МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Омский государственный технический университет»

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное текстовое электронное издание
локального распространения

Рекомендовано редакционно-издательским советом
Омского государственного технического университета

Омск
Издательство ОмГТУ
2023

Сведения об издании: 1, 2

Составители: *С. Ю. Белим, С. В. Белим*

Рецензент *С. Ю. Пестова*, канд. пед. наук

Математические основы защиты информации : метод. указания к лаб. работам / Минобрнауки России, Ом. гос. техн. ун-т ; сост.: С. Ю. Белим, С. В. Белим. – Омск : Изд-во ОмГТУ, 2023. – 1 CD-ROM (0,52 Мб). – Систем. требования: процессор с частотой 800 МГц и выше ; 128 Мб RAM и более ; свободное место на жестком диске 300 Мб и более ; Linux / Windows XP и выше ; MacOS X 10.4 и выше ; CD/DVD-ROM-дисковод ; ПО для просмотра pdf- и mp4-файлов. – Загл. с титул. экрана.

Издание содержит лабораторные работы по дисциплине «Математические основы защиты информации».

Предназначено для обучающихся по направлениям 02.03.03 «Математическое обеспечение и администрирование информационных систем» (профиль «Технологии больших данных») и 02.03.02 «Фундаментальная информатика и информационные технологии» (профиль «Технологии искусственного интеллекта»).

Редактор *А. Ю. Леонтьева*

Компьютерная верстка *Ю. П. Шелехиной*

Сводный темплан 2023 г.

Подписано к использованию 28.06.23.
Объем 0,52 Мб.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Современные методы защиты информации в значительной степени основаны на математических преобразованиях закодированного сообщения. Для этих преобразований используются алгебраические отображения и дискретные функции. Также для защиты информации применяют методы, основанные на теории чисел, но не ограничиваются ими. Используют такие разделы алгебры, как теория многочленов над конечными полями и квадратичные вычеты. Анализ стойкости средств защиты информации предполагает глубокое понимание математических идей, лежащих в их основе.

Целью изучения дисциплины «Математические основы защиты информации» является освоение студентами основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины:

1) знакомство с современными концепциями и технологиями построения криптосистем;

2) изучение вопросов построения и использования криптосистем с открытым ключом;

3) изучение базовых методов и алгоритмов криптоанализа.

В работе дано представление о современных математических подходах к разработке, реализации и криптоанализу шифров. Она может служить основой для более глубокого изучения методов защиты информации.

Лабораторная работа № 1
ШИФР ЦЕЗАРЯ

Цель работы:

– программная реализация шифра Цезаря;

– исследование стойкости шифра Цезаря.

Основные сведения

В шифре Цезаря шифрование сообщения выполняется посимвольно. Все сообщение M представляется в виде символов одного алфавита.

$$M = b_1 b_2 b_3 \dots b_n,$$

где n – количество символов в сообщении.

Если сообщение написано на естественном языке, то все буквы приводятся к нижнему регистру, пробелы и знаки препинания опускаются. Например, исходное сообщение «А судьи кто?» перед шифрованием записывается в виде «асудьикто». Считается, что носитель языка всегда сможет прочитать сообщение, записанное в таком виде.

Следующий шаг – кодирование букв алфавита. Если в языке m символов, то каждая буква сопоставляется с одним из чисел в интервале от 0 до $m - 1$. Как правило, такая процедура выполняется с помощью таблицы замен. В шифре Цезаря таблица замен организована в алфавитном порядке (табл. 1).

Таблица 1

Буква	Код	Буква	Код	Буква	Код	Буква	Код
а	0	б	1	в	2	г	3
д	4	е/ё	5	ж	6	з	7
и	8	й	9	к	10	л	11
м	12	н	13	о	14	п	15
р	16	с	17	т	18	у	19
ф	20	х	21	ц	22	ч	23
ш	24	щ	25	ъ	26	ы	27
ь	28	э	29	ю	30	я	31

Используется русский алфавит, который содержит 32 символа, т. е. $m = 32$. Такое его представление используется традиционно, так как является удобным с точки зрения разработки автоматических систем шифрования.

Операция кодирования $A()$ выполняется посимвольно:

$$A(M) = A(b_1)A(b_2)A(b_3) \dots A(b_n).$$

Обозначим код символа b_i через x_i $(i = 1, \dots, n)$. Тогда закодированное сообщение

$$A(M) = x_1 x_2 x_3 \dots x_n.$$

Сообщение «асудьикто» после кодировки примет вид

$$A(\text{асудьикто}) = 0, 17, 19, 4, 28, 8, 10, 18, 14.$$

Шифрование сообщения происходит посимвольно с помощью линейного преобразования

$$y_i = E_k(x_i) = (x_i + k) \bmod m,$$

где k – ключ шифрования.

Ключом шифрования может служить любое число от 1 до $m - 1$. Зашифрованное сообщение C конкатенируется из полученных чисел.

$$Y = y_1 y_2 y_3 \dots y_n.$$

Эта последовательность чисел преобразуется в символы исходного сообщения по таблице кодировки.

Зашифрованное сообщение представляется в символах того же алфавита, что и исходное.

$$C = A^{-1}(Y) = A^{-1}(y_1)A^{-1}(y_2)A^{-1}(y_3) \dots A^{-1}(y_n).$$

Зашифрованный текст принято называть шифр-текстом.

В результате шифрования происходит замена символа сообщения на символ, расположенный на k позиций правее в алфавите. При выходе за его пределы происходит переход в начало. Такой переход обеспечивается выполнением всех арифметических операций по модулю m.

Сообщение, приведенное выше, при ключе шифрования $k = 24$ примет вид

$$Y = 24, 9, 11, 28, 20, 0, 2, 10, 6.$$

Шифр-текст будет иметь вид

$$C = \text{шйльфавкж}.$$

Расшифрование по известному ключу выполняется посимвольно с помощью линейного преобразования, обратного шифрованию.

$$x_i = D_k(y_i) = (y_i - k) \bmod m.$$

Предварительно необходимо перевести символы в их коды. После расшифрования также необходимо преобразовать коды в символы.

Шифр Цезаря не является стойким. Взлом сообщения, зашифрованного этим шифром, может быть осуществлен с помощью прямого перебора ключей. Мощность множества возможных ключей равна $m - 1$. Для рус-

ского алфавита необходимо рассмотреть 31 вариант. Схема взлома шифра заключается в прямом переборе всех возможных ключей и просмотре вариантов расшифрованных сообщений.

Задание

1. Изучите алгоритм шифрования простым постоянным сдвигом (шифр Цезаря).

2. Создайте программу, позволяющую выполнить следующие действия:

2.1. Шифрование текста, введенного с консоли, с помощью шифра Цезаря с ключом, задаваемым пользователем. Шифровать необходимо только символы русского алфавита. Символы, принадлежащие к другому алфавиту, не следует изменять. Зашифрованный текст и ключ выводить в текстовый файл.

2.2. Расшифрование текста, введенного с консоли, с помощью шифра Цезаря с ключом, задаваемым пользователем. Расшифрованный текст и ключ выводить в текстовый файл. Предусмотреть возможность сохранения в файле нескольких вариантов расшифровки при разных значениях ключа.

2.3. Установление прямым полным перебором ключа, с помощью которого был зашифрован текст, приведенный в вашем варианте задания. В качестве ответа надо зашифровать тем же ключом фамилию автора и название произведения, из которого была взята зашифрованная цитата.

Пример выполнения.

ШИФР-ТЕКСТ (ШТ): шйльфавкж

РАСШИФРОВАННЫЙ ТЕКСТ (ОТ): асудьикто

КЛЮЧ: 24

АВТОР И ПРОИЗВЕДЕНИЕ (ОТ): грибоедовгореотума

ЗАШИФРОВАННЫЕ ФАМИЛИЯ И НАЗВАНИЕ (ШТ):
ыиащжэьжъыжиэжклдш

3. По результатам выполнения лабораторной работы оформите отчет (прил. 1).

Требования к программе.

1. Текст программы оформляется согласно общепринятым правилам (удобно для чтения, с описанием всех функций, переменных и особо важных мест).

2. Интерфейс программы – любой удобный.

3. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Вариант 1

Къыуоцльуцнльощьъщпльэрчвэщмжьщшмдуэзнлчъыршръыукэшщру тнрьэурхшлчрпрэырнутщы

Вариант 2

юэукычбфыьфсфщчьфсчхващпцпъюэуцфыькытэъэаэысчшчсафаэьыч ифщчьвъэалюэукыпблфывсфщч

Вариант 3

кшюбхшэребхшюыэбюшвабребъхжкыецбгчб

Вариант 4

юмуумфгямнмфапфъувтеипущмутмкюмфчзйпушжувмрпщмумм ймчфммкъипушчмлгхихтгшщпщмтгфвьшмщмр

Вариант 5

извлитевлцьиезъвдъжязцлмвпввйкибъеяювйеъжязцзялмиецкъбевсзхж яалиыиг

Вариант 6

шзоэсягфчфэиыъщсшщъпягсшящфнярифцмцщфняриюмцоъэыфю мщисшэчмомнъпяящмэщсшярьсщънчсэщяюи

Вариант 7

ьцнчзйбийяажчицзтажйэаейзгяозынчйелымаийюнад

Вариант 8

фцщткititфхцлцкеъцфпкытнмузщншмюишыщщтцлцщуруцщдтит фхцлцкхнфцъцпкиуцщд

Вариант 9

пътрьяшигзхуюцхсюыхзвюпьюугхйхбърчрвм

Вариант 10

ъюацеынцбтгцвдбнцбюшцацабцгтбызгцхчдхэбюшцдгцшзывтызшды яждъгдяацэцбцзтъышднадянйьдя

Вариант 11

вегфобдобнъипцоцнгелхярсвзуцжспцсхзгргвдцзцеинипцеиург

Вариант 12

ягйггрнюоспмвжлмимзарскюлгкмоэбмйсямкхрмжчгрмлапроюлгвю йгимзхрмижлсймлаиоюьомвлмк

Вариант 13

ючнухчнсмсмптсйътснэыщщыючпнюьнштъънмьыунэыщбэнъгафаы яснън

Вариант 14

чпмечпыхкоэвкщшзькщшсшъкцпхшбчеяшлтомшыыькхшчщъшьтмцч пчтуымпькшотчфкфщъпроптэлть

Вариант 15

ауцаугзмэьвифвгжзехввгуауцгчсувъдгцъщэзъъехжжищгябгю

Вариант 16

юяингщжсадвгмюруюцэьцгтяфдщшуцшхсвшуцшхяпфяуябщг

Вариант 17

нцпшьтунихшцчтунткпусшхшпшфуйечбзснтшчшйшэкзтуоткзмиуйа

Вариант 18

юнбнуьноздючбнбишдлкскводампяйьампяьжьваыыйбнуьноздюыын бишыйбнуьноздюылкнюкбип

Вариант 19

енуждимонуошфсврфкижклпчшиошлсвублулчэжчшвещйцбнлуолчфи лчшоозфслнувочэжчшоллчшвшфсврффшчщшчшиолгшоыкищынфс

Вариант 20

дьштйуйышыщгеибщьдьэяйуйышьивхыугяжеычвььейфйяммщчйещ щыьзыщдхбйьйбыщъвкпущичзчйещ

Вариант 21

гэешъдоунвтцбвъгэешъфтдогсдакяа

Вариант 22

ъайъыфслдоайъчлцоцйкфзнйзы

Вариант 23

дишвьдшзеопнэхкввмеопливпэ

Вариант 24

шйльфавкж

Вариант 25

злрюьздчэбжюдюлщчлшьзызйчзлрюьздчэбжюдюлщчллщггщгилбпф

Вариант 26

реущьрушутьщфыьпйакряуэюушюояыьцщцдьцьтуфтоцтбжоцъйящц

Вариант 27

южвгьефябщыбфтфушздфюльжфт

Вариант 28

увтеипуйшмпнзчьхтхлфвьюпштплзчихнмшщймффвьйплмфпрфзуй фжщфхйшяпхшщчврkзттгшспршувштпшъучзюфврkмчузфшспркмфпр

Вариант 29

ъыупуэрхшлчщэюсльщннщфшжъыупуэрнчуышжрщмекэзкъщхлшръщтпшщьэлыжфчрвншщсшжэщнлыудучжьэлшрчмылэзк

Вариант 30

руяьыяэтмумфбмштпбяыбсгщшэыэсюхсгсэаяигцющрюцгдыьптмэицбгрэвэсгцбрэщысгщвньптсртдэсчысюяогд

Контрольные вопросы

1. Какое преобразование используется в шифре Цезаря для шифрования текста?

2. Какое преобразование используется в шифре Цезаря для расшифрования текста?

3. Каким требованиям должен удовлетворять открытый текст, подаваемый на вход алгоритма шифрования?

4. Какие значения может принимать ключ шифрования?

5. Какова трудоемкость полного перебора для взлома шифра Цезаря?

Лабораторная работа № 2
КРИПТОАНАЛИЗ АФФИННОГО ШИФРА

Цель работы:

– проведение криптоанализа сообщения, зашифрованного аффинным шифром;

– определение ключа шифрования и открытого текста.

Основные сведения

В аффинном шифре, как и в шифре Цезаря, шифрование производится посимвольно. Сообщение представляется в виде последовательности символов без пробелов и знаков препинания в нижнем регистре. Кодирование символов выполняется по алфавитной таблице (табл. 2).

Таблица 2

Буква	Код	Буква	Код	Буква	Код	Буква	Код
а	0	б	1	в	2	г	3
д	4	е/ё	5	ж	6	з	7
и	8	й	9	к	10	л	11
м	12	н	13	о	14	п	15
р	16	с	17	т	18	у	19
ф	20	х	21	ц	22	ч	23
ш	24	щ	25	ъ	26	ы	27
ь	28	э	29	ю	30	я	31

Пусть сообщение M представлено в виде последовательности кодов символов.

$$A(M) = x_1 x_2 x_3 \dots x_n.$$

Шифрование выполняется ключом, состоящим из двух чисел, т. е. $k = (a, b)$. Число a должно быть взаимно простым с мощностью алфавита m. При работе с текстами на русском языке $m = 32$. Число b может быть любым – от 0 до $m - 1$.

Шифрование осуществляется с помощью аффинного преобразования:

$$y_i = E_k(x_i) = (ax_i + b) \bmod m,$$

где $i = 1, \dots, n$.

Зашифрованное сообщение представляется в символах того же алфавита, что и открытый текст. К зашифрованному тексту применяется таблица кодировки.

$$C = A^{-1}(Y) = A^{-1}(y_1)A^{-1}(y_2)A^{-1}(y_3) \dots A^{-1}(y_n).$$

Расшифрование выполняется с помощью обратного преобразования.

$$x_i = a^{-1}(y_i - b) \bmod m,$$

где $i = 1, \dots, n$.

Элемент a^{-1} является обратным к числу a и удовлетворяет равенству

$$a^{-1} \cdot a = 1 \bmod m.$$

Чтобы расшифровать сообщение, необходимо предварительно вычислить элемент, обратный к первой части ключа. Для небольших алфавитов этот элемент может быть найден прямым перебором. Если алфавит произвольный, то необходимо использовать расширенный алгоритм Евклида для поиска обратного элемента.

Криптоанализ аффинного шифра осуществляется на основе частотного анализа текста. Его целью является определение двух наиболее часто встречающихся букв. Для русского языка частоты знаков алфавита (в порядке убывания) приведены в табл. 3. При частотном анализе отождествляются буквы «е» и «ё», а также буквы «ъ» и «ь». Если текст содержит пробелы, то для них используется символ «–».

Таблица 3

Символ	Частота	Символ	Частота	Символ	Частота	Символ	Частота
–	0,175	О	0,090	Е/Ё	0,072	А	0,062
И	0,062	Т	0,053	Н	0,053	С	0,045
Р	0,040	В	0,038	Л	0,035	К	0,028
М	0,026	Д	0,025	П	0,023	У	0,021
Я	0,018	Ы	0,016	З	0,016	Ъ/Ь	0,014
Б	0,014	Г	0,013	Ч	0,012	Й	0,010
Х	0,009	Ж	0,007	Ю	0,006	Ш	0,006
Ц	0,004	Щ	0,003	Э	0,003	Ф	0,002

Двумя наиболее часто встречающимися буквами в русском тексте являются «е» и «о». В аффинном шифре эти буквы соотносятся с двумя какими-то другими буквами. Таким образом можно составить систему уравнений, решение которой дает ключ шифрования.

Рассмотрим примерную процедуру криптоанализа аффинного шифра.

Пример 1.

Пусть по результатам частотного анализа шифр-текста было определено, что наиболее частыми буквами будут «и» и «у». Выдвигаем два предположения:

$$E_k(\text{о}) = \text{и}, E_k(\text{е}) = \text{у},$$

или

$$E_k(\text{о}) = \text{у}, E_k(\text{е}) = \text{и}.$$

Используя таблицу кодировок, получаем две системы сравнений

$$\begin{cases}(14a + b) \bmod 32 \equiv 8, \\ (5a + b) \bmod 32 \equiv 19, \end{cases}$$

или

$$\begin{cases}(14a + b) \bmod 32 \equiv 19, \\ (5a + b) \bmod 32 \equiv 8, \end{cases}$$

В обеих системах в качестве модуля взято число 32, так как используется алфавит из 32 символов. Получаем следствие $9a \bmod 32 \equiv \pm 11$, которое решаем стандартным способом (умножая обе части получившегося сравнения на элемент, обратный 9 в кольце вычетов по модулю 32). Вычисляем возможные ключи шифрования.

В первой системе сравнений $a = 13, b = 18,$ во второй – $a = 19,$ $b = 9.$

Получаем два варианта ключа шифрования: $k_1 = (13, 18), k_2 = = (19, 9).$

Какой из них правильный, можно определить только попытавшись расшифровать весь текст. Если после расшифрования не получился осмысленный текст, то надо посмотреть на результаты частотного анализа шифр-текста и сделать новое предположение со следующей по частоте буквой.

В результате предположения может получиться неразрешимая система сравнений. Она не будет иметь решения, если невозможно вычислить обратный элемент (в кольце вычетов по модулю 32 не каждый элемент обратим).

Если система сравнений не имеет решения, то предположение о соответствии букв неверное и надо выдвигать новое.

Пример 2.

Пусть в тексте вторыми по частоте буквами будут «й» и «п». Выдвигаем два предположения:

$$E_k(\text{а}) = \text{й}, E_k(\text{и}) = \text{п},$$

или

$$E_k(\text{и}) = \text{й}, E_k(\text{а}) = \text{п}.$$

Используя таблицу кодировок, получаем две системы сравнений:

$$\begin{cases}(0a+b)\bmod 32 \equiv 9,\\ (8a+b)\bmod 32 \equiv 15,\end{cases}$$

или

$$\begin{cases}(8a+b)\bmod 32 \equiv 9,\\ (0a+b)\bmod 32 \equiv 15.\end{cases}$$

Попытка решить эти две системы сравнений не будет успешной, т. к. полученное следствие $8a \bmod 32 \equiv \pm 6$ неразрешимо. Поэтому следует выдвинуть другие предположения.

Задание

1. Изучите алгоритм аффинного шифрования.

2. Создайте программу, позволяющую выполнить следующие действия:

2.1. Вычисление элемента, обратного к данному элементу в кольце вычетов по заданному модулю (для проверки работоспособности должна быть предусмотрена возможность с консоли ввести сам элемент и модуль). Следует учесть, что не все элементы обратимы.

2.2. Решение сравнения вида $ax \bmod m \equiv b$ (должна быть предусмотрена возможность ввода элементов a, b и m с консоли). Следует учесть, что не все сравнения разрешимы, а некоторые имеют несколько решений.

2.3. Решение системы сравнений вида

$$\begin{cases}(ax+y)\bmod m \equiv b,\\ (cx+y)\bmod m \equiv d.\end{cases}$$

Следует предусмотреть, что система сравнений может быть неразрешима или иметь несколько решений.

2.4. Выполнение частотного анализа шифр-текста и определение двух самых часто встречающихся букв.

Таблица частот встречаемости символов составлена для длинных текстов, для коротких наиболее частыми могут оказаться другие буквы. Определить их в каждом отдельном случае можно только с помощью процедуры перебора с учетом таблицы частот.

2.5. Выдвижение предположений о том, какие буквы открытого текста соответствуют выявленной паре самых часто встречающихся символов шифр-текста.

2.6. Расшифрование текста, представленного в вашем варианте задания, если известно, что это аффинный шифр. Предусмотреть процедуру постепенного поиска истинного ключа с возможностью прерывания процесса перебора ключей в случае успешной дешифровки. Варианты расшифрованного текста и текущий вариант ключа сохранять в текстовом файле.

3. По результатам выполнения лабораторной работы оформите отчет (прил. 2).

Требования к программе.

1. Текст программы оформляется согласно общепринятым правилам (удобно для чтения, с описанием всех функций, переменных и особо важных мест).

2. Интерфейс программы – любой удобный.

3. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Вариант 1

щковмтчгфюсякяфртичгфдесявжтрдясзруярдэсчфбефючхрэръвжмвгя чхбрйебэчфчфгстнгюамвмякуежюутвщжнбеъкгфнчдщтндвсэчфкфмкукфм вежвэвссолкмгкжкфявруэеймчдфеэебчдмтвгяромеъвмч

Вариант 2

шмиснякнижшмъмшзйюкчолвршбкчкырвфплрпумбкжвшбнсгшрмег уънмсъкывшткчпепфыкюмъмывчукчолврнюпвсмчоемвбюнтемкюкиояъ мывинюпшмрем

Вариант 3

щгзшмпвжгщгзфвлыоцунпыщумжгфбгъгйвщйртжыпыщщгзъгъвйвпн здтпнунхбгтжфвпдъвйыпгъъдтийвувоыицмлбгщгзъгбмучытънхбгтжщны щцвинбнъцвипйвуво

Вариант 4

ртжпещкофпакоеэкблфпэяртжфутвелвкхпяэзрафпэяэтйвечлещгтэяб клзщрфбкрвкомтрцакрыуеблвешвтщэяхгвеофбкуафоаяхфоырыщэяхкщ экжкоыоцшткхжфвщшфб

Вариант 5

эызхщлщюингкзгзщшщящзвюиртиэцлщърщцщбылтэызнщдюыхышви лиярылщящзкилиъюифыкилиъзщлтхщюяжррифиэдщцыэолтнэизргбиэыз былинрыэжсгэыджломнщюхимнилрщфюжсгэ

Вариант 6

ъдичъэсдчздзоюбнояьруъзфуруъчдидчозояъдиждфшвдпуялдрщедъои йдглуъъдифэччвьярэгъдифэчшюсдглуъъъдибзхеьиурбсьеэиофбкьруерэзщ уеулхясорльичьруеьвоъэйулхячкоьилучвдщвьнокофье

Вариант 7

цжсзьбоъяьсфзкьсхфьчфжфыфясзьсицхутлрчевэлэзузстфеьсфхуяфьч фэлэкфьуиоуресиэылрсевхесзтфьчцдкыъреуафюьляфйьсихеыфхсклдгъ зьсиръфевюхъолтзьфясткскстсрьфйьвиурьутурчзутвфофыев

Вариант 8

лкывщзъштгяющгъэпонмсфъагуиимокюгмсфымпмжнъыоцушъкнэща вщкщифмсфъанэщыфмшмифъмжмгнъэвктлыэщпгуемцунщжмфяонофткы ияныьщзфыпщышмцшщсминэушмцэзщьфщэмфяошмцикмцшмцсыцфыш мцкйшэы

Вариант 9

индульчвьхцбмцзнюиулруфтцвцбсврстфхьчрвекькафацхувлцутфиул рукькэулфящфчвцякмьчцвефчумиоузрувчстнбцулруфихслуэцтцчкмучхф тлцтрфзцюучвтцфтицглцтулруфюфйлрфчхуйефхжзцтр

Вариант 10

ньжсфпншсавъужвлвъньиясрпзхшискнньядгшъхпхгпхсэйэвншхпхцг вянузнсозжмвлвъъвзгвшээвхрпжснньщзэвчуэсфясгъсглсгвшщцявлуфсяш зтмсисниясэсщдлъзъпцсмсг

Вариант 11

етъмахдфснпбоцпуощпнкоеаобспыпгтмэмкркпхпьреэзмюъъмфплъо щпапзехьпэьпзрпазмтмэмкрзоъйтаоплзпгнмгкзолиощпяокртмхщюцмщо гкдяьмзеъйзогкмъдкпапзе

Вариант 12

эщфуфзфыатзуфцрбтцсзфлтжсдрцсатсятэцчшфжчщспгщфзьнщьотяш фотяшфнщфшскшпыьасзфбтцрдсшотбтцржщсшсзвдфгжшсдсжщсщфмсх жьшсцржф эуцтнцтзротэзчмфцржфмьдсуьжфаэзтжтатзжьцрьлтцтажэсш пафцршпафцртнтшщтаьшсщрьщтур штщтжтхжэцдсуь

Вариант 13

слелрэтлдюуцйцюбамйцтюфкцъцяфйецсдцнбйемьшецдцтяюфкшлех чехтхпэухшелтюэтблячелктлсчюмяфюцьлкпрлефюхптяецамтцпцеюлкх пелефрпцрйлытцпцехипэтб

Вариант 14

цыщыхунфбйэъюифрыфнфъбфйспщвюыупуяцвюиуйюрфйуныщвюрф ижцвюпйуяшэыцяфйыьуяыубйумюшнжфежцхыщчйуяфъюыхужыуушюу йтярифе тюыучеуйуыуушюжухрцнфъфйтъфвпйуяшюш

Вариант 15

ыдеыжуювыушуйуивйошяжыаоадпщйаспсцсфежнцухвяадйвеэндсицу ыыутсяыубскцсбтойщчнцукжкотяэпубсыуиуцнуйошдбдадыэоыжшуяиотн дйэнсяищуйуяжыукжшыдяидйвб сяищуопуцубтойщчкйэтуыэ

Вариант 16

взщэоюнщмфасзедшоэзгждюзцоиынщэтдцнтсзтзщмнгюцохецфшзгшз шмзгждщнгмзщнгмзужпщфхбсфмтужвзщзымзсшгзфашгфуцеяжюзэчфхби ощузмнъншндесфщцтувзсемоумзшвеяжгугзед мнсзэрфммждэоынд

Вариант 17

оюэсолахуьимиыпжщыхкаинъуплыпнатдуаисъаижэнэьлилаэнпщаэо лнпюэыпжаиььоытеипаквэыпяаиюпупнапдэвиуьэащнхдьупкпьлпвюэаил ыиьбоаиъснъщъеэыжэыилапдвхнис пдюнэшюиничхыилхлвиабоъмичхлх ьвэыиамъщъощпупвбыюпщвъаапссхничхымъщилшплбпщхаюххл

Вариант 18

пгсаистшгшэюыабтюфюцьцчзсгшдэсдшнвэнчгстзрюьапзскмзстшщгч адэсныскщювэсепкнюенсввачнпаьвнстсгшпыпасвэлемчгяпымзпфрнчаню аюцлбтсщпбсышфчтшглмсвашяцчстпгрцювэзчячвлцюэзютшьнюцйчонча шпеаюнюэшмзпюыапзчнцсгшяцспцюсвмсзпнчкиашмйч

Вариант 19

ъшъсзсйехаишйвеытйнаэочйповфевавдсйишгяфсзфщогшишфащейчш асатзгшхяэсзэсшхйпохийъосфйушфаложшишфемияжасоэетойэтцшийпи шмеъоэхиосйъсыгдлолочюймйвсштйисофъосйагвйфсопочйешсштевийуяй фяамйвтмощсотйссзэъямйесаълоъоисзэлйиясяевшиаъомсофягштйвотпиы мянйпотйевсаъ

Вариант 20

аоювэеъизпийищжюозйгдфифределеюищдеэлозйгаоювйозфоэыоужю лейфэисйезйаоюжаестизиъисоуифитлейфэчепийфжэоьюидофвйзиэидис ьийфжуизиржзжтизиъчхжийфоджзжиъэжх

Вариант 21

бцъушгыэдчзкъэычохйздшыаэмнаэфспгэшмбцъушгфюэчкюышхшй чо хйзфшчыеодоышсбшфшжшмфъэмгашъшфанйзйфпапезспиэтзгэчшг хпжзфъэмгашъшфанйзйышбпезтзбэыэмъэосчояжз

Вариант 22

юпицьпгцлбицьпгцлапвьбьлбюибсдгьбвуюмнгшфьрепнйупуапвьдщ юпгадуэапуцлйлдусдгпшгсбуйьврврепнасйюцвпювнцсуюдявнпьдебгц угэвдгрещйнйьйвубнййапуаптьцеюпндицьдвусдйьвржьбеюмнйсдиэрнй

Вариант 23

фсыкжщйрбрязуьпярэислрфвйуьпфзуйэтриивьпирпутруйртэутуеуьэуь ъйкфяивьяупщйсмэщащозйвтуэзйупщпкгюсмкзтгряюуеузиуэзтгрясдйуф щрясфэуяйсяпузиузщздкеяуфуэиугжщекэщтуеиужупряэриопжътоеуэсзйсз уэфпусэспвэутпсянауцряещпщьктрясээвпутниврюяслвюуйщдйщяюуйщ

Вариант 24

шжрапьмщяпщдоъщдпящхпжгомязьежпужоехщьмящкпагжпьняптпа йвайьмрчжщомязящыршхьыпжгохвпияосзхфщащещщыоероаотпхзютожь юхоеяпчшузтхобооырюпжгозуиащъхщажзтещймщнярержовотпзяоынзът щажспашдзмояхроущящфрзщеыпаожжротоыщъфзуршиящфр

Вариант 25

лэццэхжкэьэхйъхпцзчдбъцрэцчэялэхтваъцсгцзэщърэцээаэтхээяпбъцст эюжфбфчжсрърэчжхзнсэрэщтвыатврбзавчфнчвюхфштфахзщхвпшфщ счваъчсгчдбфахфщсвцфсэбэаэыюэртпбгъхвсчвьювгсжхэчдбг

Вариант 26

йцоюзхпзаьъгьъпьмцеуиьыгпзйцьгрьмцеуиьыбьхьрьмижиабвьхоргщ бьхьржщцеуижньхьгьввьхаорсзхьазстовьрйэгрорегржцсзвзпщавьцзъьцьн ьыбжгзущъжвьриэйьриэйхмгтсзврьхтиьйьфзхжзют

Вариант 27

тсвсштсвсшвядозчлвязощусафнвирвчлвятопщчсафнрщсдошстнюьчтс сафщигшонвошсщсэорафнущръозоъшодсэозиоьщозоипфовъижсафдщсто втсвсщстрьиппрзьсщинтсвсвяцишстщядопоьое

Вариант 28

умбйэдднйбофжлвъыдумкймйндыблвшдэытнръыдшдкдяйнръбдатын чжйбоыйндарътбнрайббъчнйбонзйяъыоблювуюдюдэбъмъыъноыдмтынчб

ъздычруюъбгунйхшктшыталщшъкъаъбрчбуынчшфгузктэытмъыънождад ыобдншуябъчзд кънрдчыбдчэкоумужадкъ

Вариант 29

бчтмкликжцсабмтшюжычюрцчбжбкцбщлнчбчфрымтрыйккьчикьбчаи мтклектэгсгцрелчьчткычикщжгбчклжмфсгбсючгбрптшъачбьшисюгснщт ынчкюьржлшттчюгкиэкслшыщтччжктткюжлрпщебраьбчикюнткыабреэ члбсетчкьчънкиэкнщтрлтчкфсцыктэкачбэгщънрг

Вариант 30

ыияыоняымйэычящючбрвжемюдцычызъчкщыизфафмнъеждбыкючию мысбшыячщжемюдбцфмбркйщйеыяиызещжцбиожвйршыцбтышщфчйчфон

Контрольные вопросы

1. Какое преобразование используется в аффинном шифре для шифрования текста?

2. Какое преобразование используется в аффинном шифре для расшифрования текста?

3. Каким требованиям должен удовлетворять ключ шифрования?

4. Какой анализ текста необходимо провести для криптоанализа аффинного шифра?

5. Какие предположения делаются при криптоанализе аффинного шифра?

Лабораторная работа № 3
МОДЕЛЬ ОТКРЫТОГО ТЕКСТА

Цель работы:

– проведение частотного анализа открытого текста;

– определение зависимости энтропии k-грамм для текста на русском языке.

Основные сведения

Энтропия открытого текста позволяет сделать предположение о языке, на котором он написан. Эта информация важна при криптоанализе шифров простой замены (шифр Цезаря, аффинный шифр и др.). При использовании таких шифров сохраняются частотные характеристики символов и сочетаний символов. Поэтому зашифрованный текст имеет такую же энтропию, как и открытый.

Для частотного анализа текста используется понятие k-граммы. k-граммой называется упорядоченный набор символов. 1-граммы – это отдельные буквы, 2-граммы – это сочетания из двух букв и т. д. Если задан текст, то для него можно посчитать частоту встречаемости каждой k-граммы. Обозначим k-грамму z_i^k, где i – номер k-граммы, а частоту встречаемости набора k-граммы – $p(z_i^k)$. Для каждого текста T можно рассчитать энтропию k-грамм

$$H_k(T) = -\sum_{i=1}^{n} p\left(z_i^k\right) log_2\left(p\left(z_i^k\right)\right),$$

где n – количество различных k-грамм, встречающихся в тексте T.

Суммирование выполняется по всем k-граммам.

В криптоанализе интерес представляет величина $H_k(T)/k$. Для всех текстов на одном языке она убывает с ростом k. При больших значениях k это отношение стремится к некоторому асимптотическому значению, характерному для языка, на котором написан текст. Для большинства текстов график энтропии выходит на значение, близкое к асимптотическому, уже при $k = 5$.

Перед расчетом энтропии текст приводится к тому те же виду, что и для аффинного шифра (все символы в нижнем регистре, удаляются пробелы и знаки препинания).

Задание

1. Для текста, представленного в вашем варианте задания, рассчитайте $H_k(T)/k$ для значений k от 1 до 5. Учитывайте только буквы русского алфавита, опуская пробелы и знаки препинания. Большие и маленькие буквы следует считать эквивалентными.

2. Постройте график зависимости $H_k(T)/k$ от k для вашего текста.

3. По результатам выполнения лабораторной работы оформите отчет (прил. 3).

Требования к программе.

1. Текст программы оформляется согласно общепринятым правилам (удобно для чтения, с описанием всех функций, переменных и особо важных мест).

2. Интерфейс программы – любой удобный.

3. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Вариант 1

«Мильоны – вас. Нас – тьмы, и тьмы, и тьмы. Попробуйте, сразитесь с нами! Да, скифы – мы! Да, азиаты – мы, С раскосыми и жадными очами! Для вас – века, для нас – единый час. Мы, как послушные холопы, Держали щит меж двух враждебных рас Монголов и Европы!» [Александр Блок. Скифы]

Вариант 2

«Летун отпущен на свободу. Качнув две лопасти свои, Как чудище морское в воду, Скользнул в воздушные струи. Его винты поют, как струны... Смотри: недрогнувший пилот К слепому солнцу над трибуной Стремит свой винтовой полет...» [Александр Блок. Авиатор]

Вариант 3

«Гул затих. Я вышел на подмостки. Прислонясь к дверному косяку, Я ловлю в далеком отголоске, Что случится на моем веку. На меня наставлен сумрак ночи Тысячью биноклей на оси. Если только можно, Авва Отче, Чашу эту мимо пронеси.» [Борис Пастернак. Гамлет]

Вариант 4

«Я был разбужен спозаранку Щелчком оконного стекла. Размокшей каменной баранкой В воде Венеция плыла. Все было тихо, и, однако, Во сне я слышал крик, и он Подобьем смолкнувшего знака Еще тревожил небосклон.» [Борис Пастернак. Венеция]

Вариант 5

«Глухая пора листопада, Последних гусей косяки. Расстраиваться не надо: У страха глаза велики. Пусть ветер, рябину занянчив, Пугает ее перед сном. Порядок творенья обманчив, Как сказка с хорошим концом.» [Борис Пастернак. Иней]

Вариант 6

«Я пропал, как зверь в загоне. Где-то люди, воля, свет, А за мною шум погони, Мне наружу ходу нет. Темный лес и берег пруда, Ели сва-

ленной бревно. Путь отрезан отовсюду. Будь что будет, все равно.» [Борис Пастернак. Нобелевская премия]

Вариант 7

«Снег идет, снег идет. К белым звездочкам в буране Тянутся цветы герани За оконный переплет. Снег идет, и всё в смятеньи, Всё пускается в полет, – Черной лестницы ступени, Перекрестка поворот.» [Борис Пастернак. Снег идет]

Вариант 8

«Я сразу смазал карту будня, плеснувши краску из стакана; я показал на блюде студня косые скулы океана. На чешуе жестяной рыбы прочел я зовы новых губ. А вы ноктюрн сыграть могли бы на флейте водосточных труб?» [Владимир Маяковский. А вы могли бы?]

Вариант 9

«Разворачивайтесь в марше! Словесной не место кляузе. Тише, ораторы! Ваше слово, товарищ маузер. Довольно жить законом, данным Адамом и Евой. Клячу истории загоним. Левой! Левой! Левой!» [Владимир Маяковский. Левый марш]

Вариант 10

«Вашу мысль, мечтающую на размягченном мозгу, как выжиревший лакей на засаленной кушетке, буду дразнить об окровавленный сердца лоскут: досыта изъиздеваюсь, нахальный и едкий.» [Владимир Маяковский. Облако в штанах]

Вариант 11

«Послушайте! Ведь, если звезды зажигают – значит – это кому-нибудь нужно? Значит – кто-то хочет, чтобы они были? Значит – кто-то называет эти плевочки жемчужиной?» [Владимир Маяковский. Послушайте!]

Вариант 12

«Я волком бы выгрыз бюрократизм. К мандатам почтения нету. К любым чертям с матерями катись любая бумажка. Но эту... По длинно-

му фронту купе и кают чиновник учтивый движется. Сдают паспорта, и я сдаю мою пурпурную книжицу.» [Владимир Маяковский. Стихи о советском паспорте]

Вариант 13

«Скажи-ка, дядя, ведь не даром Москва, спаленная пожаром, Французу отдана? Ведь были ж схватки боевые, Да, говорят, еще какие! Недаром помнит вся Россия Про день Бородина!» [Михаил Лермонтов. Бородино]

Вариант 14

«Скажи мне, ветка Палестины: Где ты росла, где ты цвела, Каких холмов, какой долины Ты украшением была? У вод ли чистых Иордана Востока луч тебя ласкал, Ночной ли ветр в горах Ливана Тебя сердито колыхал?» [Михаил Лермонтов. Ветка Палестины]

Вариант 15

«Выхожу один я на дорогу; Сквозь туман кремнистый путь блестит; Ночь тиха. Пустыня внемлет богу, И звезда с звездою говорит. В небесах торжественно и чудно! Спит земля в сияньи голубом... Что же мне так больно и так трудно? Жду ль чего? Жалею ли о чём?» [Михаил Лермонтов. Выхожу один я на дорогу…]

Вариант 16

«Белеет парус одинокой В тумане моря голубом!.. Что ищет он в стране далекой? Что кинул он в краю родном?.. Играют волны – ветер свищет, И мачта гнется и скрыпит... Увы! Он счастия не ищет И не от счастия бежит!» [Михаил Лермонтов. Парус]

Вариант 17

«Погиб поэт! – невольник чести – Пал, оклеветанный молвой, С свинцом в груди и жаждой мести, Поникнув гордой головой!.. Не вынесла душа поэта Позора мелочных обид, Восстал он против мнений света Один, как прежде... и убит!» [Михаил Лермонтов. Смерть поэта]

Вариант 18

«Несчастная кошка порезала лапу – Сидит, и ни шагу не может ступить. Скорей, чтобы вылечить кошкину лапу Воздушные шарики надо купить! И сразу столпился народ на дороге – Шумит, и кричит, и на кошку глядит. А кошка отчасти идет по дороге, Отчасти по воздуху плавно летит!» [Даниил Хармс. Удивительная кошка]

Вариант 19

«Когда вода всемирного потопа Вернулась вновь в границы берегов, Из пены уходящего потока На берег тихо выбралась любовь И растворилась в воздухе до срока, А срока было сорок сороков.» [Владимир Высоцкий. Баллада о любви]

Вариант 20

«Средь оплывших свечей и вечерних молитв, Средь военных трофеев и мирных костров Жили книжные дети, не знавшие битв, Изнывая от мелких своих катастроф. Детям вечно досаден Их возраст и быт, – И дрались мы до ссадин, До смертных обид. Но одежды латали Нам матери в срок, Мы же книги глотали, Пьянея от строк.» [Владимир Высоцкий. Баллада о борьбе]

Вариант 21

«Живописцы, окуните ваши кисти в суету дворов арбатских и в зарю, чтобы были ваши кисти словно листья. Словно листья, словно листья к ноябрю. Окуните ваши кисти в голубое, по традиции забытой городской, нарисуйте и прилежно и с любовью, как с любовью мы проходим по Тверской.» [Булат Окуджава. Живописцы]

Вариант 22

«В раннем детстве верил я, что от всех болезней капель датского короля не найти полезней. И с тех пор горит во мне огонек той веры... Капли датского короля пейте, кавалеры!» [Булат Окуджава. Капли датского короля]

Вариант 23

«Надоело говорить и спорить, И любить усталые глаза... В флибустьерском дальнем море Бригантина подымает паруса... Капитан, обветренный, как скалы, Вышел в море, не дождавшись нас... На прощанье поднимай бокалы Золотого терпкого вина.» [Павел Коган. Бригантина]

Вариант 24

«Если я заболею, к врачам обращаться не стану, Обращаюсь к друзьям (не сочтите, что это в бреду): постелите мне степь, занавесьте мне окна туманом, в изголовье поставьте ночную звезду.» [Ярослав Смеляков. Если я заболею, к врачам обращаться не стану]

Вариант 25

«По крутой тропинке горной Шел домой барашек черный И на мостике горбатом Повстречался с белым братом. И сказал барашек белый: "Братец, вот какое дело: Здесь вдвоем нельзя пройти, Ты стоишь мне на пути".» [Сергей Михалков. Бараны]

Вариант 26

«Я не люблю фатального исхода. От жизни никогда не устаю. Я не люблю любое время года, Когда веселых песен не пою. Я не люблю открытого цинизма, В восторженность не верю, и еще, Когда чужой мои читает письма, Заглядывая мне через плечо.» [Владимир Высоцкий. Я не люблю]

Вариант 27

«На Братских могилах не ставят крестов, И вдовы на них не рыдают, К ним кто-то приносит букеты цветов, И Вечный огонь зажигают. Здесь раньше – вставала земля на дыбы, А нынче – гранитные плиты. Здесь нет ни одной персональной судьбы – Все судьбы в единую слиты.» [Владимир Высоцкий. Братские могилы]

Вариант 28

«На рынке корову старик продавал, Никто за корову цены не давал. Хоть многим была коровёнка нужна, Но, видно, не нравилась людям она. – Хозяин, продашь нам корову свою? – Продам. Я с утра с ней на рынке стою! – Не много ли просишь, старик, за неё? – Да где наживаться! Вернуть бы своё!» [Сергей Михалков. Как старик корову продавал]

Вариант 29

«Кто на лавочке сидел, Кто на улицу глядел, Толя пел, Борис молчал, Николай ногой качал. Дело было вечером, Делать было нечего. Галка села на заборе, Кот забрался на чердак. Тут сказал ребятам Боря Просто так: – А у меня в кармане гвоздь! А у вас?» [Сергей Михалков. А что у вас? (Дело было вечером, делать было нечего)]

Вариант 30

«Месяц над нашею крышею светит, Вечер стоит у двора. Маленьким птичкам и маленьким детям Спать наступила пора. Завтра проснешься – и ясное солнце Снова взойдет над тобой… Спи, мой воробышек, спи, мой сыночек, Спи, мой звоночек родной. Спи, моя крошка, мой птенчик пригожий, – Баюшки-баю-баю. Пусть никакая печаль не тревожит Детскую душу твою.» [Михаил Исаковский. Колыбельная]

Контрольные вопросы

1. Какое преобразование используется в аффинном шифре для шифрования текста?
2. Какое преобразование используется в аффинном шифре для расшифрования текста?
3. Каким требованиям должен удовлетворять ключ шифрования?
4. Какой анализ текста необходимо провести для криптоанализа аффинного шифра?
5. Какие предположения делаются при криптоанализе аффинного шифра?

Лабораторная работа № 4
ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ. АЛГОРИТМ RSA

Цель работы: реализация алгоритма шифрования с открытым ключом RSA.

Основные сведения

Рассмотрим схему шифрования с открытым ключом по алгоритму RSA.

Блок сообщения M представляется числом из интервала $[0; n-1]$ и шифруется с помощью алгоритма вычисления степени.

$$C = M^e \bmod n.$$

Блок M восстанавливается с помощью той же операции, но с другим показателем степени.

$$M = C^d \bmod n.$$

Пара чисел (e, n) называется ключом шифрования, или открытым ключом, пара чисел (d, n) называется ключом расшифрования, или секретным ключом.

В схеме RSA число n является произведением двух больших простых чисел p и q.

$$n = pq.$$

Числа e и d являются взаимно обратными в кольце вычетов по модулю $\varphi(n)$, поэтому подбираются таким образом, чтобы

$$ed = 1 \bmod (p-1)(q-1).$$

При этом $\text{НОД}(e, (p-1)(q-1)) = 1$.

Тогда практически для любого M из множества $[0; n-1]$ выполняется равенство

$$M^{ed} = M \bmod n.$$

Для нахождения числа d, обратного к e, используется расширенный алгоритм Евклида, степени числа в кольце вычетов – бинарный алгоритм возведения в степень.

Все буквы текста необходимо приводить к верхнему регистру. Использовать таблицу замен для русского алфавита.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

Пробел между словами заменять числом 99.

Важно! Разбиение на блоки должно быть организовано так, чтобы ни один блок не начинался с цифры 0. Если такой блок образуется, то надо укоротить предыдущий блок, чтобы исключить эту ситуацию.

Например, открытый текст «Вася молодец» будет иметь представление: 1210274199222421241415 32. Его необходимо разбить на блоки, меньшие модуля шифрования. Например, для n = 22213 текст преобразовать в следующие блоки: М1 = 12102, М2 = 7419, М3 = 9222, М3 = 4212, М4 = 4141, М5 = 532. Каждый из блоков шифруется по отдельности.

Требования к программе.

1. Интерфейс программы – любой удобный.

2. Среда разработки и язык программирования могут быть произвольными.

Задание

1. Изучите алгоритм шифрования с открытым ключом RSA.

2. Создайте программу, позволяющую выполнить следующие действия:

2.1. Генерация не менее трех пар открытого/закрытого ключа для чисел p и q, заданных в табл. 4 для вашего варианта задания (использовать расширенный алгоритм Евклида).

2.2. Шифрование и расшифрование заданной текстовой строки (определяется в момент выполнения программы) по алгоритму RSA с выбором ключей из п. 2.1 (использовать бинарный алгоритм возведения в степень).

3. По результатам выполнения лабораторной работы оформите отчет (прил. 4).

Варианты заданий

Таблица 4

Вариант	p	q
1	227	373
2	97	229
3	101	233
4	103	239
5	107	241
6	109	251
7	113	257
8	127	263
9	131	269
10	137	271
11	139	277
12	149	281
13	151	283
14	157	293
15	163	307

Окончание табл. 4

Вариант	p	q
16	167	311
17	173	313
18	179	317
19	181	331
20	191	337
21	193	347
22	197	349
23	199	353
24	211	359
25	223	367
26	167	131
27	263	107
28	317	151
29	251	173
30	373	101

Контрольные вопросы

1. Каким требованиям должно удовлетворять число n, используемое в качестве модуля?

2. Что является открытым ключом шифрования?

3. Как вычисляется закрытый ключ шифрования по открытому ключу?

4. Как шифруемое сообщение разбивается на блоки?

5. По какой формуле осуществляется шифрование сообщения?

6. По какой формуле осуществляется расшифрование сообщения?

Лабораторная работа № 5
КРИПТОАНАЛИЗ ШИФРА RSA

Цель работы: исследование стойкости алгоритма RSA к атаке на факторизацию модуля.

Основные сведения

Одна из возможных атак на алгоритм RSA может быть реализована, если злоумышленнику удается факторизовать модуль n. Открытый ключ состоит из двух чисел: показателя степени e и модуля n. Если известно $n = p \cdot q$ (разложение модуля на произведение двух простых чисел, т. е. факторизация числа n), то может быть найден закрытый ключ системы. Для этого злоумышленник на первом этапе вычисляет функцию Эйлера

$$\varphi(n) = (p-1)(q-1).$$

После этого находит элемент d, обратный e по модулю $\varphi(n)$.

$$d = e^{-1} \bmod \varphi(n).$$

Обратный элемент эффективно вычисляется с помощью расширенного алгоритма Евклида.

Если модуль n является недостаточно большим числом, то его факторизация может быть выполнена с помощью пробного деления. Для этого проводится прямой перебор чисел от 2 до $\sqrt{n}$. Для каждого такого числа проверяют, является ли оно делителем числа n. Таким методом может быть найдено меньшее из двух чисел p или q. Второе число получают с помощью деления n на известный делитель.

Задание

1. В табл. 5 для каждого варианта задания даны открытый ключ шифрования RSA и зашифрованное сообщение. Напишите программу, позволяющую выполнить следующие действия:

1.1. Проведение факторизации числа n методом пробного деления.

1.2. Определение закрытого ключа.

1.3. Расшифрование сообщения.

2. По результатам выполнения лабораторной работы оформите отчет (прил. 5).

Требования к программе.

1. Интерфейс программы – любой удобный.

2. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Таблица 5

Вариант	(e, n)	C
1	(131, 21733)	258
2	(137, 25199)	19155
3	(59, 28829)	16357
4	(59, 29999)	21959
5	(259, 31921)	28368
6	(251, 33221)	25619
7	(251, 35909)	28498
8	(251, 37901)	238
9	(251, 40349)	39620
10	(251, 42869)	9491
11	(251, 44923)	14134
12	(251, 46883)	12351

Окончание табл. 5

Вариант	(e, n)	C
13	(251, 49583)	38076
14	(251, 50861)	8261
15	(251, 54053)	13047
16	(251, 56549)	20844
17	(251, 60479)	27990
18	(251, 61889)	23824
19	(251, 66043)	23262
20	(251, 70691)	18291
21	(251, 75137)	25028
22	(251, 77173)	37325
23	(251, 80851)	23313
24	(251, 83411)	59021
25	(251, 85073)	81019
26	(59, 28141)	9148
27	(59, 80057)	56943
28	(59, 113803)	28184
29	(59, 57377)	2948
30	(59, 70691)	41370

Контрольные вопросы

1. Как факторизация позволяет взломать шифр RSA?

2. Как можно вычислить закрытый ключ по известному открытому ключу?

3. Как можно факторизовать недостаточно большие числа? Какое количество шагов необходимо выполнить?

Лабораторная работа № 6
МЕТОДЫ ФАКТОРИЗАЦИИ ЧИСЛА

Цель работы: изучение методов факторизации числа.

Основные сведения

Факторизаций числа называется его разложение на произведение двух множителей. Факторизовать число m означает, что необходимо представить его в виде произведения двух чисел, т. е. $m = p \cdot q$.

Рассмотрим алгоритмы факторизации чисел на примерах (факторизация выполняется вручную).

Пример 1. Метод квадратичного решета.

Пусть необходимо провести факторизацию числа $m = 667$. Выберем решета по модулям $a = 3$, $b = 5$, $c = 7$ (это осуществляет пользователь).

Шаг 1. Строятся квадратичные решета по модулям a, b и c. Представим решета в виде таблиц. Во второй строке каждой таблицы окажется список квадратичных вычетов по выбранному модулю. Символ X в нижней строке означает, что число Z является квадратичным невычетом, поэтому соответствующий ему x отсеется в процессе поиска чисел, позволяющих найти делители числа m.

1) Для $a = 3$.

x	0	1	2
$x^2 \bmod 3$	0	1	1
$Z = x^2 - 667 \bmod 3$	2	0	0
S_3	X		

2) Для $b = 5$.

x	0	1	2	3	4
$x^2 \bmod 5$	0	1	4	4	1
$Z = x^2 - 667 \bmod 5$	3	4	2	2	4
S_5	X		X	X	

3) Для $c = 7$.

x	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1
$Z = x^2 - 667 \bmod 7$	5	6	2	0	0	2	6
S_7	X	X					X

Шаг 2. Наложим решета на последовательность чисел, расположенных в интервале от $\lceil\sqrt{m}\rceil + 1$ до $(m+1)/2$. Для числа $m = 667$ – это интервал чисел от 26 до 334. Рассмотрим 17 первых значений числа x. Установим первое число, с которого начинается наложение для каждого из решет a, b и c.

Для $a = 3$: $\lceil\sqrt{m}\rceil + 1 \bmod a = 26 \bmod 3 = 2$. Наложение решета S_3 необходимо начинать с $S_3(2)$.

Для $b = 5$: $\lceil\sqrt{m}\rceil + 1 \bmod b = 26 \bmod 5 = 1$. Наложение решета S_5 необходимо начинать с $S_5(1)$.

Для $c = 7$: $\lceil\sqrt{m}\rceil + 1 \bmod c = 26 \bmod 7 = 5$. Наложение решета S_7 необходимо начинать с $S_7(5)$.

В табл. 6 представлено наложение.

Таблица 6

x	26	~~27~~	~~28~~	~~29~~	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	~~37~~	~~38~~	~~39~~	~~40~~	~~41~~	~~42~~
S_3		X			X			X			X			X			X
S_5		X	X		X		X	X		X		X	X		X		X
S_7		X	X	X					X	X	X					X	X

Шаг 3. Проверяем первое ни разу не вычеркнутое число.

$x = 26,\ x^2 = 676,\ z = x^2 - m = 9 = 3^2$, число Z оказалось полным квадратом, поэтому $y = 3$.

Шаг 4. Если числа x и y найдены, то вычисляем делители числа m:

$p = x + y = 29, q = x - y = 23.$

Если числа x и y не найдены (y не целое), то переходим к следующему не вычеркнутому в списке значений x числу.

Ответ: 667 = 23 · 29.

Пример 2. ρ-*метод факторизации*.

Выполним факторизацию того же числа $m = 667$ ρ-методом. Сначала необходимо выбрать циклическую функцию. Будем использовать функцию

$$f(x) = (x^2 + 1) \bmod m.$$

Далее необходимо составить две рекуррентные последовательности

$$x_n^{(1)} = f\left(x_{n-1}^{(1)}\right),$$
$$x_n^{(2)} = f\left(f\left(x_{n-1}^{(2)}\right)\right).$$

Пусть первые члены рекуррентных последовательностей $x_0^{(1)} = 2$, $x_0^{(2)} = 2$. Номер члена последовательности принято называть номером шага алгоритма.

Вычислим первые члены последовательностей:

$$x_1^{(1)} = \left(\left(x_0^{(1)}\right)^2 + 1\right) \bmod m = (2^2 + 1) \bmod 667 = 5,$$

$$x_2^{(1)} = \left(\left(x_1^{(1)}\right)^2 + 1\right) \bmod m = (5^2 + 1) \bmod 667 = 26,$$

$$x_1^{(2)} = \left(\left(\left(x_0^{(2)}\right)^2 + 1\right)^2 + 1\right) \bmod m = ((2^2 + 1)^2 + 1) \bmod 667 = 26,$$

$$x_2^{(2)} = \left(\left(\left(x_1^{(2)}\right)^2 + 1\right)^2 + 1\right) \bmod m = ((26^2 + 1)^2 + 1) \bmod 667 = 101.$$

Также на каждом шаге будем вычислять модуль разности членов этих двух последовательностей:

$$a_n = \left|x_n^{(1)} - x_n^{(2)}\right|,$$
$$d_n = \text{НОД}(a_n, m).$$

Если на каком-то шаге будет получено значение d_n, удовлетворяющее условию $1 < d_n < m$, то это значение d_n является делителем числа m.

В табл. 7 представлены вычисления для данного примера.

Таблица 7

n	0	1	2	3	4	5
$x_n^{(1)}$	2	5	26	10	101	197
$x_n^{(2)}$	2	26	101	398	224	427
$a_n = \left\|x_n^{(1)} - x_n^{(2)}\right\|$	–	21	75	388	123	230
$d_n = \text{НОД}(a_n, 667)$	–	1	1	1	1	23

На пятом шаге алгоритма получено значение $d_5 = 23$, удовлетворяющее условию $1 < d_5 < 667$. Отсюда можно сделать вывод, что число 23 является делителем числа 667.

Ответ: $667 = 23 \cdot 29$.

Задание

1. Изучите алгоритмы факторизации с помощью квадратичных решет и ρ-метода.

2. Изучите вспомогательный алгоритм вычисления целозначного квадратного корня.

3. Создайте программу, выполняющую факторизацию числа m:

1) методом квадратичного решета с решетами по модулям a, b, c. Эти три числа программа должна запрашивать у пользователя в процессе работы. Определение числа Z на третьем шаге выполняйте с использованием алгоритма вычисления целозначного квадратного корня;

2) ρ-методом (циклическая функция $f(x) = (x^2 + 1) \bmod m$). Программа должна запрашивать начальные члены последовательностей и показывать, на каком шаге получен результат.

4. По результатам выполнения лабораторной работы оформите отчет (прил. 6).

Требования к программе.

1. Текст программы оформляется согласно общепринятым правилам (удобно для чтения, с описанием всех функций, переменных и особо важных мест).

2. Интерфейс программы – любой удобный.

3. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Вариант 1. $m = 898531$.
Вариант 2. $m = 547721$.
Вариант 3. $m = 578287$.
Вариант 4. $m = 445051$.
Вариант 5. $m = 467983$.
Вариант 6. $m = 503071$.
Вариант 7. $m = 1153987$.
Вариант 8. $m = 525829$.
Вариант 9. $m = 452351$.
Вариант 10. $m = 607567$.
Вариант 16. $m = 527707$.
Вариант 17. $m = 551987$.
Вариант 18. $m = 562013$.
Вариант 19. $m = 587663$.
Вариант 20. $m = 59833$.
Вариант 21. $m = 70247$.
Вариант 22. $m = 69841$.
Вариант 23. $m = 56743$.
Вариант 24. $m = 53491$.
Вариант 25. $m = 103459$.

Вариант 11. $m = 540737$.

Вариант 12. $m = 561293$.

Вариант 13. $m = 512327$.

Вариант 14. $m = 531803$.

Вариант 15. $m = 518293$.

Вариант 26. $m = 57619$.

Вариант 27. $m = 93011$.

Вариант 28. $m = 103861$.

Вариант 29. $m = 33401$.

Вариант 30. $m = 74483$.

Контрольные вопросы

1. В каком интервале выбираются значения чисел, являющихся модулями решет?

2. Как по невычеркнутым числам определяются делители?

3. Какие последовательности строятся в ρ-методе?

4. Как определяется делитель числа по членам последовательности?

Лабораторная работа № 7
ВЫЧИСЛЕНИЕ ДИСКРЕТНОГО ЛОГАРИФМА

Цель работы: изучение алгоритма «шаг младенца – шаг великана».

Основные сведения

Задача дискретного логарифмирования состоит в поиске такого числа x по известным числам a, b и p, чтобы выполнялось равенство

$$a^x = b \bmod p.$$

При ограниченной памяти данная задача является трудоемкой и может быть решена только прямым перебором. Если имеется достаточно большая память, то она может быть решена быстрее, например с помощью алгоритма «шаг младенца – шаг великана», который рассмотрен ниже.

Вычисляется целое число

$$k = \left[\sqrt{p}\right] + 1.$$

Строятся две последовательности

$$y_n = a^{nk} \bmod p,$$
$$z_n = b \cdot a^n \bmod p,$$

где $n = 1, 2, \ldots$.

Все числа обеих последовательностей запоминаются.

Выполняется поиск совпадения чисел в первой и второй последовательностях. Пусть число с номером i из первой последовательности совпадает с числом с номером j из второй последовательности.

$$y_i = z_j.$$

Такое совпадение чисел из последовательностей позволяет вычислить значение дискретного логарифма

$$x = i \cdot k - j.$$

Пример работы алгоритма.

Найти такое x, чтобы выполнялось равенство $6^x = 15 \bmod 109$ при $p = 109$, $a = 6$, $b = 15$.

Если $p = 109$, то $k = \left[\sqrt{p}\right] + 1 = \left[\sqrt{109}\right] + 1 = 11$.

Вычислим первые члены последовательностей y_n и z_n:

$y_1 = a^k \bmod p = 6^{11} \bmod 109 = 39$,

$y_2 = a^{2k} \bmod p = 6^{22} \bmod 109 = 104$,

$y_3 = a^{3k} \bmod p = 6^{33} \bmod 109 = 23$ и т. д.

$z_1 = b \cdot a \bmod p = 15 \cdot 6 \bmod 109 = 90$,

$z_2 = b \cdot a^2 \bmod p = 15 \cdot 6^2 \bmod 109 = 104$,

$z_3 = b \cdot a^3 \bmod p = 15 \cdot 6^3 \bmod 109 = 79$ и т. д.

Первые одиннадцать членов этих последовательностей представлены в табл. 8.

Таблица 8

n	1	2	3	4	5	6	7	8	9	10	11
z_n	90	*104*	79	38	10	60	33	89	98	43	40
y_n	39	*104*	23	25	103	93	30	80	68	36	96

Совпадение элементов происходит при $i = 2$ и $j = 2$: $y_2 = z_2 = 104$.

Найдем $x = i \cdot k - j = 2 \cdot 11 - 2 = 20$.

Выполним проверку: $6^{20} \bmod 109 = 15$.

Примечания. Для нахождения числа k потребуется алгоритм вычисления целочисленного значения квадратного корня из числа p. Для

нахождения элементов последовательностей y_n и z_n потребуется алгоритм быстрого возведения в степень в кольце вычетов по $\mathrm{mod}\, p$.

Задание

1. Изучите алгоритм вычисления дискретного логарифма «шаг младенца – шаг великана».

2. Изучите вспомогательный алгоритм вычисления целозначного квадратного корня.

3. Создайте программу, выполняющую поиск дискретного логарифма x при известных a, b и p методом «шаг младенца – шаг великана», чтобы $a^x = b \bmod p$.

4. По результатам выполнения лабораторной работы оформите отчет (прил. 7).

Требования к программе.

1. Интерфейс программы – любой удобный.

2. Среда разработки и язык программирования могут быть произвольными.

Варианты заданий

Вариант 1. $a = 2,\ b = 3,\ p = 101.$

Вариант 2. $a = 2,\ b = 24322,\ p = 30203.$

Вариант 3. $a = 2,\ b = 12161,\ p = 30203.$

Вариант 4. $a = 2,\ b = 18441,\ p = 30203.$

Вариант 5. $a = 4,\ b = 24322,\ p = 30203.$

Вариант 6. $a = 3,\ b = 24322,\ p = 30203.$

Вариант 7. $a = 7,\ b = 24322,\ p = 30203.$

Вариант 8. $a = 9,\ b = 24322,\ p = 30203.$

Вариант 9. $a = 2,\ b = 21740,\ p = 30323.$

Вариант 10. $a = 2,\ b = 10870,\ p = 30323.$

Вариант 11. $a = 15,\ b = 10870,\ p = 30323.$

Вариант 12. $a = 17,\ b = 10870,\ p = 30323.$

Вариант 13. $a = 2,\ b = 28620,\ p = 30539.$

Вариант 14. $a = 4,\ b = 28620,\ p = 30539.$

Вариант 15. $a = 5,\ b = 28620,\ p = 30539.$

Вариант 16. $a = 7,\ b = 28620,\ p = 30539.$

Вариант 17. $a = 2,\ b = 16190,\ p = 30803.$

Вариант 18. $a = 5,\ b = 16190,\ p = 30803.$

Вариант 19. $a = 8,\ b = 16190,\ p = 30803.$

Вариант 20. $a = 2,\ b = 30994,\ p = 31607.$

Вариант 21. $a = 4,\ b = 30994,\ p = 31607.$

Вариант 22. $a = 5,\ b = 30994,\ p = 31607.$

Вариант 23. $a = 2,\ b = 6,\ p = 107.$

Вариант 24. $a = 2,\ b = 7,\ p = 107.$

Вариант 25. $a = 2,\ b = 19,\ p = 107.$

Вариант 26. $a = 12,\ b = 11542,\ p = 31793.$

Вариант 27. $a = 12,\ b = 15762,\ p = 31793.$

Вариант 28. $a = 22,\ b = 15762,\ p = 31793.$

Вариант 29. $a = 12,\ b = 4758,\ p = 31793.$

Вариант 30. $a = 22,\ b = 4758,\ p = 31793.$

Контрольные вопросы

1. Как выводится формула, по которой вычисляется значение дискретного логарифма числа a по основанию b?

2. Предложите несколько способов поиска совпадающих элементов в двух последовательностях y_n, z_n.

3. Можно ли использовать методы сортировки массива для организации поиска совпадающих элементов последовательностей?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для вузов по специальности «Компьютерная безопасность» / А. В. Черемушкин. – Москва : Академия, 2009. – 271 с. – ISBN 978-5-7695-5748-4.

2. Гуменюк, А. С. Теория информации и кодирования : учеб. пособие / А. С. Гуменюк ; Ом. гос. техн. ун-т. – Омск : Изд-во ОмГТУ, 2015. – 1 CD-ROM (1,83 Мб). – Загл. с этикетки диска. – ISBN 978-5-8149-2111-6.

3. Игошин, В. И. Теория алгоритмов : учеб. пособие / В. И. Игошин. – Москва : ИНФРА-М, 2012. – 317 с. – ISBN 978-5-16-005205-2.

4. Нестеренко, А. Ю. Теоретико-числовые методы в криптографии : учеб. пособие / А. Ю. Нестеренко ; Московский гос. ин-т электроники и математики (технический ун-т). – Москва : Изд-во Московский гос. ин-т электроники и математики, 2012. – 222 с. – ISBN 978-5-94506-320-4.

5. Маховенко, Е. Б. Теоретико-числовые методы в криптографии : учеб. пособие / Е. Б. Маховенко. – Москва : Гелиос АРВ, 2006. – 318, [1] с. – ISBN 5-85438-143-5.

ПРИЛОЖЕНИЕ 1
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 1

Лабораторная работа № 1

Шифр Цезаря

Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Прямое преобразование шифра Цезаря:

Обратное преобразование шифра Цезаря:

Таблица кодировки символов:

Результаты

ШИФР-ТЕКСТ (ШТ):

РАСШИФРОВАННЫЙ ТЕКСТ (ОТ):

КЛЮЧ:

АВТОР И ПРОИЗВЕДЕНИЕ (ОТ):

ЗАШИФРОВАННЫЕ ФАМИЛИЯ И НАЗВАНИЕ (ШТ):

Варианты расшифрования исходного ШТ при различных значениях ключа:

$k = 1$:

$k = 2$:

...

$k = 31$:

Код программы

ПРИЛОЖЕНИЕ 2
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 2

Лабораторная работа № 2

Криптоанализ аффинного шифра

Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Формула для зашифрования текста:

Формула для расшифрования текста:

Результаты

ШИФР-ТЕКСТ (ШТ):

Результаты частотного анализа ШТ:

буква	**а**	**б**	**в**	**г**	**д**	**е/ё**	**ж**	**з**	**и**	**й**
частота										
буква	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**
частота										
буква	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ъ**	**ы**	**ь**	**э**
частота										
буква	**ю**	**я**								
частота										

Наиболее часто встречающиеся символы:

Системы уравнений:

Решения систем уравнений:

ВЕРНЫЙ КЛЮЧ:

РАСШИФРОВАННЫЙ ТЕКСТ (ОТ):

Код программы

ПРИЛОЖЕНИЕ 3
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 3

Лабораторная работа № 3

Модель открытого текста

Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Энтропия открытого текста определяется формулой:

Результаты

Энтропия для k-грамм открытого текста:

$k = 1,\ H_1 = \ldots,\quad \frac{H_1}{1} = \ldots,$

$k = 2, H_2 = \ldots,\quad \frac{H_2}{2} = \ldots,$

$k = 3, H_3 = \ldots,\quad \frac{H_3}{3} = \ldots,$

$k = 4, H_4 = \ldots,\quad \frac{H_4}{4} = \ldots,$

$k = 5, H_5 = \ldots,\quad \frac{H_5}{5} = \cdots.$

График зависимости H_k/k от k.

Асимптотическое значение H_k/k при $k \to \infty$: $\frac{H_k}{k} = \ldots.$

Код программы

ПРИЛОЖЕНИЕ 4
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 4

Лабораторная работа № 4
Шифрование с открытым ключом. Алгоритм RSA
Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Формула зашифрования:

Формула расшифрования:

Формула, связывающая открытый ключ и закрытый ключ:

Результаты

Параметр $n =$

1) Открытый ключ шифрования e = … .

Закрытый ключ шифрования d = … .

2) Открытый ключ шифрования e = … .

Закрытый ключ шифрования d = … .

3) Открытый ключ шифрования e = … .

Закрытый ключ шифрования d = … .

Открытый текст:

Блоки открытого текста:

$M_1 = \ldots, \quad M_2 = \ldots, \quad M_3 = \ldots, \quad \ldots$

Шифр-текст:

Код программы

ПРИЛОЖЕНИЕ 5
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 5

Лабораторная работа № 5

Криптоанализ шифра RSA

Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Факторизация числа $n =$

Функция Эйлера:

Формула для нахождения закрытого ключа по известному открытому ключу:

Результаты

Параметр $n =$

Открытый ключ шифрования $e = \dots$.

Факторизация числа n: $p = \dots, q = \dots$.

Закрытый ключ шифрования $d = \dots$.

Шифр-текст:

Открытый текст:

Код программы

ПРИЛОЖЕНИЕ 6
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 6

Лабораторная работа № 6
Методы факторизации числа
Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Результаты

$m = \dots .$

Метод квадратичного решета

$a = \ ..., b = \ ..., c = \ \dots .$

$x = \ ..., y = \ ...,$

$p = \ ..., \ q = \ \dots .$

ρ-метод факторизации

$n = \ \dots .$

$a_n = \ ..., \ \ d_n = \ \dots .$

$p = \ ..., \quad q = \ \dots .$

Код программы

ПРИЛОЖЕНИЕ 7
ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 7

Лабораторная работа № 7
Вычисление дискретного логарифма
Вариант №

Ф. И. О. студента:

Группа:

Проверил: Дата:

Основные сведения

Формулы вычисления последовательностей для параметров из варианта:

$y_n =$

$z_n =$

Результаты

$i =$ ..., $j =$ ... .

$y_i = z_j =$ ... .

$x = i \cdot k - j =$ ... .

Проверка по формуле $a^x = b \bmod p$:

Код программы