651.
6. Зашифруем сообщение, используя ключ {7, 33}. С1 = 67 mod(33) = 279936 mod(33) =30;

С2= 57 mod(33) = 78125 mod(33) = 14;

С3= l7mod(33) = 1 mod(33)= 1;

1. Попытаемся расшифровать сообщение (30,14,1), полученное в результате зашифрования по известному ключу, на основе секретного ключа {3,33}:

М, = 303 mod(33) = 27000 mod(33) - 6;

М2 = 143 mod(33) = 2744 mod(33) = 5;

М3 = 13 mod (33) = 1 mod(33) = 1;

1. Таким образом, в результате расшифрования сообщения получено исходное сообщение «ЕДА».

**2. Задания для лабораторной работы**

Зашифровать информацию по методу **RSA** для последующей передачи, а затем расшифровать его. Для шифрования (дешифрования) использовать таблицу 1. Каждому студенту выдать по 2 варианта.



**Задания для самостоятельной работы**

1. Укажите в письменной форме, можно ли по известному ключу получить секретный ключ.
2. Укажите в письменной форме, для решения каких задач используются криптосистемы с открытым ключом.
3. Укажите в письменной форме, где используется алгоритм RSA.

**Вопросы к лабораторной работе**

1. Какова особенность методов криптографической защиты с открытым ключом?
2. Какой ключ используется для зашифрования?
3. Какой ключ используется для расшифрования?

# Лабораторная работа 11. Исследование принципов хеширования сообщений, ч.1

**Цель:** исследовать метод Х-509 для получения хеш-кода сообщения.

**Содержание:**

1. Изучить теоретический материал;

2. Получить хеш-код сообщения согласно варианта.

**1. Теоретическая часть**

Хэш-функция представляет собой криптографическую функцию от сообщения произвольной длины, значение которой зависит сложным образом от каждого бита сообщения.

Хэш-функция реализуется обычно в виде некоторого итеративного механизма, который позволяет вычислить для сообщения *М* произвольной длины так называемый хэш-код *Н(М)* фиксированного размера *т* (обычно *т =* 128 бит). Этот код является подобием «слепка» сообщения *М.*

В системах электронной цифровой подписи вместо подписывания сообщений (например, документов большого объема) используется подписывание соответствующих им хэш-функций.

**Основные требования к хэш-функциям:**

1. Вычислительно неосуществимо нахождение сообщения М по его хэш- коду.
2. Вычислительно неосуществимо нахождение двух различных сообщений с равными значениями хэш-функции
3. Существуют различные функции хеширования, например SHA, MD5, ГОСТ Р 34.11-94 и др. В качестве примера выбрана хеш-функция из рекомендаций МККТТХ.509.

**Пример получения хеш-кода сообщения**

1. Пусть хешируемое слово ДВА . Выберем коэффициенты р = 7, q=3;

Вектор инициализации H0 выберем равным 9 (выбираем случайным образом) Определим *п* = *pq* = 7 • 3 =21

Слово ДВА в числовом эквиваленте можно представить как 531 (по номерам букв в алфавите).

Тогда хеш-код сообщения 531 получается следующим образом:

**1яитерация:**

М1+Н0=5+9=14; [М1+Н0]2mod(21)=142mod(21)=7=H1

**2яитерация:**

М2+Н1=3+7=10; [М2+Н1]2 mod(21)=102mod(21)=16=H2

**3яитерация:**

М3+Н2=1+16=17; [М3+Н2]2 mod(21)=172 mod(21)=16=H3

В итоге получаем хеш-код сообщения, равный 16.

**2.Задания к лабораторной работе**

**Задание 1**. Рассчитать хеш-код для сообщения, согласно варианта (вариант выдает преподаватель, каждому студенту - по 2 варианта). Вектор инициализации H0студент выбирает самостоятельно.





**Задание 2.** Рассчитать хеш-код сообщения для выданных вариантов, с другим вектором инициализацииH0. Сравнить результаты, сделать выводы.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, какая длина хеш-кода используется в ГОСТ.
2. Дайте письменно определения понятиям: хэш-код, однонаправленной функции, хеш-функции.

**Вопросы к лабораторной работе**

1. Что из себя представляет хеш-код сообщения?
2. Почему в системах ЭП подписывают не само сообщение, а его хеш-код?

# Лабораторная работа 12. Исследование принципов хеширования сообщений, ч.2

**Цель:** исследовать метод Х-509 для получения хеш-кода сообщения.

**Содержание:**

1. Изучить теоретический материал;

2. Получить хеш-код сообщения согласно варианта.

**1. Теоретическая часть**

Хэш-функция представляет собой криптографическую функцию от сообщения произвольной длины, значение которой зависит сложным образом от каждого бита сообщения.

Хэш-функция реализуется обычно в виде некоторого итеративного механизма, который позволяет вычислить для сообщения *М* произвольной длины так называемый хэш-код *Н(М)* фиксированного размера *т* (обычно *т =* 128 бит). Этот код является подобием «слепка» сообщения *М.*

В системах электронной цифровой подписи вместо подписывания сообщений (например, документов большого объема) используется подписывание соответствующих им хэш-функций.

**Основные требования к хэш-функциям:**

1. Вычислительно неосуществимо нахождение сообщения М по его хэш- коду.
2. Вычислительно неосуществимо нахождение двух различных сообщений с равными значениями хэш-функции
3. Существуют различные функции хеширования, например SHA, MD5, ГОСТ Р 34.11-94 и др. В качестве примера выбрана хеш-функция из рекомендаций МККТТХ.509.

**Пример получения хеш-кода сообщения**

1. Пусть хешируемое слово ДВА . Выберем коэффициенты р = 7, q=3;

Вектор инициализации H0 выберем равным 9 (выбираем случайным образом) Определим *п* = *pq* = 7 • 3 =21

Слово ДВА в числовом эквиваленте можно представить как 531 (по номерам букв в алфавите).

Тогда хеш-код сообщения 531 получается следующим образом:

**1яитерация:**

М1+Н0=5+9=14; [М1+Н0]2mod(21)=142mod(21)=7=H1

**2яитерация:**

М2+Н1=3+7=10; [М2+Н1]2 mod(21)=102mod(21)=16=H2

**3яитерация:**

М3+Н2=1+16=17; [М3+Н2]2 mod(21)=172 mod(21)=16=H3

В итоге получаем хеш-код сообщения, равный 16.

**2.Задания к лабораторной работе**

**Задание 1**. Рассчитать хеш-код для сообщения, согласно варианта (вариант выдает преподаватель, каждому студенту - по 2 варианта). Вектор инициализации H0студент выбирает самостоятельно.





**Задание 2.** Рассчитать хеш-код сообщения для выданных вариантов, с другим вектором инициализацииH0. Сравнить результаты, сделать выводы.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, какая длина хеш-кода используется в ГОСТ.
2. Дайте письменно определения понятиям: хэш-код, однонаправленной функции, хеш-функции.

**Вопросы к лабораторной работе**

1. Что из себя представляет хеш-код сообщения?
2. Почему в системах ЭП подписывают не само сообщение, а его хеш-код?

# Лабораторная работа 13. Исследование процедур формирования и проверки электронной подписи, ч.1

**Цель:** Знакомство с основными положениями федеральной целевой программы “Электронная Россия”. Ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной подписи (ЭП), исследование принципа формирования и проверки подлинности ЭП.

**1. Теоретическая часть**

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе.

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является *электронная подпись.*

Первая схема ЭП - *RSA* - была разработана еще в конце 1970-х годов. Однако проблема подтверждения авторства стала актуальной настолько, что потребовалось установление стандарта, только в 1990-х годах, во время взрывного роста глобальной сети Интернет и массового распространения электронной торговли и оказания услуг. Именно по указанной причине стандарты ЭП (тогда ЭЦП) в России и США были приняты практически одновременно, в 1994году.

Из предложенных криптологами схем ЭП наиболее удачными оказались *RSA* и схема Эль-Гамаля. Но первая из них была запатентована в США и ряде других стран (патент на *RSA* прекратил свое действие совсем недавно). Во второй же схеме существует большое количество ее возможных модификаций, и все их запатентовать весьма затруднительно. Именно по этой причине схема ЭП Эль-Гамаля осталась по большей части свободной от патентов. Кроме того, эта схема имеет и определенные практические преимущества: размер блоков, которыми оперируют алгоритмы, и соответственно размер ЭП в ней оказались значительно меньше, чем в *RSA*, при той же самой стойкости. Именно поэтому стандарты ЭП России и США вначале базировались на схеме Эль-Гамаля.

Законы об ЭП сегодня имеют уже более 60-ти государств. В этом списке значится и Россия. Закон “Об электронной цифровой подписи”, был принят в 2002 году должен был оказать стимулирующее воздействие на развитие отечественной электронной коммерции, особенно если в соответствие с ним будут своевременно приведены иные нормативно-правовые акты.

* Правительство РФ финансово поддерживает осуществление федеральной целевой программы «Электронная Россия».
* Принят закон «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации».
* Ещевянваре2001г.правлениеПенсионногофондапостановлением

«О введении в системе Пенсионного фонда РФ криптографической защиты информации и электронной цифровой подписи» регламентировало регистрацию и подключение юридических и физических лиц к системе своего электронного документооборота.

* В 2002 г. вышел приказ МНС России «Об утверждении порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи», благодаря которому сегодня любое физическое или юридическое лицо может связаться с налоговой инспекцией, используя защищенную электронную почту.

В 2004 г. были утверждены поправки к статьям 13 и 15 закона «О бухгалтерском учете», согласно которым бухгалтерская отчетность предприятия может вестись, храниться и предоставляться в контролирующие органы в электронном виде. В настоящее время действует ФЗ «Об электронной подписи» №63-ФЗ от 06.04.2011г. Современный отечественный стандарт ЭП ГОСТ Р 34.10-2012 был принят в 2012 г. До этого в РФ действовали стандарты электронной подписи ГОСТ Р 34.10-1994 и ГОСТ Р 34.10-2001. Необходимость разработки стандарта ГОСТ Р 34.10-2012 была вызвана потребностью в повышении стойкости ЭП к несанкционированным изменениям. Стойкость ЭП в новом стандарте основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, определенной над конечным полем *Fp*, а также на повышенной стойкости используемой хеш-функции по ГОСТ Р 34.11-2012 с размером хеша 256 или 512 бит.

**Принцип построения ЭП**

Асимметрия ролей отправителя и получателя в схемах ЭП требует наличия двух тесно связанных ключей: *секретного*, или ключа подписи, и *открытого*, или ключа проверки подписи.

Любая схема ЭП обязана определить три следующих алгоритма:

* алгоритм генерации ключевой пары для подписи и ее проверки;
* алгоритм формирования подписи;
* алгоритм проверки подписи.

ЭП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает основными ее достоинствами:

* + удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
	+ не дает самому этому лицу возможность отказаться от обязазельств, связанных с подписанным текстом;
	+ гарантирует целостность подписанного текста.

ЭП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом, и включает две процедуры:

* процедуру формирования подписи, в которой используется секретный ключ отправителя сообщения;
* процедуру проверки подписи, в которой используется открытый ключ отправителя.

Процедура формирования подписи

При формировании ЭП, отправитель, прежде всего, вычисляет хэш- функцию *h(M)* подписываемого текста *М*. Вычисленное значения хэш- функции *h(M)* представляет собой один короткий блок информации *m* , характеризующий весь текст *М* в целом. Затем значение *m* шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭП для данного текста *М*.

Процедура проверки подписи

При проверке ЭП, получатель сообщения снова вычисляет хэш- функцию *m = h(M)* принятого по каналу текста *М*, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению *m* хэш-функции.

Принципиальным моментом в системе ЭП является невозможность подделки ЭП пользователя без знания его секретного ключа.

Каждая подпись, как правило, содержит следующую информацию:

* дату подписи;
* срок окончания действия ключа данной подписи;
* информацию о лице, подписавшем текст;
* идентификатор подписавшего (имя открытого ключа);
* собственно цифровую подпись.

**Алгоритм цифровой подписи *DSA***

Алгоритм электронной подписи *DSA (Digital Signature Authorization)* предложен в 1991 году в США.

Отправитель и получатель электронного документа используют при вычислении большие целые числа:

*G, P – простые числа по L-бит каждое (L = 512 .. 1024 бит); q – простое число длиной 160 бит делитель числа (P –1).*

*G, P, q* являются открытыми и могут быть общими для всех пользователей сети.

*Описание алгоритма*

1. Отправитель выбирает случайное целое число *Х, 1< X< q.* Число *Х* является *секретным ключом* отправителя для формирования электронной подписи.
2. Отправитель вычисляет значение

*Y = GX modP.*

Число *Y* является *открытым ключом* для проверки подписи отправителя и предается всем получателям документа.

1. Для того чтобы подписать документ *М*, отправитель хэширует его в целое хэш-значение *m:*

*m = h(M), 1<m<q.*

Затем генерирует случайное целое число *К, 1<K<q* и вычисляет число *r*: *r = (GK mod P) mod q.*

1. При помощи секретного ключа Х отправитель вычисляет число s:

*s = ((m + r · X)/ K) mod q.*

Пара чисел *r , s* образуют ЭП*S = (r , s )* под документом *М*.

1. Доставленное получателю сообщение вместе с подписью представляет собой тройку чисел *[M, r, s].* Прежде всего получатель проверяет выполнение соотношений:

*0<r<q;0<s<q.*

1. Далее получатель вычисляет значения:

*w = 1/s mod q;*

*m=h(M) – хэш-значение;*

*u1 = (m·w) modq;*

*u2 = (r·w ) modq.*

Затем при помощи открытого ключа *Y* вычисляется значение

*v = (( Gu1 · Yu2 ) mod P) mod q,*

и проверяется выполнение равенства *v = r.* Если оно выполняется, то подпись признается подлинной, так как можно строго математически доказать, что последнее равенство будет выполняться тогда и только тогда, когда подпись *S = (r ,s)* под документом *M* получена при помощи именно того секретного ключа *X*, из которого был получен открытый ключ *Y*.

**2.Задания к лабораторной работе**

**Задание 1**. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы “Электронная Россия”, а также со сведениями о порядке использования и действующих алгоритмах постановки цифровой.

Запустить программу *labWork6.exe****,*** предназначенную для демонстрации порядка постановки и проверки ЭП (выдает преподаватель).

**Задание 2.** Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

**Задание 3.**  Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

**Задание 4.** Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭП и восстановить исходный текст сообщения.

**Задание 5.** Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и формирования ЭП.

**Задание 6.** Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, какая информация содержится в ЭП.

2. Укажите в письменной форме, стандарты ЭП, действующие в Российской федерации.

3. Укажите в письменной форме, на каких принципах основана криптостойкость современных алгоритмов ЭП.

4. Укажите в письменной форме, пример реализации алгоритма ЭП (*RSA, El-Gamal, DSA*).

**Вопросы к лабораторной работе**

1. В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭП?

2. Какие вы знаете стандарты хэш-функций, действующие в Российской федерации?

3. Каковы процедуры постановки и проверки ЭП?

# Лабораторная работа 14. Исследование процедур формирования и проверки электронной подписи, ч.2

**Цель:** Знакомство с основными положениями федеральной целевой программы “Электронная Россия”. Ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной подписи (ЭП), исследование принципа формирования и проверки подлинности ЭП.

**1. Теоретическая часть**

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе.

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является *электронная подпись.*

Первая схема ЭП - *RSA* - была разработана еще в конце 1970-х годов. Однако проблема подтверждения авторства стала актуальной настолько, что потребовалось установление стандарта, только в 1990-х годах, во время взрывного роста глобальной сети Интернет и массового распространения электронной торговли и оказания услуг. Именно по указанной причине стандарты ЭП (тогда ЭЦП) в России и США были приняты практически одновременно, в 1994году.

Из предложенных криптологами схем ЭП наиболее удачными оказались *RSA* и схема Эль-Гамаля. Но первая из них была запатентована в США и ряде других стран (патент на *RSA* прекратил свое действие совсем недавно). Во второй же схеме существует большое количество ее возможных модификаций, и все их запатентовать весьма затруднительно. Именно по этой причине схема ЭП Эль-Гамаля осталась по большей части свободной от патентов. Кроме того, эта схема имеет и определенные практические преимущества: размер блоков, которыми оперируют алгоритмы, и соответственно размер ЭП в ней оказались значительно меньше, чем в *RSA*, при той же самой стойкости. Именно поэтому стандарты ЭП России и США вначале базировались на схеме Эль-Гамаля.

Законы об ЭП сегодня имеют уже более 60-ти государств. В этом списке значится и Россия. Закон “Об электронной цифровой подписи”, был принят в 2002 году должен был оказать стимулирующее воздействие на развитие отечественной электронной коммерции, особенно если в соответствие с ним будут своевременно приведены иные нормативно-правовые акты.

* Правительство РФ финансово поддерживает осуществление федеральной целевой программы «Электронная Россия».
* Принят закон «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации».
* Ещевянваре2001г.правлениеПенсионногофондапостановлением

«О введении в системе Пенсионного фонда РФ криптографической защиты информации и электронной цифровой подписи» регламентировало регистрацию и подключение юридических и физических лиц к системе своего электронного документооборота.

* В 2002 г. вышел приказ МНС России «Об утверждении порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи», благодаря которому сегодня любое физическое или юридическое лицо может связаться с налоговой инспекцией, используя защищенную электронную почту.

В 2004 г. были утверждены поправки к статьям 13 и 15 закона «О бухгалтерском учете», согласно которым бухгалтерская отчетность предприятия может вестись, храниться и предоставляться в контролирующие органы в электронном виде. В настоящее время действует ФЗ «Об электронной подписи» №63-ФЗ от 06.04.2011г. Современный отечественный стандарт ЭП ГОСТ Р 34.10-2012 был принят в 2012 г. До этого в РФ действовали стандарты электронной подписи ГОСТ Р 34.10-1994 и ГОСТ Р 34.10-2001. Необходимость разработки стандарта ГОСТ Р 34.10-2012 была вызвана потребностью в повышении стойкости ЭП к несанкционированным изменениям. Стойкость ЭП в новом стандарте основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, определенной над конечным полем *Fp*, а также на повышенной стойкости используемой хеш-функции по ГОСТ Р 34.11-2012 с размером хеша 256 или 512 бит.

**Принцип построения ЭП**

Асимметрия ролей отправителя и получателя в схемах ЭП требует наличия двух тесно связанных ключей: *секретного*, или ключа подписи, и *открытого*, или ключа проверки подписи.

Любая схема ЭП обязана определить три следующих алгоритма:

* алгоритм генерации ключевой пары для подписи и ее проверки;
* алгоритм формирования подписи;
* алгоритм проверки подписи.

ЭП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает основными ее достоинствами:

* + удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
	+ не дает самому этому лицу возможность отказаться от обязазельств, связанных с подписанным текстом;
	+ гарантирует целостность подписанного текста.

ЭП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом, и включает две процедуры:

* процедуру формирования подписи, в которой используется секретный ключ отправителя сообщения;
* процедуру проверки подписи, в которой используется открытый ключ отправителя.

Процедура формирования подписи

При формировании ЭП, отправитель, прежде всего, вычисляет хэш- функцию *h(M)* подписываемого текста *М*. Вычисленное значения хэш- функции *h(M)* представляет собой один короткий блок информации *m* , характеризующий весь текст *М* в целом. Затем значение *m* шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭП для данного текста *М*.

Процедура проверки подписи

При проверке ЭП, получатель сообщения снова вычисляет хэш- функцию *m = h(M)* принятого по каналу текста *М*, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению *m* хэш-функции.

Принципиальным моментом в системе ЭП является невозможность подделки ЭП пользователя без знания его секретного ключа.

Каждая подпись, как правило, содержит следующую информацию:

* дату подписи;
* срок окончания действия ключа данной подписи;
* информацию о лице, подписавшем текст;
* идентификатор подписавшего (имя открытого ключа);
* собственно цифровую подпись.

**Алгоритм цифровой подписи *DSA***

Алгоритм электронной подписи *DSA (Digital Signature Authorization)* предложен в 1991 году в США.

Отправитель и получатель электронного документа используют при вычислении большие целые числа:

*G, P – простые числа по L-бит каждое (L = 512 .. 1024 бит); q – простое число длиной 160 бит делитель числа (P –1).*

*G, P, q* являются открытыми и могут быть общими для всех пользователей сети.

*Описание алгоритма*

1. Отправитель выбирает случайное целое число *Х, 1< X< q.* Число *Х* является *секретным ключом* отправителя для формирования электронной подписи.
2. Отправитель вычисляет значение

*Y = GX modP.*

Число *Y* является *открытым ключом* для проверки подписи отправителя и предается всем получателям документа.

1. Для того чтобы подписать документ *М*, отправитель хэширует его в целое хэш-значение *m:*

*m = h(M), 1<m<q.*

Затем генерирует случайное целое число *К, 1<K<q* и вычисляет число *r*: *r = (GK mod P) mod q.*

1. При помощи секретного ключа Х отправитель вычисляет число s:

*s = ((m + r · X)/ K) mod q.*

Пара чисел *r , s* образуют ЭП*S = (r , s )* под документом *М*.

1. Доставленное получателю сообщение вместе с подписью представляет собой тройку чисел *[M, r, s].* Прежде всего получатель проверяет выполнение соотношений:

*0<r<q;0<s<q.*

1. Далее получатель вычисляет значения:

*w = 1/s mod q;*

*m=h(M) – хэш-значение;*

*u1 = (m·w) modq;*

*u2 = (r·w ) modq.*

Затем при помощи открытого ключа *Y* вычисляется значение

*v = (( Gu1 · Yu2 ) mod P) mod q,*

и проверяется выполнение равенства *v = r.* Если оно выполняется, то подпись признается подлинной, так как можно строго математически доказать, что последнее равенство будет выполняться тогда и только тогда, когда подпись *S = (r ,s)* под документом *M* получена при помощи именно того секретного ключа *X*, из которого был получен открытый ключ *Y*.

**2.Задания к лабораторной работе**

**Задание 1**. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы “Электронная Россия”, а также со сведениями о порядке использования и действующих алгоритмах постановки цифровой.

Запустить программу *labWork6.exe****,*** предназначенную для демонстрации порядка постановки и проверки ЭП (выдает преподаватель).

**Задание 2.** Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

**Задание 3.**  Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

**Задание 4.** Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭП и восстановить исходный текст сообщения.

**Задание 5.** Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и формирования ЭП.

**Задание 6.** Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

**Задания для самостоятельной работы**

1. Укажите в письменной форме, какая информация содержится в ЭП.

2. Укажите в письменной форме, стандарты ЭП, действующие в Российской федерации.

3. Укажите в письменной форме, на каких принципах основана криптостойкость современных алгоритмов ЭП.

4. Укажите в письменной форме, пример реализации алгоритма ЭП (*RSA, El-Gamal, DSA*).

**Вопросы к лабораторной работе**

1. В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭП?

2. Какие вы знаете стандарты хэш-функций, действующие в Российской федерации?

3. Каковы процедуры постановки и проверки ЭП?

# Лабораторная работа 15. Исследование принципов формирования общего секретного ключа на основе схемы Диффи-Хеллмана, ч.1

**Цель:** сформировать практические умения исследования этапов формирования секретного ключа на основе схемы Диффи-Хеллмана, изучения ее характеристик и умений делать самостоятельные выводы по результатам исследований.

**Содержание:**

1. Разобрать пример генерации секретного ключа, проверки ключа.

2. Выполнить генерацию и проверку правильности выработки ключа согласно варианта.

**1. Теоретическая часть**

Данный протокол позволяет пользователям обмениваться ключами по открытым (незащищенным) каналам связи. Сформированный таким образом общий секретный ключ используется для симметричного шифрования. Генерацию общего ключа шифрования проводится только для пары абонентов сети.

 Схема данного способа проиллюстрирована на рис. 6.5.



Рисунок 6.5 - Схема симметричного шифрования секретным ключом, сформированным по протоколу Диффи-Хеллмана (М – открытое сообщение, Е - криптограмма)

Безопасность протокола обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле. Суть метода Диффи-Хеллмана заключается в следующем (рис. 1). Каждой паре абонентов в открытом виде рассылаются большие простые числа Р и λ: Р – модуль расчетов, λ – любое простое число от 2 до р-1. Числа Р и λ могут не хранится в секрете. Как правило эти значения являются общими для всех пользователей сети.

Вычисление открытого ключа уа

Вычисление открытого ключа уb

Вычисление общего ключа Кab

Вычисление общего ключа Кba

Пользователь В

Секретный ключ хb

Пользователь А

Секретный ключ ха

Незащищенный канал

Общий ключ Кab

Общий ключ Кba

уа

уb

Рисунок 1 - Схема открытого распределения ключей Диффи-Хеллмана

Пользователи А и В генерируют независимо друг от друга свои секретные ключи ха и хb (случайные большие целые числа).

Затем пользователь А вычисляет на основании своего секретного ключа ха открытый ключ как уа= λ Ха mod Р.

Пользователь В производит аналогичные вычисления уb= λ Хbmod Р.

Затем пользователи А и В обмениваются своими открытыми ключами уа и уb по незащищенному каналу и используют их для вычисления общего ключа.

Пользователь А вычисляет: Кab = уbХаmod Р = (λ Хb) Ха mod Р.

Пользователь В вычисляет: Кba = уа Хbmod Р = (λ Хa) Хbmod Р.

Как видим Кab = Кba , общий секретный ключ получен.

Злоумышленник, перехвативший значения открытых ключей уа и уb, не может вычислить общий ключ Кab, потому что он не имеет соответствующих значений секретных ключей Ха и Хb. Благодаря использованию однонаправленной функции операция вычисления открытого ключа необратима, то есть невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи-Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом – применяя симметричное шифрование с использованием общего секретного ключа.

Протокол Диффи-Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что любое хранение секретов повышает вероятность попадания их в руки конкурентов или злоумышленников.

Кроме этого, протокол Диффи-Хеллмана позволяет реализовать метод комплексной защиты конфиденциальности и аутентичности передаваемых данных, то есть использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования данных.

Важным достоинством протокола распределения ключей Диффи-Хеллмана является то, что он позволяет обойтись без защищенного канала для доставки ключей. Однако необходимо иметь гарантию того, что пользователь А получил открытый ключ именно от пользователя Б, и наоборот. Эта проблема решается с помощью сертификатов открытых ключей, создаваемых и распространяемых центрами сертификации СА (CertificationAuthority) в рамках инфраструктуры управления открытыми ключами PKI (PublicKeyInfrastructure).

Пример.

Пусть р=31, λ = 7.

Пользователь А сгенерировал случайное число ха = 11.

Пользователь В сгенерировал случайное число хb = 13.

Затем пользователь А вычисляет свой открытый ключ как уа  = λ Ха modp = 711 mod 31 = 20, и передает уа по открытому каналу пользователю В.

Пользователь В вычисляет свой открытый ключ как уb = λ Хб modp = 713 mod 31 = 19 и передает уbпо открытому каналу пользователю А.

Затем оба пользователя вычисляют общий секретный ключ.

Пользователь А: Каb= (уб )Хаmodp = 1911 mod 31 = 10.

Пользователь В: Кbа = (уа )Хбmodp = 2013 mod 31 = 10.

Общий ключ сформирован и равен 10.

**2. Задания к лабораторной работе**

**Задание 1**. В лабораторной работе исходные данные из табл. 1, а именно р, λ, ха, хb необходимо выбрать в соответствии со своим вариантом задания (варианты назначает преподаватель: по два варианта – на каждого студента).

Таблица 1 – Варианты заданий

| Номер варианта | р | λ | Ха | Хb | Номер варианта | р | λ | Ха | Хb |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 19 | 11 | 5 | 13 | 16 | 41 | 31 | 9 | 3 |
| 2 | 23 | 5 | 14 | 16 | 17 | 43 | 7 | 12 | 7 |
| 3 | 29 | 13 | 9 | 4 | 18 | 47 | 23 | 5 | 8 |
| 4 | 31 | 7 | 4 | 8 | 19 | 53 | 29 | 3 | 6 |
| 5 | 37 | 13 | 6 | 11 | 20 | 59 | 5 | 7 | 15 |
| 6 | 41 | 19 | 4 | 9 | 21 | 19 | 5 | 8 | 13 |
| 7 | 43 | 17 | 11 | 8 | 22 | 23 | 17 | 4 | 14 |
| 8 | 47 | 23 | 6 | 4 | 23 | 29 | 23 | 3 | 6 |
| 9 | 53 | 13 | 8 | 5 | 24 | 31 | 19 | 5 | 7 |
| 10 | 59 | 17 | 13 | 6 | 25 | 37 | 23 | 6 | 8 |
| 11 | 19 | 13 | 12 | 5 | 26 | 41 | 29 | 4 | 12 |
| 12 | 23 | 7 | 18 | 8 | 27 | 43 | 13 | 9 | 15 |
| 13 | 29 | 17 | 5 | 3 | 28 | 47 | 5 | 11 | 14 |
| 14 | 31 | 11 | 7 | 12 | 29 | 53 | 11 | 6 | 12 |
| 15 | 37 | 19 | 3 | 5 | 30 | 59 | 7 | 8 | 11 |

**Задание 2.** В соответствии со своими вариантами рассчитать общий ключ Каb  и Кbа. Все расчеты оформить в отчете используя программу Mathcad

**Задания для самостоятельной работы**

1. Укажите в письменной форме, что подразумевается под незащищенным каналом связи.

2. Укажите в письменной форме, каким образом и где в схеме Диффи–Хеллмана фигурирует однонаправленная функция.

3. Укажите в письменной форме, в каких случаях необходимо применять открытое распределение клячей Диффи–Хеллмана.

4. Укажите в письменной форме, можно ли многократно использовать секретный ключ Диффи–Хеллмана при обмене секретной информацией.

5. Укажите в письменной форме, каким числом в схеме Диффи–Хеллмана должно быть число λ.

**Вопросы к лабораторной работе**

1. Поясните схему открытого распределения ключей Диффи–Хеллмана.

2. Что в схеме Диффи–Хеллмана означают переменные λ , *р*?

3. Что в схеме Диффи–Хеллмана означают переменные *Ха* и *Хb?*

# Лабораторная работа 16. Исследование принципов формирования общего секретного ключа на основе схемы Диффи-Хеллмана, ч.2

**Цель:** сформировать практические умения исследования этапов формирования секретного ключа на основе схемы Диффи-Хеллмана, изучения ее характеристик и умений делать самостоятельные выводы по результатам исследований.

**Содержание:**

1. Разобрать пример генерации секретного ключа, проверки ключа.

2. Выполнить генерацию и проверку правильности выработки ключа согласно варианта.

**1. Теоретическая часть**

Данный протокол позволяет пользователям обмениваться ключами по открытым (незащищенным) каналам связи. Сформированный таким образом общий секретный ключ используется для симметричного шифрования. Генерацию общего ключа шифрования проводится только для пары абонентов сети.

 Схема данного способа проиллюстрирована на рис. 6.5.



Рисунок 6.5 - Схема симметричного шифрования секретным ключом, сформированным по протоколу Диффи-Хеллмана (М – открытое сообщение, Е - криптограмма)

Безопасность протокола обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле. Суть метода Диффи-Хеллмана заключается в следующем (рис. 1). Каждой паре абонентов в открытом виде рассылаются большие простые числа Р и λ: Р – модуль расчетов, λ – любое простое число от 2 до р-1. Числа Р и λ могут не хранится в секрете. Как правило эти значения являются общими для всех пользователей сети.

Вычисление открытого ключа уа

Вычисление открытого ключа уb

Вычисление общего ключа Кab

Вычисление общего ключа Кba

Пользователь В

Секретный ключ хb

Пользователь А

Секретный ключ ха

Незащищенный канал

Общий ключ Кab

Общий ключ Кba

уа

уb

Рисунок 1 - Схема открытого распределения ключей Диффи-Хеллмана

Пользователи А и В генерируют независимо друг от друга свои секретные ключи ха и хb (случайные большие целые числа).

Затем пользователь А вычисляет на основании своего секретного ключа ха открытый ключ как уа= λ Ха mod Р.

Пользователь В производит аналогичные вычисления уb= λ Хbmod Р.

Затем пользователи А и В обмениваются своими открытыми ключами уа и уb по незащищенному каналу и используют их для вычисления общего ключа.

Пользователь А вычисляет: Кab = уbХаmod Р = (λ Хb) Ха mod Р.

Пользователь В вычисляет: Кba = уа Хbmod Р = (λ Хa) Хbmod Р.

Как видим Кab = Кba , общий секретный ключ получен.

Злоумышленник, перехвативший значения открытых ключей уа и уb, не может вычислить общий ключ Кab, потому что он не имеет соответствующих значений секретных ключей Ха и Хb. Благодаря использованию однонаправленной функции операция вычисления открытого ключа необратима, то есть невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи-Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом – применяя симметричное шифрование с использованием общего секретного ключа.

Протокол Диффи-Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что любое хранение секретов повышает вероятность попадания их в руки конкурентов или злоумышленников.

Кроме этого, протокол Диффи-Хеллмана позволяет реализовать метод комплексной защиты конфиденциальности и аутентичности передаваемых данных, то есть использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования данных.

Важным достоинством протокола распределения ключей Диффи-Хеллмана является то, что он позволяет обойтись без защищенного канала для доставки ключей. Однако необходимо иметь гарантию того, что пользователь А получил открытый ключ именно от пользователя Б, и наоборот. Эта проблема решается с помощью сертификатов открытых ключей, создаваемых и распространяемых центрами сертификации СА (CertificationAuthority) в рамках инфраструктуры управления открытыми ключами PKI (PublicKeyInfrastructure).

Пример.

Пусть р=31, λ = 7.

Пользователь А сгенерировал случайное число ха = 11.

Пользователь В сгенерировал случайное число хb = 13.

Затем пользователь А вычисляет свой открытый ключ как уа  = λ Ха modp = 711 mod 31 = 20, и передает уа по открытому каналу пользователю В.

Пользователь В вычисляет свой открытый ключ как уb = λ Хб modp = 713 mod 31 = 19 и передает уbпо открытому каналу пользователю А.

Затем оба пользователя вычисляют общий секретный ключ.

Пользователь А: Каb= (уб )Хаmodp = 1911 mod 31 = 10.

Пользователь В: Кbа = (уа )Хбmodp = 2013 mod 31 = 10.

Общий ключ сформирован и равен 10.

**2. Задания к лабораторной работе**

**Задание 1**. В лабораторной работе исходные данные из табл. 1, а именно р, λ, ха, хb необходимо выбрать в соответствии со своим вариантом задания (варианты назначает преподаватель: по два варианта – на каждого студента).

Таблица 1 – Варианты заданий

| Номер варианта | р | λ | Ха | Хb | Номер варианта | р | λ | Ха | Хb |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 19 | 11 | 5 | 13 | 16 | 41 | 31 | 9 | 3 |
| 2 | 23 | 5 | 14 | 16 | 17 | 43 | 7 | 12 | 7 |
| 3 | 29 | 13 | 9 | 4 | 18 | 47 | 23 | 5 | 8 |
| 4 | 31 | 7 | 4 | 8 | 19 | 53 | 29 | 3 | 6 |
| 5 | 37 | 13 | 6 | 11 | 20 | 59 | 5 | 7 | 15 |
| 6 | 41 | 19 | 4 | 9 | 21 | 19 | 5 | 8 | 13 |
| 7 | 43 | 17 | 11 | 8 | 22 | 23 | 17 | 4 | 14 |
| 8 | 47 | 23 | 6 | 4 | 23 | 29 | 23 | 3 | 6 |
| 9 | 53 | 13 | 8 | 5 | 24 | 31 | 19 | 5 | 7 |
| 10 | 59 | 17 | 13 | 6 | 25 | 37 | 23 | 6 | 8 |
| 11 | 19 | 13 | 12 | 5 | 26 | 41 | 29 | 4 | 12 |
| 12 | 23 | 7 | 18 | 8 | 27 | 43 | 13 | 9 | 15 |
| 13 | 29 | 17 | 5 | 3 | 28 | 47 | 5 | 11 | 14 |
| 14 | 31 | 11 | 7 | 12 | 29 | 53 | 11 | 6 | 12 |
| 15 | 37 | 19 | 3 | 5 | 30 | 59 | 7 | 8 | 11 |

**Задание 2.** В соответствии со своими вариантами рассчитать общий ключ Каb  и Кbа. Все расчеты оформить в отчете используя программу Mathcad

**Задания для самостоятельной работы**

1. Укажите в письменной форме, что подразумевается под незащищенным каналом связи.

2. Укажите в письменной форме, каким образом и где в схеме Диффи–Хеллмана фигурирует однонаправленная функция.

3. Укажите в письменной форме, в каких случаях необходимо применять открытое распределение клячей Диффи–Хеллмана.

4. Укажите в письменной форме, можно ли многократно использовать секретный ключ Диффи–Хеллмана при обмене секретной информацией.

5. Укажите в письменной форме, каким числом в схеме Диффи–Хеллмана должно быть число λ.

**Вопросы к лабораторной работе**

1. Поясните схему открытого распределения ключей Диффи–Хеллмана.

2. Что в схеме Диффи–Хеллмана означают переменные λ , *р*?

3. Что в схеме Диффи–Хеллмана означают переменные *Ха* и *Хb?*

## Список рекомендуемой литературы

**Основная литература**

1. Сычев, Ю.Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. - Москва: ИНФРА-М, 2021. - 201 с. - Текст: электронный. - URL: https://znanium.com/catalog/document?id=388766.

2. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2021. - 400 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/1210523.

**Дополнительная литература**

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР : ИНФРА-М, 2021. – 336 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/1189326.