ВЫСШЕЕ ОБРАЗОВАНИЕ

А. В. Зенков

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УМО ВО РЕКОМЕНДУЕТ

Юрайт издательство

А. В. Зенков

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УЧЕБНОЕ ПОСОБИЕ ДЛЯ ВУЗОВ

Рекомендовано Учебно-методическим отделом высшего образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по ИТ направлениям

Книга доступна на образовательной платформе «Юрайт» urait.ru, а также в мобильном приложении «Юрайт.Библиотека»

Москва • Юрайт • 2022

УДК 004.056(075.8)
ББК 16.8я73
З-56

Автор:

Зенков Андрей Вячеславович — кандидат физико-математических наук, доцент института менеджмента и информационных технологий Уральского государственного экономического университета (г. Екатеринбург), доцент кафедры моделирования управляемых систем института экономики и управления Уральского федерального университета имени первого Президента России Б. Н. Ельцина (г. Екатеринбург).

Зенков, А. В.

З-56 Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — Текст : непосредственный.

ISBN 978-5-534-14590-8

Какие права в информационной сфере гарантирует гражданам Конституция Российской федерации? Чем криптография отличается от стеганографии? Каковы сравнительные преимущества и недостатки симметричных и асимметричных шифров? Существуют ли шифры, абсолютно устойчивые к взлому? Как теория чисел обеспечивает конфиденциальность и аутентичность при обмене сообщениями? Ответы на эти и другие вопросы читатель найдет в данном издании. Курс является кратким введением в информационную безопасность и защиту информации и содержит лекции для студентов ИТ-специальностей, упражнения, материалы для практических занятий и лабораторных работ.

Издание отражает многолетний опыт преподавания автора в Уральском федеральном университете и Уральском государственном экономическом университете.

Содержание курса соответствует актуальным требованиям федерального государственного образовательного стандарта высшего образования.

Для студентов вузов, обучающихся по ИТ направлениям.

УДК 004.056(075.8)
ББК 16.8я73

ISBN 978-5-534-14590-8

Оглавление

Предисловие

Издание соответствует односеместровому (15 недель, два лекционных часа в неделю на протяжении полусеместра; практические занятия и лабораторные работы в течение всего семестра) курсу «Информационная безопасность и защита информации», читавшемуся автором в разные годы в Уральском федеральном университете и Уральском государственном экономическом университете, в зависимости от учебного плана, студентам II—IV курсов бакалавриата по направлениям «Бизнес-информатика», «Информатика и вычислительная техника», «Фундаментальная информатика и информационные технологии».

Этот учебный предмет имеет три характерные особенности:

• во-первых, он отличается чрезвычайно широким охватом тем — от геополитики и юриспруденции до алгебры и теории чисел; невозможно сколько-нибудь подробно рассмотреть все вопросы, входящие в образовательный стандарт (и не найдется преподавателя, которому это было бы по силам);

• во-вторых, предмет отличается чрезвычайно быстрым поступлением нового фактического материала, поэтому акцент сознательно сделан на принципах, а не на технических и программных подробностях (которые, вероятно, успели бы устареть к моменту выхода книги в свет);

• в-третьих, предмет (в указанном выше объеме часов), конечно, носит общеобразовательный характер, и ожидать от него узконаправленных практических рекомендаций (которые должны последовать в специальных курсах), не следует. Цель курса — представить читателю вводный обзор тем, относящихся к учебному предмету «Информационная безопасность и защита информации», сознательно сделав акцент на вопросах, допускающих не утомительное механическое перечисление «угроз», «уязвимостей» и «мероприятий» суконным языком (что делает очень скучными многие книги по информационной безопасности), а связное логически последовательное из-

ложение. Вопросы, и без того знакомые ИТ-студентам (классификация вирусов, антивирусные программы и др.), затронуты лишь вскользь.

Автор убежден, что студент ИТ-направления не может не обладать хотя бы *элементарными* навыками программирования на каком-нибудь алгоритмическом языке[1]. Из трех тем лабораторных работ (по криптографии), предлагаемых автором студентам по курсу информационной безопасности, две большей частью направлены именно на развитие программистских навыков. Современная криптография требует изощренного знания глубоких разделов математики, недостижимого во вводном общеобразовательном курсе, поэтому не должен удивлять выбор старых классических разделов криптографии в качестве тем двух лабораторных работ. Еще одна тема связана с освоением одного популярного криптографического пакета, и выполнение соответствующей лабораторной работы является тем безусловным минимумом, который позволяет получить положительную оценку по предмету тем студентам, которые так и не освоили программирование.

В результате освоения дисциплины студент должен:

знать

• базовые понятия, связанные с информационной безопасностью и защитой информации;

• основные правовые акты, касающиеся информационной безопасности и защиты информации;

• некоторые элементы криптографии;

• математические основы некоторых криптографических алгоритмов;

уметь

• делать осмысленный выбор между продуктами для защиты информации;

• учитывать в профессиональной деятельности рекомендации, связанные с информационной безопасностью и защитой информации;

владеть

• навыками защищенного документооборота с использованием программы PGP;

• навыками программной реализации некоторых криптографических алгоритмов.

---

[1] Увы, даже это скромное допущение далеко не всегда оправдывается.

Литература по информационной безопасности и защите информации неисчерпаема. В конце курса приведены ссылки на некоторые пособия, которые либо повлияли на содержание настоящего издания, либо рекомендуются для более глубокого ознакомления с предметом.

Автор просит присылать сообщения о найденных недостатках по адресу zenkow@mail.ru.

Тема 1
ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Информационная безопасность — это защищенность информации от незаконного получения, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Источниками этих воздействий могут быть проникновение злоумышленников, ошибки персонала, выход из строя аппаратных и программных средств, стихийные бедствия (землетрясение, ураган, пожар и т. п.).

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию[1].

Цели защиты информации:

- целостность данных;
- конфиденциальность данных;
- доступность данных.

Целостность данных гарантирует, что они не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей. Обеспечение целостности данных — одна из самых сложных задач защиты информации.

Конфиденциальность данных — это статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизацию) субъектам информационной системы (пользователям, процессам, программам). Примеры конфиденциальных данных:

- личная информация пользователей;
- учетные записи (имена и пароли);
- данные о кредитных картах;
- бухгалтерские сведения.

---

[1] ГОСТ Р 50922—2006 «Защита информации. Основные термины и определения».

Доступность данных. Условием работы с данными является доступ пользователя к ним. Под *доступом к информации* понимаются ознакомление с ней и ее обработка, в частности копирование, модификация, уничтожение.

Различают санкционированный и несанкционированный доступ.

Санкционированный доступ — это доступ в соответствии с установленными правилами разграничения доступа. *Несанкционированный доступ* нарушает эти правила. Он является наиболее распространенным видом компьютерных нарушений.

Угрозы и препятствия на пути к достижению безопасности информации можно разделить на две группы: «технические угрозы» и «человеческий фактор».

Технические угрозы

К основным техническим угрозам относятся:

- ошибки в программном обеспечении;
- сетевые атаки, в том числе DoS- и DDoS-атаки;
- компьютерные вирусы, черви, троянские кони;
- анализаторы протоколов и прослушивающие программы («снифферы» — от англ. *sniff*: чуять, принюхиваться);
- технические средства съема информации.

Ошибки в программном обеспечении (ПО) могут приводить к тяжелым последствиям, таким как обретение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование компьютера в качестве плацдарма для атак и т. д.). Обычно такие ошибки устраняются с помощью пакетов обновлений и «заплаток» (patch) — выпускаемых производителем ПО кодов для оперативного исправления или нейтрализации ошибок.

DoS-атаки (*Denial of Service* — отказ в обслуживании) — это атаки, направленные на выведение сети или сервера из работоспособного состояния. Целью DoS-атаки является создание таких условий работы сайта, при которых пользователь не может получить к нему доступ. Чаще всего злоумышленники добиваются этого, забрасывая сайт огромным количеством «мусорных» запросов, и пользователи уже не могут пробиться к сайту: правомерные запросы тонут в «шуме».

При DoS-атаках могут использоваться ошибки в ПО или законные операции, но в большом масштабе — например, уста-

новка с атакуемым сервером большого количества соединений, обработка которых потребует всех ресурсов сервера с невозможностью обслуживания добросовестных пользователей. Несмотря на то, что методы проведения DoS-атак хорошо известны, противостоять такой атаке удается не всегда, поскольку быстро и точно отделить «мусорные» запросы от правомерных трудно. Принцип DoS-атак: «используй в дурных целях хороший контент» («legitimate content but bad intent»).

DDoS-атаки (*Distributed Denial of Service* — распределенный DoS) отличаются от DoS наличием у атакующего большого числа компьютеров, предварительно захваченных им в качестве инструмента для DDoS-атаки. Такие атаки перегружают канал связи и мешают прохождению полезной информации.

DDoS-атака опирается на сеть компьютеров-зомби или botnet. Компьютер заражается троянской программой чаще всего при неосторожном обращении с электронной почтой, например, открытии вложений в письмо, или при посещении зараженного сайта, когда злоумышленник может, используя уязвимости браузера или операционной системы, установить на компьютер пользователя вредоносную программу.

Компьютерные вирусы и ***троянские кони*** — старая категория опасностей; но если прежде эти опасности заключались в разрушительных функциях, то в последние годы на первое место выходят функции удаленного управления, похищения информации и использования зараженной системы для дальнейшего распространения вредоносной программы, для участия в DDoS-атаках.

Анализаторы протоколов и снифферы. К ним относятся аппаратные и программные средства перехвата передаваемых по сети данных.

Технические средства съема информации. Сюда относятся клавиатурные жучки, звукозаписывающие устройства и т. п.

Человеческий фактор. Проблемными факторами, так или иначе связанными с людьми, являются:

- уволенные или недовольные сотрудники;
- промышленный шпионаж;
- халатность;
- низкая квалификация.

Уволенные, недовольные сотрудники — самая опасная группа, если они имели доступ к конфиденциальной информации. Обиженный системный администратор опасен вдвойне,

ибо может оставить «черные ходы» для последующего злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж. Проблема весьма актуальна, хотя для получения информации конкурирующая фирма может найти пути более дешевые, чем взлом хорошо защищенной сети. Источником угрозы могут быть те же недовольные сотрудники, шпионящие для конкурента.

Халатность — самый распространенный порок, выражающийся, например, в неустановке пакетов обновлений, неизмененных настройках по умолчанию и т. п.

Низкая квалификация пользователей может обесценить трудоемкие и дорогостоящие мероприятия по защите информации. Специально поставленными «невинными» вопросами можно выведать у низкоквалифицированного или беспечного пользователя любые, в том числе и конфиденциальные сведения об информационной системе предприятия, а предостережение об опасности запуска исполняемых файлов, вложенных в e-mail, по-прежнему актуально…

Никакие аппаратные, программные и любые другие решения не могут гарантировать абсолютную надежность и безопасность данных в компьютерных системах. Минимизировать риск потерь возможно лишь при комплексном подходе к вопросам безопасности.

Приведем некоторый (неисчерпывающий) список мер, направленных на обеспечение информационной безопасности и защиты информации.

***Технические меры*:** защита от несанкционированного доступа к информационной системе; резервирование особо важных компьютерных подсистем; организация вычислительных сетей с возможностью перераспределения ресурсов при нарушении в работе отдельных звеньев; установка средств обнаружения и тушения пожара, обнаружения утечек воды; принятие конструкционных мер защиты от хищений, диверсий, взрывов; установка резервного электропитания; оснащение помещений замками, сигнализацией и др.

***Организационные меры*:** охрана вычислительного центра (ВЦ); тщательный подбор персонала; недопущение ведения важных работ одним человеком; наличие плана восстановления работоспособности ВЦ после выхода его из строя; обслуживание ВЦ сторонней организацией или лицами, незаинтересо-

ванными в сокрытии фактов нарушения работы центра; выбор места расположения центра и т. п.

К ***правовым мерам*** относятся разработка норм, устанавливающих ответственность за компьютерные преступления, защита авторских прав программистов, а также совершенствование законодательства и судопроизводства. К правовым мерам относятся общественный контроль над разработчиками компьютерных систем и принятие международных договоров, регламентирующих эту деятельность.

Вопросы и задания для самопроверки

1. Каковы цели защиты информации?
2. В чем состоит целостность данных?
3. В чем состоит конфиденциальность данных?
4. В чем состоит доступность данных?
5. Приведите примеры технических угроз информационной безопасности.
6. Какие проблемы для информационной безопасности порождает человеческий фактор?
7. Приведите примеры технических средств обеспечения информационной безопасности и защиты информации.
8. Назовите организационные меры обеспечения информационной безопасности и защиты информации. Обоснуйте целесообразность этих мер.
9. Назовите правовые меры обеспечения информационной безопасности и защиты информации.

Тема 2
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривая законодательные акты, действующие на территории РФ и связанные с информационной безопасностью, следует помнить, что, к сожалению, правоприменительная практика в нашей стране традиционно далека от буквы и духа законов; кроме того, обилие запретительных и ужесточающих законодательных новелл в последнее время (особенно в сфере информационной безопасности) может сделать данный обзор неактуальным уже к моменту публикации книги.

Начнем с ***Международного пакта о гражданских и политических правах***, принятого в 1966 г. и вступившего в силу в 1976 г. Это договор обязателен к исполнению в 168 государствах-участниках (в том числе в России). Процитируем статьи, имеющие отношение к информационным правам и свободам.

Статья 17

1. Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию.

2. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

Статья 18

1. Каждый человек имеет право на свободу мысли, совести и религии. Это право включает свободу иметь или принимать религию или убеждения по своему выбору и свободу исповедовать свою религию и убеждения как единолично, так и сообща с другими, публичным или частным порядком, в отправлении культа, выполнении религиозных и ритуальных обрядов и учении.

2. Никто не должен подвергаться принуждению, умаляющему его свободу иметь или принимать религию или убеждения по своему выбору.

Статья 19

1. Каждый человек имеет право беспрепятственно придерживаться своих мнений.

2. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору.

3. Пользование предусмотренными в п. 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

а) для уважения прав и репутации других лиц;

б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Статья 20

1. Всякая пропаганда войны должна быть запрещена законом.

2. Всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом.

Статья 21

Признается право на мирные собрания. Пользование этим правом не подлежит никаким ограничениям, кроме тех, которые налагаются в соответствии с законом и которые необходимы в демократическом обществе в интересах государственной или общественной безопасности, общественного порядка, охраны здоровья и нравственности населения или защиты прав и свобод других лиц.

Информационные права и свободы закреплены в действующей ***Конституции РФ*** 1993 г.:

Статья 13

В Российской Федерации признается идеологическое многообразие.

Статья 15

1. Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей терри-

тории Российской Федерации. Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.

3. Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

4. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Статья 16

1. Положения настоящей главы Конституции составляют основы конституционного строя Российской Федерации и не могут быть изменены иначе как в порядке, установленном настоящей Конституцией.

2. Никакие другие положения настоящей Конституции не могут противоречить основам конституционного строя Российской Федерации.

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 28

Каждому гарантируется свобода совести, свобода вероисповедания, включая право исповедовать индивидуально или со-

вместно с другими любую религию или не исповедовать никакой, свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними.

Статья 29

1. Каждому гарантируется свобода мысли и слова.

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 31

Граждане Российской Федерации имеют право собираться мирно, без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование.

Статья 41

3. Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.

Статья 42

Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением.

Статья 44

1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

Уголовный кодекс РФ, гл. 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение,

блокирование, модификацию либо копирование компьютерной информации, — наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, — наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, — наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, — наказываются лишением свободы на срок до семи лет.

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, — наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, — наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, — наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, — наказывается штрафом в размере до пятисот тысяч рублей или в размере за-

работной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью 1 настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, — наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, — наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, — наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона ру-

блей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, — наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью 1, 2 или 3 настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, — наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

5. Деяния, предусмотренные частью 1, 2, 3 или 4 настоящей статьи, если они повлекли тяжкие последствия, — наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Федеральный закон «Об информации, информационных технологиях и о защите информации» (2006 г.)

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами

не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использова-

нии бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации

о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2-1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи).

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональ-

ную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 11-1. Обмен информацией в форме электронных документов при осуществлении полномочий органов государственной власти и органов местного самоуправления

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия,

может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности.

Статья 15-1. Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено

1. В целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети ”Интернет” и сетевых адресов, позволяющих идентифицировать сайты в сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено» (далее — реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет»:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных ве-

ществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено.

7. В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети «Интернет» и уведомить его о необходимости незамедлительного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

8. В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр владелец сайта в сети «Интернет» обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети «Интернет» провайдер хостинга обязан ограничить доступ к такому сайту в сети «Интернет» в течение суток.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети «Интернет» мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к такому сайту в сети «Интернет».

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации (пункт 7 введен Федеральным законом от 21 июля 2014 г.).

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Федеральный закон «О безопасности» (Принят Государственной Думой в 2010 г.)

Статья 2. Основные принципы обеспечения безопасности

Основными принципами обеспечения безопасности являются:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность.

Статья 4. Государственная политика в области обеспечения безопасности

1. Государственная политика в области обеспечения безопасности является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Статья 5. Правовая основа обеспечения безопасности

Правовую основу обеспечения безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

Статья 8. Полномочия Президента Российской Федерации в области обеспечения безопасности

Президент Российской Федерации:

1) определяет основные направления государственной политики в области обеспечения безопасности;

7) решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты:

а) информации и государственной тайны.

Доктрина информационной безопасности Российской Федерации (утверждена указом президента РФ в 2016 г.)

Документ многословен и декларативен, состоит из 38 статей, разбитых на пять глав; начинается с указания национальных интересов в сфере национальной безопасности. Далее идет перечисление основных информационных угроз в современном мире. На основании этих угроз формируются стратегические цели национальной политики, касающиеся экономики, военной сферы, дипломатии, науки и образования.

Национальные интересы: обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации; обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры; развитие информационных технологий и электронной промышленности; продвижение достоверной информации о России и ее официальной позиции по социально значимым событиям в стране и мире; содействие формированию системы международной информационной безопасности.

Основные информационные угрозы: западные страны наращивают воздействие на информационную инфраструктуру в военных целях; усиливается деятельность организаций, осуществляющих техническую разведку в России; спецслужбы отдельных государств пытаются дестабилизировать внутриполитическую и социальную ситуацию в различных регионах мира (цель — подрыв суверенитета и нарушение территориальной целостности государств, методы — использование информационных технологий, а также религиозных, этнических и правозащитных организаций); в зарубежных СМИ растет предвзятость оценки российской политики; российским журналистам за рубежом создаются препятствия, российские СМИ подвергаются дискриминации; террористические и экстремистские группировки нагнетают межнациональную и социальную напряженность, благодаря пропаганде привлекают новых сторонников; расширяется компьютерная преступность (прежде всего, в кредитно-финансовой сфере); учащаются преступления, связанные с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных; иностранные государства усиливают разведывательную деятельность в России, учащаются компьютерные атаки на объекты критической информационной инфраструктуры, их масштабы и сложность растут; отечественная промышленность зависит от зарубежных информационных технологий (электронная компонентная база, программное обеспечение, вычислительная техника, средства связи); низка эффективность российских научных исследований в области перспективных информационных технологий; отдельные государства используют технологическое превосходство для доминирования в информационном пространстве, это препятствует управлению Интернетом на принципах справедливости и доверия между странами.

Стратегическая цель обеспечения информационной безопасности в области обороны страны — защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе для враждебных действий и агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности РФ и представляющих угрозу международному миру, безопасности и стратегической стабильности.

В военной политике надо стремиться: к стратегическому сдерживанию и предотвращению военных конфликтов, которые могут возникнуть в результате применения информационных технологий; к совершенствованию обеспечения информационной безопасности армии; прогнозированию, обнаружению и оценке информационных угроз; к обеспечению защиты интересов союзников РФ в информационной сфере; к нейтрализации информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

В области государственной и общественной безопасности следует: противодействовать использованию информационных технологий для пропаганды экстремизма, ксенофобии и национализма; повышать защищенность критической информационной инфраструктуры; усиливать защиту информации, содержащей государственную тайну; бороться с информационным воздействием, направленным на размывание традиционных российских духовно-нравственных ценностей.

В экономике требуется: инновационное развитие отрасли информационных технологий; ликвидация зависимости отечественной промышленности от зарубежных информационных технологий; развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов.

В науке и образовании важны: достижение конкурентоспособности российских информационных технологий; развитие кадрового потенциала в области информационной безопасности; формирование у граждан культуры личной информационной безопасности.

В международных отношениях нужны: самостоятельная и независимая информационная политика; участие в форми-

ровании системы международной информационной безопасности; обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере, продвижение российской позиции в международных организациях.

Организационная основа обеспечения информационной безопасности: Совет федерации, Государственная дума, правительство, Совет безопасности, федеральные органы исполнительной власти (федеральные службы и агентства), Центральный банк, межведомственные органы, создаваемые президентом и правительством, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, собственники и эксплуатанты объектов критической информационной инфраструктуры, СМИ, банки, операторы связи и информационных систем, разработчики информационных систем и сетей связи.

Вопросы для самопроверки

1. Что запрещено пропагандировать согласно Конституции РФ?
2. Если международным договором РФ установлены иные правила, чем предусмотрено законом РФ, то правила какого нормативного акта должны применяться, согласно конституции?
3. На какие виды подразделяется информация в зависимости от порядка ее предоставления (распространения) согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»?
4. К каким видам информации не может быть ограничен доступ согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»?
5. Распространение каких видов информации запрещается Федеральным законом «Об информации, информационных технологиях и о защите информации»?
6. Каковы национальные интересы РФ согласно Доктрине информационной безопасности Российской Федерации?

Тема 3
КРИПТОГРАФИЯ

3.1. Основные определения

Криптография[1] **—** это прикладная наука, разрабатывающая математические методы, алгоритмы, программные и аппаратные средства преобразования информации (*шифрования*) в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

***Криптоанализ* —** прикладная наука, исследующая возможности доступа к информации без знания ключей (взлома шифров).

***Криптология* —** наука, объединяющая в себе криптографию и криптоанализ.

Некоторые области применения криптографии в современном мире:

• шифрование данных при передаче по открытым каналам связи;

• обслуживание банковских карт;

• хранение и обработка паролей пользователей в сети;

• сдача бухгалтерских и иных отчетов по каналам связи;

• безопасное (на случай несанкционированного доступа) хранение данных на компьютере.

Криптография призвана решать следующие задачи:

• шифрование для защиты от несанкционированного доступа;

• проверка подлинности сообщений: получатель сообщения может проверить его источник;

• проверка целостности передаваемых данных: получатель может проверить, не было ли сообщение изменено или подменено при пересылке;

• обеспечение невозможности отказа от факта передачи сообщения как для отправителя, так и для получателя.

---

[1] От греч. κρυπτός — «потайной», «секретный»; γράφω — «пишу».

Шифрование — основной криптографический метод защиты информации, обеспечивающий ее конфиденциальность и аутентичность.

Под *конфиденциальностью* понимается невозможность получения информации из криптографически преобразованного массива без знания некоторой (секретной) информации — ключа.

Аутентичность информации состоит в подлинности авторства и целостности.

Существует ряд смежных, но не входящих в криптологию дисциплин. Обеспечением скрытности передачи информации занимается *стеганография*[1]. Обеспечение целостности информации в условиях случайного воздействия помех — предмет теории *помехоустойчивого кодирования*. Смежной областью по отношению к криптологии являются и математические методы *сжатия информации*.

Шифрование информации — это процесс преобразования открытой информации в зашифрованную и наоборот. Первая часть процесса называется *зашифрованием*, вторая — *расшифрованием* (или *дешифрованием*).

Общая формула зашифрования:

$$C = E_{k_E}(M),$$

где M (*message*) — открытая информация, называемая также *исходным* или *открытым* текстом; C (*cipher text*) — по-

---

[1] От греч. στεγᾰνός — «плотно закрывающий», «непроницаемый». Если криптография позволяет создать «*открытое* секретное письмо» — открытое в том смысле, что очевидна зашифрованность письма, то стеганография создает «*скрытое* секретное письмо»: тайной является сам факт наличия секретного сообщения в потоке передаваемой информации.

Пример «стеганографии» в эпоху античности: раба брили наголо, писали на его голове секретное послание и, дождавшись отрастания волос, посылали к адресату письма. Другой пример из докомпьютерной эпохи: В. И. Ленин вел из царской тюрьмы секретную переписку, вписывая потайные сообщения между строк открытого письма жирным молоком, макая ручку в «чернильницу» из хлебного мякиша. «Современный» пример: формат графических файлов *bmp* настолько информационно избыточен, что позволяет изменить значение многих бит (для записи тайной информации) без визуального изменения изображения.

В настоящее время стеганография применяется, например, для скрытой маркировки данных с помощью «водяных знаков». Назначение последних — защита электронных произведений (книг, музыки, видео) от пиратского копирования.

лученный в результате зашифрования шифрованный текст; E (*encryption*) — функция зашифрования, криптографически преобразующая исходный текст; k_E (*key*) — параметр функции E, называемый *ключом шифрования*.

Ключ — это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Зашифрованную с помощью конкретного ключа информацию можно расшифровать только с использованием того же ключа (при симметричном шифровании) или ключа, связанного с ним определенным соотношением (при асимметричном шифровании).

Общая формула расшифрования:

$$M' = D_{k_D}(C),$$

где M' — текст, полученный при расшифровании; D (*decryption*) — функция расшифрования, выполняющая криптографическое преобразование зашифрованного текста; k_D — ключ расшифрования.

Алгоритмы шифрования можно разделить на алгоритмы *симметричного* шифрования и алгоритмы *асимметричного* шифрования.

При симметричном шифровании

$$k_E = k_D = k.$$

Общий ключ зашифрования/расшифрования k называют *ключом* (*симметричного*) *шифрования*. Симметричным шифрованием занимается *криптография с закрытым ключом*.

При асимметричном шифровании ключ зашифрования (открытый ключ) k_E вычисляется из ключа расшифрования (закрытого ключа) k_D таким образом, что обратное вычисление невозможно. Под *невозможностью* здесь и ниже будем понимать факт того, что при существующих вычислительных ресурсах такое вычисление потребовало бы неприемлемо большого времени. Асимметричным шифрованием занимается *криптография с открытым ключом*.

Успешность расшифрования, т. е. получение

$$M' = M,$$

предполагает совместное выполнение двух условий:

1) функция D соответствует функции E;

2) ключ k_D соответствует ключу k_E.

В случае асимметричного шифрования даже при правильной функции расшифрования D получить исходное сообщение $M' = M$ невозможно, если неизвестен ключ расшифрования k_D.

Основной характеристикой алгоритма шифрования является *криптостойкость*, т. е. его устойчивость к раскрытию (*взлому*) методами криптоанализа. Обычно криптостойкость определяется временем, необходимым для взлома шифра, или количеством всех возможных ключей.

3.2. Алгоритмы симметричного шифрования

Алгоритмы симметричного шифрования (в отличие от асимметричного, появившегося в 1970-х гг.) известны с древности. Остановимся на некоторых наиболее известных.

Скитала[1]. Так называлось шифрующее устройство, использовавшееся греками в V–IV вв. до н. э. Оно состояло из двух одинаковых палок. Одну оставляли себе, а другую давали отъезжающему. Чтобы послать тайное сообщение, на скиталу плотно наматывали длинную тонкую ленту папируса, писали на нем (вдоль скиталы) послание, затем снимали папирус и отправляли адресату. Поскольку буквы на папирусе оказывались в беспорядке, адресат мог прочитать послание, лишь намотав ленту на свою скиталу (рис. 3.1). Аристотель предложил способ расшифрования этого шифра. Нужно изготовить длинный конус и, начиная с основания, обертывать его лентой с шифротекстом. В том месте, где диаметр сечения конуса совпадет с диаметром скиталы, начнут просматриваться куски текста. Так можно определить диаметр скиталы, являющийся ключом для данного способа шифрования.

Рис. 3.1. **Скитала**

[1] σκῦτάλη — булава, палица, дубина (греч.).

Шифр Цезаря[1] (шифр простой замены). При шифровании каждая буква алфавита *циклически*[2] сдвигается на m позиций. Число m является *ключом* шифрования: достаточно знать его, чтобы расшифровать сообщение (сам Цезарь брал $m = 3$).

Пример (из «Вакхической песни» А. С. Пушкина при $m = 3$ и игнорировании буквы *Ё*; в криптографии обычно *Е* и *Ё* не различают; см. номера букв в табл. П.1):

М = ДА ЗДРАВСТВУЮТ МУЗЫ, ДА ЗДРАВСТВУЕТ РАЗУМ;

С = ЗГ КЗУГЕФХЕЦБХ ПЦКЮ, ЗГ КЗУГЕФХЕЦИХ УГКЦП.[3]

Шифр Цезаря *абсолютно не стоек*, поскольку раскрыть ключ можно простым перебором возможных вариантов (их всего 32 — количество букв в русском алфавите без *Ё*) до появления осмысленного текста даже вручную.

Казалось бы, стойкость шифра Цезаря должна существенно повыситься, если использовать для каждой буквы индивидуальную величину сдвига (конечно, так, чтобы между исходным и преобразованным алфавитом было взаимно однозначное соответствие). В действительности это иллюзия.

Если текст достаточно длинен, то частота встречаемости каждой буквы стремится к некоторой постоянной величине (*вероятности*), характерной для данного языка и независящей от конкретного текста. Так, в русском языке чаще других используется буква *О*, за ней следуют *Е*, *Ё* и т. д.; самая редкая — *Ф*[4] (см. табл. П.1). Поэтому, подсчитав частоты символов шифрованного текста, можно предположить, что самый часто встречающийся символ обозначает *О*, второй по встречаемости — *Е* (или *Ё*) и т. д. Разгадав значение нескольких первых символов, обычно можно в целом понять содержание шифрованного послания и установить значение всех символов в нем[5]. Для короткого послания задача усложняется, поскольку частоты могут сильно отличаться от табличных (как в примере выше).

---

[1] Гай Юлий Цезарь (C. I. Caesar, 100—44 до н. э.), римский политический деятель; считается, что данный шифр был известен еще до него.

[2] Это означает, что при достижении конца алфавита выполняется переход к его началу (и наоборот — при отрицательных m).

[3] На самом деле разбивать шифрованный текст на слова и ставить знаки препинания в соответствии с открытым текстом *категорически не следует*: это резко облегчает взлом шифра. Обычно шифротекст делят на пятерки букв.

[4] Это неудивительно: за исключением звукоподражаний («*фыркать*» и т. п.) все слова с *Ф* — заимствованные, иностранного происхождения.

[5] На этом основан *статистический криптоанализ*.

Шифр Полибия. Система Цезаря не является старейшей. Возможно, что наиболее древней из известных является система Полибия[1]. Рассмотрим прямоугольник, называемый доской Полибия:

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

Каждая буква шифруется парой букв, указывающих строку и столбец, в которых расположена данная буква. Так, букве А соответствует слог АА, букве Б — АБ, …, букве Ч — ГЕ и т. д. Зашифруем текст «ПРИКЛАДНАЯ МАТЕМАТИКА»:

ВГВДБВБДБЕАААДВБААЕБ ВАААГАААЕВАААГАБВБДАА

При произвольном расписывании алфавита по таблице и шифровании по ней короткого сообщения шифр является стойким даже для нашего времени. Идея была использована в более сложных шифрах в Первую мировую войну.

Шифр Виженера[2]**.** Для шифрования и расшифрования используется квадратная таблица («*таблица Виженера*»); для русского алфавита — размерности 32×32 из 1024 ячеек. В ячейки первой строки вписываются по порядку буквы алфавита, начиная с *А*, в ячейки второй строки — они же с циклическим сдвигом на одну букву, т. е. *Б*, *В*, *Г*, …, *Я*, *А*; в третьей строке — сдвиг на две буквы и т. д. (см. табл. П.2).

Для шифрования выбирается ключевое слово, записываемое нужное число раз *под* буквами шифруемого текста. Очередная буква открытого текста отыскивается в первом столбце таблицы Виженера и определяет *рабочую строку* в ней. Соответствующая буква подписанного ниже ключевого слова отыскивается

---

[1] Полибий (Πολύβιος, около 200—120 до н. э.), греческий историк, из 40 томов всемирной истории которого до нас дошли полностью первые пять.

[2] Блэз де Виженер (B. de Vigenère, 1523—1596), французский дипломат. На протяжении трех веков предложенный им шифр считался невзламываемым и использовался для военных депеш.

в первой строке таблицы Виженера и определяет *рабочий столбец* в ней. На пересечении рабочих строки и столбца находится буква шифрованного текста.

Пример.

Зашифруем строфу из стихотворения В. Я. Брюсова «Грядущие гунны», взяв в качестве ключа слово «Брюсов». В строке № 1 записываем исходный текст, в строке № 2 — ключ с повторениями, в строке № 3 — текст, зашифрованный по Виженеру; столбцы букв пронумерованы (смысл выделения некоторых букв рамкой и другими способами выяснится ниже):

	1	2	3		4	5	6	7	8	9	10	11	12	13	14	15	16
1	А	М	Ы	,	М	У	Д	Р	Е	Ц	Ы	И	П	О	Э	Т	Ы
2	Б	Р	Ю		С	О	В	Б	Р	Ю	С	О	В	Б	Р	Ю	С
3	Б	Ь	Щ		Э	Б	Ж	С	Х	Ф	М	Ц	С	П	Н	Р	М

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
1	Х	Р	А	Н	И	Т	Е	Л	И	Т	А	Й	Н	Ы	И	В	Е	Р	Ы
2	О	В	Б	Р	Ю	С	О	В	Б	Р	Ю	С	О	В	Б	Р	Ю	С	О
3	Г	Т	Б	Э	Ж	Г	У	Н	Й	В	Ю	Ъ	Ы	Э	Й	Т	Г	Б	Й

	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
1	У	Н	Е	С	Е	М	З	А	Ж	Ж	Е	Н	Н	*Ы*	Е	С	В	Е	Т	*Ы*
2	В	Б	Р	Ю	С	О	В	Б	Р	Ю	С	О	В	*Б*	Р	Ю	С	О	В	*Б*
3	Х	О	Х	П	Ц	Ъ	Й	Б	Ц	Д	Ц	Ы	П	*Ь*	Х	П	У	У	Ф	*Ь*

	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	
1	В	К	А	Т	А	К	О	М	Б	Ы	, В	П	У	С	Т	Ы	Н	И	,
2	Р	Ю	С	О	В	Б	Р	Ю	С	О	В	Б	Р	Ю	С	О	В	Б	
3	Т	И	С	А	В	Л	Ю	К	Т	Й	Д	Р	Г	П	Г	Й	П	Й	

	74	75	76	77	78	79	80
1	В	П	Е	Щ	Е	Р	Ы
2	Р	Ю	С	О	В	Б	Р
3	Т	Н	Ц	З	З	С	Л

Итого,

открытый текст:

М = А мы, мудрецы и поэты,
Хранители тайны и веры,
Унесем зажженные светы
В катакомбы, в пустыни,
в пещеры.

шифрованный текст:

С = БЬЩЭБ ЖСХФМ ЦСПНР МГТБЭ
ЖГУНЙ ВЮЪЫЭ ЙТГБЙ ХОХПЦ
ЪЙБЦД ЦЫПЬХ ПУУФЬ ТИСАВ
ЛЮКТЙ ДРГПГ ЙПЙТН ЦЗЗСЛ

Упражнение. Выведите правило расшифровывания сообщения при знании ключа.

При шифровании по Виженеру статистические характеристики исходного текста почти не проявляются в зашифрованном сообщении (рис. 3.2).

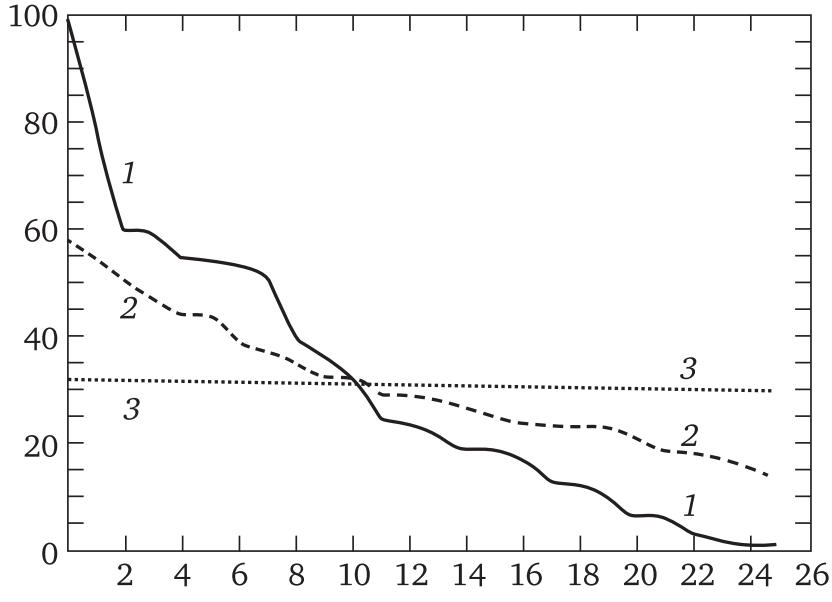


Рис. 3.2. **Относительные частоты встречаемости символов в обычном (англоязычном) тексте (*1*); тексте, зашифрованном по Виженеру (*2*) и с помощью полиалфавитного шифра, полностью выравнивающего частоты (*3*). По горизонтальной оси отложены буквы английского алфавита (по убыванию частоты), по вертикальной оси — относительная частота (в произвольных единицах)**

Чем длиннее ключ, тем устойчивее шифр к взлому. Однако нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его не приходилось записывать.

Шифр Виженера гораздо более стоек, чем шифр простой замены (шифр Цезаря). Тем не менее и он может быть взломан. Соответствующую идею впервые высказал Фридрих Казиски[1]. Рассмотрим ее на приведенном выше примере.

[1] Фридрих Казиски (F.W. Kasiski, 1805—1881) — офицер прусской армии, криптоаналитик, археолог. В 1863 г. опубликовал метод взлома шифра Виженера и других *полиалфавитных* подстановок. Значимость его идеи не была в должной мере понята в XIX в. Сейчас ее оценивают как революционный прорыв в криптоанализе.

1. Сначала нужно определить длину ключевого слова. Очевидно, что *одинаковые* комбинации букв открытого текста и ключа порождают *одинаковые* буквы шифротекста (см. в примере столбцы 7 и 79, 10 и 16, 49 и 55, 56 и 74, двухстолбцовые сочетания 31—32 и 73—74, 38—39 и 50—51). Расстояния между повторяющимися сочетаниями букв шифротекста могут быть различны, но обычно таковы, что на них *целое число раз* укладывается ключевое слово. В рассмотренном примере эти расстояния равны $79-7=72$, $16-10=6$, $55-49=6$, $74-56=18$, $73-31=42$, $50-38=12$. Все они кратны шести, поэтому логично предположить, что ключевое слово состоит из *шести* букв – как оно и есть на самом деле!

Итак, по Казискому отыскивается *наибольший общий делитель* найденных расстояний.

2. Теперь разобьем шифротекст на группы по шесть букв (в примере границы между группами отмечены вертикальными линиями). Первый символ каждой группы сдвинут по алгоритму Виженера на единицу вправо относительно буквы исходного текста (поскольку этому символу соответствует буква Б ключа «БРЮСОВ»). Поэтому совокупность всех первых символов зашифрована по Цезарю со сдвигом $m = 1$.

3. Предположим, что ключ шифра Виженера и, соответственно, m нам *неизвестны*. Тогда величину m можно найти, применяя статистический криптоанализ (см. ниже) к совокупности *первых* символов всех групп. В итоге будут разгаданы *первые* буквы в шестерках зашифрованного текста.

4. Применяя статистический криптоанализ к совокупности *вторых* символов всех групп (они тоже зашифрованы по Цезарю, но, вообще говоря, с другим m — если вторая буква ключевого слова отлична от первой), разгадаем *вторые* буквы в шестерках зашифрованного текста и т. д.

Сделаем несколько замечаний относительно метода Казиского:

• чем больше длина повторяющейся последовательности символов шифротекста, тем менее вероятно, что она образовалась *случайно* (т. е. порождена *различными* сочетаниями букв исходного текста и ключа). По этой причине одно- и двухсимвольные повторения (которые только и присутствуют в проанализированном коротком тексте) считаются непоказательными. Рекомендуется искать повторы не менее чем *трех* символов.

Эксперименты показали хорошую надежность метода Казиского в этом случае;

• искать эти повторы в сколько-нибудь длинном шифротексте вручную практически невозможно (чем может объясняться «прохладный» прием идеи Казиского у его современников). Применение ЭВМ заметно облегчает задачу;

• если для наиболее часто встречающихся символов при достаточно длинном шифротексте частотный метод достаточно надежно указывает исходные буквы открытого текста, то при переходе к менее употребительным символам, частоты которых могут различаться очень незначительно (см. табл. П.1), надежность расшифрования падает. Практически используют *метод наименьших квадратов*: минимизируют сумму квадратов отклонения частот символов в группе от табличных частот букв в языке (см. табл. П.1). Повторяют вычисления для всех групп. Таким образом, находят для каждого символа шифротекста его соответствие в исходном тексте;

• рассмотрим метод наименьших квадратов. Итак, сообразно найденной длине ключевого слова все зашифрованное сообщение разделено на группы букв и выделены подмножества из первых, вторых и т. д. букв всех групп. Для каждой из букв А, Б, В, …, Я в первом подмножестве букв зашифрованного сообщения вычислим частоту появления w_j. Предположим, что они соответствуют буквам А, Б, В, …, Я исходного сообщения (т. е. сдвиг $m = 0$). Вычислим при $m = 0$ величину $D_m = \sum_{j=1}^{32} (p_j - w_{j+m})^2$, где p_j — табличные частоты букв в русскоязычном тексте. Затем предположим, что буквы А, Б, В, …, Я в первом подмножестве букв зашифрованного сообщения соответствуют буквам Я, А, Б, В, …, Ю исходного сообщения (т. е. сдвиг $m = 1$), и снова вычислим $D_m = \sum_{j=1}^{32} (p_j - w_{j+m})^2$, теперь при $m = 1$. Будем повторять вычисление суммы квадратов разностей в предположении $m = 2, 3, \ldots, 31$. Нужно найти $\min\limits_m D_m$: когда эта сумма квадратов разностей окажется наименьшей, мы найдем истинный сдвиг m для первого подмножества букв зашифрованного сообщения, т. е. первую букву ключевого слова. Эти расчеты нужно повторить для всех подмножеств, и ключевое слово будет найдено;

• вместо поиска повторяющихся последовательностей символов современный криптоаналитик берет две копии шифро-

текста и накладывает одну на другую (разумеется, используется ЭВМ, но это не меняет сути дела). Затем нижняя копия циклически сдвигается влево на один символ, на два символа и т. д. При этом всякий раз подсчитывается число наложений одного и того же символа в обоих слоях. Это число *резко возрастает*, когда сдвиг нижнего слоя *кратен* длине ключа. Определив ее, применяют частотный анализ;

• если длина ключа *не меньше* длины шифруемого сообщения[1], то повторы в шифротексте могут быть только *случайными*, и метод Казиского *неприменим*. Конечно, длинный ключ применять на практике неудобно;

• альтернативой классическим идеям Казиского по определению длины ключа является анализ Фридмана[2], основывающийся на нетривиальной идее индекса совпадений. Рассмотрение анализа Фридмана выходит за рамки нашего вводного курса. Очень хорошее изложение см. в книге A. Sinkov «Elementary Cryptanalysis: a Mathematical Approach», указанной в списке литературы (книгу можно найти в интернете).

Шифр Тритемиуса[3] **—** родствен шифрам Цезаря, Виженера и рассматриваемому ниже методу гаммирования. Буквы алфавита нумеруются по порядку (от 1 до 32 в русском алфавите без *Ё* — см. табл. П.1). Выбирается ключевое слово, подписываемое под шифруемым сообщением с повторениями. Чтобы получить шифрованный текст, складывают номер m очередной буквы сообщения с номером n соответствующей буквы ключа. Если полученная сумма $m + n$ больше 32, то из нее вычитают 32. В результате получается последовательность чисел l снова в пределах от 1 до 32[4]. Заменяя в ней числа буквами по той же таблице, получают текст, зашифрованный по Тритемиусу.

Пример.

Зашифруем по Тритемиусу отрывок из стихотворения В. В. Набокова «Слава» с ключевым словом «Набоков».

---

[1] Такая ситуация нам еще встретится ниже при рассмотрении шифра гаммирования.

[2] Уильям Ф. Фридман (Friedman, 1891—1969) — американский криптограф, именуемый «отцом американской криптологии».

[3] Йоханнес Тритемиус (J. Trithemius, 1462—1516) — немецкий аббат, религиозный деятель.

[4] Это сложение по модулю 32, записываемое как $l = (m+n) \bmod 32$; читается: «остаток от деления $m+n$ на 32».

В строке № 1 записываем исходный текст, в строке № 2 — ключ с повторениями, в строке № 3 — зашифрованный текст.

№ 1	Н	Е	Д	О	В	Е	Р	Я	С	Ь	С	О	Б	Л	А	З	Н	А	М
№ 2	Н	А	Б	О	К	О	В	Н	А	Б	О	К	О	В	Н	А	Б	О	К
№ 3	Ы	Ж	Ж	Э	Н	Ф	У	Н	Т	Ю	А	Щ	Р	О	О	И	П	П	Ч

№ 1	Д	О	Р	О	Г	И		Б	О	Л	Ь	Ш	О	Й
№ 2	О	В	Н	А	Б	О		К	О	В	Н	А	Б	О
№ 3	У	С	Ю	П	Е	Ч		М	Э	О	К	Щ	Р	Ш

№ 1	И	Л	И	С	Н	А	М	,	О	С	В	Я	Щ	Е	Н	Н	Ы	М	В	Е	К	А	М	И
№ 2	К	О	В	Н	А	Б	О		К	О	В	Н	А	Б	О	К	О	В	Н	А	Б	О	К	О
№ 3	У	Ъ	Л	Я	О	В	Ы		Щ	А	Е	Н	Ъ	З	Ь	Ш	К	П	Р	Ж	М	П	Ч	Ч

№ 1	О	С	Т	А	Ю	С	Ь	Я	Б	Е	З	Б	О	Ж	Н	И	К	О	М
№ 2	В	Н	А	Б	О	К	О	В	Н	А	Б	О	К	О	В	Н	А	Б	О
№ 3	С	Я	У	В	Н	Ь	Л	В	П	Ж	Й	Р	Щ	Х	Р	Ц	Л	Р	Ы

№ 1	С		В	О	Л	Ь	Н	О	Й		Д	У	Ш	О	Й
№ 2	К		О	В	Н	А	Б	О	К		О	В	Н	А	Б
№ 3	Ь		С	С	Щ	Э	П	Э	Ф		У	Ц	Ж	П	Л

№ 1	В	Э	Т	О	М		М	И	Р	Е	,	К	И	Ш	А	Щ	Е	М		Б	О	Г	А	М	И
№ 2	О	К	О	В	Н		А	Б	О	К		О	В	Н	А	Б	О	К		О	В	Н	А	Б	О
№ 3	С	И	Б	С	Ъ		Н	К	Я	Р		Щ	Л	Ж	Б	Ы	Ф	Ч		Р	С	С	Б	О	Ч

Поясним процесс шифрования. Первая буква открытого текста *Н* имеет номер 14, под ней — такая же буква ключа; сумма номеров (28) соответствует букве *Ы* и т. д.

Итого,

открытый текст:

М = Не доверясь соблазнам дороги большой или снам, освященным веками, остаюсь я безбожником с вольной душой в этом мире, кишащем богами.

шифрованный текст:

С = ЫЖЖЭН ФУНТЮ
АЩРОО ИППЧУ
СЮПЕЧ МЭОКЩ
РШУЪЛ ЯОВЫЩ
АЕНЪЗ ЬШКПР
ЖМПЧЧ СЯУВН
ЬЛВПЖ ЙРЩХР
ЦЛРЫЬ ССЩЭП
ЭФУЦЖ ПЛСИБ
СЪНКЯ РЩЛЖБ
ЫФЧРС СБОЧ

Замечания относительно шифра Тритемиуса:

• если бы ключевое слово состояло из одной буквы, то все буквы открытого текста испытали бы единообразный сдвиг, т. е. шифр Тритемиуса превратился бы в шифр Цезаря;

• как и в случае шифра Виженера, повторяемость ключевого слова накладывает некоторый отпечаток на шифротекст. Это может быть обнаружено статистическими методами, которые позволяют судить о длине ключевого слова; после ее выяснения расшифровка значительно упрощается.

Упражнения

1. Выведите правило расшифровывания сообщения при знании ключа.

2. Проанализировав шифротекст в рассмотренном примере, выясните длину ключевого слова (в предположении, что оно неизвестно).

Шифрование «по книге». Это вариант шифра Тритемиуса, родственный также гаммированию. Два корреспондента договариваются об определенной книге, имеющейся у каждого из них. Пусть это будет данная книга. В качестве ключа выбирается «слово» длины не меньшей, чем передаваемое сообщение. Этот ключ кодируется парой чисел, а именно номером страницы и номером строки на ней, и передается вместе с шифрованным сообщением. Например, (4, 13) определяет «слово»

этот учебный предмет имеет три характерные особенности

Если нужно зашифровать сообщение, то каждую его букву заменяют номером из той же табл. П.1; то же делают со «словом» и складывают номера соответствующих букв сообщения и ключа. Если сумма превышает 32, то из нее вычитают 32.

Упражнение

Зашифруйте с выбранным ключом отрывок из стихотворения И. А. Бунина «Слово»:

…	И	з		д	р	е	в	н	е	й		т	ь	м	ы	,		н	а		м	и	р	о	в	о	м		п	о	г	о	с	т	е	,
	9	8		5	17	6	3	14	6	10		19	29	13	28			14	1		13	9	17	15	3	15	13		16	15	4	15	18	19	6			

	з	в	у	ч	а	т		л	и	ш	ь		П	и	с	ь	м	е	н	а
	8	3	20	24	1	19		12	9	25	29		16	9	18	29	13	6	14	1

Разумеется, для шифрования с использованием ЭВМ данный метод неудобен.

Шифрование методом перестановки. Метод заключается в том, что символы шифруемого текста *переставляются* по определенным правилам внутри шифруемого блока символов.

Пример.

Можно, например, записать исходную фразу по строкам шифровальной таблицы, а прочитать по столбцам:

Б	Е	Д	Н	Ы	Й	С	Л	А	Б	Ы	Й	В	О	И	Н
Б	О	Г	А	В	Е	С	Ь	И	С	Т	А	Я	В	Ш	И
Й	К	А	К	Д	Ы	М	П	О	Д	Ы	Ш	И	Е	Щ	Е
Н	Е	М	Н	О	Г	О	Т	Я	Ж	К	И	М	В	О	З
Д	У	Х	О	М	З	Е	М	Н	Ы	М	А	Б	В	Г	Д

(поясним, что остаток последней строки заполнен незначащими буквами — балластом[1]).

Тогда окончание последнего предсмертного стихотворения Ф. К. Сологуба

Бедный, слабый воин Бога,
Весь истаявший, как дым,
Подыши еще немного
Тяжким воздухом земным.

будет зашифровано как

ББЙНД ЕОКЕУ ДГАМХ НАКНО ЫВДОМ ЙЕЫГЗ ССМОЕ
ЛЬПТМ АИОЯН БСДЖЫ ЫТЫКМ ЙАШИА ВЯИМБ ОВЕВВ
ИШЩОГ НИЕЗД

Условливаясь с адресатом послания о способе считывания символов из таблицы, можно получить другие варианты шифротекста. Например, при считывании по диагоналям с «северо-востока» на «юго-запад»:

Б Е Д Н Ы Й С Л А Б Ы Й В О И Н
Б О Г А В Е С Ь И С Т А Я В Ш И
Й К А К Д Ы М П О Д Ы Ш И Е Щ Е
Н Е М Н О Г О Т Я Ж К И М В О З
Д У Х О М З Е М Н Ы М А Б В Г Д

[1] Добавление балласта, в действительности, нежелательно, так как дает криптоаналитику в случае перехвата шифротекста информацию о размере шифровальной таблицы.

— получим:

БЕБДО ЙНГКН ЫААЕД ЙВКМУ СЕДНХ ЛСЫОО АЬМГМ БИПОЗ
ЫСОТЕ ЙТДЯМ ВАЫЖН ОЯШКЫ ИВИИМ НШЕМА ИЩВБЕ ОВЗГД

Возможна *перестановка с ключом*. Выберем в качестве такового слова́ «ФЕДОР К. ТЕТЕРНИКОВ» (так в действительности звали поэта Сологуба). Расположим буквы ключа в алфавитном порядке и пронумеруем по порядку:

В	Д	Е	Е	Е	И	К	К	Н	О	О	Р	Р	Т	Т	Ф
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Запишем ключ в первой строке шифровальной таблицы, а номера букв ключа — во второй:

Ф	Е	Д	О	Р	К	Т	Е	Т	Е	Р	Н	И	К	О	В
16	3	2	10	12	7	14	4	15	5	13	9	6	8	11	1
Б	Е	Д	Н	Ы	Й	С	Л	А	Б	Ы	Й	В	О	И	Н
Б	О	Г	А	В	Е	С	Ь	И	С	Т	А	Я	В	Ш	И
Й	К	А	К	Д	Ы	М	П	О	Д	Ы	Ш	И	Е	Щ	Е
Н	Е	М	Н	О	Г	О	Т	Я	Ж	К	И	М	В	О	З
Д	У	Х	О	М	З	Е	М	Н	Ы	М	А	Б	В	Г	Д

Будем теперь считывать столбцы в очередности их номеров:

НИЕЗД ДГАМХ ЕОКЕУ ЛЬПТМ БСДЖЫ ВЯИМБ ЙЕЫГЗ ОВЕВВ
ЙАШИА НАКНО ИШЩОГ ЫВДОМ ЫТЫКМ ССМОЕ АИОЯН ББЙНД

Не знающему ключа злоумышленнику придется нелегко…[1]

Вообще, метод перестановки — один из *самых стойких* классических методов шифрования, поскольку существует необозримое количество видов шифровальных таблиц, способов их заполнения и прочтения.

Вместе с тем, поскольку символы шифротекста— те же, что и в открытом тексте, статистический анализ покажет, что частоты символов сильно различаются. Это дает криптоаналитику информацию о том, что использован перестановочный шифр, и (возможно) — на каком языке написано сообщение.

---

[1] Таким шифром пользовались немецкие шпионы во время Второй мировой войны. В качестве ключа они применяли первые буквы строк на определенной странице заданной книги.

Упражнение

Что является ключом при шифровании перестановкой?

Метод гаммирования заключается в том, что символы шифруемого текста последовательно складываются с символами некоторой специально подготовленной (как правило, случайной) последовательности — *гаммы*.

При работе на ЭВМ, например, символы исходного текста и гаммы можно представить в виде двоичного кода (см. табл. П.3) и сложить по модулю 2.

Стойкость шифрования методом гаммирования определяется, главным образом, свойствами гаммы — длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерности в появлении символов в пределах периода.

Если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким. Практически, при наличии дополнительной информации, исходный текст обычно может быть частично или полностью восстановлен.

Возникает вопрос о том, как получить случайную последовательность чисел. Разумеется, не может быть и речи о том, чтобы хранить в памяти ЭВМ таблицу случайных чисел (почему?). Числа должны генерироваться по мере возникновения потребности в них. Для получения случайных чисел может использоваться:

1) физический генератор — это был бы наилучший, наиболее качественный способ получения случайных чисел. Известно, например, что атомы радиоактивного вещества распадаются по закону случайных чисел: распадется ли данный атом в ближайшую секунду или через тысячу лет — предсказать невозможно. Таким образом, радиоактивный препарат в сочетании со счетчиком радиоактивных распадов был бы идеален. Но такой способ дорог, сложен в реализации, небезопасен. Поэтому почти всегда вместо физических генераторов применяется

2) компьютерная программа. Разумеется, программа работает детерминированно, и результатом ее работы являются числа не случайные, а *псевдослучайные*: до исчерпания периода повторения (для хороших программ он исчисляется миллионами чисел) псевдослучайные числа близки по свойствам к истинно случайным, но этот период нельзя превышать, поскольку иначе заново пойдут те же числа, и случайности уже не будет;

3) последовательность цифр *иррационального числа*, поскольку оно записывается как бесконечная непериодическая десятичная дробь, например, последовательность цифр числа
π = 3,14159 26535 89793 23846 26433 83279 50288 41971 693 99 37510 58209 74944 59230 78164 06286 20899 86280 34825 34211 70679 82148…,
(отношение длины окружности к ее диаметру), числа
e = 2,71828 18284 59045 23536 02874 71352 66249 77572 470 93 69995 95749 66967 62772 40766 30353 54759 45713 82178 52516 64274 27466…
(основание натуральных логарифмов) и, вообще, любого иррационального числа ($\sqrt{2}, \sqrt[3]{5}, \ldots$).

Пример.

Зашифровать методом гаммирования первую строку Марсельезы «*Allons, enfants de la Patrie*…»[1], взяв в качестве гаммы последовательность цифр числа

$$\sqrt{2} = 1{,}41421\ 35623\ 73095\ 04880\ 16887\ 24210\ldots$$

Заменим буквы исходного текста их порядковыми номерами (см. табл. П.3), сложим эти номера с последовательными цифрами гаммы; если будет получаться число, превышающее 26 (мощность алфавита), вычтем из суммы 26 (т. е. выполним сложение по модулю 26); результат преобразуем обратно в буквы:

Шифруемый текст	**№ п/п (см. табл. П.3)**	**Гамма**	**Сумма по модулю 26**	**Буква шифротекста**
A	1	1	2	B
L	12	4	16	P
L	12	1	13	M
O	15	4	19	S
N	14	2	16	P
S	19	1	20	T
E	5	3	8	H
N	14	5	19	S
F	6	6	12	L

[1] «*Вперед, сыны Отечества*…» (франц.).

Окончание таблицы

Шифруемый текст	№ п/п (см. табл. П.3)	Гамма	Сумма по модулю 26	Буква шифротекста
A	1	2	3	C
N	14	3	17	Q
T	20	7	1	A
S	19	3	22	V
D	4	0	4	D
E	5	9	14	N
L	12	5	17	Q
A	1	0	1	A
P	16	4	20	T
A	1	8	9	I
T	20	8	2	B
R	18	0	18	R
I	9	1	10	J
E	5	6	11	K

Итак, получился шифротекст

BPMSP THSLC QAVDN QATIB RJK.

Как отмечено выше, есть немало общего между гаммированием и шифром Тритемиуса. Ключевое слово в последнем — это тоже гамма, но выраженная, как правило, не в цифрах, а в буквах.

Шифр Вернама. Шифр Вернама, или *одноразовый блокнот*, реализует идеи гаммирования. Его изобрел в 1918 г. Г. Вернам (Gilbert S. Vernam), инженер *American Telephone & Telegraph Co*. В классическом понимании одноразовый блокнот есть большая неповторяющаяся последовательность символов ключа, распределенных случайным образом. Первоначально это была одноразовая лента для телетайпов. Отправитель использовал каждый символ ключа для шифрования только одного символа открытого текста. Шифрование представляет собой сложение по модулю n (мощность алфавита) символа открытого текста и символа ключа из одноразового блокнота. Каждый символ ключа используется только один раз и для единственного сообщения, иначе даже при использовании блокнота раз-

мером в несколько гигабайт получение криптоаналитиком нескольких текстов с перекрывающимися ключами позволит ему восстановить исходный текст. Если же ключ не повторяется и случаен, то криптоаналитик, перехватывает он тексты или нет, всегда имеет одинаковые знания. Случайная ключевая последовательность, сложенная с неслучайным открытым текстом, дает совершенно случайный шифротекст, и никакие вычислительные мощности не смогут это изменить.

В реальных системах сначала подготавливают две одинаковые ленты со случайными цифрами ключа. Одна остается у отправителя, а другая передается неперехватываемым способом, например, курьером с охраной, законному получателю. Когда отправитель хочет передать сообщение, он сначала преобразует его в двоичную форму и помещает в устройство, которое к каждой цифре сообщения прибавляет по модулю два цифры, считанные с ключевой ленты. На принимающей стороне кодированное сообщение записывается и пропускается через машину, похожую на устройство, использованное для шифрования, которое к каждой двоичной цифре сообщения прибавляет (или вычитает, так как сложение и вычитание по модулю 2 эквивалентны) по модулю два цифры, считанные с ключевой ленты, получая, таким образом, открытый текст. При этом, естественно, ключевая лента должна продвигаться синхронно со своим дубликатом, используемым для шифрования.

Главным недостатком данной системы является то, что для каждого бита переданной информации должен быть *заранее* подготовлен бит ключевой информации, причем эти биты должны быть случайными. При шифровании большого объема данных это является серьезным ограничением. Кроме того, гамму нужно заблаговременно переслать адресату. Поэтому данная система используется только для передачи сообщений наивысшей секретности. «Горячая линия» между США и СССР в годы Холодной войны шифровалась именно с помощью одноразового блокнота.

Класс шифров Вернама — единственный, для которого может быть доказана (и была доказана К. Шенноном) невзламываемость в абсолютном смысле этого термина.

Шифрование с помощью аналитических преобразований. Большим разнообразием отличаются аналитические преобразования, которые можно использовать для закрытия информации. В качестве примера рассмотрим матричное умножение $C = AB$.

Если квадратную матрицу A размерности $n \times n$ использовать в качестве ключа, а в качестве компонент n-мерного вектора B подставить символы исходного текста (выраженные, например, своими ASCII-кодами или номерами в алфавите), то компоненты n-мерного вектора C будут представлять собой символы зашифрованного текста (в том же числовом выражении).

Пример.

Взяв в качестве ключа матрицу

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{pmatrix},$$

зашифровать высказывание «*L'État, c'est moi*»[1].

Заменим символы исходного текста их ASCII-кодами (см. табл. П.3): 76, 69, 84, 65, 84, 67, 69, 83, 84, 77, 79, 73 (мы не учитываем никаких знаков, кроме букв в чистом виде). Разбив эту последовательность на *четверки* чисел[2], применим к каждой из них матричное умножение:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{pmatrix} \begin{pmatrix} 76 \\ 69 \\ 84 \\ 65 \end{pmatrix} = \begin{pmatrix} 726 \\ 573 \\ 164 \\ -482 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{pmatrix} \begin{pmatrix} 84 \\ 67 \\ 69 \\ 83 \end{pmatrix} = \begin{pmatrix} 757 \\ 604 \\ 137 \\ -552 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{pmatrix} \begin{pmatrix} 84 \\ 77 \\ 79 \\ 73 \end{pmatrix} = \begin{pmatrix} 767 \\ 624 \\ 167 \\ -512 \end{pmatrix}.$$

---

[1] «*Государство — это я*»; фраза, приписываемая Людовику XIV.

[2] *Блочный* шифр, в котором одновременно преобразуется блок информации, в отличие от рассмотренных выше *потоковых* шифров, где шифрование происходило последовательно, посимвольно.

Шифротекст:

726, 573, 164, –482, 757, 604, 137, –552, 767, 624, 167, –512.

Чтобы расшифровать сообщение C при *известном* ключе A, нужно обратить соотношение $C = AB$; получим:

$$B = A^{-1}C,$$

где A^{-1} — матрица, обратная исходной матрице A; напомним, что

$$A^{-1}A = AA^{-1} = E = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

— единичная матрица.

Для матрицы A из рассмотренного примера

$$A^{-1} = \begin{pmatrix} 22 & -6 & -26 & 17 \\ -17 & 5 & 20 & -13 \\ -1 & 0 & 2 & -1 \\ 4 & -1 & -5 & 3 \end{pmatrix}$$

(проверьте перемножением с A). Тогда первые четыре буквы исходного текста получим умножением

$$\begin{pmatrix} 22 & -6 & -26 & 17 \\ -17 & 5 & 20 & -13 \\ -1 & 0 & 2 & -1 \\ 4 & -1 & -5 & 3 \end{pmatrix} \begin{pmatrix} 726 \\ 573 \\ 164 \\ -482 \end{pmatrix} = \begin{pmatrix} 76 \\ 69 \\ 84 \\ 65 \end{pmatrix}$$

и т. д.

Обобщим рассмотренные способы шифрования.

Классические методы криптографического закрытия информации (симметричные шифры; криптография с закрытым ключом)

I. Шифрование

1. *Замена* (*подстановка*):

а) простая (моно- или одноалфавитная). Замена постоянна на протяжении всего текста: например, шифр Цезаря;

б) многоалфавитная (полиалфавитная) одноконтурная обыкновенная. Подстановка меняется в различных частях текста, т. е. одна и та же буква может быть зашифрована поразному. Для замены символов исходного текста используется *контур* (набор из нескольких алфавитов), причем смена алфавитов из контура осуществляется последовательно и циклически, т. е. первый символ заменяется соответствующим символом 1-го алфавита, второй — символом 2-го алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. Затем последовательность алфавитов повторяется. Это является хорошей защитой от простого подсчета частот, так как не существует единой маскировки для каждой буквы в шифротексте. Пример — шифр Виженера, в котором количество используемых алфавитов определяется числом неповторяющихся букв ключевого слова;

в) многоалфавитная одноконтурная монофоническая. Количество и состав алфавитов выбираются так, чтобы частоты появления всех символов в шифротексте были по возможности одинаковыми. Это затрудняет частотный криптоанализ. Выравнивание частот достигается тем, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих символов, чем для редких. Поэтому простой подсчет частот ничего не даст криптоаналитику. Однако доступна информация о распределении пар и троек букв в различных естественных языках. Криптоанализ, основанный на такой информации, будет более успешным;

г) многоалфавитная многоконтурная. Для шифрования циклически используются несколько наборов (*контуров*) алфавитов, причем каждый контур имеет свой индивидуальный период применения. Этот период, как правило, исчисляется количеством знаков, после шифрования которых меняется контур алфавитов. Примером многоалфавитной многоконтурной подстановки является замена по таблице Виженера, если для шифрования используются несколько ключей, каждый из которых имеет свой период применения.

2. *Перестановка*

а) простая;

б) усложненная по таблице;

в) с ключом.

3. *Аналитическое преобразование*, например — с использованием алгебры матриц.

4. *Гаммирование*:

а) с конечной гаммой. Примеры — шифр Тритемиуса, Вернама, «по книге»;

б) с бесконечной гаммой.

5. *Комбинированные методы*:

а) замена и перестановка,

б) замена и гаммирование,

в) перестановка и гаммирование, …

II. Кодирование. Как и шифрование, имеет длительную историю применения. Разница между ними сродни различию между алфавитной и иероглифической системами письменности. При *шифровании* заменяемыми единицами являются *символы* алфавита; следовательно, шифрованию могут подвергаться *любые* данные, для фиксирования которых используется данный алфавит. При *кодировании* замене кодами (цифровыми, буквенными и т. п.) подвергаются *смысловые элементы* информации, поэтому для каждого специального сообщения в общем случае приходится использовать *индивидуальную* систему кодирования. По существу, код является огромным шифром замены, в котором основными единицами открытого текста служат слова и фразы. В шифрах же основная единица — это знак, иногда — несколько знаков.

Кодирование и шифрование иногда по ошибке смешивают-ся, но нужно иметь в виду, что для восстановления закодированного сообщения достаточно знать правила кодирования, в то время как для расшифрования зашифрованного сообщения помимо знания правил шифрования требуется *ключ* к шифру.

III. Другие виды

1. *Рассечение-разнесение*. Массив данных рассекается на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным участкам запоминающего устройства или располагаются на различных носителях. Обратная процедура — сборка данных.

2. *Сжатие данных*. Сжатие представляет собой замену часто встречающихся последовательностей одинаковых символов некоторыми заранее выбранными символами.

Комбинированные методы шифрования. Ни один из рассмотренных классических методов шифрования в отдельности не удовлетворяет современным требованиям к уровню криптографической защиты информации. Перечислим некоторые требования:

• *принцип Керкхоффса*[1]: стойкость шифра к взлому должна основываться на тайне ключа, а не алгоритма шифрования. В самом деле, количество *оригинальных* идей шифрования исчисляется в лучшем случае десятками, и утаить их (особенно в эпоху информационных технологий) невозможно;

• *принцип разумной достаточности*: выбирая между высоконадежным, но дорогим в использовании шифром и более доступной альтернативой, следует считать данный шифр достаточным для шифрования данной тайны, если затраты злоумышленника на взлом превысят ценность добытой при взломе информации;

• *принцип рассеивания*: распространение влияния одного знака открытого теста на много знаков шифротекста, что позволяет скрыть статистические свойства открытого текста;

• *принцип перемешивания*: использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текста. При этом неоднократное вхождение одинаковых фрагментов в исходное сообщение не приводит к повторам в шифротексте. Достигается это тем, что каждый блок открытого текста (кроме первого) побитно складывается по модулю 2 с предыдущим результатом шифрования.

Эффективным средством повышения стойкости шифрования является *комбинированное* использование нескольких различных способов шифрования, т. е. последовательное шифрование текста с помощью двух методов или более. Стойкость комбинированного шифрования не ниже *произведения* стойкостей использованных способов.

Комбинировать можно любые методы шифрования и в любом количестве, но на практике наиболее распространены комбинации подстановок, перестановок и гаммирований. Они обеспечивают рассеивание и перемешивание.

Примером комбинированного шифра является DES — национальный стандарт США криптографического закрытия данных.

Алгоритм DES. Американский стандарт симметричного шифрования DES (Data Encryption Standard), принятый в 1977 г. и ныне устаревший, является представителем блочных

---

[1] Огюст Керкхоффс (1835—1903) — нидерландский и французский криптограф, лингвист, историк, математик.

шифров. Он допускает эффективную аппаратную и программную реализации с высокой скоростью шифрования. DES был разработан фирмой *IBM* в интересах федерального правительства США для криптографической защиты наиболее значимых компьютерных данных.

В алгоритме DES шифруются двоичные 64-битные блоки данных с использованием двоичного секретного ключа длиной также в 64 бита. Однако фактически секретными в нем являются только 56 бит, поскольку последние разряды байтов, т. е. его 8-й, 16-й, …, 64-й биты, отведены для контроля предшествующих разрядов соответствующих байтов по четности и в шифровании не участвуют. Каждый такой бит является двоичной суммой семи предыдущих и служит для обнаружения ошибок при передаче ключа по каналу связи. Число различных ключей DES-алгоритма равно $2^{56} > 7 \cdot 10^{16}$.

Алгоритм DES разработан так, что расшифрование выполняется с помощью того же процесса (в *прямом* порядке), что и шифрование. Это удобно, поскольку одно и то же устройство может использоваться как для шифрования, так и для расшифрования.

Длительное изучение алгоритма DES показало следующие его достоинства: каждый бит шифротекста зависит от всех бит ключа и открытого текста; изменение любого бита ключа или открытого текста с вероятностью 1/2 меняет каждый бит шифротекста; изменение одного бита шифротекста непредсказуемо сказывается на открытом тексте в процессе расшифровывания.

В отличие от использовавшихся ранее криптографических систем DES является полностью открытым алгоритмом — в том смысле, что его устройство известно до мельчайших подробностей и любой желающий может написать программу, реализующую его. Парадоксально: одна из лучших систем шифрования в истории криптологии наименее секретна!

DES, являясь первым опытом стандартизации шифрования, имеет недостатки. За время, прошедшее после создания DES, компьютерная техника развивалась настолько быстро, что оказалось возможным осуществлять исчерпывающий перебор ключей и тем самым раскрывать шифр[1]. Таким образом, современным требованиям секретности DES уже не удовлетворяет. Из-за небольшого размера ключа — 56 значащих бит — алго-

[1] Атака методом грубой силы (brute-force attack).

ритм DES можно использовать только для закрытия коммерческой (несекретной) информации. При этом перебор всех ключей экономически нецелесообразен, так как затраты на взлом не соответствуют ценности информации, закрываемой шифром (принцип разумной достаточности — см. выше).

Для повышения криптостойкости была предложена схема

$$C = \boldsymbol{DES}_{k_1}(\boldsymbol{DES}^{-1}_{k_2}(\boldsymbol{DES}_{k_3}(M)))$$

— так называемый *Triple* DES (тройной DES). Использование в этой формуле обратного преобразования на втором шаге вычисления нужно для того, чтобы обеспечить совместимость с обычным DES (когда ключи k_1 и k_2 совпадают). Недостаток этого алгоритма — в три раза более низкая по сравнению с DES скорость работы.

Ныне действующий стандарт шифрования AES. В конце 1990-х гг. алгоритм DES окончательно устарел из-за своего короткого ключа, Triple DES не подошел из-за медлительности. В 1997 г. в США был объявлен открытый конкурс на разработку нового стандарта блочного шифра. Победитель конкурса должен был получить статус Продвинутого стандарта шифрования AES (Advanced Encryption Standard) и рекомендоваться к повсеместному использованию на территории США.

На конкурс было прислано 15 алгоритмов, до апреля 1999 г. шло их изучение; во второй тур конкурса вышло пять алгоритмов, обладавших следующими достоинствами:

1) высокая стойкость к известным видам атак;

2) отсутствие слабых ключей;

3) понятная структура, до некоторой степени гарантирующая отсутствие потенциальных уязвимостей и незаявленных возможностей;

4) невысокие требования к оперативной и энергонезависимой памяти (последнее особо важно, например, для смарт-карт).

Итоги конкурса были подведены в октябре 2000 г.; победителем стал алгоритм RIJNDAEL (произносится: «рейндаль»). Его разработчики — бельгийцы Винсент Реймен (V. Rijmen) и Йоан Дамен (J. Daemen). Именно RIJNDAEL и стал новым стандартом симметричного шифрования AES.

Алгоритм RIJNDAEL является блочным шифром с переменной длиной блока и переменной длиной ключа. Длины бло-

ка и ключа могут быть выбраны независимо равными 128, 192 или 256 бит. Не вдаваясь в подробности его весьма сложного и нетрадиционного устройства, отметим, что отличиями его от других представленных на конкурс алгоритмов являются:

• высокая скорость шифрования на всех платформах — как в программной, так и в аппаратной реализации;

• широкие возможности для распараллеливания вычислений;

• минимальные требования к ресурсам, что важно для реализации алгоритма в устройствах с ограниченными вычислительными возможностями.

Российский алгоритм шифрования ГОСТ 28147—89 (устаревший). Является примером DES-подобных криптосистем. Принят в 1989 г. (еще в СССР) как государственный стандарт шифрования данных, обязательный для применения в государственных органах, а также организациях, предприятиях, банковских и иных учреждениях, деятельность которых связана с обеспечением информационной безопасности РФ. Для прочих организаций и частных лиц ГОСТ имел рекомендательный характер.

Стандарт формировался с учетом недостатков алгоритма DES. Алгоритм ГОСТ 28147—89 шифрует информацию блоками по 64 бита; имеет четыре режима работы: простая замена, гаммирование, гаммирование с обратной связью, выработка имитовставок[1].

В шифре ГОСТ используется 256-битовый ключ, обеспечивающий $2^{256} > 1{,}1 \cdot 10^{77}$ различных ключей.

Для взлома шифра ГОСТ не предложено более эффективных методов, чем метод «грубой силы». Высокая стойкость шифрования достигается за счет следующих факторов:

• большая длина ключа — 256 бит;

• 32 раунда шифрования. Уже после восьми раундов достигается полное рассеивание исходных данных: изменение одного бита открытого текста влияет на все биты шифротекста, что говорит о многократном запасе стойкости.

Вместе с тем длинный ключ обусловливает *медлительность* российского алгоритма.

---

[1] *Имитовставка* — это криптографическая контрольная сумма, вычисляемая с использованием секретного ключа шифрования и предназначенная для проверки целостности сообщений.

Стандарт отменен на территории России и СНГ в 2019 г. в связи с принятием заменяющих его межгосударственных стандартов ГОСТ 34.12—2018 (описывает шифры «Магма» и «Кузнечик») и ГОСТ 34.13—2018 (описывает режимы работы блочных шифров).

Ныне действующие российские алгоритмы шифрования «Магма» и «Кузнечик». «Кузнечик» — симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит. Ожидается, что «Кузнечик» будет устойчив ко всем видам атак на блочные шифры. В 2015 г. вместе с новым алгоритмом «Кузнечик» один из вариантов старого алгоритма ГОСТ 28147—89 был опубликован под названием «Магма» как часть стандарта ГОСТ Р 34.12—2015, а позже — как часть стандарта ГОСТ 34.12—2018.

Криптосистемы с открытым ключом. Слабым местом симметричного шифрования является *проблема распределения ключей*. Пусть в группе из 1000 человек любые двое должны быть обеспечены возможностью обмениваться секретными сообщениями и проверять авторство полученных писем. Тогда пользователю *A* потребуются 999 секретных ключей для корреспонденции с 999 адресатами. Один из этих ключей относится к переписке пользователя *A* с пользователем *B*, но последний должен будет хранить еще 998 ключей для переписки с другими людьми из группы и т. д. Всего потребуется 999 + 998 + + … + 2 + 1 + 0 ключей (последнему пользователю группы потребуется 0 добавочных ключей, так как все нужные ему ключи уже учтены). Складывая в этой сумме из 1000 слагаемых первое число с последним, второе — с предпоследним и т. д., получим 1000 / 2 = 500 пар, каждая из которых равна 999 = 1000 – 1. Итого, потребуется

$$\frac{1000}{2}(1000-1)=499\,500$$

различных ключей для обеспечения секретности переписки между любыми двумя представителями сообщества в 1000 человек. Для группы из n человек будет нужно

$$\frac{n(n-1)}{2}$$

секретных ключей. Итак, количество ключей возрастает слишком быстро — пропорционально *квадрату* числа пользовате-

лей! Безопасное распределение ключей среди пользователей является сложной проблемой. Единственным совершенно надежным способом передачи ключа являются личные встречи, но их потребуется очень много.

Кроме того, поскольку каждые два человека *A* и *B* из группы используют для обмена сообщениями между собой один и тот же ключ, *A должен быть уверен* в том, что *B* хранит ключ в строгой тайне, — только в этом случае *A* имеет гарантию того, что его письма к *B* останутся тайной для всех, кроме *B* (*секретны*), а получаемые им от имени *B* письма действительно написаны последним (*аутентичны*), а не подделаны злоумышленником *C*, завладевшим ключом. В дипломатической переписке условие взаимного доверия обычно выполняется: посольство *A* может быть уверено в том, что посольство *B* хранит свою копию их общего криптографического ключа должным образом. Кроме того, *A* не опасается, что

1) *B* пошлет ему сообщение, а позже дезавуирует его как подделку, изготовленную *A*;

2) *B* заявит о получении от *A* сообщения, которое *B* мошеннически сам и приготовил.

В коммерции и бизнесе ситуация обратна, у партнеров по заочным переговорам есть причины для беспокойства: покупатель не хочет, чтобы продавец мог за его спиной создать подложный договор, выдав его за подписанный покупателем; в свою очередь, продавца не устроила бы система, при которой клиент имел бы возможность безнаказанно в одностороннем порядке отказаться от законно заключенной сделки.

Итак, симметричному шифрованию присущи следующие крупные недостатки:

• *проблема распределения ключей*: количество ключей растет пропорционально квадрату числа пользователей системы, и каждый пользователь вынужден хранить в тайне столько ключей (за вычетом одного), сколько пользователей в системе;

• *проблема доверия между пользователями*, имеющая несколько аспектов:

— каждый пользователь *A*[1] должен быть уверен в том, что любой из его корреспондентов надежно хранит свою копию секретного ключа, используемого для переписки с *A*,

---

[1] Вместо *пользователя A* и *пользователя B* в криптографии укоренилось краткое именование *Alice*, *Bob*. Злоумышленника именуют *Eve* по первой букве англ. слова *Eavesdropper* — соглядатай, перехватчик, шпион, подслушивающий.

— Алиса опасается, что Боб в одностороннем порядке откажется от достигнутой письменной договоренности (проблема *отказуемости*),

— Алиса опасается, что Боб может сфабриковать письмо, якобы полученное от Алисы (проблема *фальсифицируемости*).

В симметричных криптосистемах секретные ключи шифрования k_E и расшифрования k_D, используемые, соответственно, отправителем и адресатом, либо совпадают, либо легко могут быть вычислены один из другого. В асимметричных криптосистемах это не так. Симметричное шифрование имеет многовековую историю, тогда как асимметричное сравнительно ново. В 1976 г. У. Диффи и М. Хеллман (Whitfield Diffie, Martin Hellman) из Станфордского университета (США) предложили концептуальную схему, названную ими *криптосистемой с открытым ключом*, поскольку проблема распределения ключей решалась в ней размещением ключей шифрования пользователей в открытых для свободного доступа директориях. Статья Диффи и Хеллмана «Новые направления в криптографии» стала первой публикацией об асимметричной криптографии в открытой печати.

К асимметричным криптосистемам предъявляются следующие требования:

1) пара соответствующих друг другу ключей k_E, k_D должна легко вычисляться законным пользователем, но для криптоаналитика восстановление их по перехваченному тексту должно быть непреодолимо трудно (практически невозможно) независимо от длины текста;

2) операции шифрования и расшифрования должны быть нетрудны в вычислительном отношении для законного пользователя;

3) вычисление одного ключа из пары должно быть непреодолимо трудным для криптоаналитика, даже если он знает другой ключ пары и сколь угодно длинную последовательность символов открытого и шифрованного текстов, соответствующих этому ключу.

Криптографические системы с открытым ключом используют так называемые *однонаправленные* (другие названия: *односторонние*, *необратимые*)[1] функции, обладающие следующим

[1] Однонаправленные функции не следует смешивать с функциями, являющимися *математически необратимыми* из-за того, что они не взаим-

свойством: при заданном значении x относительно просто вычислить значение $f(x)$, однако, если известно значение $y = f(x)$, то вычислить соответствующий ему x практически невозможно. Точнее: при использовании современных вычислительных средств это невозможно сделать за приемлемое время.

Простым примером однонаправленной функции являются *целочисленное умножение* и *факторизация*. Известно, что перемножить два целых числа, пусть и очень больших, относительно нетрудно, но даже мощнейший из существующих компьютеров не в состоянии за разумное время с помощью наилучшего из имеющихся алгоритмов выполнить разложение на множители (*факторизацию*) 400-значного десятичного числа, являющегося произведением двух простых чисел примерно одинакового размера. На этой задаче основан подробно рассматриваемый в следующей теме алгоритм RSA асимметричного шифрования. Если бы обнаружился более эффективный алгоритм факторизации, это сделало бы ненадежной асимметричную криптографию, основанную на целочисленном умножении. Математики, работающие в данной области, находятся под пристальным вниманием спецслужб…

Другим примером однонаправленной функции является *дискретное логарифмирование*: даны целые числа a, m и n, требуется найти такое число x (если, конечно, оно существует), что $a^x \equiv m (\mathrm{mod}\, n)$. Например, $5^3 \equiv 11 (\mathrm{mod}\, 19)$, так что 3 есть дискретный логарифм числа 11 с основанием 5 по модулю 19. На этой задаче основаны алгоритмы Diffie-Hellman и El-Gamal асимметричного шифрования. В настоящее время не известно ни одного алгоритма вычисления дискретных логарифмов больших чисел за приемлемое время даже на самых мощных компьютерах.

Наконец, для выработки электронной цифровой подписи (ЭЦП) используется криптосистема на основе эллиптических кривых $y^2 = x^3 + ax + b$. Для точек на кривой вводится операция сложения (добавления новой точки по двум известным).

Криптосистемы с открытым ключом основаны на однонаправленных функциях с люком (секретом). При этом открытый ключ определяет конкретную реализацию функции, а секретный ключ дает информацию о люке. Если располагать инфор-

---

ноднозначны (т. е. существуют *несколько* различных значений x таких, что $f(x) = y$, либо их нет вовсе).

мацией о люке, то легко можно вычислить функцию в обоих направлениях. Тот, у кого этой информации нет, может производить вычисления только в одном направлении. Прямое направление используется для шифрования и верификации цифровых подписей, а обратное — для расшифрования и выработки цифровой подписи.

Во всех криптосистемах с открытым ключом чем длиннее ключ, тем больше различие между усилиями, необходимыми для вычисления функции в прямом и обратном направлениях (для того, кто не имеет информации о люке).

Все криптосистемы с открытым ключом основаны на функциях, *считающихся* однонаправленными, но это свойство до сих пор не доказано ни для одной из них. Это означает, что теоретически возможно открытие алгоритма, позволяющего легко вычислять обратную функцию без информации о люке.

Асимметричные криптосистемы используются в трех направлениях:

1) как самостоятельные средства защиты передаваемых и хранимых данных;

2) как средство для распределения ключей. Алгоритмы асимметричного шифрования более трудоемки и медленны, чем симметричные. Поэтому на практике рационально с помощью асимметричного шифрования распределять ключи (их размер незначителен), а затем посылать большие объемы данных, защищенные с помощью обычных алгоритмов;

3) средства аутентификации пользователей (электронная подпись).

Рассмотрим теперь принципы электронного документооборота с использованием асимметричного шифрования. Пусть Алиса и Боб хотят наладить безопасную переписку, которой не были бы страшны угрозы злоумышленника (Евы). У каждого из пользователей — по два ключа: *открытый* (общедоступный; его можно обнародовать для всех, кто хотел бы направлять вам корреспонденцию) и *закрытый* (хранится в строгой тайне).

• Алиса пишет письмо Бобу и подписывает его своей электронной цифровой подписью, которую создает с помощью своего закрытого ключа k_D^A.

• Алиса шифрует письмо для Боба, используя его, Боба, открытый ключ k_E^B. Зашифрованное письмо Алиса посылает Бобу.

• Получив письмо от Алисы, Боб расшифровывает его своим закрытым ключом k_D^B.

• Боб также проверяет подлинность ЭЦП Алисы, используя ее открытый ключ k_E^A.

Каковы преимущества от наличия двух ключей, открытого и закрытого?

Отпадает необходимость делиться с кем-либо своим закрытым ключом, исчезают и опасения, связанные с ненадлежащим хранением ключа на стороне партнера. Таким образом, в значительной степени[1] исчезает проблема доверия между пользователями.

Проблемы распределения ключей уже нет!

Полное количество ключей для переписки каждого с каждым в сообществе из n пользователей составляет теперь $2n$, а не $\frac{n(n-1)}{2}$, как было при симметричном шифровании, т. е. это линейная, а не квадратичная функция n.

Если Ева перехватит письмо от Алисы, то узнать его содержание она не сможет. Для расшифрования нужен закрытый ключ Боба, которым Ева не располагает. Взлом же, скорее всего, окончится неудачей, поскольку асимметричное шифрование — высокосекретное.

Если Ева, не в силах добраться до содержания письма, попытается его фальсифицировать, то Боб узнает это, поскольку ЭЦП Алисы окажется недействительной. Дело в том, что ЭЦП привязана к исходному содержанию письма, и при изменении в нем хотя бы 1 бита привязка, скорее всего, нарушится.

Правда, возможность поддержания секретной переписки с партнером без необходимости предварительного контакта с ним таит в себе следующую опасность. Когда Алиса думает, что переписывается с Бобом, может ли она быть уверенной в том, что ее корреспондент — действительно Боб, а не Ева, выдающая себя за другое лицо (*маскарад*)? При этом ключи и подпись будут в полном порядке, но их владельцем будет самозванец. Чтобы избежать такого варианта мошенничества, вводится процедура *сертификации ключей*. Если вы доверяете сертифицирующему центру, то доверяете и ключам, на которые он выдал сертификат подлинности.

Резюмируем сравнительные характеристики симметричных и асимметричных шифров.

---

[1] Частично она остается — см. ниже.

Симметричные шифры	Асимметричные шифры
Надежность шифрования	
Современные комбинированные шифры вполне надежны	Алгоритмы асимметричного шифрования считаются надежными, пока и поскольку не обнаружены эффективные способы работы с однонаправленными функциями, лежащими в основе этих алгоритмов
Длина ключа	
Сравнительно невелика: в современных стандартах — как правило, не более 256 бит	Сравнительно велика — как минимум 2 Кбит
Скорость зашифрования/расшифрования (при прочих равных условиях)	
Сравнительно велика	Сравнительно невелика
Проблемы	
Принципиальные проблемы, связанные с распределением ключей и доверием между пользователями	Названные проблемы либо отсутствуют, либо достаточно успешно решаются

Вопросы для самопроверки

1. Криптография, криптоанализ и криптология — каково соотношение между этими науками?
2. Каково соотношение между шифрованием и кодированием?
3. Каково соотношение между стеганографией и криптографией?
4. Что такое ключ шифрования?
5. В чем принципиальное различие между симметричными и асимметричными шифрами?
6. Почему шифр Цезаря очень неустойчив к взлому?
7. На чем основан взлом шифра Виженера по Казискому?
8. В чем состоит различие между принципом устройства шифров подстановок и шифров перестановок?
9. В чем заключаются преимущества и недостатки гаммирования по сравнению с другими симметричными шифрами?
10. В чем состоит различие между блочными и потоковыми шифрами?
11. В чем состоит принцип Керкхоффса?
12. В чем заключаются принципы рассеивания и перемешивания? В чем их целесообразность?

13. Почему алгоритм DES не удовлетворяет современным требованиям к секретности?

14. В чем заключается атака методом грубой силы?

15. Что такое «проблема распределения ключей» в криптографии с закрытым ключом?

16. В чем состоит проблема доверия между пользователями в криптографии с закрытым ключом?

17. Что такое однонаправленная функция?

18. Какая однонаправленная функция лежит в основе алгоритма RSA асимметричного шифрования?

19. Для каких действий используется открытый ключ в асимметричной криптографии?

20. Для каких действий используется закрытый ключ в асимметричной криптографии?

Упражнения

1. Зашифруйте слово КРИПТОГРАФИЯ шифром Тритемиуса с ключом СКИТАЛА.

2. Зашифруйте слово КРИПТОАНАЛИЗ шифром Виженера с ключом ЦЕЗАРЬ.

3. Зашифруйте слово КРИПТОЛОГИЯ шифром гаммирования с гаммой, равной числу e.

4. Зашифруйте слово ПОДСТАНОВКА шифром гаммирования с гаммой, равной числу π.

5. Зашифруйте слово ПЕРЕСТАНОВКА шифром гаммирования с гаммой, равной числу e.

6. Зашифруйте фразу «Шифр Цезаря относится к детским шифрам» шифром перестановок с перестановочной таблицей размером 6×6 и ключевым словом ЦЕЗАРЬ.

7. Зашифруйте фразу «Скитала является механическим шифровальным устройством» шифром перестановок с перестановочной таблицей размером 8×7 и ключевым словом ВИЖЕНЕР.

8. Зашифруйте слово КРИПТОГРАФИЯ шифром Тритемиуса с ключом ПОЛИБИЙ.

9. Зашифруйте слово КРИПТОАНАЛИЗ шифром Виженера с ключом ШЕННОН.

10. Зашифруйте слово КАЗИСКИЙ шифром гаммирования с гаммой, равной числу e.

11. Зашифруйте слово КОДИРОВАНИЕ шифром гаммирования с гаммой, равной числу π.

12. Зашифруйте слово ШИФРОБЛОКНОТ шифром гаммирования с гаммой, равной числу e.

13. Зашифруйте фразу «Шифр Цезаря относится к шифрам замены» шифром перестановок с перестановочной таблицей размером 6×6 и ключевым словом ПАРОЛЬ.

14. Зашифруйте фразу «Кодирование является частью криптографии» шифром перестановок с перестановочной таблицей размером 6×7 и ключевым словом ВИЖЕНЕР.

15. Зашифруйте фразу «Стеганография не является частью криптографии» шифром перестановок с перестановочной таблицей размером 8×6 и ключевым словом ВЕРНАМ.

16. Зашифруйте слово КРИПТОСТОЙКОСТЬ шифром Полибия.

Тема 4
МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ: ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

1. Каноническое разложение. Это разложение *составного* целого числа z на простые множители p_i (p — первая буква англ. *prime* — «простой»):

$$z = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

с натуральными показателями степеней α_i. Это вычислительно *сложная* операция.

Пример 1.

$$2346 = 2 \cdot 1173 = 2 \cdot 3 \cdot 391 = 2 \cdot 3 \cdot 17 \cdot 23;$$

$$646 = 2 \cdot 323 = 2 \cdot 17 \cdot 19.$$

2. Наибольший общий делитель и наименьшее общее кратное. Будем обозначать *парный наибольший общий делитель* (НОД) двух чисел a и b как (a, b), а наименьшее общее кратное (НОК) — как $[a, b]$.

Некоторые их *свойства*:

1) $(a_1, a_2, \dots, a_{n-1}, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n)$

и аналогично для НОК:

$$[a_1, a_2, \dots, a_{n-1}, a_n] = [[a_1, a_2, \dots, a_{n-1}], a_n].$$

Смысл этих рекуррентных формул – в том, что они позволяют заменить вычисление НОД, НОК большого количества чисел вычислением *парных* НОД, НОК;

2) если имеются только два числа, то $(a, b)[a, b] = ab$. С помощью этой формулы можно выразить НОК через НОД (см. ниже).

Заметим, что два числа называются *взаимно простыми*, если их НОД равен единице.

Пример 2.

$$(161, 3) = 1;\ (33, 13) = 1.$$

Это показано в примерах 6 и 7.

Вычисление НОД.

А. «*Школьный*» *способ*: для вычисления (a, b) нужно составить каноническое разложение каждого из чисел, а затем из обоих разложений взять *общие* простые множители в *наименьших* степенях.

Пример 3.

На основании примера 1

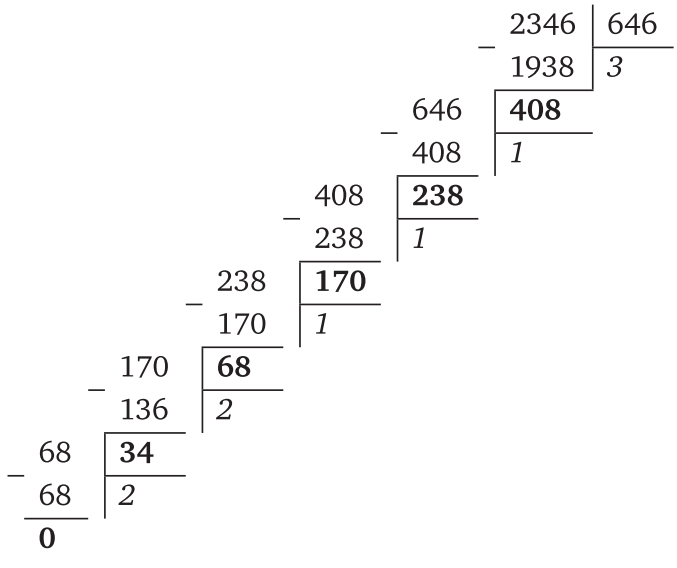
$$(2346, 646) = 2 \cdot 17 = 34.$$

Недостаток этого способа состоит в необходимости предварительного (трудоемкого!) канонического разложения.

Б. Вычисление НОД *по алгоритму Евклида*. Последний ненулевой остаток даст НОД.

Пример 4.

Вычислить НОД для тех же чисел, что и в примере 3.



Делители всякий раз становятся делимыми, а остатки — делителями. Доказывается, что алгоритм Евклида всегда конечен.

Остатки выделены **жирным** шрифтом. Последний ненулевой остаток равен 34; это и есть НОД (2346, 646) (сравните с примером 3).

Смысл выделения частных *курсивом* выяснится ниже, при рассмотрении цепных дробей.

Вычисление НОК

А. «*Школьный*» *способ*: для вычисления $[a, b]$ составить каноническое разложение каждого из чисел, а затем из обоих разложений взять простые множители, присутствующие хотя бы в одном разложении — в *наибольших* степенях.

Пример 5.

На основании примера 1

$$[2346, 646] = 2 \cdot 3 \cdot 17 \cdot 19 \cdot 23 = 44\,574.$$

Можно сделать проверку на основании 2-го свойства НОД и НОК:

$$(a, b)[a, b] = ab,\ 34 \cdot 44\,574 = 2346 \cdot 646.$$

Б. Вычисление НОК через посредство НОД с помощью алгоритма Евклида (к сожалению, непосредственно для НОК нет алгоритма вычисления, сопоставимого с алгоритмом Евклида):

$$[a, b] = \frac{ab}{(a, b)}.$$

Дополнительные примеры

Пример 6.

$(161, 3) = 1$, так что эти числа являются взаимно простыми:

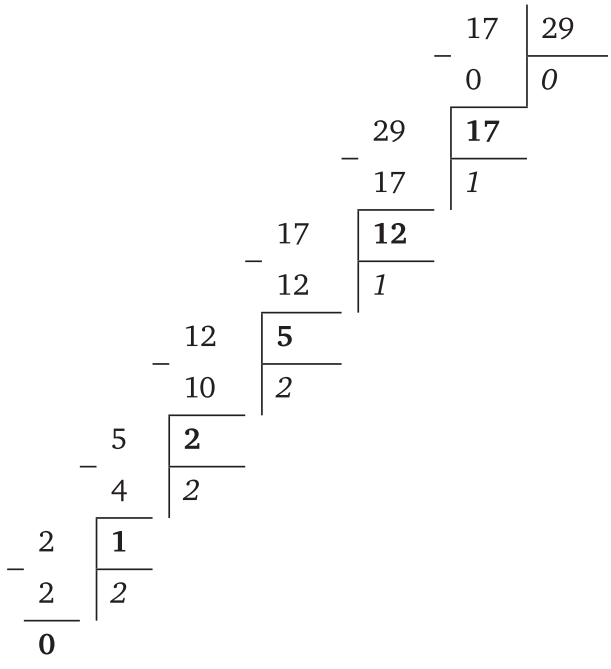
	161	3	
−	159	*53*	
	3	**2**	
−	2	*1*	
	2	**1**	
	2	*2*	
	0		

Пример 7.

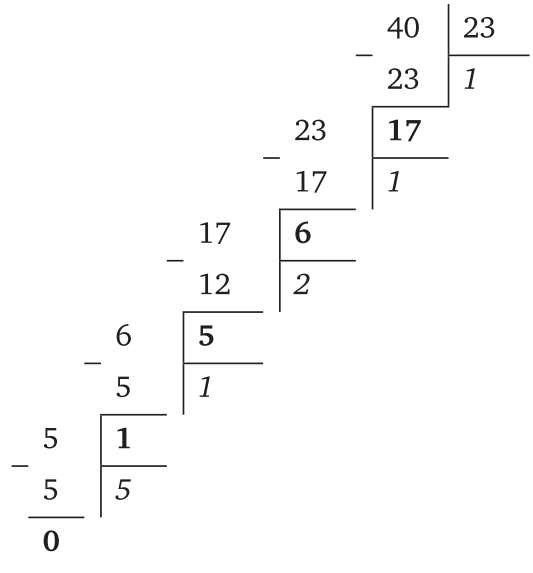
$(33, 13) = 1$ (взаимно простые числа):

	33	13	
−	26	*2*	
	13	**7**	
−	7	*1*	
	7	**6**	
−	6	*1*	
	6	**1**	
−	6	*6*	
	0		

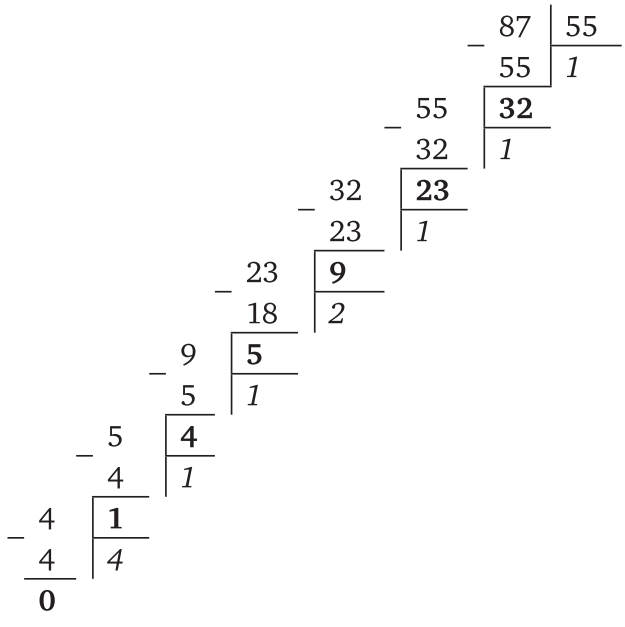
Пример 8.
$(17, 29) = 1$ (взаимно простые числа):



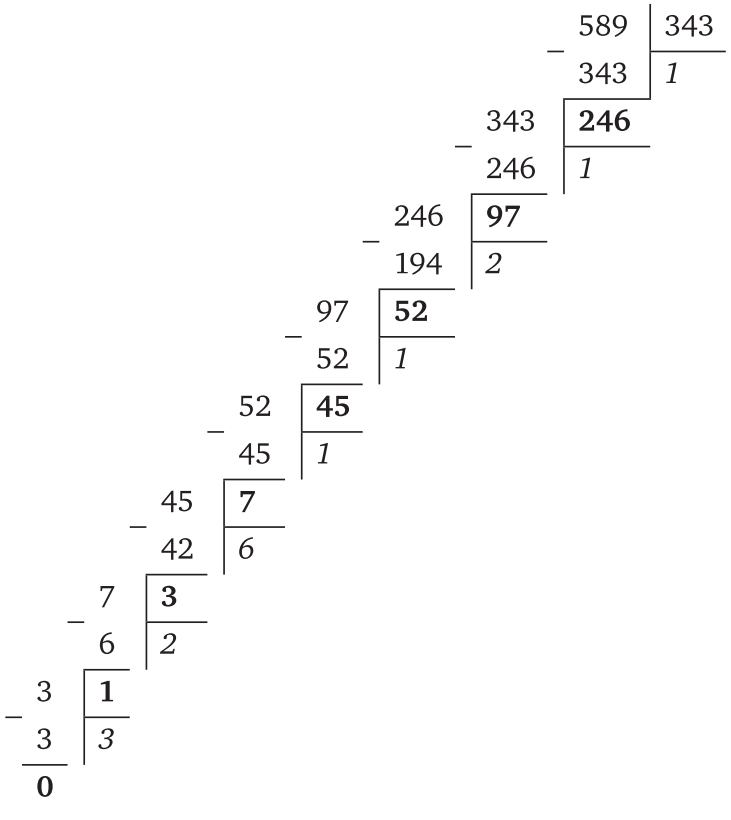
Пример 9.
$(40, 23) = 1$ (взаимно простые числа):



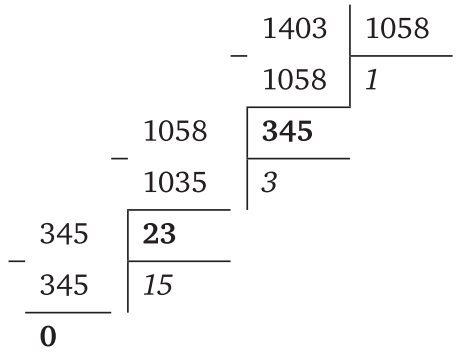
Пример 10.
$(87, 55) = 1$ (взаимно простые числа):



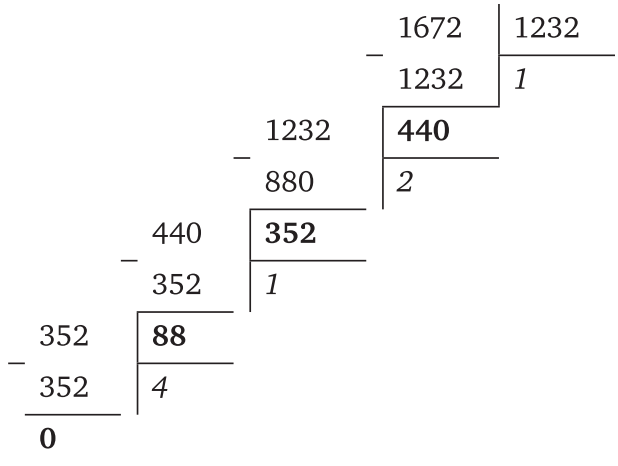
Пример 11.
$(589, 343) = 1$ (взаимно простые числа):



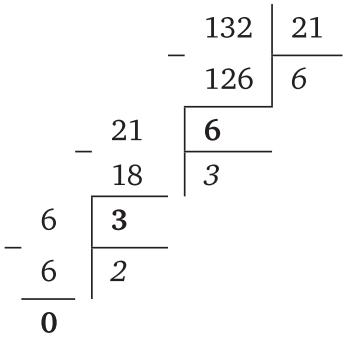
Пример 12.
$(1403, 1058) = 23$:



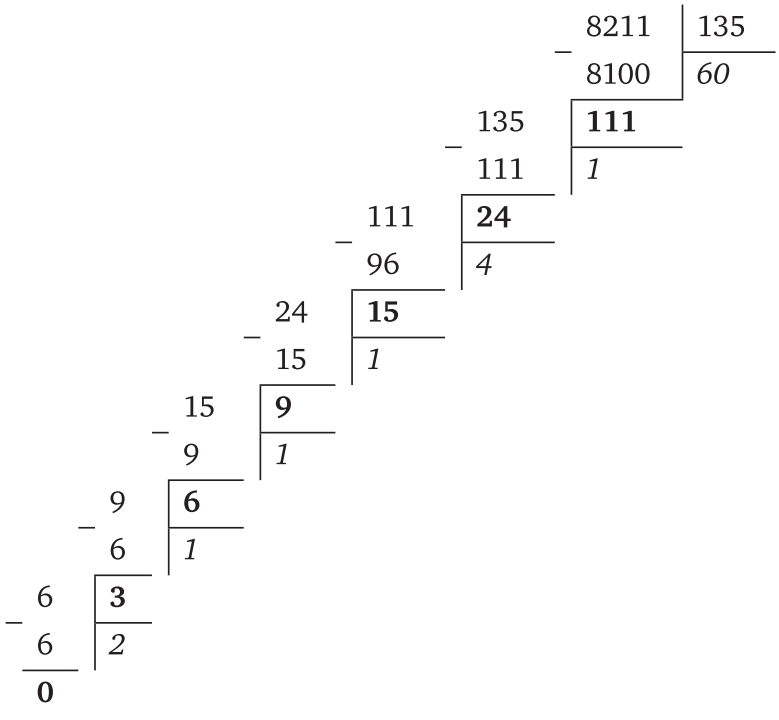
Пример 13.
$(1672, 1232) = 88$:



Пример 14.
$(132, 21) = 3$:



Пример 15.
$(8211,135)=3$:



3. Сравнения по модулю. Высказывание «a сравнимо с b по модулю m»:

$$a \equiv b (\mathrm{mod}\, m)$$

означает, что разность $(a - b)$ делится без остатка на m:

$$(a-b) \vdots m.$$

Тогда $\dfrac{a-b}{m} = k \in \mathbb{Z}$, $a = b + mk$.

Свойства сравнений:

а) $a \equiv b (\mathrm{mod}\, m) \equiv (a+mk) (\mathrm{mod}\, m) \equiv (b+mk) (\mathrm{mod}\, m)$, $k \in \mathbb{Z}$.
Итак, к любой части сравнения можно целое число раз прибавить модуль сравнения;

б) если $a \equiv b (\mathrm{mod}\, m)$ и $c \equiv d (\mathrm{mod}\, m)$, то

$$a \cdot c \equiv b \cdot d (\mathrm{mod}\, m),$$

т. е. сравнения по *одному* модулю можно перемножать. Следствие отсюда:

в) если $a \equiv b (\mathrm{mod}\, m)$, то $a^n \equiv b^n (\mathrm{mod}\, m)$, $n \in \mathbb{N}$.

Пример 16.

$21 \equiv 7 (\mathrm{mod}\, 2)$, так как разность $21 - 7 = 14 \vdots 2$.

4. Цепные (непрерывные) дроби. Начнем с примера преобразования простой дроби.

Пример 17.

$$\frac{25}{7} = 3 + \frac{4}{7} = 3 + \frac{1}{\frac{7}{4}} = 3 + \frac{1}{1 + \frac{3}{4}} = 3 + \frac{1}{1 + \frac{1}{\frac{4}{3}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}} = [3;\ 1, 1, 3].$$

Получена цепная дробь, записанная сначала в развернутом, а затем — в сокращенном виде. Этот пример иллюстрирует теорему о существовании единственной *конечной* цепной дроби, в которую раскладывается любое *рациональное* число.

Пример 18.

Разложим *иррациональное* число $\sqrt{2}$ в цепную дробь. Начнем с легко проверяемого тождества

$$\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}.$$

Подставляя в знаменателе вместо $\sqrt{2}$ его выражение из тождества, получим:

$$\sqrt{2} = 1 + \frac{1}{1 + \left(1 + \frac{1}{1 + \sqrt{2}}\right)} = 1 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}} =$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \left(1 + \frac{1}{1 + \sqrt{2}}\right)}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}} = \ldots,$$

итого, $\sqrt{2} = [1;\ 2, 2, 2, \ldots] = [1;\ \overline{2}]$.

Этот пример иллюстрирует теорему о существовании единственной *бесконечной периодической* цепной дроби, в которую раскладывается любая *квадратичная иррациональность* (типа $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$).

Пример 19.

Известные математические константы — числа e и π — раскладываются в следующие *бесконечные непериодические* цепные дроби:

$$e = [2;\ \overline{1, 2n, 1}]_{n=1}^{\infty} = [2;\ 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots];$$

$$\pi = [3;\ 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, \ldots].$$

Для основания натуральных логарифмов цепная дробь, будучи непериодической, имеет прозрачное строение, тогда как для числа π никакая закономерность следования чисел не известна.

Обрывая цепную дробь на некотором звене, получим *подходящую* дробь — простую дробь, являющуюся наилучшим рациональным приближением исходной цепной дроби.

Пример 20.

Получим первые подходящие дроби для числа π.

Нулевая подходящая дробь — целая часть числа:

$$\frac{P_0}{Q_0} = 3 = \frac{3}{1};$$

первая подходящая дробь получается при учете одного дробного звена:

$$\frac{P_1}{Q_1} = 3 + \frac{1}{7} = \frac{22}{7} \approx 3{,}143 \text{ (\textit{архимедово число})};$$

вторая подходящая дробь:

$$\frac{P_2}{Q_2} = 3 + \frac{1}{7 + \dfrac{1}{15}} = \frac{333}{106} \approx 3{,}14151;$$

третья подходящая дробь:

$$\frac{P_3}{Q_3} = 3 + \frac{1}{7 + \dfrac{1}{15 + \dfrac{1}{1}}} = \frac{355}{113} \approx 3{,}1415929;$$

четвертая подходящая дробь:

$$\frac{P_4}{Q_4} = 3 + \frac{1}{7 + \dfrac{1}{15 + \dfrac{1}{1 + \dfrac{1}{292}}}} = \frac{103993}{33102} \approx 3{,}1415926530$$

и т. д.

Для сравнения приведем десятичное представление числа π:

$$\pi = 3{,}14159265359\ldots$$

При учете каждого добавочного звена цепной дроби количество верных десятичных знаков прирастает в среднем на два.

Поскольку каждая последующая подходящая дробь вычисляется все более трудоемко, прямое вычисление подходящих дробей неудобно; обычно пользуются следующим правилом: *первые две* подходящих дроби для цепной дроби

$$[q_0;\ q_1, q_2, q_3, \ldots]$$

вычисляют непосредственно:

$$\frac{P_0}{Q_0} = q_0 = \frac{q_0}{1};$$

$$\frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1},$$

а для нахождения последующих подходящих дробей применяют *рекуррентную* формулу

$$\frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}},\ k = 2, 3, \ldots$$

Здесь q_k — частные, которые возникают при реализации алгоритма Евклида (они помечены курсивом в приведенных выше примерах). Таким образом, алгоритм Евклида применяется не только для вычисления НОД, но и для разложения простой дроби в цепную.

Пример 21.

Разложить простую дробь $\frac{40}{23}$ в цепную и найдите для нее все подходящие дроби.

В примере 9 было выполнено деление 40 на 23 по алгоритму Евклида:

$$\begin{array}{rr|l}
 & 40 & 23 \\
- & 23 & \hline
 & 17 & 1 \\
- & 17 & \hline
 & 6 & 1 \\
- & 5 & \hline
 & 1 & 5 \\
- & 5 & \hline
 & 0 &
\end{array}$$

$$\begin{array}{rr|l}
 & 23 & 17 \\
- & 17 & \hline
 & 6 & 2 \\
- & 12 & \hline
 & 5 & 1 \\
- & 5 & \hline
 & 1 & 5 \\
- & 5 & \hline
 & 0 &
\end{array}$$

Разложение в цепную дробь имеет вид:

$$\frac{40}{23}=[q_0;\ q_1,q_2,q_3,q_4]=[1;\ 1,2,1,5]=1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{5}}}}.$$

Подходящие дроби:

- нулевая

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{1}{1};$$

- первая

$$\frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=1+\frac{1}{1}=\frac{2}{1};$$

далее — по рекуррентной формуле:

- вторая

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{2\cdot 2+1}{2\cdot 1+1}=\frac{5}{3};$$

- третья

$$\frac{P_3}{Q_3}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{1\cdot 5+2}{1\cdot 3+1}=\frac{7}{4};$$

- четвертая

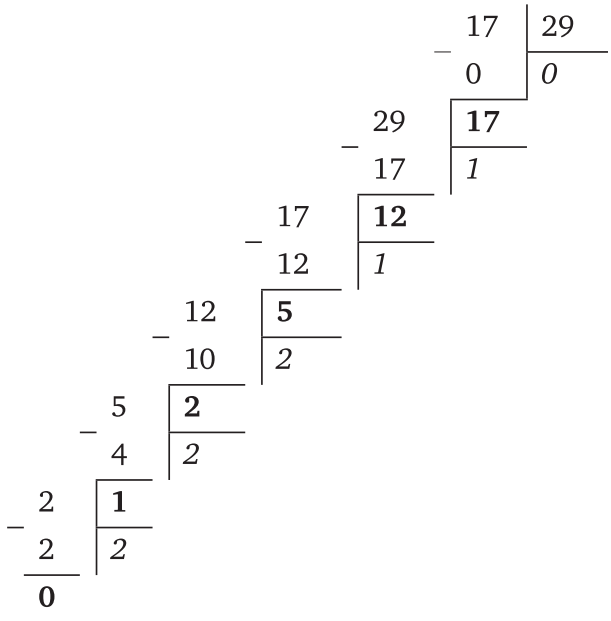
$$\frac{P_4}{Q_4}=\frac{q_4P_3+P_2}{q_4Q_3+Q_2}=\frac{5\cdot 7+5}{5\cdot 4+3}=\frac{40}{23}.$$

Получена исходная дробь.

Пример 22.

Разложить простую дробь $\frac{17}{29}$ в цепную и найти для нее все подходящие дроби.

В примере 8 было выполнено деление 17 на 29 по алгоритму Евклида:



Разложение в цепную дробь имеет вид

$$\frac{17}{29}=[q_0;\ q_1,q_2,q_3,q_4,q_5]=[0;\ 1,1,2,2,2]=0+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}}.$$

Подходящие дроби:

- нулевая

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{0}{1};$$

- первая

$$\frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=0+\frac{1}{1}=\frac{1}{1};$$

- вторая

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{1\cdot1+0}{1\cdot1+1}=\frac{1}{2};$$

- третья

$$\frac{P_3}{Q_3}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{2\cdot1+1}{2\cdot2+1}=\frac{3}{5};$$

• четвертая

$$\frac{P_4}{Q_4}=\frac{q_4P_3+P_2}{q_4Q_3+Q_2}=\frac{2\cdot3+1}{2\cdot5+2}=\frac{7}{12};$$

• пятая

$$\frac{P_5}{Q_5}=\frac{q_5P_4+P_3}{q_5Q_4+Q_3}=\frac{2\cdot7+3}{2\cdot12+5}=\frac{17}{29}.$$

Получена исходная дробь.

Дополнительные примеры

Пример 23.

Разложить простую дробь $\frac{87}{55}$ в цепную и найти для нее подходящие дроби.

На основании примера 10

$$\frac{87}{55}=[q_0;\ q_1,q_2,q_3,q_4,q_5,q_6]=$$

$$=[1;\ 1,1,2,1,1,4]=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4}}}}}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{1}{1},\ \frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=1+\frac{1}{1}=\frac{2}{1};$$

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{3}{2},\ \frac{P_3}{Q_3}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{8}{5};$$

$$\frac{P_4}{Q_4}=\frac{q_4P_3+P_2}{q_4Q_3+Q_2}=\frac{11}{7},\ \frac{P_5}{Q_5}=\frac{q_5P_4+P_3}{q_5Q_4+Q_3}=\frac{19}{12},\ \frac{P_6}{Q_6}=\frac{q_6P_5+P_4}{q_6Q_5+Q_4}=\frac{87}{55}.$$

Получена исходная дробь.

Пример 24.

Разложить простую дробь $\frac{589}{343}$ в цепную и найти для нее подходящие дроби.

На основании примера 11

$$\frac{589}{343}=[q_0;\ q_1,q_2,q_3,q_4,q_5,q_6,q_7]=$$

$$=[1;\ 1,2,1,1,6,2,3]=1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{2+\cfrac{1}{3}}}}}}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{1}{1},\ \frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=1+\frac{1}{1}=\frac{2}{1};$$

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{5}{3},\ \frac{P_3}{Q_3}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{7}{4};$$

$$\frac{P_4}{Q_4}=\frac{q_4P_3+P_2}{q_4Q_3+Q_2}=\frac{12}{7},\ \frac{P_5}{Q_5}=\frac{q_5P_4+P_3}{q_5Q_4+Q_3}=\frac{79}{46},\ \frac{P_6}{Q_6}=\frac{q_6P_5+P_4}{q_6Q_5+Q_4}=\frac{170}{99};$$

$$\frac{P_7}{Q_7}=\frac{q_7P_6+P_5}{q_7Q_6+Q_5}=\frac{589}{343}.$$

Получена исходная дробь.

5. Сравнения первой степени. Это *линейные* уравнения вида

$$ax\equiv b(\mathrm{mod}\,m),$$

сформулированные в терминах сравнений. Здесь a, x, b, m — целые числа. Искомым является x, а остальные числа известны.

Если $(a, m) = 1$, т. е. числа взаимно простые, то существует единственное решение сравнения, которое можно найти, например, по формуле

$$x\equiv(-1)^s bP_{s-1}(\mathrm{mod}\,m),$$

где P_{s-1} — числитель предпоследней подходящей дроби при разложении $\frac{m}{a}$ в цепную дробь.

Если

$$a \cdot c \equiv 1 (\mathrm{mod}\, m),$$

то числа a и c называются *мультипликативно обратными* по модулю m. Понятие мультипликативной обратности можно считать обобщением понятия взаимно обратных чисел:

$$3 \cdot \frac{1}{3} = 1, \;\; 5 \cdot \frac{1}{5} = 1$$

с тем отличием, что *равенство* единице заменяется *сравнимостью* с единицей по данному модулю сравнения.

Пример 25.

Решить сравнение

$$3x \equiv 20 (\mathrm{mod} 161).$$

Во-первых, нужно разложить простую дробь $\frac{161}{3}$ в цепную. На основании примера 6

$$\frac{161}{3} = [53;\ 1, 2] = 53 + \frac{1}{1 + \frac{1}{2}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0} = \frac{q_0}{1} = \frac{53}{1}, \; \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = 53 + \frac{1}{1} = \frac{\mathbf{54}}{1},$$

$$\frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{161}{3}.$$

Предпоследняя подходящая дробь — это $\frac{P_1}{Q_1} = \frac{54}{1}$. Тогда числитель предпоследней подходящей дроби $P_{s-1} = P_1 = 54$, откуда $s = 2$.

Решение сравнения

$$x \equiv (-1)^s b P_{s-1} (\mathrm{mod}\, m) \equiv (-1)^2 \cdot 20 \cdot 54 (\mathrm{mod} 161) = 1080 (\mathrm{mod} 161) \equiv$$
$$\equiv (1080 - 161 \cdot 6) (\mathrm{mod} 161) = 114 (\mathrm{mod} 161).$$

Покажем, как можно сделать проверку этого результата. По определению сравнения по модулю

$$(x - 114) \vdots 161, \text{ откуда } \frac{x - 114}{161} = k \in \mathbb{Z}.$$

Таким образом, найденные значения x принадлежат серии решений

$$x_k = 114 + 161k.$$

Придавая k конкретное целое значение и подставляя соответствующий x в исходное сравнение, можно проверить, удовлетворяется ли сравнение.

Пусть, например, $k = -1$. Тогда $x_{-1} = 114 - 161 = -47$ и имеем

$$3 \cdot (-47) \equiv 20 (\mathrm{mod}\, 161).$$

Это верное сравнение, что и доказывает правильность решения.

Дополнительные примеры

Пример 26.

Решить сравнение

$$55x \equiv 7 (\mathrm{mod}\, 87).$$

Разложим дробь $\frac{87}{55}$ в цепную. На основании примера 10

$$\frac{87}{55} = [q_0;\ q_1, q_2, q_3, q_4, q_5, q_6] =$$

$$= [1;\ 1, 1, 2, 1, 1, 4] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0} = \frac{q_0}{1} = \frac{1}{1},\ \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = 1 + \frac{1}{1} = \frac{2}{1},$$

$$\frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{1 \cdot 2 + 1}{1 \cdot 1 + 1} = \frac{3}{2},\ \frac{P_3}{Q_3} = \frac{8}{5},\ \frac{P_4}{Q_4} = \frac{11}{7},$$

$$\frac{P_5}{Q_5} = \frac{\mathbf{19}}{12},\ \frac{P_6}{Q_6} = \frac{87}{55}.$$

Предпоследняя подходящая дробь — это $\frac{P_5}{Q_5}=\frac{19}{12}$. Числитель предпоследней подходящей дроби $P_{s-1}=P_5=19$, откуда $s=6$.

Решение сравнения:

$$x\equiv(-1)^s bP_{s-1}(\mathrm{mod}\,m)\equiv(-1)^6\cdot 7\cdot 19(\mathrm{mod}\,87)=$$
$$=133(\mathrm{mod}\,87)\equiv(133-87)(\mathrm{mod}\,87)=46(\mathrm{mod}\,87).$$

Проверка:

$$(x-46)\vdots 87,\ \text{откуда}\ \frac{x-46}{87}=k\in\mathbb{Z}.$$

Получаем серию решений

$$x_k=46+87k.$$

Пусть, например, $k=2$. Тогда $x_2=46+87\cdot 2=220$, и имеем

$$55\cdot 220\equiv 7(\mathrm{mod}\,87).$$

Это *верное* сравнение, что и доказывает правильность решения.

Пример 27.

Найти числа, мультипликативно обратные числу 29 по модулю 17.

Требуется решить сравнение

$$29x\equiv 1(\mathrm{mod}\,17).$$

Разложим дробь $\frac{17}{29}$ в цепную. На основании примера 22

$$\frac{17}{29}=[q_0;\ q_1,q_2,q_3,q_4,q_5]=[0;\ 1,1,2,2,2]=0+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{0}{1},\ \frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=0+\frac{1}{1}=\frac{1}{1},$$

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{1\cdot1+0}{1\cdot1+1}=\frac{1}{2},\ \frac{P_3}{Q_3}=\frac{3}{5},\ \frac{P_4}{Q_4}=\frac{7}{12},$$

$$\frac{P_5}{Q_5}=\frac{17}{29}.$$

Предпоследняя подходящая дробь — это $\frac{P_4}{Q_4}=\frac{7}{12}$. Числитель предпоследней подходящей дроби $P_{s-1}=P_4=7$, откуда $s=5$.

Решение сравнения

$$x\equiv(-1)^s bP_{s-1}(\mathrm{mod}\,m)\equiv(-1)^5\cdot1\cdot7(\mathrm{mod}17)=$$
$$=-7(\mathrm{mod}17)\equiv(-7+17)(\mathrm{mod}17)=10(\mathrm{mod}17).$$

Проверка:

$$(x-10)\vdots17,\ \frac{x-10}{17}=k\in\mathbb{Z}.$$

Получаем серию решений

$$x_k=10+17k.$$

Пусть, например, $k=-2$. Тогда $x_{-2}=10-17\cdot2=-24$ и имеем

$$29\cdot(-24)\equiv1(\mathrm{mod}17).$$

Это *верное* сравнение; решение верно.

Пример 28.

Найти числа, мультипликативно обратные числу 23 по модулю 40.

Решим сравнение

$$23x\equiv1(\mathrm{mod}\,40).$$

Разложим дробь $\frac{40}{23}$ в цепную. На основании примеров 9 и 21

$$\frac{40}{23}=[q_0;\ q_1,q_2,q_3,q_4]=[1;\ 1,2,1,5]=1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{5}}}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0}=\frac{q_0}{1}=\frac{1}{1},\ \frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=1+\frac{1}{1}=\frac{2}{1},$$

$$\frac{P_2}{Q_2}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{2\cdot 2+1}{2\cdot 1+1}=\frac{5}{3},\ \frac{P_3}{Q_3}=\frac{7}{4},\ \frac{P_4}{Q_4}=\frac{40}{23}.$$

Предпоследняя подходящая дробь — это $\frac{P_3}{Q_3}=\frac{7}{4}$. Числитель предпоследней подходящей дроби $P_{s-1}=P_3=7$, откуда $s=4$.

Решение сравнения

$$x\equiv(-1)^s bP_{s-1}(\mathrm{mod}\,m)\equiv(-1)^4\cdot 1\cdot 7(\mathrm{mod}\,40)=7(\mathrm{mod}\,40).$$

Проверка:

$$(x-7)\vdots 40,\ \frac{x-7}{40}=k\in\mathbb{Z},$$

$$x_k=7+40k.$$

Пусть $k=-1$. Тогда $x_{-1}=7-40=-33$;

$$23\cdot(-33)\equiv 1(\mathrm{mod}\,40).$$

Есть *верное* сравнение, что доказывает правильность решения.

6. Функция Эйлера $\varphi(z)$. Пусть для составного целого числа z известно его каноническое разложение:

$$z=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}.$$

Тогда значение функции Эйлера вычисляется как

$$\varphi(z)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1).$$

Частные случаи:

а) $\varphi(p)=p-1$ если p — простое число;

б) $\varphi(p\cdot q)=(p-1)(q-1)$, если p, q — простые числа.

Примеры вычисления:

1) $\varphi(2)=1$;

2) $\varphi(12)=\varphi(2^2\cdot 3^1)=2^{2-1}(2-1)\cdot 3^{1-1}(3-1)=4$;

3) $\varphi(1000)=\varphi(2^3\cdot 5^3)=2^{3-1}(2-1)\cdot 5^{3-1}(5-1)=400$.

Смысл функции Эйлера: $\varphi(z)$ — это количество натуральных чисел, меньших, чем z и взаимно простых с ним.

Пример 29.

Только что было вычислено значение $\varphi(12)=4$. Покажем это, исходя из смысла функции.

Выпишем натуральные числа, меньшие 12, и вычеркнем из них те, которые имеют с 12 иные общие делители, кроме единицы (т. е. не взаимно простые с 12):

$$\mathbf{1}, \cancel{2}, \cancel{3}, \cancel{4}, \mathbf{5}, \cancel{6}, \mathbf{7}, \cancel{8}, \cancel{9}, \cancel{10}, \mathbf{11}.$$

Итак, взаимно простые с двенадцатью — *четыре* числа

$$\mathbf{1}, \mathbf{5}, \mathbf{7}, \mathbf{11}.$$

7. Малая теорема Ферма. Для любого *простого* p и любого целого $a \geq 1$, не делящегося на p, выполняется:

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Это условие простоты числа p является необходимым, но, к сожалению, не является достаточным: если сравнение верно, отсюда еще не следует, что p — простое число.

Заметим, что, беря $a < p$, мы автоматически удовлетворяем требованию, чтобы a не делилось на p.

Пример 30.

Проиллюстрируем малую теорему Ферма на примере простого $p = 13$ и не делящегося на него целого $a = 27$: верно ли сравнение

$$27^{13-1} \equiv 1 (\mathrm{mod} 13)?$$

Иными словами, будет ли разность

$$27^{12} - 1 = (3^3)^{12} - 1 = 3^{36} - 19$$

делиться без остатка на 13?

$$\frac{3^{36}-1}{13} = \frac{(3^{18}+1)(3^{18}-1)}{13} = \frac{(3^{18}+1)(3^9+1)(3^9-1)}{13} =$$
$$= \frac{(3^{18}+1)(3^9+1)(3^3-1)(3^6+3^3+1)}{13}.$$

Поскольку

$$\frac{3^3-1}{13} = \frac{27-1}{13} = 2,$$

первоначальная дробь также имеет целое значение, что и требовалось показать.

8. Теорема Эйлера. Для любого *натурального* m и любого целого $a \geq 1$, взаимно простого с m, выполняется:

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Теорема Эйлера является обобщением малой теоремы Ферма, поскольку условие простоты p в последней заменяется более мягким требованием целости m. Но если $m = p$ (т. е. является *простым*), то, по свойству функции Эйлера, $\varphi(m) = \varphi(p) = p - 1$.

Пример 31.

Проиллюстрируем теорему Эйлера на примере натурального $m = 11$ и взаимно простого с ним $a = 7$: верно ли сравнение

$$7^{\varphi(11)} \equiv 1 (\mathrm{mod}\, 11)?$$

Иными словами, будет ли разность

$$7^{\varphi(11)} - 1 = 7^{10} - 1$$

делиться без остатка на 11?

$$\frac{7^{10} - 1}{11} = \frac{(7^5 - 1)(7^5 + 1)}{11} = \frac{(16\,807 - 1)(16\,807 + 1)}{11} =$$

$$= \frac{16\,806 \cdot 16\,808}{11} = 16\,806 \cdot 1528.$$

Получилось деление нацело, что и требовалось показать.

Представленных сведений из теории чисел достаточно, чтобы подробно рассмотреть алгоритм RSA асимметричного шифрования.

Алгоритм RSA

Боб желает получать секретные сообщения от Алисы с использованием алгоритма RSA асимметричного шифрования. Перечислим их действия:

1. ***Шаг Боба.*** Он берет два больших простых числа p и q и вычисляет их произведение

$$n = p \cdot q.$$

Множители p и q должны храниться Бобом *в строгой тайне*, а их произведение n тайной *не является*.

При современном быстродействии ЭВМ для устойчивости шифра к взлому требуется, чтобы p и q были числами порядка не менее 10^{100} в десятичной системе счисления или занимали не менее 1024 разрядов при записи в двоичной системе, т. е. p и q – порядка 1024 бит или 1 кбит.

Возникает вопрос, как для астрономически огромных чисел проверить, что они являются простыми. Ответим на этот вопрос позже.

2. ***Шаг Боба.*** Он выбирает число e (первая буква англ. слова *Encryption* — зашифрование; это не основание натуральных логарифмов!); оно должно быть *взаимно простым* с

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

— значением функции Эйлера, т. е. их НОД должен быть равен единице:

$$(e,\varphi(n))=1.$$

Разумеется, выбор e неоднозначен.

Совокупность чисел n и e составляет *открытый* ключ Боба или его ключ для *зашифрования*:

$$\{n;e\}=k_E^B.$$

Этот ключ Боб может сообщить всем, с кем ведет переписку.

3. ***Шаг Алисы.*** Перед шифрованием сообщения для Боба Алиса заменяет буквы письма числами (это можно сделать разными способами — подставить вместо букв их порядковые номера в алфавите, их ASCII-коды и т. п.) и удаляет все пробелы. Таким образом, исходное сообщение Алисы превращается в длинное число X. Оно должно удовлетворять ограничению

$$X\le n-1,$$

где $n\sim 10^{200}$ — число, полученное Бобом на первом шаге. Если сообщение достаточно длинно, то для выполнения ограничения Алиса его разбивает на блоки $X_1, X_2, \ldots$, для каждого из которых ограничение соблюдается.

После всех этих предварительных манипуляций Алиса шифрует сообщение (целиком или по блокам), используя функцию $E(X)$ зашифрования в алгоритме RSA:

$$Y = E(X) \equiv X^e (\mathrm{mod}\, n),$$

где Y — шифрованное сообщение (или один из его блоков).

Алиса посылает шифрованное сообщение Бобу по открытому (незащищенному) каналу связи — шифрование очень надежное; опасаться взлома (при перехвате шифровки) не приходится.

4. ***Шаг Боба.*** Для расшифрования полученного от Алисы сообщения Бобу потребуется число d (первая буква англ. слова *Decryption* — расшифрование), которое он вычисляет как мультипликативно обратное числу e по модулю $\varphi(n)$:

$$e \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n)).$$

Это сравнение первой степени разрешимо единственным образом, так как по построению $(e, \varphi(n)) = 1$. Из полученной серии решений d можно взять любое, удовлетворяющее ограничению

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

Совокупность чисел n и d составляет *закрытый* ключ Боба или его ключ для *расшифрования*:

$$\{n; d\} = k_D^B.$$

Этот ключ Боб должен хранить *в строгой тайне*.

Заметим, что в случае перехвата шифровки злоумышленницей (Евой) вычислить d она не сможет, поскольку не знает, на какие простые множители раскладывается число n, а эта информация требуется для вычисления $\varphi(n)$. Законный пользователь (Боб) легко вычисляет значение функции Эйлера $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.

5. ***Шаг Боба.*** Вычислив d, Боб применяет функцию $D(Y)$ расшифрования в алгоритме RSA:

$$X = D(Y) \equiv Y^d (\mathrm{mod}\, n),$$

где Y — шифрованное сообщение (или один из его блоков), и получает *исходное* сообщение Алисы.

Покажем, что при расшифровании получится исходное сообщение, которое написала Алиса. Действительно,

$$Y^d (\mathrm{mod}\, n) = (X^e)^d (\mathrm{mod}\, n) = X^{e \cdot d} (\mathrm{mod}\, n).$$

Но $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$, т. е. $ed = 1 + \varphi(n) \cdot k,\ k \in \mathbb{Z}$. Тогда

$$X^{e \cdot d} (\mathrm{mod}\, n) = X^{1 + \varphi(n) \cdot k} (\mathrm{mod}\, n) = X^1 \cdot (X^{\varphi(n)})^k (\mathrm{mod}\, n).$$

Поскольку по теореме Эйлера $X^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$,

$$(X^{\varphi(n)})^k (\mathrm{mod}\, n) \equiv (1)^k (\mathrm{mod}\, n) = 1 (\mathrm{mod}\, n).$$

В итоге $Y^d (\mathrm{mod}\, n) \equiv X^1 (\mathrm{mod}\, n) = X (\mathrm{mod}\, n)$, т. е. расшифрование оказывается *успешным*.

Замечания к алгоритму RSA:

1) не зная, на какие простые множители p и q раскладывается составное n, Ева может попытаться их найти (факторизовать n). Но эта задача — *трудно решаемая*, в том смысле, что время ее решения зависит от объема входных данных по *экспоненциальному* закону и не сводится к *полиномиальному* (не столь катастрофически возрастающему с ростом объема входных данных). Для разложения 200-значного составного числа на простые множители лучшим современным компьютерам по лучшим современным алгоритмам могут потребоваться сотни лет, что фактически делает задачу факторизации неразрешимой;

2) ответим на вопрос, как для большого числа проверить, является ли оно простым. Если бы эта задача была сродни трудно решаемой задаче факторизации, применение алгоритма RSA было бы бессмысленным.

К счастью, есть методы проверки простоты числа, не прибегающие к факторизации. Эти методы делятся на детерминированные и вероятностные.

Детерминированные методы (например, применявшийся для генерации ЭЦП в ныне недействующем ГОСТ Р 34.10—94), исходя из числа q, о котором доподлинно известно, что оно простое, позволяют построить новое число p, которое тоже *заведомо будет простым*.

Вероятностные методы со 100 %-й гарантией позволяют определить, что тестируемое число является составным, и лишь с вероятностью, сколь угодно близкой к единице (но не равной единице), определить, что число простое.

Общая схема большинства вероятностных методов такова:

а) выбирается большое нечетное число;

б) это число тестируется на простоту. Если число оказалось простым, то алгоритм заканчивает работу. В противном случае нужно перейти к этапу а).

В основе большинства вероятностных тестов простоты *лежит малая теорема Ферма*.

Пусть требуется протестировать нечетное число p_1 на простоту. Выберем целое $a_1 \geq 1$, не делящееся на p_1 (можно взять для этого $a_1 < p_1$), и проверим, выполняется ли условие:

$$a_1^{p_1-1} \equiv 1 (\mathrm{mod}\, p_1).$$

Если условие не выполнено, то кандидат в простое число p_1 не выдержал проверку: число p_1 — составное (в самом деле, если бы оно было простым, то малая теорема Ферма выполнялась бы). Нужно выбрать для тестирования другого кандидата p_2.

Если же условие $a_1^{p_1-1} \equiv 1 (\mathrm{mod}\, p_1)$ выполнилось, неверно было бы сразу утверждать, что число p_1 простое, поскольку малая теорема Ферма дает лишь необходимое, но не достаточное условие простоты. Возможно лишь осторожное утверждение, что простота числа p_1 не исключается.

В этом случае придется продолжить тестирование. Выберем *другое* целое $a_2 \geq 1$, не делящееся на p_1, и снова проверим выполнение малой теоремы Ферма:

$$a_2^{p_1-1} \equiv 1 (\mathrm{mod}\, p_1).$$

Если она опять выполнилось (снова не исключена простота числа p_1), перейти к числу a_3 и т. д.

Пусть k проверок на простоту выдержаны. Тогда вероятность того, что число p_1 — составное, равна $(1/2)^k$. При большом k эта вероятность исчезающе мала.

Пример 32.

Проиллюстрируем алгоритм RSA числовым примером. По необходимости, для возможности ручного счета, придется работать с небольшими числами.

Боб выбирает два *небольших* простых числа $p = 3$ и $q = 11$ и вычисляет их произведение

$$n = p \cdot q = 33.$$

Множители p и q Боб хранит *в строгой тайне* (в самом деле, разве кто-нибудь сможет догадаться, как разложить на множители число 33?); их произведение n несекретно.

Боб выбирает число e так, чтобы оно было *взаимно простым* с

$$\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1) = (3-1)(11-1) = 20$$

— значением функции Эйлера, т. е. их НОД должен быть равен единице:

$$(e, \varphi(n)) = 1.$$

Можно, например, взять $e = 7$.

Совокупность чисел n и e составляет *открытый* ключ Боба или его ключ для *зашифрования*:

$$\{n = 33;\ e = 7\} = k_E^B.$$

Этот ключ Бобу рекомендуется сообщить всем, с кем он ведет переписку.

Для расшифрования приходящих секретных сообщений Бобу потребуется число d, которое вычисляется как мультипликативно обратное числу e по модулю $\varphi(n)$:

$$e \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n)) \Rightarrow 7d \equiv 1 (\mathrm{mod}\, 20).$$

Для решения сравнения разложим дробь $\frac{20}{7}$ в цепную. Применим алгоритм Евклида:

$$\begin{array}{r|l} 20 & 7 \\ \hline 14 & \boldsymbol{2} \\ \hline 7 & 6 \\ \hline 6 & \boldsymbol{1} \\ \hline 6 & 1 \\ \hline 6 & \boldsymbol{6} \\ \hline 0 & \end{array}$$

$$\frac{20}{7} = [q_0;\ q_1, q_2] = [2;\ 1, 6] = 2 + \frac{1}{1 + \frac{1}{6}}.$$

Подходящие дроби:

$$\frac{P_0}{Q_0} = \frac{q_0}{1} = \frac{2}{1},\ \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = 2 + \frac{1}{1} = \frac{\mathbf{3}}{1},\ \frac{P_2}{Q_2} = \frac{20}{7}.$$

Предпоследняя подходящая дробь — это $\frac{P_1}{Q_1} = \frac{\mathbf{3}}{1}$. Числитель предпоследней подходящей дроби $P_{s-1} = P_1 = 3$, откуда $s = 2$.

Решение сравнения

$$x \equiv (-1)^s b P_{s-1} (\mathrm{mod}\, m) \equiv (-1)^2 \cdot 1 \cdot 3 (\mathrm{mod}\, 20) = 3 (\mathrm{mod}\, 20).$$

Получили серию решений

$$d_k = 3 + 20k,\ k \in \mathbb{Z}.$$

Из полученной серии решений d можно взять любое, удовлетворяющее ограничению

$$1 \le d \le n - 1 = 32.$$

Выберем $d = 3$, получаемое при $k = 0$.

Совокупность чисел n и d составляет *закрытый* ключ Боба или его ключ для *расшифрования*:

$$\{n = 33; d = 3\} = k_D^B.$$

Этот ключ Боб должен хранить *в строгой тайне*.

Перед шифрованием сообщения для Боба Алиса заменяет буквы письма числами (пусть это будут порядковые номера букв в алфавите: А = 01, Б = 02, …, Я = 32) и удаляет все пробелы. Таким образом, исходное сообщение Алисы превращается в длинное число X. С учетом ограничения

$$X \le n - 1 = 32,$$

где $n = 33$ — число, полученное Бобом на первом шаге, Алисе придется шифровать сообщение побуквенно, т. е. блоками X_1, X_2, …, длиной в одну букву. Разумеется, это — следствие малости используемых чисел.

Алиса шифрует сообщение, используя функцию $E(X)$ зашифрования в алгоритме RSA:

$$Y = E(X) \equiv X^e \pmod{n} = X^7 \pmod{33},$$

где Y — результат зашифрования каждой буквы.

Алиса шифрует букву А = 01:

$$Y \equiv (01)^7 \pmod{33} = 1 \pmod{33};$$

поскольку первая буква алфавита — это А, имеем

$$\text{А} \to \text{А}$$

(буква перешла в себя).

Алиса шифрует букву Б = 02:

$$Y \equiv (02)^7 \,(\mathrm{mod}\, 33) = 128 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (128 - 33 \cdot 3) \,(\mathrm{mod}\, 33) = 29 (\mathrm{mod}\, 33);$$

поскольку 29-я буква алфавита — это Ь, имеем

$$\text{Б} \to \text{Ь}.$$

Алиса шифрует букву В = 03:

$$Y \equiv (03)^7 \,(\mathrm{mod}\, 33) = 2187 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (2187 - 33 \cdot 66) \,(\mathrm{mod}\, 33) = 9 (\mathrm{mod}\, 33),$$

поскольку девятая буква алфавита — это И, имеем

$$\text{В} \to \text{И}.$$

Алиса шифрует букву Г = 04:

$$Y \equiv (04)^7 \,(\mathrm{mod}\, 33) = 16\,384 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (16\,384 - 33 \cdot 496) \,(\mathrm{mod}\, 33) = 16 (\mathrm{mod}\, 33);$$

поскольку 16-я буква алфавита — это П, имеем

$$\text{Г} \to \text{П}.$$

Алиса шифрует букву Д = 05:

$$Y \equiv (05)^7 \,(\mathrm{mod}\, 33) = 78\,125 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (78\,125 - 33 \cdot 2367) \,(\mathrm{mod}\, 33) = 14 (\mathrm{mod}\, 33);$$

поскольку 14-я буква алфавита — это Н, имеем

$$\text{Д} \to \text{Н}.$$

Алиса шифрует букву Е = 06:

$$Y \equiv (06)^7 \,(\mathrm{mod}\, 33) = 279\,936 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (279\,936 - 33 \cdot 8482) \,(\mathrm{mod}\, 33) = 30 (\mathrm{mod}\, 33);$$

поскольку 30-я буква алфавита — это Э, имеем

$$\text{Е} \to \text{Э}.$$

Алиса шифрует букву Ж = 07:

$$Y \equiv (07)^7 \pmod{33} = 823543 \pmod{33} \equiv$$
$$\equiv (823543 - 33 \cdot 24955) \pmod{33} = 28 \pmod{33};$$

поскольку 28-я буква алфавита — это Ы, имеем

$$Ж \to Ы.$$

Алиса шифрует букву З = 08:

$$Y \equiv (08)^7 \pmod{33} = 2097152 \pmod{33} \equiv$$
$$\equiv (2097152 - 33 \cdot 63550) \pmod{33} = 2 \pmod{33};$$

поскольку вторая буква алфавита — это Б, имеем

$$З \to Б.$$

Алиса шифрует букву И = 09:

$$Y \equiv (09)^7 \pmod{33} = 4782969 \pmod{33} \equiv$$
$$\equiv (4782969 - 33 \cdot 144938) \pmod{33} = 15 \pmod{33};$$

поскольку 15-я буква алфавита — это О, имеем

$$И \to О.$$

Алиса шифрует букву Й = 10:

$$Y \equiv (10)^7 \pmod{33} = 10000000 \pmod{33} \equiv$$
$$\equiv (10000000 - 33 \cdot 303030) \pmod{33} = 10 \pmod{33};$$

поскольку 10-я буква алфавита — это Й, имеем

$$Й \to Й$$

(буква перешла в себя) и т. д.

Сводная шифровальная таблица:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	…	22	23	…	29	…
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	…	Х	Ц	…	Ь	…
А	Ь	И	П	Н	Э	Ы	Б	О	Й	К	Л	Ж	У	Ъ	…	Х	Т	…	Р	…

Из рассмотренных букв уже можно составить осмысленную фразу. Пусть, например, Алиса хочет послать Бобу вопрос:

ГДЕ ДЕНЬГИ?

Шифровка будет иметь вид

ПНЭНЭУРПО

(пробел и знак вопроса убраны).

Боб начинает побуквенное расшифрование.

Функция расшифрования в алгоритме RSA:

$$X = D(Y) \equiv Y^d (\mathrm{mod}\, n) = Y^3 (\mathrm{mod}\, 33),$$

где Y — зашифрованная буква.

Боб расшифровывает букву П = 16:

$$X \equiv (16)^3 (\mathrm{mod}\, 33) = 4096 (\mathrm{mod}\, 33) \equiv$$
$$\equiv (4096 - 33 \cdot 124) (\mathrm{mod}\, 33) = 4 (\mathrm{mod}\, 33);$$

поскольку четвертая буква алфавита — это Г, имеем

$$\text{П} \to \text{Г}$$

(расшифрование верное) и т. д.

Итак, получился шифр простой (одноалфавитной) замены, но не шифр Цезаря, поскольку сдвиг для каждой буквы индивидуален. Разумеется, этот шифр поддается взлому с помощью статистического криптоанализа. При астрономически огромных p и q, которые реально используются на практике, повторение одинаковых блоков в шифрованном сообщении (на котором основан статистический криптоанализ) крайне маловероятно, и шифр оказывается устойчивым к взлому (по меньшей мере, этим методом).

Вопросы для самопроверки

1. Что такое каноническое разложение?
2. Какие числа называются взаимно простыми?
3. Какие числа называются мультипликативно обратными?
4. В чем состоит смысл функции Эйлера $\varphi(z)$?

Лабораторный практикум

Для получения экзаменационной оценки «отлично» нужно выполнить и защитить лабораторные работы 2, 3; на оценку «хорошо» — работы 1, 3. Выполнение только лабораторной работы 3 оценивается как «удовлетворительно».

Лабораторная работа 1. Шифр Цезаря

На любом языке программирования составить компьютерную программу, реализующую алгоритм Цезаря.

Технические условия:

• зашифрование и расшифрование текстов, записанных кириллицей и латиницей;

• взлом зашифрованного русскоязычного текста методом наименьших квадратов;

• замена во вводимом тексте буквы Ё на Е;

• очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов; приведение всех букв к строчному регистру;

• приведение введенного значения ключа к диапазону [0; 32] для кириллицы, [0; 26] для латиницы;

• выдача обработанного текста группами по пять символов;

• защита от неправильных действий пользователя («дураковустойчивость»);

• дружественный интерфейс.

Лабораторная работа 2. Шифр Виженера

На любом языке программирования составить компьютерную программу, реализующую алгоритм Виженера.

Технические условия:

• зашифрование и расшифрование текстов, записанных кириллицей;

• взлом зашифрованного русскоязычного текста методом наименьших квадратов на основе идей Казиского (в случае использования идей Фридмана необходимо уметь внятно объяснить эти идеи);

• замена во вводимом тексте и ключе буквы Ё на Е;

• очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов; приведение всех букв к строчному регистру;

• выдача обработанного текста группами по пять символов;

• защита от неправильных действий пользователя («дураковустойчивость»);

• дружественный интерфейс.

Лабораторная работа 3. Освоение программы PGP

Программа PGP (Pretty Good Privacy) — чрезвычайно удачная программа для шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде. Первоначально разработана Ф. Циммерманном в 1991 г. Существуют реализации PGP для всех распространенных операционных систем. Кроме свободно распространяемых версий, есть и коммерческие. На данный момент не известно ни одного случая взлома данных, зашифрованных PGP, с помощью полного перебора или уязвимости криптоалгоритма.

Лабораторная работа выполняется двумя студентами. Нужно уметь создать пару ключей шифрования (открытый и закрытый), подписать сообщение электронной цифровой подписью, зашифровать сообщение для напарника, расшифровать полученное от него сообщение, проверить подлинность ЭЦП в полученном сообщении; уметь объяснить смысл выполняемых операций.

Библиографический список

Источники, повлиявшие на содержание данного курса

1. *Александров, В. А.* Задачник-практикум по теории чисел / В. А. Александров, С. М. Горшенин. — Москва : Просвещение, 1972.

2. *Бабаш, А. В.* Информационная безопасность. Лабораторный практикум / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2016.

3. *Бухштаб, А. А.* Теория чисел / А. А. Бухштаб. — Москва : Просвещение, 1966.

4. *Виноградов, И. М.* Основы теории чисел / И. М. Виноградов. — Москва : URSS, 2021.

5. *Нечаев, В. И.* Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. — Москва : Высшая школа, 1999.

6. *Панасенко, С. П.* Основы криптографии для экономистов / С. П. Панасенко, В. П. Батура. — Москва : Финансы и Статистика, 2005.

7. *Партыка, Т. Л.* Информационная безопасность / Т. Л. Партыка, И. И. Попов. — Москва : Форум, 2014.

8. *Харин, Ю. С.* Математические и компьютерные основы криптологии : учебное пособие / Ю. С. Харин [и др.]. — Минск : Новое знание, 2003.

9. *Хорев, П. Б.* Методы и средства защиты информации в компьютерных системах / П. Б. Хорев. — Москва : Академия, 2007.

Некоторые книги, удачно дополняющие данный курс

1. *Гомес, Ж.* Математики, шпионы и хакеры. Кодирование и криптография / Ж. Гомес. — Москва : Де Агостини, 2014.

2. *Нестеров С. А.* Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2017.

3. *Панасенко, С. П.* Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. — Санкт-Петербург : БХВ-Петербург, 2009.

4. *Черчхаус, Р.* Коды и шифры. Юлий Цезарь, «Энигма» и Интернет / Р. Черчхаус. — Москва : Весь Мир, 2009.

5. *Шаньгин, В. Ф.* Информационная безопасность и защита информации / В. Ф. Шаньгин. — Саратов : Профобразование, 2017.

6. *Sinkov, A.* Elementary Cryptanalysis: a Mathematical Approach / A. Sinkov. — Washington, D. C. : The Mathematical Association of America, 1966.

Книги родственной тематики от «Издательства Юрайт»

1. *Бабенко, Л. К.* Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва: Издательство Юрайт, 2020.

2. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020.

3. *Запечников, С. В.* Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020.

4. *Лось, А. Б.* Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020.

5. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 частях. Ч. 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Изд-во Юрайт, 2020.

6. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 частях. Ч. 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020.

7. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020.

Новые издания по дисциплине «Информационная безопасность и защита информации» и смежным дисциплинам

1. *Бабенко, Л. К.* Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2021.

2. *Богатырев, В. А.* Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2021.

3. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021.

4. *Внуков, А. А.* Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021.

5. *Запечников, С. В.* Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2021.

6. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021.

7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021.

8. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021.

9. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021.

Приложение

Таблица П.1

Относительные частоты встречаемости букв в русском языке (по результатам анализа текста объемом в 1 млн букв)

№ п/п	Буква	Относительная частота	№ п/п	Буква	Относительная частота	№ п/п	Буква	Относительная частота
1	А	0,062	12	Л	0,035	23	Ц	0,003
2	Б	0,014	13	М	0,026	24	Ч	0,012
3	В	0,038	14	Н	0,053	25	Ш	0,006
4	Г	0,013	15	О	0,090	26	Щ	0,003
5	Д	0,025	16	П	0,023	27	Ъ	0,014 (с Ь)
6	Е, Ё	0,072	17	Р	0,040	28	Ы	0,016
7	Ж	0,007	18	С	0,045	29	Ь	0,014 (с Ъ)
8	З	0,016	19	Т	0,053	30	Э	0,003
9	И	0,062	20	У	0,021	31	Ю	0,006
10	Й	0,010	21	Ф	0,002	32	Я	0,018
11	К	0,028	22	Х	0,009			

Те же данные в порядке убывания относительных частот:

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

Таблица П.2

Таблица Виженера для русского алфавита

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

Таблица П.3

Коды некоторых символов

№ п/п	Символ	ASCII-код	Двоичный код	№ п/п	Символ	ASCII-код	Двоичный код
1	A	65	0 1 0 0 0 0 0 1	19	S	83	0 1 0 1 0 0 1 1
2	B	66	0 1 0 0 0 0 1 0	20	T	84	0 1 0 1 0 1 0 0
3	C	67	0 1 0 0 0 0 1 1	21	U	85	0 1 0 1 0 1 0 1
4	D	68	0 1 0 0 0 1 0 0	22	V	86	0 1 0 1 0 1 1 0
5	E	69	0 1 0 0 0 1 0 1	23	W	87	0 1 0 1 0 1 1 1
6	F	70	0 1 0 0 0 1 1 0	24	X	88	0 1 0 1 1 0 0 0
7	G	71	0 1 0 0 0 1 1 1	25	Y	89	0 1 0 1 1 0 0 1
8	H	72	0 1 0 0 1 0 0 0	26	Z	90	0 1 0 1 1 0 1 0
9	I	73	0 1 0 0 1 0 0 1		0		0 0 0 0 0 0 0 0
10	J	74	0 1 0 0 1 0 1 0		1		0 0 0 0 0 0 0 1
11	K	75	0 1 0 0 1 0 1 1		2		0 0 0 0 0 0 1 0
12	L	76	0 1 0 0 1 1 0 0		3		0 0 0 0 0 0 1 1
13	M	77	0 1 0 0 1 1 0 1		4		0 0 0 0 0 1 0 0
14	N	78	0 1 0 0 1 1 1 0		5		0 0 0 0 0 1 0 1
15	O	79	0 1 0 0 1 1 1 1		6		0 0 0 0 0 1 1 0
16	P	80	0 1 0 1 0 0 0 0		7		0 0 0 0 0 1 1 1
17	Q	81	0 1 0 1 0 0 0 1		8		0 0 0 0 1 0 0 0
18	R	82	0 1 0 1 0 0 1 0		9		0 0 0 0 1 0 0 1