Министерство образования Республики Беларусь
Учреждение образования «Витебский государственный университет имени П.М. Машерова»
Кафедра информатики и информационных технологий

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Методические рекомендации

Витебск
ВГУ имени П.М. Машерова
2019

УДК [004.056:003.26:519.72](075.8)
ББК 32.811.4я73
К82

Печатается по решению научно-методического совета учреждения образования «Витебский государственный университет имени П.М. Машерова». Протокол № 6 от 26.06.2019.

Составитель: заведующий кафедрой информатики и информационных технологий ВГУ имени П.М. Машерова, кандидат физико-математических наук **Е.А. Витько**

Р е ц е н з е н т :
доцент кафедры алгебры и методики преподавания математики
ВГУ имени П.М. Машерова,
кандидат физико-математических наук *А.П. Мехович*

Криптографические методы : методические рекомендации / сост. Е.А. Витько. – Витебск : ВГУ имени П.М. Машерова, 2019. – 39 с.

К82

Данное издание подготовлено в соответствии с учебными программами дисциплин «Криптографические методы» и «Криптографический инженеринг» специальностей I ступени и дисциплины «Теоретико-числовые алгоритмы и криптография» специальности «Математика и компьютерные науки» II ступени высшего образования. Приводятся варианты заданий лабораторных работ и основные теоретические сведения, необходимые для их решения.

УДК [004.056:003.26:519.72](075.8)
ББК 32.811.4я73

Содержание

Введение

В современном мире информация, являющаяся основой для принятия решений, становится все более высокоценным товаром, который необходимо не только передавать и хранить, но и защищать. Среди способов защиты информации наиболее надежным считается криптографический, предусматривающий такое преобразование информации, при котором она становится доступной для прочтения лишь обладателю некоторого секретного параметра (ключа). Современные криптографические алгоритмы имеют серьезную математическую основу и опираются на такие фундаментальные математические дисциплины как алгебра, дискретная математика, теория вероятностей и математическая статистика. В методических рекомендациях рассмотрены основные теоретические сведения из алгебры, необходимые для понимания принципов работы ассиметричных криптографических алгоритмов или криптографических алгоритмов с открытым ключом. Данные системы криптографических преобразований характеризуются тем, что для зашифрования данных используется один ключ (открытый, т.е. доступный пользователям), а для расшифрования – другой (секретный) ключ. Такое свойство асимметричных систем шифрования позволяет в какой-то мере решить проблему распределения ключей между пользователями, которая является основным недостатком симметричных систем.

Данное издание подготовлено в соответствии с учебными программами дисциплин «Криптографические методы» и «Криптографический инженеринг» специальностей I ступени и дисциплины «Теоретико-числовые алгоритмы и криптография» специальности «Математика и компьютерные науки» II ступени высшего образования.

В определениях и обозначениях мы следуем [1–6].

Исторические шифры

До появления компьютеров криптография состояла из алгоритмов на символьной основе. Различные криптографические алгоритмы либо заменяли одни символы другими, либо переставляли символы. Лучшие алгоритмы делали и то и другое много раз. В настоящее время алгоритмы стали работать с битами, а не с символами, поэтому размер алфавита сократился до двух элементов. При этом, многие криптографические алгоритмы до сих пор комбинирует подстановки и перестановки:

1) шифры замены (подстановки) заменяют один символ открытого текста на другой символ в зашифрованном тексте.

2) шифры перестановки меняют местами позиции символов открытого текста.

Будем использовать следующие обозначения.

K – множество ключей. Каждый ключ $k \in K$ определяет некоторую преобразование E (*encryption*) на множестве открытых текстов PT (*plaintext*) и обратное преобразование D (*deciphering*) на множестве зашифрованных сообщений CT (*ciphertext*).

$E(k, p)$ – шифртекст открытого текста p, полученный в результате использования функции шифрования E с заданным ключом k;

$D(k, c)$ – открытый текст, соответствующий шифртексту c, полученный в результате использования функции расшифрования D с заданным ключом k.

Рассмотрим применение замены и перестановки символов в криптографических алгоритмах на примере некоторых исторических шифров.

***Шифр Цезаря* (*шифр сдвига, шифр простой замены*)**. В I веке н. э. Юлий Цезарь во время войны с галлами, в переписке с Римом, заменял в сообщении первую букву латинского алфавита A на четвертую D , вторую B – на пятую E , и т.д. последнюю – на третью в соответствии со следующей таблицей

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

т.е. каждая буква латинского алфавита сдвигается циклически вправо на $k = 3$ позиций.

Например, донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHQL YLGL YLFL

("Veni, vidi, vici" – лат. "Пришел, увидел, победил").

Понятно, что выбор ключа $k = 3$ не является единственно возможным. При других ключах k имеем $E($25, IBM) = HAL, E(6, IBM) = OHS.

Нетрудно показать, что функция расшифрования $D(k, c) = E(26 – k, c)$. Исключая слабый ключ $k = 0$, множество ключей имеет мощность $|K| = 25$.

Тарабарская грамота. Первое известное применение тайнописи в России относится к XIII в. Эту систему называли «тарабарской грамотой». В этой системе согласные буквы заменяются по схеме:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Например, ШЧУ – шифр слова ВГУ.

Еще один пример шифра простой замены – ***модулярный (аффинный) шифр***. Выберем число a, взаимно простое с модулем $m = 26$. Пусть p – буква английского алфавита, отождествленная со своим порядковым номером (0, 1, ... , 25). Тогда $E((a,k), p) = ap + k (\mathrm{mod}\ m)$, где k – фиксировано. В этом случае ключом является пара чисел (a, k). Условие взаимной простоты необходимо для обратимости шифра.

Криптосхема, принадлежащая ***Л. Хиллу***, основана на линейной алгебре. При шифровании заменяются пары букв (биграммная криптосхема). Осуществим цифровую кодировку букв английского алфавита: A = 0, B = 1, C = 2, ... , Z = 25. Выберем какую-нибудь обратимую по модулю 26 квадратную матрицу M порядка 2. Это – ключ. Пусть, например,

$$M = \begin{pmatrix} 2 & 5 \\ 3 & 3 \end{pmatrix}, M^{-1} = \begin{pmatrix} 17 & 15 \\ 9 & 20 \end{pmatrix}.$$

Биграммы будем записывать в виде матриц-столбцов. Например,

$$p_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, p_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Шифрование биграмм определим формулой $c = Mp$. Зашифруем, для примера, слово p = HELP = p_1p_2, тогда c = IHTA.

Шифр Виженера. Ключ образуется последовательностью букв k_1k_2 ... k_d (слово-лозунг), при этом для i-ой буквы сообщения a функция шифрования $f_i(a) = (a + k_i) (\mathrm{mod}\ m)$. Для реализации этой формулы можно воспользоваться следующей таблицей, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите.

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

Чтобы зашифровать сообщение, слово-лозунг подписывается с повторением над буквами сообщения. Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого, в вертикальном алфавите, а соответствующий ему знак сообщения в горизонтальном. На пересечении выделенных столбца и строки находим зашифрованную букву.

Например, зашифруем фразу «криптографические методы» с помощью слова-лозунга «вгу»:

в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г	у	в	г
к	р	и	п	т	о	г	р	а	ф	и	ч	е	с	к	и	е	м	е	т	о	д	ы
м	у	ь	с	х	в	е	у	у	ц	л	к	ж	ф	ю	к	з	а	ж	х	в	ё	ю

Наряду с подстановочными шифрами известны так называемые перестановочные (транспозиционные) шифры. При этом буквы сообщения остаются прежними, но меняют свое расположение в тексте.

Постолбцовая транспозиция **(XIX век).** К классу «перестановка» относится шифр «постолбцовая транспозиция». В данный прямоугольник [$m \times n$] вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Например, зашифруем фразу «Без труда не выловишь рыбку из пруда».

Решение. Фраза содержит 30 символов с учетом тире. Ее можно записать в прямоугольники размером 2×15, 3×10, 5×6 и т. д. Выберем прямоугольник 5×6.

б	е	з	т	р	у
д	а	н	е	в	ы
л	о	в	и	ш	ь
р	ы	б	к	у	и
з	п	р	у	д	а

Выписываем шифрованное сообщение по столбцам:

бдлрз еаоып знвбр теику рвшуд уыьиа.

Лабораторная работа 1

Цель работы: изучить алгоритмы, используемые в классических криптосистемах.

Задания. 1. Расшифровать криптограмму Цезаря (неалфавитные символы (пробелы, знаки препинания, цифры) – не преобразуются.).

2. Расшифровать криптограмму Виженера, если для шифрования было использовано слово-лозунг «шифр».

3. Реализовать схему шифрования посредством постолбцового варианта маршрутной транспозиции.

Входные параметры: сообщение, ключ (количество строк и столбцов в прямоугольнике, используемом для шифрования).

Выходные параметры: шифртекст.

4. Реализовать схему расшифрования посредством постолбцового варианта маршрутной транспозиции.

Входные параметры: шифртекст, ключ (количество строк и столбцов в прямоугольнике, используемом для шифрования).

Выходные параметры: открытый текст.

Вариант 1

1. Нгн ргцнг нултхсёугчлв ескрлног тсфоз чцржгпзрхгоярюш угдсх гпзулнгрфнсёс пгхзпгхлнг л аознхусхзшрлнг Носжг Ызррсрг (1916–2001).

2. Ачаякч шящдцрцы эш анбьб, и ьюшцэп – бр яюблэ.

Вариант 2

1. Е угдсхгш Носжг Ызррсрг «Пгхзпгхлъзфнгв хзсулв февкл» л «Хзсулв февкл е фзнузхрюш флфхзпгш» (1949) фсжзуйлхфв сдсдьзрлз дсояысёс стюхг фскжгрлв ылчусе, ргнстозррсёс жс рзёс, л угкугдгхюегзхфв тсорсщзррюм пгхзпгхлъзфнлм гттгугх жов нултхсёугчлъзфнлш кгжгъ.

2. Есе яйкщйшнжвч ъгьёящэ, ш ащьжкщы — ацфюбнб.

Вариант 3

1. Грголклуцв угрзз фцьзфхесегеылз ылчую, Носж Ызррср тулыио н еюесжц, ъхс дсояылрфхес лк рлш (жгйз фгпюз фосйрюз ылчую) фнсрфхуцлусегрю лк тусфхюш хлтлърюш нсптсрзрх, сфцьзфхеовбьлш кгпзрц л тзузфхгрсенц.

2. Ъъуыжн дядьыюшцрх ныых ъъуыжлг юэрврёеу.

Вариант 4

1. Дсозз ёоцдснсз тсрлпгрлз хсёс, нгн жсойрю фхуслхяфв ргжийрюз ылчую, тулезос Ызррсрг н еюжзозрлб жецш сдьлш тулрщлтсе тсфхусзрлв нултхсёугчлъзфнлш тузсдугксегрлм: тзузпзылегрлз л угффзлегрлз.

2. Еьшбух вщ гыг юэ щгфббфёп, ш цфдпсавч.

Вариант 5

1. Тзузпзылегрлз скргъгзх цфосйрзрлз ефзескпсйрюш февкзм пзйжц длхгпл схнуюхсёс л ылчусегррсёс хзнфхсе. Угффзлегрлз тсжугкцпзегзх угфтусфхугрзрлз еолврлв сжрсёс длхг схнуюхсёс хзнфхг рг дсояысз ълфос длхсе ылчусегррсёс хзнфхг.

2. Ымщ вбфф юэ хгчэы, жре ьб ажхгчэы.

Вариант 6

1. Носж Ызррср етзуеюз пгхзпгхл ъзфнл фхусёс фчсупцолусего естусфю с хзсузхлъзфнсм фхсмнсфхл ылчусе. Г лпзррс, ргфнсоянс цфхсмълесм веовзхфв ылчуфлфхзпг жов косцпюыозррлнг, сдогжгбьзёс рзсёугрлъзррюпл узфцуфгпл (еузпзрзп, тгпвхяб л х. ж.)?

2. Лхщюфн э гиьш тйн дхинжблы.

Вариант 7

1. Г фцьзфхецбх ол ылчуфлфхзпю, е нсхсуюш косцпюыозррлн рз тсоцълх рлнгнсм лрчсупгщлл, фнсоянс дю ср рл тзузшегхюего ылчухзнфх? Схезх снгкгофв тсосйлхзоярюп. Ылчуфлфхзпю, сдогжгбълз хгнлп фесмфхесп, ргкюегбхфв фсезуызррс фзнузхрюпл.

2. Ён чяъчещ, пыг фэффь, ш лгтжщэ, зкч ёфэффь.

Вариант 8

1. Флппзхулъргв ылчуфлфхзпг — флфхзпг ылчусегрлв, е нсхсусм нобъл кгылчусегрлв л угфылчусегрлв фсетгжгбх, олдс озёнс стузжзовбхфв сжлр тс жуцёспц. Тзузж лфтсояксегрлзп флппзхулърсм ылчуфлфхзпю гдсрзрхгп рзсдшсжлпс кгугрзз жсёсегулегхяфв с зжлрсп фзнузхрсп нобъз.

2. Анбьц уерйсж вжфвжэ, и лхдчцхги жблм.

Вариант 9

1. Гфлппзхулъргв ылчуфлфхзпг — флфхзпг ылчусегрлв, е нсхсусм лфтсоякцбхфв нобъл жецш елжсе — схнуюхюз нобъл л фзнузхрюз нобъл. Схнуюхюм нобъ тулпзрвзхфв е тусщзффз кгылчусегрлв л, нгн тугелос, веовзхфв сдьзжсфхцтрюп..

2. Ацфюфн вх ъчшщои - ц бжы ёреч вх йыфюэы ащкеёп.

Вариант 10

1. Нултхсёугчлъзфнгв фхсмнсфхя гфлппзхулърсм флфхзпю стузжзовзхфв хуцжсзпнсфхяб, ф нсхсусм косцпюыозррлн псйзх еюълфолхя фзнузхрюм нобъ лфшсжв лк кргрлв схнуюхсёс нобъг л жуцёсм жстсорлхзоярсм лрчсупгщлл с ылчуфлфхзпз. Сфрсерюп тузлпцьзфхесп гфлппзхулърсм ылчуфлфхзпю веовзхфв хс, ъхс гдсрзрхгп рз рцйрс кгугрзз жсёсегулегхяфв сд сдьзп фзнузхрсп нобъз.

2. Лаъсш с жблм я ажйщфшх цхььж.

Базовые алгоритмы криптографии

Алгоритмы арифметики больших чисел

Диапазон чисел, которые используются в реальных задачах криптографии, доходит до нескольких сот и даже тысячи десятичных цифр. Приведем алгоритмы арифметических операций над числами с произвольным числом разрядов (большими числами). Предполагается, что архитектура ЭВМ дает возможность выполнять элементарные арифметические операции над одно- и двухразрядными числами.

Пусть b – основание системы счисления. Целому неотрицательному числу u поставим в соответствие набор целых чисел $(u_{k-1}\ u_{k-2}\ \dots\ u_1\ u_0)_b$ такой, что

$$u = u_{k-1}b^{k-1} + u_{k-2}b^{k-2} + \dots + u_1 b + u_0,$$

где $0 \le u_{k-1}, u_{k-2}, \dots, u_1, u_0 < b$.

Алгоритм 1 (сложение). Сложение $u + v = (w_k \dots w_1 w_0)_b$ чисел $u = (u_{k-1}\ u_{k-2}\ \dots\ u_1\ u_0)_b$ и $v = (v_{k-1}\ v_{k-2}\ \dots\ v_1\ v_0)_b$.

1. Установить $c \leftarrow 0$.

2. Для $i = 0, \dots, k-1$ выполнить:

а) $w_i \leftarrow (u_i + v_i + c) \bmod b$;

б) положить $c \leftarrow 0$, если $u_i + v_i + c < b$ и $c \leftarrow 1$ в противном случае.

3. Установить $w_k \leftarrow c$.

Алгоритм 2 (вычитание). Вычитание $u - v = (w_{k-1} \dots w_1 w_0)_b$ числа $v = (v_{k-1}\ v_{k-2}\ \dots\ v_1\ v_0)_b$ из числа $u = (u_{k-1}\ u_{k-2}\ \dots\ u_1\ u_0)_b$, $u \ge v$.

1. Установить $c \leftarrow 0$.

2. Для $i = 0, \dots, k-1$ выполнить:

а) $w_i \leftarrow (u_i - v_i - c) \bmod b$;

б) положить $c \leftarrow 0$, если $u_i - v_i + c \ge 0$ и $c \leftarrow 1$ в противном случае.

Замечание. Если $u < v$, то по окончании выполнения алгоритма $c = 1$ и результат $w = u - v + b^k$.

Алгоритм 3 (умножение). Умножение $uv = (w_{k+l-1} \dots w_1 w_0)_b$ чисел $u = (u_{k-1}\ u_{k-2}\ \dots\ u_1\ u_0)_b$ и $v = (v_{l-1}\ v_{l-2}\ \dots\ v_1\ v_0)_b$.

1. Для $i = 0, \dots, k+l-1$ установить $w_i \leftarrow 0$.

2. Для $i = 0, \dots, l-1$ выполнить:

а) $c \leftarrow 0$;

б) для $j = 0, \dots, k-1$ вычислить $(xy)_b \leftarrow w_{i+j} + u_j v_i + c$ и установить $w_{i+j} \leftarrow y$, $c \leftarrow x$;

в) $w_{i+k} \leftarrow c$.

Алгоритм 4 (деление с остатком). Деление числа $u = (u_{k+l-1} \dots u_1\ u_0)_b$ на число $v = (v_{k-1} \dots v_1\ v_0)_b$, $k \geq 2$, $v_{k-1} \neq 0$, т.е. нахождение частного $q = (q_l \dots q_1\ q_0)_b$ и остатка $r = (r_{k-1} \dots r_1\ r_0)_b$ таких, что $u = qv + r$ и $0 \leq r < v$.

1. Выбрать произвольное целое число d такое, что

$$vd < b^k \text{ и}$$

$$\left[\frac{b}{2}\right] \leq v_{k-1}d < b,$$

Установить:

а) $u \leftarrow ud$, $u = (u_{k+l} \dots u_1\ u_0)_b$;

б) $v \leftarrow vd$, $v = (v_{k-1} \dots v_1\ v_0)_b$.

2. Для $i = k + l, k + l - 1, \dots, k$ выполнить:

а) вычислить пробное частное

$$\tilde{q} \leftarrow \min\left(\left[\frac{u_i b + u_{i-1}}{v_{k-1}}\right], b - 1\right)$$

б) пока $\tilde{q}(v_{k-1}b + v_{k-2}) > u_i b^2 + u_{i-1}b + u_{i-2}$, выполнить $\tilde{q} \leftarrow \tilde{q} - 1$;

в) $u \leftarrow u - \tilde{q}vb^{i-k}$;

г) (*корректирующее сложение*) если $u < 0$, то установить $\tilde{q} \leftarrow \tilde{q} - 1$,

$$u \leftarrow u + vb^{i-k};$$

д) $q_{i-k} \leftarrow \tilde{q}$.

3. Установить $r \leftarrow u/d$.

Действие на шаге 1 алгоритма называется *нормализацией*. При нормализации цикл 2б выполняется не более 2 раз. В общем случае можно выбрать

$$d = \left[\frac{b}{v_{k-1} + 1}\right].$$

Проверка чисел на простоту

Проверка чисел на простоту является составной частью алгоритмов генерации простых чисел, применяемых в криптографии с открытым ключом. Алгоритмы проверки на простоту можно разделить на вероятностные и детерминированные.

Детерминированный алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа).

Для того, чтобы проверить вероятностным алгоритмом, является ли число n простым, выбирают случайной число a ($1 < a < n$) и проверяют условия алгоритма. Если число n не проходит тест по основанию a, то алгоритм выдает результат «Число n составное». Если же n проходит тест по основанию a, ничего нельзя сказать о том, действительно ли число n является простым. Последовательно проведя ряд проверок таким тестом для разных a и получив для каждого из них ответ «Число n, вероятно, простое», можно утверждать, что число n является простым с вероятностью, близкой к 1. После T независимых выполнений теста вероятность того, что

составное число n будет T раз объявлено простым (вероятность ошибки), не превосходит $\frac{1}{2^T}$.

Для проверки чисел на простоту часто используется тест Миллера–Рабина.

Алгоритм 5 (тест Миллера–Рабина). Входные данные: нечетное число $n \geq 5$ и число итераций T.

1. Представить n в виде $2^s r + 1$, где s – натуральное число, r – нечетное натуральное число.

2. Для $t = 1,2,\ldots,T$ выполнить:

1) выбрать случайное целое число u, $2 \leq u \leq n - 2$;

2) $v \leftarrow u^r \, mod \, n$;

3) если $v = 1$ или $v = n - 1$, то перейти к 2.6;

4) для $i = 1,2,\ldots,s-1$ выполнить:

(a) $v \leftarrow v^2 \, mod \, n$;

(b) если $v = 1$, то возвратить “Число n составное”;

(c) если $v = n - 1$, то перейти к шагу 2.6;

5) возвратить “Число n составное”;

6) продолжить.

3 Возвратить “Число n, вероятно, простое“.

Лабораторная работа 2

Цель работы: изучить алгоритмы выполнения арифметических операций над числами с произвольным числом разрядов (большими числами) и тест Миллера–Рабина для проверки чисел на простоту.

Задания. 1. Разработайте класс «BigNumberOperations». Реализуйте в данном классе методы для выполнения арифметических операций над большими числами. Доработайте алгоритм вычитания для случая, когда результат операции является отрицательным.

2. Реализуйте алгоритм 5 (тест Миллера–Рабина) для проверки чисел на простоту.

Входные данные: нечетное число $n \geq 5$ и число итераций T.

Выходные данные: представление числа n в виде $2^s r + 1$,
значения чисел u и v на каждой итерации,
ответ “Число n составное” или “Число n, вероятно, простое“.

Теория чисел

Приведем некоторые теоретические сведения из теории чисел.

Пусть a, $b \in Z$, где Z – множество целых чисел, $b \neq 0$. Говорят, что

1) a делится на b, если существует целое число q такое, что $a = bq$.

Обозначается $a \vdots b$.

Таким образом, $a \vdots b \leftrightarrow \exists q \in Z, a = bq$.

2) a делится на b с остатком, если найдутся целые числа q и r такие, что $0 \leq r < |b|$ и $a = bq + r$.

Число r называют остатком, а q – частным (неполным частным при $r \neq 0$) от деления a на b. При $r = 0$ величины b и q называют делителями числа a.

Теорема (о делении с остатком). Для любых целых чисел a и b, $b \neq 0$, существует единственные целые числа q и r, $0 \leq r < |b|$ такие, что

$$a = b\,q + r.$$

Определение (деление по модулю). При заданных целых числа целых чисел a и b, $b \neq 0$ операция «a mod b» возвращает остаток от деления числа a на число b, т.е. целое неотрицательное число r, удовлетворяющее условию $0 \leq r < |b|$ такое, что $a = b\,q + r$.

Определение. Если целые числа $a_1, a_2, ..., a_n$ делятся на целое d, то d называют их общим делителем.

В дальнейшем речь идет только о положительных целых делителях.

Определение. Максимальный из общих делителей целых чисел $a_1, a_2, ..., a_n$ называется их наибольшим общим делителем и обозначается как НОД($a_1, a_2, ..., a_n$).

Теорема. Если $a = b \cdot q + c$, то НОД (a, b) = НОД (b, c).

Данная теорема позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема. Наибольший общий делитель целых чисел a и b ($a > b$) равен последнему отличному от нуля остатку в цепочке равенств:

$$\begin{gathered} a = bq_1 + r_1, \\ b = r_1 q_2 + r_2 \\ \cdots \\ r_{n-2} = r_{n-1} q_n + r_n \\ r_{n-1} = r_n q_{n+1} \end{gathered}$$

то есть r_n = НОД (a,b).

Пример. Найти НОД (442 818, 191 187).

Решение.

Способ 1. Воспользуемся разложением заданных чисел на простые множители

442 818 | 2 191187 | 3

221409	3
73803	3
24601	73
337	337
1	

63729	3
21243	3
7081	73
97	97
1	

Таким образом, $442818 = 2 \cdot 3^2 \cdot 73 \cdot 337$ и $191187 = 3^3 \cdot 73 \cdot 97$. Следовательно, НОД(442 818, 191 187) = $3^2 \cdot 73 = 657$.

Способ 2. Воспользуемся алгоритмом Евклида.

$$442\,818 = 191\,187 \cdot 2 + 60\,444;$$
$$191\,187 = 60\,444 \cdot 3 + 9\,855;$$
$$60\,444 = 9\,855 \cdot 6 + 1\,314;$$
$$9\,855 = 1\,314 \cdot 7 + 657;$$
$$1\,314 = 657 \cdot 7.$$

Следовательно, НОД(442 818, 191 187) = 657.

Теорема. Если d = НОД (a, b), то существуют такие целые u и v, что выполняется следующее соотношение (Безу):

$$d = au + bv.$$

Для нахождения u и v из соотношения Безу используют расширенный алгоритм Евклида. Он состоит из двух этапов:

1) проход вниз – собственно алгоритма Евклида;

2) проход вверх – последовательное выражение остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

Пример. Из предыдущего примера следует, что

$$657 = 9855 + 1314 \cdot (-7) =$$
$$= 9855 + \big(60444 + 9855 \cdot (-6)\big) \cdot (-7) =$$
$$= 9855 \cdot 43 + 60444 \cdot (-7) =$$
$$= \big(191187 + 60444 \cdot (-3)\big) \cdot 43 + 60444 \cdot (-7) =$$
$$= 191187 \cdot 43 + 60444 \cdot (-136) =$$
$$= 191187 \cdot 43 + \big(442818 + 191187 \cdot (-2)\big) \cdot (-136) =$$
$$= 442818 \cdot (-136) + 191187 \cdot 315$$

Определение. Натуральное число $p > 1$ называется простым, если оно имеет ровно два делителя (1 и p).

Заметим, что из соотношения $n = pq$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку $[2; \sqrt{n}]$. Исторически первый метод проверки натурального числа $n > 1$ на простоту заключается в делении его на простые числа, не превосходящие $\sqrt{n}$.

Теорема (Евклида). Простых чисел бесконечно много.

Определение. Целые числа a и b называются взаимно простыми, если НОД (a,b) = 1.

Теорема (*критерий взаимной простоты целых чисел*). Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство

$$au + bv = 1.$$

Определение. Целые числа a и b называются сравнимыми по модулю m тогда и только тогда, когда $(a - b) \vdots m$.

Другими словами, целые числа a и b называются сравнимыми по модулю m тогда и только тогда, когда a и b дают одинаковые остатки при делении на m.

Обозначают $a \equiv b \pmod m$ и называют это выражение сравнением.

Пример. $23 \equiv 3 \pmod 4$;

$-7 \equiv 1 \pmod 4$.

Замечание. Если $a = mq + r$, то $a - r = mq$, т.е. $a - r$ делится на m. Таким образом $a \equiv r \pmod m$ – всякое целое число сравнимо по модулю m со своим остатком от деления на m.

Основные свойства сравнений

1. Пусть $a \equiv b \pmod m$. Тогда $(a \pm c) \equiv (b \pm c) \pmod m$ для всякого целого c, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

2. Сравнения можно почленно складывать и вычитать: если $a \equiv b \pmod m$, $c \equiv d \pmod m$ то $(a + c) \equiv (b + d) \pmod m$, и $(a - c) \equiv (b - d) \pmod m$.

3. Сравнения можно почленно перемножать: $a \equiv b \pmod m$, $c \equiv d \pmod m$ то $ac \equiv bd \pmod m$.

4. Сравнения можно почленно возводить в любую натуральную степень n: если $a \equiv b \pmod m$ то $a^n \equiv b^n \pmod m$.

5. Если в сравнении $a \equiv b \pmod m$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить:

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right).$$

6. Сравнение можно сократить на общий множитель, взаимно простой с модулем: если $a = da_1$, $b = db_1$, НОД$(d,m) = 1$, то из сравнения $da_1 \equiv db_1 \pmod m$ следует сравнимость $a_1 \equiv b_1 \pmod m$.

7. Сравнение можно умножить на любой целый множитель: если $a \equiv b \pmod m$, то $at \equiv bt \pmod m$ для всякого целого t.

8. Рефлексивность: $a \equiv a \pmod m$ для любого целого a и всякого натурального m.

9. Симметричность: если $a \equiv b \pmod m$, то $b \equiv a \pmod m$.

10. Транзитивность: если $a \equiv b \pmod m$, $b \equiv c \pmod m$, то

$$a \equiv c \pmod m.$$

Рассмотрим задачу [4] нахождения остатка от деления числа a^s на m.

При решении данной задачи мы не можем вначале подсчитать значение a^s и затем взять его по модулю m, так как числа a и s могут быть в ты-

сячи бит длиной. Используя свойства, мы можем применять сравнение по модулю m ко всем промежуточным результатам, что не позволит числам разрастись до гигантских размеров.

Пример. Найдем остаток от деления 51^{43} на 19

Представим число 43 в двоичной системе $43_{10} = 101011_2$, т.е.

$$43 = 2^5 + 2^3 + 2^1 + 2^0$$

Вычислим остаток от деления 51^{2^k}, где $k \in \{0;\ 1;\ 3; 5\}$на 19.

$$51^1 \equiv 13 (\mathrm{mod}\ 19)$$
$$51^2 \equiv 13^2 = 169 \equiv 17 (\mathrm{mod}\ 19)$$
$$51^4 \equiv 17^2 = 289 \equiv 4 (\mathrm{mod}\ 19)$$
$$51^8 \equiv 4^2 = 16 (\mathrm{mod}\ 19)$$
$$51^{16} \equiv 16^2 = 256 \equiv 9 (\mathrm{mod}\ 19)$$
$$51^{32} \equiv 9^2 = 81 \equiv 5 (\mathrm{mod}\ 19)$$

Получим

$$51^{43} = 51^{32} \cdot 51^8 \cdot 51^2 \cdot 51^1 \equiv 5 \cdot 16 \cdot 17 \cdot 13 =$$
$$= 80 \cdot 221 \equiv 4 \cdot 12 = 48 \equiv 10 (\mathrm{mod}\ 19)$$

Чтобы подсчитать остаток от деления числа a^s на m, используют также приведенные ниже правила.

α_1) Если $s = 0$, тогда ответом будет 1.

α_2) Если $s > 0$ и является четным числом, тогда вначале вычислим

$$y \equiv a^{\frac{s}{2}} (\mathrm{mod}\ m),$$

используя эти же правила. Тогда окончательный результат

$$a^s \equiv y^2 (\mathrm{mod}\ m)$$

α_3) Если $s > 0$ и является нечетным числом, тогда вначале вычислим

$$y \equiv a^{\frac{s-1}{2}} (\mathrm{mod}\ m),$$

используя эти же правила. Тогда окончательный результат

$$a^s \equiv ay^2 (\mathrm{mod}\ m).$$

Это рекурсивная формулировка так называемого двоичного алгоритма, по которому показатель степени формируется бит за битом от наиболее значимой части двоичного представления показателя к наименее значимой его части. Сколько операций умножения потребуется, чтобы вычислить остаток? Пусть k – это число бит значения s; другими словами,

$$2^{k-1} \le s < 2^k.$$

Тогда данный алгоритм требует выполнения не более чем $2k$ умножений по модулю m. Если длина s будет составлять около 2000 бит, то понадобится лишь 4000 вычислений. Этот объем работы, хотя и достаточно большой, определенно доступен вычислительным возможностям современных настольных компьютеров.

Лабораторная работа 3

Цель работы: изучить способы нахождения наибольшего общего делителя двух чисел и остатка от деления при возведении в степень посредством применения теории сравнений.

Задания. 1. Реализуйте метод «Factorization» для разложения натурального числа a на простые множители.

2. Реализуйте методы «NodFactorization» и «NodEuclidean» для нахождения наибольшего общего делителя двух чисел a и b посредством разложения на простые множители и по алгоритму Евклида соответственно.

3. Реализуйте метод «IdentityBezu» для вычисления коэффициентов u и v, удовлетворяющих соотношению Безу $au + bv = НОД(a,b)$.

4. Реализуйте метод «DegreeRemainder1» и «DegreeRemainder2» для вычисления остатка от деления степени a^m на число n по алгоритмам, описанным выше.

Используйте разработанные методы для случая, если входные параметры имеют следующие значения.

	a	b	a^m	n
Вариант 1	8128575	39303	15214587^{20157}	3511
Вариант 2	1533825	198495	23548756^{32097}	4111
Вариант 3	647856	83436	43598756^{31455}	5023
Вариант 4	1843600	117320	19264584^{51487}	2347
Вариант 5	2758392	294700	14458521^{24589}	2529
Вариант 6	1260675	107750	24788747^{33013}	2237
Вариант 7	810576	128601	54541926^{20710}	2573
Вариант 8	597040	603625	47811801^{34009}	4145
Вариант 9	5681475	1016685	78587926^{40011}	2243
Вариант 10	6910110	179600	75859801^{2010}	4451

Классы вычетов

При делении целых чисел на натуральное целое $m > 1$ существует m различных остатков: 0, 1, 2, …, $m - 1$. Соответственно этим остаткам множество Z разбивается на m непересекающихся классов сравнимых друг с другом чисел, то есть имеющих один и тот же остаток от деления на m. В соответствии с остатками от деления на m эти классы будем обозначать через $\bar{0}, \bar{1}, \ldots, \overline{m-1}$. Таким образом, класс $\bar{r} = \{r + mk | k \in Z\}$ для каждого $r = 0, 1, 2, \ldots, m - 1$. Множество всех классов сравнимых друг с другом чисел по данному модулю называют множеством классов вычетов по модулю и обозначают через Z/mZ.

Определим операции сложения и умножения на множестве классов вычетов следующим образом:

$$\bar{k} \oplus \bar{l} = \overline{k + l};$$
$$\bar{k} \otimes \bar{l} = \overline{k \cdot l}.$$

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то в Z/mZ справедливы следующие свойства

1) коммутативность
$\bar{k} \otimes \bar{l} = \bar{l} \otimes \bar{k}$,
$\bar{k} \oplus \bar{l} = \bar{l} \oplus \bar{k}$,

2) ассоциативность
$\bar{k} \otimes (\bar{l} \otimes \bar{r}) = (\bar{k} \otimes \bar{l}) \otimes \bar{r}$,
$\bar{k} \oplus (\bar{l} \oplus \bar{r}) = (\bar{k} \oplus \bar{l}) \oplus \bar{r}$,

3) существует нейтральный элемент
по умножению $\bar{k} \otimes \bar{1} = \bar{1} \otimes \bar{k} = \bar{k}$,
по сложению $\bar{k} \oplus \bar{0} = \bar{0} \oplus \bar{k} = \bar{k}$,

4) для каждого класса $\bar{k} \in Z/mZ$ существует противоположный элемент $\bar{l}$ такой что

$$\bar{k} \oplus \bar{l} = \bar{0},$$

им является класс $\bar{l} = \overline{m - k}$.

5) $(\bar{k} \oplus \bar{l}) \otimes \bar{r} = (\bar{k} \otimes \bar{r}) \oplus (\bar{l} \otimes \bar{r})$ – дистрибутивность.

Следовательно, множество Z/mZ является коммутативным кольцом с единицей, которое называют кольцом классов вычетов по модулю m.

Определение. Элемент $\bar{k} \in Z/mZ$ называется обратимым, если найдется такой класс $\bar{l} \in Z/mZ$, что

$$\bar{k} \otimes \bar{l} = \bar{1}.$$

Тогда класс $\bar{l}$ называют обратным к классу $\bar{k}$.

Множество всех обратимых элементов кольца классов вычетов по модулю m обозначают Z_m^*.

Теорема. Класс $\bar{k}$ из кольца Z/mZ обратим тогда и только тогда, когда НОД(m,k) = 1. В частности, если $m = p$ – простое число, то в кольце Z/mZ каждый ненулевой класс обратим.

Замечание. В условиях теоремы НОД(m,k) = 1. Поэтому существуют такие целые u и v, что выполняется соотношение Безу:

$$1 = ku + mv.$$

Тогда $\bar{1} = \overline{ku} \oplus \overline{mv}$. Так как $mv \equiv 0 \pmod{m}$, то

$$\bar{1} = \overline{ku}.$$

Следовательно, $\bar{u}$ – обратный класс к $\bar{k}$.

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример. Запишем таблицы сложения и умножения в $Z/7Z$.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Из таблицы умножения непосредственно видно, что все строки, за исключением строки $\bar{0}$, содержат элемент $\bar{1}$, то есть обратимы все ненулевые классы $Z/7Z$ (в полном соответствии с теоремой).

Определение. Функция Эйлера – функция $\varphi(m)$, которая каждому натуральному числу $m > 1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.

Свойства функции Эйлера

i) $\varphi(p) = p - 1$ для каждого простого числа p.

ii) $\varphi(p^n) = p^n - p^{n-1}$ для каждого простого числа p и для произвольного натурального n.

iii) если НОД(n,m) = 1, то

$$\varphi(nm) = \varphi(m)\,\varphi(m).$$

iv) если $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_t^{k_t}$ – каноническое разложение, то

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_t}\right).$$

Пример. Вычислим φ(48).

Поскольку $48 = 3 \cdot 2^4$, то согласно свойству 4

$$\varphi(48) = 48\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) = 16.$$

Замечание. В кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов.

Лабораторная работа 4

Цель работы: изучить свойства бинарных алгебраических операций в кольце классов вычетов и способы вычисления значения функции Эйлера.

Задания. 1. Постройте таблицы сложения и умножения элементов кольца классов вычетов.

2. Реализуйте методы для нахождения значения функции Эйлера по формулам i-iv.

3. Реализуйте два метода для вычисления обратных элементов. Метод «InverseClass» – нахождение обратного элемента непосредственным перебором всех элементов кольца классов вычетов, метод «InverseBezu» – нахождение обратного элемента посредством использования соотношения Безу. Оба метода должны вначале проверить, является ли заданный элемент обратимым.

Входные данные: *m* – модуль кольца классов вычетов,
n – элемент кольца классов вычетов, к которому нужно найти обратный элемент.

Выходные данные: обратный элемент n^{-1} или ответ "*n* не обратим в кольце классов вычетов по модулю *m*".

Группы и подгруппы

Определение. Группой называется непустое множество G с определенной на нем бинарной алгебраической операцией, относительно которой выполняются следующие свойства:

1) ассоциативность

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

для любых $a, b, c \in G$;

2) существует нейтральный элемент (единица), то есть такой элемент $e \in G$, что

$$e \cdot g = g \cdot e = g$$

для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, то есть такой элемент $h \in G$, что $g \cdot h = h \cdot g = e$ (в этом случае пишут: $h = g^{-1}$).

Определение. Группа G называется коммутативной, или абелевой, если определенная в ней операция обладает свойством коммутативности:

4) $a \cdot b = b \cdot a$ для всех $a, b \in G$.

Определение. Порядком конечной группы G называется количество элементов этой группы и обозначается $|G|$.

Подмножество H группы G называется подгруппой, если H – группа относительно той же операции, которая определена на группе G. Для подгруппы используется следующее обозначение: $H \leq G$.

Теорема (Лагранжа). Порядок конечной группы делится на порядок любой ее подгруппы.

Пусть a – фиксированный элемент произвольной группы G. Обозначим

$$\langle a \rangle = \{a^m | m \in Z\}$$

множество всевозможных целых степеней элемента a, где

$$a^0 = e,$$
$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}},$$
$$a^{-n} = (a^{-1})^n.$$

Тогда $\langle a \rangle$ – абелева группа, которая называется циклической группой, порожденной элементом a.

Теорема. Для каждого простого числа p множество всех ненулевых классов из кольца классов вычетов образуют группу относительно операции умножения, причем эта группа является циклической.

Пусть a – произвольный элемент группы G. Рассмотрим два возможных случая:

1) Все степени элемента a различны, т.е. $a^m \neq a^n$ для всех целых $m \neq n$. В этом случае говорят, что элемент a имеет бесконечный порядок.

2) Имеются совпадения $a^m = a^n$ при $m \neq n$. Если, например, $m > n$, то $m - n > 0$ и

$$a^{m-n} = e,$$

т.е. существуют натуральные степени элемента a, равные единичному элементу. Наименьшее натуральное число k, при котором $a^k = e$, называют порядком элемента a и пишут $|a| = k$.

Теорема. Пусть элемент $a \in G$ имеет конечный порядок k. Тогда

$$\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}.$$

Кроме того, $a^m = e$ в точности тогда, когда k делит m.

Теорема. Если G – конечная группа из n элементов, то для каждого $a \in G$ выполняется равенство $a^n = e$. Другими словами, в конечной группе порядок любого ее элемента делит порядок самой группы.

Теорема. Для всякого простого числа p мультипликативная группа Z_p^* является циклической.

Пусть g –элемент конечной мультипликативной группы G. Если порядок элемента g равен порядку группы G, то g называют *первообразным корнем или примитивным элементом* группы G.

Пусть Ω – конечное множество из n элементов. Поскольку природа его элементов для нас не существенна, удобно считать, что $\Omega = \{1,2,\dots,n\}$.

Определение. Всякая биекция, то есть взаимно однозначное отображение Ω в себя, называется подстановкой на Ω.

Подстановку f изображают в виде двустрочной таблицы:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

В этой таблице каждый i-й столбец указывает, в какой элемент $f(i)$ преобразуется элемент i, $1 \le i \le n$.

Подстановки перемножаются в соответствии с общим правилом композиции отображений:

$$(gf)(i) = g(f(i)).$$

Очевидно, тождественная подстановка

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

является нейтральным элементом относительно композиции подстановок. Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1} достаточно в таблице

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки. Таким образом, подстановки на Ω образуют группу относительно операции композиции отображений – умножения

подстановок. Ее называют симметрической группой степени n и обозначают через S_n.

Теорема. Порядок группы S_n равен $n!$.

Пример. Пусть $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$. Найти произведение fg, обратный элемент f^{-1}, выписать циклическую группу $\langle f \rangle$, указать ее порядок.

Решение.

Произведение подстановок

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Обратная подстановка

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}.$$

Действительно,

$$ff^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Выпишем циклическую группу, порожденную подстановкой f:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$$

$$f^2 = ff = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

$$f^3 = ff^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

$$f^4 = ff^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$$

$$f^5 = ff^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\langle f \rangle = \{e, f, f^2, f^3, f^4\}, |\langle f \rangle| = 5.$

Лабораторная работа 5

Цель работы: изучить основные сведения о группах и подгруппах.

Задания. 1. Выпишите циклическую группу, порожденную подстановкой f. Укажите порядок полученной группы. Вычислите натуральное число n, для которого выполняется равенство $f^n = f^{-1}$.

2. Расшифруйте сообщение по криптосхеме Л. Хилла, если задана матрица M, используемая при шифровании. Предварительно проверьте условие обратимости матрицы M.

3. Выпишите все элементы мультипликативной группы кольца классов вычетов по модулю m. Сравните их количество и значение функции Эйлера $\varphi(m)$.

4. Для заданного элемента $g \in Z/mZ$ выпишите множество степеней $\{g^n \bmod m | \ n \in N\}$. Если полученное множество

1) является группой, то найдите её порядок;

2) совпадает с мультипликативной группой кольца классов вычетов по модулю m, то выведите сообщение «g – примитивный элемент мультипликативной группы кольца классов вычетов по модулю m (первообразный корень по модулю m)».

5. Определите, является ли циклической мультипликативная группа кольца классов вычетов по модулю m. Если группа является циклической, то выпишите все первообразные корни по данному модулю.

Используйте разработанные методы для случая, если входные параметры имеют следующие значения.

Задание 1

Вариант 1

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 6 & 8 & 4 & 1 & 3 & 7 \end{pmatrix}$$

Вариант 2

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 1 & 7 & 8 & 5 & 2 & 4 \end{pmatrix}$$

Вариант 3

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 3 & 1 & 4 & 2 & 6 & 7 \end{pmatrix}$$

Вариант 4

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 2 & 8 & 1 & 3 & 4 & 7 & 5 \end{pmatrix}$$

Вариант 5

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 2 & 1 \end{pmatrix}$$

Вариант 6

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 3 & 4 & 8 \end{pmatrix}$$

Вариант 7

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 1 & 6 & 3 & 7 & 4 & 5 & 2 \end{pmatrix}$$

Вариант 8

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 7 & 5 & 9 & 3 & 6 & 1 & 2 \end{pmatrix}$$

Вариант 9

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 6 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}$$

Вариант 10

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}$$

Задания 2, 3, 4.

Вариант 1 $m = 11$, $g = 5$

$m = 24$, $g = 7$

Вариант 2	$m = 13, g = 11$
	$m = 18, g = 12$
Вариант 3	$m = 11, g = 15$
	$m = 25, g = 12$
Вариант 4	$m = 17, g = 13$
	$m = 21, g = 12$
Вариант 5	$m = 19, g = 17$
	$m = 26, g = 15$
Вариант 6	$m = 13, g = 10$
	$m = 27, g = 7$
Вариант 7	$m = 17, g = 14$
	$m = 30, g = 8$
Вариант 8	$m = 33, g = 16$
	$m = 29, g = 15$
Вариант 9	$m = 17, g = 14$
	$m = 22, g = 13$
Вариант 10	$m = 16, g = 13$
	$m = 23, g = 19$

Криптосистема RSA

Историю асимметричной криптографии принято отсчитывать с момента публикации в 1976 году работы американских математиков У. Диффи и М. Хеллмана [7]. В асимметричных криптосистемах нашла своё применение математическая теория сложных задач. Оказалось возможным строить такие математические функции, которые «легко» вычисляются, а обращаются «очень трудно»: для этого необходимы нереальные вычислительные ресурсы и время. Однако если для подобной функции известна некоторая дополнительная информация (её часто называют «лазейкой»), то обратить функцию можно тоже «легко». Такие функции называются односторонними или односторонними с лазейкой.

Используя одностороннюю функцию f с лазейкой s абонент А может построить асимметричную шифрсистему, например так. Алгоритм вычисления функции f объявить открытым ключом и сделать общедоступным. «Лазейку» s назвать своим секретным ключом и сохранить в тайне. Любой другой абонент, скажем В, используя открытый ключ, может зашифровать секретное сообщение m для абонента А. Для этого он вычисляет значение $f(m)$, которое и передает абоненту А по открытому каналу связи. Злоумышленник, перехватив значение $f(m)$, не может восстановить сообщение m так как задача обращения функции f «очень трудна». Только абонент А может справиться с задачей обращения, так как ему известна «лазейка» s. Вычисляя $f^{-1}(m, s)$, он «легко» восстанавливает сообщение m.

До сих пор существование односторонних функций строго не доказано. Но имеется несколько функций-кандидатов, обладающих свойствами односторонних функций. Они используются для построения современных асимметричных шифрсистем. Среди них, например, функция произведения двух простых чисел, скажем, p и q. Обратить такую функцию, т. е. решить задачу факторизации (разложения на множители числа $n = pq$, очень сложно, если p и q достаточно большие, например имеют в десятичной записи не менее 100 знаков. Дополнительной информацией для быстрого обращения может служить, например, один из делителей или значение функции Эйлера от числа n. На основе функции произведения двух простых чисел строится криптосистема RSA.

Другая функция-кандидат – возведение в степень по модулю. Пусть n и g – целые числа такие, что $2 \le g \le n - 1$. Пусть функция f сопоставляет произвольному целому числу m $(2 \le m \le n - 1)$ значение $x = g^m \bmod n$. Восстановить m по значениям x, g и n – это тоже очень трудная задача, которая называется задачей дискретного логарифмирования. На её основе строится криптосистема Эль-Гамаля, которая описана в последнем пункте данного пособия.

Рассмотрим принципы работы криптосистемы RSA.

Пусть p и q – большие простые числа. Вычислим их произведение $n = pq$. Тогда функция Эйлера

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

Выбираем натуральное число e, такое, что

$$0 < e < n$$

и

$$\text{НОД}\,(e, \varphi(n)) = 1.$$

Пара (e,n) и будет открытым ключом. Шифруемая информация переводится в цифровую форму. Например, в первоисточнике буквы латинского алфавита заменялись двузначными числами: «*a*» = 01, «*b*» = 02, …, пробел = 00. Получается некоторое число m. Предполагается, что,

$$0 < m < n$$

и

$$\text{НОД}\,(m, n) = 1.$$

Сообщение передается числом

$$c = m^e \bmod n.$$

Адресат получает сообщение (c,e,n). Он, как и все, знает n и e. Он также должен знать секретный ключ – такое натуральное $d < n$, что

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Значит,

$$ed = \varphi(n)\cdot k + 1.$$

для некоторого целого k. Тогда по теореме Эйлера

$$c^d = m^{ed} = m \cdot \left(m^{\varphi(n)}\right)^k \equiv m \cdot 1 = m \pmod{n}.$$

Итак, для нахождения m достаточно найти остаток от деления c^d на n.

Взломать RSA можно, только если найти d – решение сравнения $ed \equiv 1 \pmod{\varphi(n)}$. Для этого надо знать $\varphi(n)$. Из свойств $\varphi(n)$ следует, что единственно надежный путь для этого – разложить n на множители – трудоемкая задача, составляющая основу криптографической стойкости *RSA*.

Пример. Зашифровать в системе RSA сообщение $m = 156$.

Решение. Выбираем число n (произведение двух простых чисел) такое, что

$$n > 156 \text{ и } \text{НОД}(156,n) = 1.$$

Пусть $n = 11 \cdot 19 = 209$, т.е. $p = 11$ и $q = 19$. Тогда

$$\phi(209) = \phi(11) \cdot \phi(19) = 10 \cdot 18 = 180.$$

Выбираем натуральное число e, такое, что

$$0 < e < n \text{ и } \text{НОД}(e, \phi(n)) = 1,$$

т.е. $0 < e < 209$ и $\text{НОД}(e, 180) = 1$. Выбираем $e = 7$. Тогда шифртекст

$$c \equiv m^e \equiv 156^7 \pmod{209}.$$

Возведем в степень, используя свойства α_1–α_3, сформулированные в теме «Теория чисел». Получим следующую последовательность вычислений:

$$156^1 \equiv 156 \pmod{209};$$

$$156^3 = 156^2 \cdot 156 = 24336 \cdot 156 \equiv 92 \cdot 156 =$$

$$= 14352 \equiv 140 \pmod{209};$$

$$156^7 = 156 \cdot (156^3)^2 \equiv 156 \cdot 140^2 = 156 \cdot 19600 \equiv$$
$$\equiv 156 \cdot 163 = 25428 \equiv 139(\text{mod } 209).$$

Пара (7, 209) – открытый ключ. Передаваемое сообщение (139, 7, 209).

Ответ: (139, 7, 209).

Пример. Расшифровать сообщение (139, 7, 209).

Решение.

Раскладываем $n = 209$ на простые множители

$$209 = 11 \cdot 19,$$

т.е. $p = 11$ и $q = 19$.

Находим значение функции Эйлера

$$\phi(209) = (p-1)(q-1) = 10 \cdot 18 = 180.$$

Находим секретный ключ d. Так как $ed \equiv 1(mod\, \phi\,(n))$, то d – обратный элемент для e в кольце классов вычетов по модулю 180. Используем алгоритма Евклида.

Прямой ход алгоритма Евклида. Находим НОД$(\phi(n), e) =$ НОД(180,7):

$$180 = 7 \cdot 25 + 5$$
$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Обратный ход алгоритма Евклида.

Находим u и v такие, что

$$\text{НОД}(\phi(n), e) = u \cdot \phi(n) + v \cdot e$$

т.е.

$$1 = u \cdot 180 + v \cdot 7$$

Тогда $\bar{v} = (\bar{e})^{-1}$ – секретный ключ d.

$$1 = 5 + (-2) \cdot 2 = 5 + (-2) \cdot (7 + (-1) \cdot 5) = 3 \cdot 5 + (-2) \cdot 7 =$$
$$= 3 \cdot (180 + (-25) \cdot 7) + (-2) \cdot 7 = 3 \cdot 180 + (-77) \cdot 7.$$

Тогда $(\bar{e})^{-1} = (\bar{7})^{-1} = \overline{-77} = \overline{-77 + 180} = \overline{103}$. Следовательно, $d =$ 103.

Так как $m \equiv c^d (mod\, n)$, то $m \equiv 139^{103}(\text{mod } 209)$.

$$139^1 \equiv 139(\text{mod } 209);$$
$$139^3 = 139 \cdot 139^2 = 139 \cdot 19321 \equiv 139 \cdot 93 = 12927 \equiv 178(\text{mod } 209);$$
$$139^6 \equiv 178^2 = 31684 \equiv 125(\text{mod } 209);$$
$$139^{12} \equiv 125^2 = 15625 \equiv 159(\text{mod } 209);$$
$$139^{25} \equiv 139 \cdot 159^2 = 139 \cdot 25281 \equiv 139 \cdot 201 = 27939 \equiv 142(\text{mod } 209);$$
$$139^{51} \equiv 139 \cdot 142^2 = 139 \cdot 20164 \equiv 139 \cdot 100 = 13900 \equiv 106(\text{mod } 209);$$
$$139^{103} \equiv 139 \cdot 106^2 = 139 \cdot 11236 \equiv 139 \cdot 159 = 22101 \equiv$$
$$\equiv 156(\text{mod } 209).$$

Ответ: $m = 156$.

Лабораторная работа 6

Цель работы: изучить алгоритмы шифрования и расшифрования в криптосистеме RSA.

Задания. 1. Реализуйте метод «RSAEncryption» для шифрования сообщения по алгоритму RSA.

Входные данные: m – открытый текст.

Выходные данные: c – шифртекст,

n, e – открытый ключ.

2. Реализуйте метод «RSADecryption» для дешифрования сообщения по алгоритму RSA. Если введены некорректные параметры, то вывести соответствующее сообщение об ошибке.

Входные данные: c – шифртекст,

n, e – открытый ключ.

Выходные данные: m – открытый текст;

d – секретный ключ.

Используйте разработанные методы для случая, если входные параметры имеют следующие значения.

	Задание 2		
	c	n	e
Вариант 1	313180	654583	457
Вариант 2	138398	688927	487
Вариант 3	33101	654659	431
Вариант 4	132869	748081	593
Вариант 5	126721	689863	701
Вариант 6	272846	654583	457
Вариант 7	174355	688927	487
Вариант 8	583561	654659	431
Вариант 9	643830	748081	593
Вариант 10	563103	689863	701

Китайская теорема об остатках

Теорема. Пусть $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ – разложение натурального числа m в произведение попарно взаимно простых множителей. Пусть $b_1, b_2, \ldots, b_n$ – произвольные фиксированные целые числа. Тогда система сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ \ldots \\ x \equiv b_n (\mathrm{mod}\, m_n) \end{cases}$$

всегда имеет решения и все они сравнимы друг с другом по модулю m.

Название теоремы объясняется тем, что исторически впервые она рассматривалась в китайском «Учебнике математики мастера Сана», написанном между 287 и 473 годами нашей эры.

Пусть целое число x имеет n остатков b_i от деления на каждый из делителей m_i числа m. Набор $(b_1, b_2, \ldots, b_n)$ называется *CRT*-представлением числа x.

Тогда из свойств сравнений получим

Следствие. Если $(b_1, b_2, \ldots, b_n)$ – *CRT*-представление числа x, $(c_1, c_2, \ldots, c_n)$– *CRT*-представление числа y, то

$\big((b_1 + c_1) \mathrm{mod}\, m_1, (b_2 + c_2) \mathrm{mod}\, m_2, \ldots, (b_n + c_n) \mathrm{mod}\, m_n\big)$ – *CRT*-представление числа $(x + y) \mathrm{mod} m$;

$\big((b_1 \cdot c_1) \mathrm{mod}\, m_1, (b_2 \cdot c_2) \mathrm{mod}\, m_2, \ldots, (b_n \cdot c_n) \mathrm{mod}\, m_n\big)$ – *CRT*-представление числа $(x \cdot y) \mathrm{mod} m$;

$\big((b_1^s) \mathrm{mod}\, m_1, (b_2^s) \mathrm{mod}\, m_2, \ldots, (b_n^s) \mathrm{mod}\, m_n\big)$ – *CRT*-представление числа $(x^s) \mathrm{mod} m$.

Таким образом, если $n = pq$ – произведение двух простых чисел, то для каждого x из кольца классов вычетов Z_n можно вычислить пару

$$(x \bmod p, x \bmod q).$$

Обозначим $a = x \bmod p$, $b = x \bmod q$.

Китайская теорема об остатках утверждает, что можно выполнить и обратную операцию: зная (a,b), восстановить исходное значение x.

Чтобы вычислить x по заданным (a,b), следует убедиться, что в Z_n не существует второго такого числа x', для которого

$$a = x' \bmod p,\ b = x' \bmod q.$$

В противном случае и x и x' привели бы к появлению одной и той же пары (a,b), и ни один алгоритм не смог бы распознать, какое из этих значений является исходным.

Пусть $d = x - x'$ – это разность чисел, которым соответствует одна и та же пара (a,b). Имеем

$$d = x - x' \equiv a - a = 0 \ (\mathrm{mod}\ p),$$

а следовательно, d кратно p. Аналогичным образом получаем, что d кратно q. Отсюда следует, что d является общим кратным чисел p и q, т.е. делится

на НОК(p,q). Поскольку p и q – это различные простые числа, то НОК(p,q) = pq = n, а значит, $d = x - x'$ кратно n. Но x и x' – элементы из множества $\{0, 1, \dots, n-1\}$, поэтому разность $d = x - x'$ удовлетворяет двойному неравенству

$$-n + 1 \le d \le n - 1.$$

Единственным числом из этого промежутка, кратным числу n, является число 0, т.е.

$$d = x - x' = 0$$
$$x = x'.$$

Таким образом, *CRT*-теорема устанавливает взаимно однозначное соответствие между целыми числами на отрезке от нуля до $n - 1$ включительно и всеми возможными парами чисел (a,b) для целых a и b таких, что $0 \le a \le p$, $0 \le b \le q$.

Формула Гарнера

Самым удобным способом вычисления x по его CRT-представлению в виде пары (a,b) является так называемая формула Гарнера (Garner's formula):

$$x = \left(\left((a-b)(q^{-1} \bmod p)\right) \bmod p\right) \cdot q + b.$$

Здесь множитель $q^{-1} \bmod p$ (*обратный элемент к q в кольце классов вычетов по модулю p*) – это константа, которая зависит только от p и q.

Заметим, что значение $q^{-1} \bmod p$ обычно подсчитывают предварительно, поэтому применение формулы Гарнера требует выполнения одного вычитания по модулю p, одного умножения по модулю p, одного полного умножения и одного сложения.

Пример. Зашифровать сообщение m = 49 по схеме RSA, используя китайскую теорему об остатках, если p = 13, q = 17, e = 143.

Шифрование. CRT-представление сообщения m

$$(49 \bmod 17, 49 \bmod 13) = (15,10)$$

Тогда CRT-представление шифра c

$$(15^{143} \bmod 17, 10^{143} \bmod 13).$$

Вычислим $15^{143} \bmod 17$.

$$15^1 \bmod 17 = 15$$
$$15^2 \bmod 17 = 225 \bmod 17 = 4$$
$$15^4 \bmod 17 = 4^2 \bmod 17 = 16$$
$$15^8 \bmod 17 = 16^2 \bmod 17 = 256 \bmod 17 = 1$$
$$15^{16} \bmod 17 = 1 \bmod 17$$
$$15^{32} \bmod 17 = 1 \bmod 17$$
$$15^{64} \bmod 17 = 1 \bmod 17$$
$$15^{128} \bmod 17 = 1 \bmod 17$$

Так как $143_{10} = 1000\ 1111_2$, то

$$15^{143} \bmod 17 = 1 \cdot 1 \cdot 16 \cdot 4 \cdot 15 \bmod 17 = 16 \cdot 60 \bmod 17 = 16 \cdot 9 \bmod 17$$
$$= 144 \bmod 17 = 8.$$

Вычислим $10^{143} \bmod 13$.

$$10^1 \bmod 13 = 10$$
$$10^2 \bmod 13 = 100 \bmod 13 = 9$$
$$10^4 \bmod 13 = 9^2 \bmod 13 = 81 \bmod 13 = 3$$
$$10^8 \bmod 13 = 3^2 \bmod 13 = 9$$
$$10^{16} \bmod 13 = 81 \bmod 13 = 3$$
$$10^{32} \bmod 13 = 9$$
$$10^{64} \bmod 13 = 81 \bmod 13 = 3$$
$$10^{128} \bmod 13 = 9$$

Таким образом,

$$10^{143} \bmod 13 = 9 \cdot 9 \cdot 3 \cdot 9 \cdot 10 \bmod 13 = 81 \cdot 27 \cdot 10 \bmod 13 =$$
$$= 3 \cdot 27 \cdot 10 \bmod 13 = 81 \cdot 10 \bmod 13 = 3 \cdot 10 \bmod 13 = 4.$$

CRT-представление шифртекста $(15^{143} \bmod 17, 10^{143} \bmod 13) = (8, 4)$

Из соотношения Безу получим $13^{-1} \bmod 17 = 4$. Следовательно, по формуле Гарнера

$$c = (((8 - 4) \cdot 4) \bmod 17) \cdot 13 + 4 = 212.$$

Расшифрование. Функция Эйлера $\varphi(n) = 12 \cdot 16 = 192$. Тогда секретный ключ $d = 47$. Представим число 47 в двоичной системе счисления

$$47_{10} = 101111_2$$

Так как CRT-представление шифртекста c

$$(212 \bmod 17, 212 \bmod 13) = (8,4),$$

то CRT-представление открытого текста m

$$(8^{47} \bmod 17, 4^{47} \bmod 13).$$

После возведения в степень получим

$$(8^{47} \bmod 17, 4^{47} \bmod 13) = (15, 10).$$

Так как $13^{-1} \bmod 17 = 4$, то по формуле Гарнера

$$m = (((15 - 10) \cdot 4) \bmod 17) \cdot 13 + 10 = 49.$$

Лабораторная работа 7

Цель работы: изучить алгоритмы шифрования и расшифрования в криптосистеме RSA с применением китайской теоремы об остатках.

Задания. 1. Реализуйте метод «RSAEncryptionCRT» с использованием CRT-представления для шифрования сообщения по алгоритму RSA. Шифруемую информацию перевести в цифровую форму, заменяя буквы русского алфавита двузначными числами («а» = 01, «б» = 02 и т.д.).

Входные данные: m – открытый текст (на русском языке).

Выходные данные: c – шифртекст (в цифровой форме),

n, e – открытый ключ,

разложение числа n на простые множители p и q.

2. Реализуйте метод «RSADecipheringCRT» с использованием CRT-представления для расшифрования сообщения по алгоритму RSA. Если введены некорректные параметры, то вывести соответствующее сообщение об ошибке.

Входные данные: *c* – шифртекст (в цифровой форме),
e – открытый ключ,
разложение числа *n* на простые множители *p* и *q*.
Выходные данные: m – открытый текст (на русском языке).
d – секретный ключ.

Используйте разработанные методы для случая, если входные параметры имеют следующие значения.

	Задание 2			
	c	*p*	*q*	*e*
Вариант 1	358838056161475	20995031	20995063	3560023
Вариант 2	293410589432528	20995031	20995063	7015049
Вариант 3	107337160016060	20995721	20997113	7084811
Вариант 4	366652477881957	20995721	20997113	5092069
Вариант 5	70418932741432	20997187	20997349	5091013
Вариант 6	14781653830609	20997187	20997349	3562193
Вариант 7	372350347322655	20997523	20997541	5091643
Вариант 8	289354094732043	20997523	20997541	3564983
Вариант 9	289752064160339	20997649	20997701	7084907
Вариант 10	287890288077681	20997649	20997701	5092909

Криптосистема Эль-Гамаля

Криптосистема Эль-Гамаля создана американским специалистом по криптографии в 1985 году после появления криптосистемы RSA. Она послужила основой для целого ряда систем цифровой подписи.

Криптосистема Эль-Гамаля строится на основе большого простого числа $p \approx 2^q$, где $512 \le q \le 1024$, то есть имеющее 150–300 десятичных знаков. Кольцо классов вычетов Z/pZ в силу простоты числа p обладает тем свойством, что все ненулевые классы в нем обратимы относительно умножения.

Пусть g – первообразный корень по модулю p. Это означает, что степени g как элемента группы Z/pZ^* исчерпывают всю эту группу. Иными словами, мультипликативная подгруппа $\langle g \rangle$ совпадает со всей группой: $\langle g \rangle = \{g, g^2, \dots, g^{p-1} = 1\} = Z/pZ$.

Для шифрования по алгоритму Эль-Гамаля фиксируем два секретных ключа x и k как элементы Z/pZ^*. При этом k – это сеансовый ключ, выбираемый отправителем на короткий промежуток работы системы – один или несколько сеансов передачи информации.

Вычисляем величину $y = g^x \bmod p$. Тройка чисел (p,g,y) − есть тройка открытых ключей криптосистемы Эль-Гамаля.

Передаваемая информация в криптосистеме Эль-Гамаля, как и в криптосистеме RSA, предварительно преобразуется в десятичное число – сообщение m, рассматриваемое как элемент группы Z/pZ^*. Сообщение шифруется умножением m на

$$K = y^k \bmod p.$$

Таким образом, зашифрованное сообщение

$$ш = m \cdot K = m \cdot y^k \bmod p.$$

При этом адресату идет расширенное сообщение: $(ш, O_{СК})$, где

$$O_{СК} = g^k \bmod p.$$

$O_{СК}$ – число-подсказка, называемое открытым сеансовым ключом.

Получатель послания знает секретный ключ x. Он возводит $O_{СК}$ в степень x

$$O_{СК}^x = g^{kx} \bmod p$$

тогда

$$(g^x)^k = y^k \bmod p.$$

Таким образом,

$$O_{СК}^x = K \bmod p.$$

Вычислив K, получатель находит K^{-1} в кольце Z/pZ. Это несложно сделать, например, обратным ходом алгоритма Евклида с учетом соотношения НОД$(K,p) = 1$. Теперь сообщение легко восстанавливается

$$m = c \cdot K^{-1} \bmod p.$$

Проблема взлома данной криптосистемы: надо найти x – степень числа g по модулю p, равную y. Это так называемая проблема дискретного ло-

гарифма. Приемлемых решений этой проблемы, кроме прямого последовательного перебора степеней g по модулю p до искомой на сегодняшний день не существует.

Пример. Зашифруем сообщение $m = 20$.

Пусть $p = 23$. Покажем, что в качестве g можно взять число 5.

$5^1 \bmod 23 = 5$, $5^{12} \bmod 23 = 18$,
$5^2 \bmod 23 = 2$, $5^{13} \bmod 23 = 21$,
$5^3 \bmod 23 = 10$, $5^{14} \bmod 23 = 13$,
$5^4 \bmod 23 = 4$, $5^{15} \bmod 23 = 19$,
$5^5 \bmod 23 = 20$, $5^{16} \bmod 23 = 3$,
$5^6 \bmod 23 = 8$, $5^{17} \bmod 23 = 15$,
$5^7 \bmod 23 = 17$, $5^{18} \bmod 23 = 6$,
$5^8 \bmod 23 = 16$, $5^{19} \bmod 23 = 7$,
$5^9 \bmod 23 = 11$, $5^{20} \bmod 23 = 12$,
$5^{10} \bmod 23 = 9$, $5^{21} \bmod 23 = 14$,
$5^{11} \bmod 23 = 22$, $5^{22} \bmod 23 = 1$.

Таким образом, порядок элемента 5 равен 22, т.е. 5 – первообразный корень по модулю 23.

Положим в качестве секретного ключа число $x = 7$. Тогда третий открытый ключ y:

$$y = g^x (\bmod p) = 5^7 (\bmod 23) = (5^2)^2 \cdot 5^2 \cdot 5 (\bmod 23) \equiv$$
$$\equiv 4 \cdot 2 \cdot 5 (\bmod 23) \equiv 40 (\bmod 23) \equiv 17$$

В качестве секретного сеансового ключа возьмем $k = 3$. В таком случае можно вычислить

$$K = y^k (mod\, p) = 17^3 (\bmod 23) = 289 \cdot 17 (\bmod 23) \equiv$$
$$\equiv 13 \cdot 17 (\bmod 23) \equiv 14.$$

Тогда шифртекст

$$c = m \cdot K (\bmod p) = 20 \cdot 14 (\bmod 23) = 4.$$

Следовательно, адресат получает сообщение $(c, O_{CK}) = (4,10)$. Напомним, что у него в распоряжении имеется тройка открытых ключей $(p, g, y) = (23,5,17)$ и секретный ключ $x = 7$.

Для расшифровки принятого сообщения он вычисляет

$$K = O_{CK}^x = g^{kx} (mod\, p) = 10^7 (mod\, 23) = 14.$$

Затем получатель находит в кольце $Z/23Z$ значение $K^{-1} = 5$ и, наконец, вычисляет открытый текст:

$$m = c \cdot K^{-1} (\bmod p) = 4 \cdot 5 (\bmod 23) = 20.$$

Лабораторная работа 8

Цель работы: изучить алгоритмы шифрования и расшифрования в криптосистеме Эль-Гамаля.

Задания. 1. Реализуйте метод «ElGamalEncryption» для шифрования сообщения по алгоритму Эль-Гамаля. Шифруемую информацию перевести

в цифровую форму, заменяя буквы русского алфавита двузначными числами («а» = 01, «б» = 02 и т.д.).

Входные данные: m – открытый текст (на русском языке).

Выходные данные: c – шифртекст (в цифровой форме),

$p, g, y, O_{ск}$ – открытый ключ.

2. Реализуйте метод «ElGamalDecryption» для дешифрования сообщения по алгоритму Эль-Гамаля. Если введены некорректные параметры, то вывести соответствующее сообщение об ошибке.

Входные данные: c – шифртекст (в цифровой форме),

$p, g, y, O_{ск}$ – открытый ключ.

Выходные данные: m – открытый текст (на русском языке).

x – секретный ключ.

Используйте разработанные методы для случая, если входные параметры имеют следующие значения.

	Задание 2				
	c	p	g	y	$O_{ск}$
Вариант 1	2112	5039	17	738	2129
	1112103225	1209223439	57	1049323232	389307680
Вариант 2	5025	5039	17	2468	1254
	918812233	1209223439	63	866680062	606042995
Вариант 3	1725	5039	17	1644	3709
	1107977625	1209223439	65	332989756	138529962
Вариант 4	1222	5039	17	2753	1716
	1147970139	1209223439	69	800884057	1056584975
Вариант 5	1987	5039	17	1450	3219
	926197209	1209223439	70	242870000	554986115
Вариант 6	1551	5039	51	2206	338
	1030873439	1209223439	71	1176958609	298490028
Вариант 7	1353	5039	51	1648	428
	1033355383	1209223439	73	1017895821	15901505
Вариант 8	4351	5039	51	3424	4925
	1044751482	1209223439	76	566300322	335201077
Вариант 9	4079	5039	51	3298	3374
	709271343	1209223439	77	821380924	1100764221
Вариант 10	3693	5039	51	1911	979
	490175059	1209223439	78	298818278	860389750

Литература

1. Венбо, М. Современная криптография: теория и практика / М. Венбо. – М.: Издательский дом “Вильямс”, 2005. – 768 с.
2. Крупенкова, Т.Г. Криптографические средства защиты информации [Электронный ресурс]. В 2 ч. Ч. 1. : учебно-методическое пособие для студентов спец. 1-38 02 03 "Техническое обеспечение безопасности" специализации 1-38 02 03 02 ""Аппаратно-программные средства защиты компьютерной информации" / Т.Г. Крупенкова. – БНТУ, 2012. – 83 с.
3. Токарева, Н.Н. Симметричная криптография / Н.Н. Токарева. – Новосибирск: Новосиб. гос. ун-т., 2012. – 234 с.
4. Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Издательский дом “Вильямс”, 2004. – 432 с.
5. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации / Ю.С. Харин, С.В. Агиевич. – Минск: БГУ, 2001. – 190 с.
6. Харин, Ю.С. Криптология / Ю.С. Харин, Агиевич С.В., Васильев Д.В., Матвеев Г.В. – Минск: БГУ, 2013. – 511 с.
7. Diffie, W. New Directions in Cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. IT-22, № 6. – P. 644-654.

Учебное издание

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Методические рекомендации

Составитель

ВИТЬКО Елена Анатольевна

Технический редактор *Г.В. Разбоева*

Компьютерный дизайн *Е.А. Барышева*

Подписано в печать 2019. Формат 60x84 $^{1}/_{16}$. Бумага офсетная.

Усл. печ. л. 2,27. Уч.-изд. л. 1,36. Тираж экз. Заказ .

Издатель и полиграфическое исполнение – учреждение образования
«Витебский государственный университет имени П.М. Машерова».

Свидетельство о государственной регистрации в качестве издателя,
изготовителя, распространителя печатных изданий
№ 1/255 от 31.03.2014 г.

Отпечатано на ризографе учреждения образования
«Витебский государственный университет имени П.М. Машерова».
210038, г. Витебск, Московский проспект, 33.