

Министерство внутренних дел Российской Федерации
Омская академия

А. А. Симаков, А. В. Кургuzов

**ЗАЩИТА ИНФОРМАЦИИ
В КОМПЬЮТЕРНЫХ СИСТЕМАХ**

Учебное пособие

Омск
ОМА МВД России
2022

УДК 004(075)
ББК 32.97я73
С37

Рецензенты:

доктор технических наук, профессор *А. И. Примакин*
(Санкт-Петербургский университет МВД России);
доктор технических наук, профессор *А. В. Еськов*
(Краснодарский университет МВД России)

Симаков, А. А.

С37

Защита информации в компьютерных системах : учеб. пособие / А. А. Симаков, А. В. Кургузов. — Омск : Омская академия МВД России, 2022. — 108 с.

ISBN 978-5-88651-802-3

В учебном пособии рассматриваются вопросы криптографической и стеганографической защиты информации, знание которой требуется при предотвращении, выявлении, раскрытии и расследовании преступлений, связанных с использованием информационно-коммуникационных технологий.

Предназначено для курсантов и слушателей образовательных организаций МВД России.

УДК 004(075)
ББК 32.97я73

ISBN 978-5-88651-802-3

© Омская академия МВД России, 2022

ВВЕДЕНИЕ

Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом.

Блез Виженер

Хранение, передача и обработка информации являются основополагающими процессами в компьютерных системах. Развитие информационных технологий за последние десятилетия изменило качественные характеристики всех трех информационных процессов. Возросшие объемы хранения, скорости передачи и быстродействие обработки информации привнесли не только широкий спектр возможностей, но и множество вопросов защиты информации.

Практически все государственные и коммерческие организации в той или иной мере сталкиваются с проблемами информационной безопасности (далее — ИБ). И если в государственных структурах деятельность в области защиты информационной среды контролируется, то коммерческим организациям приходится самостоятельно заниматься вопросами защиты своей информации. Нередко политика ИБ в коммерческих структурах находится либо на низком уровне, либо отсутствует полностью. Естественно, эффективность действий в этом направлении, прежде всего, зависит от грамотных решений руководителя, основанных на его знаниях в области ИБ. Так как криптография и стеганография — неотъемлемые части теории и практики ИБ, то изучение общих понятий этих разделов выступает важным элементом информационной культуры человека.

Сотрудники правоохранительных органов выполняют сложную работу по раскрытию и расследованию преступлений с применением современных информационно-коммуникационных технологий (далее — ИКТ) и криптовалют. Для этого требуются грамотные специалисты, обладающие знаниями не только в юриспруденции, но и в области ИБ.

В деятельности органов внутренних дел (далее — ОВД) широко используется как общедоступная информация, так и сведения ограниченного доступа (конфиденциальные). Бесспорно, защите конфиденциаль-

ных данных уделяется особое внимание. В преступном же мире сокрытие информации от правоохранительных органов — главная цель. В связи с этим по обе стороны ведется борьба, в том числе за современные научные достижения в сфере защиты информации. Меры защиты информации в компьютерных системах имеют три основных направления: организационные, правовые, технические¹. В учебном пособии рассматриваются криптографические и стеганографические методы защиты информации, относящиеся к техническим мерам.

Термин «**криптология**» происходит от греческих слов *kryptos* — тайный и *logos* — мысль, слово и используется для обозначения всей научной области, включающей *криптографию* и *криптоанализ*. Криптография направлена на создание шифров и их исследование, в то время как криптоанализ ориентирован на создание способов раскрытия шифров.

Стеганология (от греч. *steganos* — скрытый, *logos* — мысль, слово) — наука о сокрытии информации (*стеганография*) и обнаружении скрытых данных (*стеганоанализ*).

Криптография и стеганография — два древнейших направления, развивавшиеся параллельно друг другу со времен зарождения письменности и предназначавшиеся для защиты информации от посторонних лиц. То и другое имеют единую цель — утаить по тем или иным причинам информацию от всех людей, кроме «избранных», тех, кто знает тайну (ключ) о том, как прочесть секретные сведения.

Но в чем заключается различие между криптографией и стеганографией?

Прежде всего — в способах достижения цели. Цель одна, подходы разные.

Стеганография — это разработка средств и способов сокрытия информации, когда сам факт ее наличия неочевиден. **Криптография** — это разработка средств и способов видоизменения письма таким образом, чтобы прочесть информацию мог только узкий круг лиц, обладающий правилом и ключом (тайной) для ее прочтения.

Как сказано выше, слова «криптография» и «стеганография» имеют греческие корни. Их смысловая нагрузка сходна, несмотря на различия в написании. Однако из определений усматривается существенное различие в способах достижения цели. общепризнанной классификации в этих областях нет до сих пор.

¹ Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ. Здесь и далее, если не указано иного, доступ из справ.-правовой системы «КонсультантПлюс».

Для понимания различий между криптографическими и стеганографическими методами нелишне вспомнить пример совместного использования возможностей этих двух направлений в рассказе Эдгара По «Золотой жук». Старая карта пирата, найденная одним из персонажей произведения, интриговала не одно поколение читателей. Но наш интерес к ней сугубо исследовательский. Начертание карты проявилось только после нагревания поверхности бумаги пламенем свечи. До этого у персонажа не было ни малейшего подозрения о существовании карты на пожелтевшем от старости мятом листке бумаги. Это не что иное, как один из стеганографических приемов, суть которого заключается в нанесении информации (которую требуется скрыть) на бумагу определенными органическими жидкостями (молоком, лимонным соком и т. д.). При высыхании поверхности листа нанесенный текст становится практически невидимым и проявляется лишь при нагревании. А вот текстовая информация на этой карте представлена в виде непонятных знаков и цифр. Бессодержательность их беспорядочного нагромождения привела главного героя к мысли о тайном тексте, скрытом одним из криптографических способов.

Мы приблизились к существенному отличию криптографии от стеганографии. Если применение стеганографии нужно обнаружить, т. е. догадаться о сокрытии тайного, то использование криптографических методов очевидно сразу, а разгадка — в ключе, хранимом втайне. Совмещение этих двух направлений устраняет их собственные недостатки, которые нетрудно заметить. Несовершенство любого метода стеганографии заключается в его бесполезности в случае обнаружения, в то время как в криптографии изначально предполагается, что противник знает о наличии информации, скрываемой под непонятными знаками и символами. Более того, возможно, ему известен применяемый метод изменения письма.

Таким образом, криптография и стеганография — это не только два разных направления в защите информации, но и два направления, совместное использование которых гармонично дополняет друг друга.

Если одни защищают информацию, то разумно предположить, что те, кому эта информация не предназначена или от кого она защищается, будут прилагать все усилия для ее получения. Поэтому неудивительно зарождение параллельно криптографии и стеганографии еще двух таких направлений, как криптоанализ и стеганоанализ (стегоанализ), цель которых заключается в обнаружении и получении защищаемой информации в доступном (открытом) виде.

Криптоанализ — это разработка и применение специальных методов для исследования шифров в целях их раскрытия или подделки таким образом, чтобы они были приняты как подлинные, при условии, что секретный ключ неизвестен.

Стеганоанализ — это разработка и применение специальных методов для решения задач обнаружения скрытых сообщений, их извлечение, удаление или модификация.

В области защиты информации существует достаточно устоявшаяся терминология.

Открытый текст после стеганографических преобразований, как правило, называется **стеганограммой** (*стегограммой*).

Исходное сообщение, к которому применяет свое искусство криптограф, называется открытым текстом сообщения или просто открытым текстом, а результат его работы — шифрованным текстом сообщения, **шифротекстом** или **криптограммой**.

Шифр — это метод преобразования открытого текста по определенному криптографическому алгоритму в целях защиты информации от посторонних лиц, причем параметры алгоритма задаются ключом.

Ключ — это значения некоторых параметров алгоритма криптографического преобразования данных, обеспечивающие выбор одного из множества вариантов преобразования. Только благодаря ключу можно закрыть информацию от прочтения и сделать ее доступной для ограниченного круга. Поэтому знание ключа необходимо и тому, кто зашифровывает, и тому, кто расшифровывает, т. е. кому предназначено это сообщение.

Очевидно, что **шифрование** — это процесс применения шифра к защищаемой информации. **Дешифрование** — процесс, обратный шифрованию, иначе говоря, преобразование шифрованного сообщения в защищаемую информацию (открытый текст).

Криптостойкость называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно она определяется периодом времени, необходимым для дешифрования, и количеством всех возможных ключей.

Нередко можно наблюдать употребление слов «код», «кодирование» в том же смысле, что и «шифр», «шифрование». Действительно, на протяжении веков кодами назывались известные способы тайнописи, направленные на сознательное изменение открытого текста, например, омофонические коды (шифры). Однако усложнение кодов и бурное развитие средств связи после изобретения электричества в прикладной матема-

тике привело к разделению интересующей нас области на теорию кодирования и теорию шифрования. В настоящее время коды и кодирование применяются в теории для удобной и безошибочной передачи и хранения сообщений. Таким образом, в современном понимании *кодирование* в широком смысле слова — это процесс представления сообщений в форме, удобной для их безошибочной передачи по каналам связи и хранения на электронных носителях. В узком смысле кодирование — это представление букв одного алфавита в другом, меньшем по объему. Например, в компьютерных системах обработка данных осуществляется в двоичной системе счисления, поэтому любая текстовая информация вначале путем кодирования преобразуется в двоичный вид, лишь затем применяется один из машинных методов шифрования.

ТЕМА 1. КРИПТОГРАФИЯ

Вопрос 1. История криптографии

Косвенные упоминания о системах и способах тайнописи можно найти в источниках древних цивилизаций Индии, Египта, Месопотамии. К сожалению, большинство фактов, касающихся письменности древних народов, утрачены. Из ранних документальных источников о применяемых системах шифров большая их часть относится к периоду возникновения государств Древней Греции. Ее культура вобрала наследие шумеров и этрусков, цивилизаций Крита и Египта. Поэтому можно сделать предположение о глубокой древности способа шифрования, применявшегося, например, в городе-государстве Спарте (XI–II вв. до н. э.) — способ сци-тала (от греч. *жезл*). Текст наносили на пергаментную ленту и накручивали ее на жезл (древк), поворачивая жезл. Строка за строкой исписывалась вся лента. Развернув ее, получали шифротекст. Дешифровка выполнялась с использованием жезла такого же диаметра.

Большой вклад в криптографию внес Эней Тактик¹, живший в Греции в IV в. до н. э. (предположительно уроженец Аркадии). Помимо знаменитых военных трактатов, он признан автором двух шифров, известных как «диск Энея» и «книжный шифр». Принцип работы «диска Энея» прост. На диске диаметром 10–15 см и толщиной 1–2 см высверливались отверстия по числу букв в алфавите. В центре диска помещалась катушка с ниткой достаточной длины. Шифрование осуществлялось протягиванием нитки через отверстия в соответствии с буквами шифруемого текста. Адресат, получив такой диск, мог прочесть послание путем последовательного вытягивания нитки из отверстий, что позволяло ему извлекать передаваемое сообщение, но в обратном порядке следования букв. При угрозе захвата диска достаточно было выдернуть катушку с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий.

¹ Сингх С. Книга кодов: тайная история кодов и их «взлома». М., 2007. С. 5.

Позднее идея Энея была модернизирована в методе, где вместо диска применялась линейка с числом отверстий, равных количеству букв алфавита. Каждое обозначалось своей буквой, буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на нее ниткой, рядом с катушкой имелась прорезь. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения ее через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т. д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Имея идентичную линейку, он протягивал нить через прорезь до отверстий, определяемых узлами, и восстанавливал исходный текст по буквам отверстий. Это устройство получило название «линейка Энея». Сходство с ней, как полагают некоторые зарубежные ученые, имеет узелковая письменность инков «кипу», до сих пор не поддающаяся дешифрованию (на языке инков «кипу» означает «узел»). Свои сообщения они передавали в виде нитки, на которой завязывались разноцветные узелки, определявшие содержание сообщения.

В истории описывается случай, происшедший в конце XVI в., когда у одного старого индейца конкистадоры обнаружили и забрали связку цветных веревочек с узелками на них. То, с каким почтением и бережностью индеец относился к этой необычной вещи, подстегнуло любопытство конкистадоров, потребовавших рассказать о назначении этих веревочек. Индеец ответил: «Здесь записаны все дела завоевателей, как дурные, так и добрые». По одной из гипотез, отголоски узелковой письменности можно найти и у древних славян в замысловатой вязи буквиц и необычных узорах на старинных прялках и нарядах. До настоящего времени все попытки расшифровать узелковую письменность не принесли результата.

«Книжный шифр» описан Энеем Тактиком в его сочинении «Об обороне укрепленных мест». Он предложил делать малозаметные проколы в книге или каком-либо документе над буквами (или под ними) секретного сообщения. Примечательно, что во время Первой мировой войны германские шпионы использовали аналогичный шифр, заменив проколы на точки, наносимые симпатическими чернилами на буквы газетного текста.

Окончательный вид «книжного шифра» сложился значительно позже, его современный аналог представляет собой способ, заключающийся в замене букв на номер строки и номер этой буквы в строке на заранее оговоренной странице какой-либо книги. Дополнительным ключом та-

кого шифра является книга и используемая страница в ней. Шифр применялся даже во времена Второй мировой войны.

Значительным прорывом в развитии криптографии по праву считается шифр, предложенный греческим историком Полибием (II в. до н. э.), известный как «квадрат Полибия» или «тюремный шифр». Применительно к современному латинскому алфавиту из 26 букв для шифрования нужен квадрат размером 5x5 клеток, в который выписываются все буквы алфавита, при этом буквы I, J не различаются (J отождествляется с буквой I). Каждая клетка квадрата имеет двузначные координаты, на которые и заменялась шифруемая буква. При дешифровании каждая такая пара определяла соответствующую букву сообщения. Ключ шифра — расположение букв в таблице 5x5.

Благодаря высокой криптостойкости «квадрат Полибия» был широко распространен. В несколько измененном виде этот шифр дошел до наших дней и получил название «тюремный шифр». Его модификация состоит в том, что стороны квадрата обозначаются не буквами (ABCDE), а числами (12345). Тогда для его использования нужно знать только естественный порядок расположения букв алфавита, что позволяет перестукиваться шифрованными сообщениями через стенку, если ваша свобода общения ограничена. Число 3, например, передается путем тройного стука. При передаче буквы сначала отстукивается число, соответствующее строке, в которой находится буква, а затем — номер соответствующего столбца. Известен исторический факт, что декабристы, заключенные в тюрьму после неудавшегося восстания, не смогли установить связь с находившимся в одиночной камере князем А. И. Одоевским, который был не только блестящим гвардейским офицером, но и высокообразованным по тем временам человеком. Оказалось, что князь никак не мог запомнить порядок расположения букв в русском и французском алфавитах (самими языками он владел в совершенстве). Декабристы для русского алфавита использовали прямоугольник размером 5x6 (5 строк и 6 столбцов) и редуцированный до 30 букв алфавит.

Этот же принцип применяется при переговорах на расстоянии прямой видимости с помощью обыкновенного платка. Горизонтальная отмашка указывает строку, а вертикальная отсчитывает позицию буквы.

История упоминает о частом использовании различных шифров Гаем Юлием Цезарем. Его страсть к тайнописи сподвигла Марка Валерия Проба написать целый трактат о применяемых Цезарем шифрах. Увы, сочинение не дошло до наших дней. Осталось описание лишь одного шифра, упомянутого в сочинении Гая Транквила Светония «Жизнь двенад-

цати Цезарей» (II в. н. э.). Юлий Цезарь просто заменял каждую букву в послании буквой, сдвинутой в алфавите на три позиции вправо.

Уверенность в надежности методов шифрования, применявшихся практически все первое тысячелетие нашей эры, сохранялась до тех пор, пока не был найден простой способ вскрытия одноалфавитных шифров. Произошло это на Востоке, где в золотой век исламской цивилизации, во времена правления династии Аббасидов (с 750 г.), в равной мере процветали искусства и науки. Уже тогда для обеспечения безопасности передачи сообщений широко использовалась криптография. Кроме документов государственной важности, зашифровывали также сведения о налогах. Например, практически во все руководства для чиновников входил раздел, посвященный криптографии. В исламском государстве применялись достаточно простые шифры перестановки и подстановки, соизмеримые по своей стойкости с европейскими шифрами того периода. Однако если европейцы были уверены в надежности одноалфавитных шифров замены еще несколько веков спустя, то арабские ученые уже в первой половине IX в. успешно взламывали эти шифры.

Криптоанализ обусловлен развитием религиозного образования. Ведь именно теологи в поисках доказательств подлинности изречений Пророка Мухаммеда обратились к изучению этимологии слов и структуры предложений, чтобы проверить, согласуются ли отдельные тексты с лингвистическим стилем Пророка. Помимо этого религиоведы, исследовав отдельные буквы, выяснили, что их повторяемость в тексте различна. Неизвестно, кто первый открыл возможность применения особенностей появления букв в тексте с разной частотой как инструмент криптоанализа, но наиболее раннее описание (IX в.) представлено в работе крупного арабского ученого аль-Кинди «Рукопись по дешифрованию криптографических сообщений»². В произведении содержится подробный анализ статистики, фонетики и синтаксиса арабского языка, а также революционная система криптоанализа одноалфавитных шифров замены.

Для Европы период с IX в. по XIII в. не благоприятствовал науке и искусству. В истории за этой эпохой закреплен термин «темные века». По большей части науки в европейских странах развивались в монастырях и, естественно, только в тех направлениях, которые считались приоритетными (религия, политика, сельское хозяйство и др.). Криптография была в их числе. С одной стороны, монахи были заинтересованы в изучении библейских текстов, где достаточно часто встречаются криптограммы, зашифрованные с помощью традиционного одноалфавитного

² Кан Д. Взломщики кодов. М., 2000. С. 15.

шифра замены, применяющегося в еврейском алфавите, иврите, — *Ат-баиш*. Хотя простота шифра явно указывала на шифрование не в целях сокрытия информации, а для акцентирования внимания на ней. Монахи не прекращали поиски других криптограмм в письменах, скрывающих тайные сообщения. С другой стороны, внимание к криптографии подогревалось тайной перепиской между монастырями и хранением знаний для посвященных.

Первая книга о криптографии в Европе принадлежит английскому францисканскому монаху и энциклопедисту Роджеру Бэкону (1214–1294) — «Тайные опыты и недействительность магии», где он приводит семь способов тайнописи. Видимо, восприняв предупреждение Бэкона: «Дурак тот, кто пишет о тайне каким-либо способом, но не так, чтобы скрыть ее от простонародья», к XIV в. криптографией стали пользоваться повсеместно. Алхимики и ученые с помощью шифрования хранили свои открытия в секрете. Например, Джеффри Чосер (1344–1400), известный английский поэт Средневековья, астроном и криптограф в своем трактате «Об астролябии» (трактат предназначался его сыну) зашифровал несколько разделов шифром простой замены букв на символы иного алфавита.

Европа в средние века находилась под влиянием католической церкви, поэтому криптография вне ее стен не приветствовалась. Лишь церковь была обителью просвещения. Неудивительно, что до рассвета наук и ремесел, начавшегося в эпоху Возрождения, именно в лоне католической церкви в XIV в. появляется книга служителя папской канцелярии Чикко Симонетти. Она примечательна тем, что, помимо описания известных шифров, автор предлагает в ней способ усложнения одноалфавитного шифра замены путем замены гласных букв не одним символом, а несколькими. Тем самым достигалось выравнивание в тексте частот встречаемости гласных букв — это так называемый *омофонический шифр* (от греч. *homos* — тот же самый, *phonos* — звук), активно применяемый вплоть до XIX в. Кроме того, Симонетти в своей рукописи (написанной на трех кусках пергамента) установил 13 правил вскрытия шифров простой замены, где сохранены разделители слов.

Комбинацию омофонического шифра и кодирования более десятка широко распространенных слов или имен (нескольким десяткам названиям городов, рек, имен известных личностей ставились в соответствие двухбуквенные кодовые эквиваленты) использовал «антипапа» Климентий VII. Объявив себя законным владельцем папского трона, он пытался внести тем самым раскол в римско-католическую церковь. Метод шифрования по указанию «антипапы» разработал Габриэли Лавинде, служа-

щий в его представительстве в одном из северо-итальянских городов-государств.

К XV в. европейская криптография превратилась в целую отрасль, развивающуюся стремительными темпами. Эпоха Ренессанса возродила вновь науки и искусства, в том числе и криптографию. Политические интриги в странах Европы обеспечивали постоянную потребность государств в методах тайнописи, и здесь первое место занимала Италия, состоящая из постоянно соперничающих городов-государств. Расцвет дипломатии способствовал развитию не только криптографии, но и криптоанализа. По сути, каждый дипломат был по совместительству шпионом, собирающим интересующие сведения и направляющим ее ко двору, пославшему его. Любое государство также стремилось перехватить информацию соседей. Так в европейских государствах началась эра исследований в области криптоанализа.

Выдающейся личностью эпохи Возрождения является художник, архитектор, композитор, поэт и философ, муж Флоренции Леон Батист Альберти (автор проекта первого римского фонтана «Треви» и первой печатной книги «Об архитектуре»), открывший новую страницу в криптографии³. Несмотря на то, что Леон Альберти был человеком светским, именно по просьбе своего друга Леонардо Дато (служившего секретарем у папы римского) он в 60-е гг. XV в. занялся исследованиями в области криптографии. Выслушав Дато об успехах вскрытия одноалфавитных шифров, Альберти поставил перед собой задачу определить в общих чертах, каким должен быть шифр, стойкий к криптоанализу. Изучив известные шифры, Альберти пришел к выводу, что использование одного алфавита при шифровании не может обеспечить необходимую стойкость шифра. Он предложил применять два или более шифралфавита, переходя от одного к другому в процессе шифрования, что существенно затрудняло криптоанализ.

Такая постановка задачи привела к новому витку в развитии криптографии. Решить поставленную Леоном Альберти задачу предстояло другим. Сначала ее продолжил родившейся в 1462 г. Иоганн Тритемий, немецкий аббат, настоятель монастыря в Вюрцбурге (автор первой печатной книги по криптографии «Полиграфия», изданной в 1518 г.). Затем в этом направлении работал Джованни Баттиста делла Порта, итальянский ученый-энциклопедист, педагог и драматург, описавший в своем произведении «О тайной переписке» (1563) все известные системы шифрования. Завершить начатое Леоном Альберти исследование методов

³ Сингх С. Указ. соч. С. 31.

многоалфавитной подстановки предстояло французскому дипломату Блезу Виженеру (1523 г. р.). Находясь в Риме с дипломатической миссией, 26-летний Блез Виженер в течение двух лет изучал труды Альберти, Тритемия и Порта. Оставив службу к сорока годам, он вплотную занялся воплощением идеи создания шифра, использовавшего механизм перехода с одного шифралфавита к другому. В итоге Виженер создал новый шифр, который был назван в его честь — «шифр Виженера». Венцом его работы стал «Трактат о шифрах», опубликованный в 1586 г.

Надежность «шифра Виженера» не обеспечила его продвижения в Европе — криптографы того времени отнеслись к нему с пренебрежением. Шифр оставался в забвении целых два века. Вместо этого шифрование производилось менее стойкими и более простыми шифрами, например, применялся шифр перестановки, предложенный итальянским математиком и философом Джероламо Кардано, названный «решетка Кардано», либо разрабатывались различные вариации омофонического шифра. Ярким примером усовершенствованного омофонического шифра служит «великий шифр» Людовика XIV (иногда в литературе он упоминается как «дипломатический шифр»). Его создателями являются отец и сын Россиньоли. Их популярность во Франции была настолько высока, что слово «россиньоль» стало французским жаргонным названием отмычки. Вскрытие «великого шифра» оказалось тщетным как при жизни его авторов, так и после их смерти, так как принцип шифрования был утерян. Лишь в 1890 г. Этьену Базери, служившему в шифровальном отделе французской армии, после кропотливой трехлетней работы удалось вскрыть «великий шифр». Это позволило историкам прочитать огромное количество зашифрованных этим шифром документов, которые в то время считались утерянными навсегда. В 1901 г. свои достижения в криптоанализе «великого шифра» Этьен Базери представил в книге «Раскрытые секретные шифры».

Борьба криптографов и криптоаналитиков европейских стран склоняла чашу весов то в одну, то в другую сторону. Омофонические шифры усложнялись, криптоанализ совершенствовался. Увеличившийся поток криптограмм потребовал создания «мозговых центров» по сбору информации и дешифрованию сообщений. В ведении каждой европейской державы был свой так называемый черный кабинет.

Самым известным эффективно действующим «черным кабинетом» был *Geheime Kabinets-Kanzlei* в Вене⁴. Он поставлял дешифрованную информацию не только императорам Австрии, но и продавал собран-

⁴ Там же. С. 35.

ные сведения в другие государства Европы. Известен факт, когда в 1774 г. в обмен на 1000 дукатов секретарь французского посольства аббат Жоржель получил возможность дважды в неделю просматривать полученные данные, из которых важные пересылались непосредственно Людовику XV в Париж.

Криптография в России развивалась по пути христианских стран. Датой появления криптографической службы следует считать 1549 г. (царствование Ивана IV), с момента образования Посольского приказа, имевшего «цифирное отделение». Используемые шифры были аналогичны европейским.

Император Петр I полностью реорганизовал криптографическую службу, создав Посольскую канцелярию. В это время для шифрования коды применяются как приложения к «цифирным азбукам». В знаменитом «деле царевича Алексея» в обвинительных материалах фигурировали и «цифирные азбуки»⁵.

Криптографией и криптоанализом в России занимались многие приглашенные иностранные ученые: с 1725 г. — математик Христиан Гольбах (1690–1764); с 1727 г. — математик Леонард Эйлер (1707–1783); с 1757 г. — математик и физик Франц Эпинус (1724–1802).

Совместная работа состоящих на службе у правительства криптоаналитиков позволяла взламывать большую часть сложных одноалфавитных шифров, поэтому криптографам пришлось применять более стойкий «шифр Виженера». Особенно остро необходимость в нем возникла после появления в XIX в. телеграфа, так как большой поток информации с его использованием был полностью открыт, в том числе и телеграфистам, которых всегда можно было подкупить в целях получения частных сообщений. Зашифрованные по методу Виженера данные без опаски нарушения конфиденциальности передавались телеграфисту.

Однако в Европе не спешили применять многоалфавитную подстановку при шифровании. Отсутствие механизации и сложность запоминания ключа большой длины сделало «шифр Виженера» не самым популярным. Короткий же ключ практически сводил на нет все достоинства метода. Так, в 1854 г. известный английский ученый XIX в. Чарльз Бэббидж (именно он разработал разностную машину, ставшую прототипом современной вычислительной техники) доказал, что метод Виженера может быть вскрыт⁶. Правда, факт успешного применения Ч. Бэббиджом криптоанализа к методу Виженера был обнаружен лишь в XX в., так как свои ре-

⁵ Соболева Т. А. История шифровального дела в России. М., 2002. С. 7.

⁶ Сингх С. Указ. соч. С. 41.

зультаты он так и не опубликовал. Тем временем, независимо от исследований Ч. Бэбиджа, этот же способ был найден офицером прусской армии майором Фридрихом Вильгельмом Касиски. Свою работу «Тайнопись и искусство дешифрования» (*Die Geheimschriften und die Dechiffirkunst*) он опубликовал в 1863 г.

Первая мировая война обнажила все изъяны в государственной системе обращения секретной информации многих стран. Передача данных в то время осуществлялась по проводным и беспроводным каналам связи. Требовалась защита информации в обоих каналах. Считалось, что проводная связь в местах боевых действий соединяла между собой войсковые подразделения достаточно надежно. Вместе с тем вероятность дистанционного съема информации существовала, ею пренебрегали. Уже в русско-японскую войну японцы в Порт-Артуре успешно использовали дистанционный съем информации с проводных сетей русских войск, причем русское командование по непонятным причинам отвергало такую возможность. Кроме того, нехватка проводных линий связи, невозможность прокладки кабеля из-за особенностей местности либо больших расстояний, частые разрывы и диверсии вынуждали пользоваться телеграфом. А здесь перехват сообщений противником был неизбежен, и шифры становились единственным способом защиты информации.

Во второй половине XIX в. почти все шифры европейских государств заключались в кодировании слогов или слов (аналогично шифру Россиньоли) обычно двух-, трех- или четырехзначными числами. Например, в России большинство шифров военного министерства представляли собой коды малого (до 1000 словарных величин) объема. Кодовыми обозначениями здесь являлись трех- и четырехзначные числа. Военные шифры этого типа обычно использовались в течение длительного времени. Перерабатывался лишь относительно быстро устаревавший словарь.

До Первой мировой войны ни в одном государстве, кроме Франции и Австро-Венгрии, не существовало военных криптоаналитических подразделений. Уверенность стран в надежности своих шифров позволила и Франции, и Австро-Венгрии читать перехваченные сообщения противников.

Франция была вынуждена начать исследования криптоанализа после серьезного поражения в войне против Пруссии в 1870 г. Вновь объединившаяся Германия стала большой угрозой для Франции, поэтому сбор подробной информации о планах противника имел приоритетное значение во французском криптографическом отделе.

Во многом французские криптоаналитики своими успехами обязаны преподавателю иностранных языков, филологу, археологу и математику Датчману А. Керкхоффу (Dutchman A. Kerckhoffs). Благодаря его труду «Военная криптография», изданному им в 1883 г., французы получили исключительное руководство по способам криптоанализа. К началу Первой мировой войны в вооруженных силах Франции его идеи были реализованы практически полностью. Именно в этой работе Керкхофф предлагает конвейерный способ выполнения криптоанализа, вводит предписание по секретности по ключам и не требует секретности криптосистемы, определяет, что практический интерес в новых средствах связи представляют те шифры, которые остаются стойкими при интенсивной переписке.

Уже упоминалось, что профессионализм криптографического отдела Австрии был известен с XVIII в. Созданное в ноябре 1911 г. при Генштабе австро-венгерской армии криптографическое бюро во главе с капитаном А. Фиглем безуспешно пыталось взломать русские дипломатические и военные криптосистемы, но уже в Первую мировую войну такое могло случиться из-за бесчисленных недоразумений, связанных с военной мобилизацией в России.

Пренебрежительное и халатное отношение к защите информации привело к трагическим событиям в августе 1914 г. — гибели российской армии Ранненкампа⁷.

Русский план ведения военной кампании против Германии предусматривал вторжение двух армий на территорию Восточной Пруссии. Армия под командованием генерала Ранненкампа должна была вести наступление строго в западном направлении и боевыми действиями сковывать немцев.

Перед армией генерала Самсонова, расположенной южнее, была поставлена задача обойти Мазурские болота, войти в тыл к немцам и, блокировав пути отхода, уничтожить их. Естественно, что ее успешное решение предполагало согласованное и тщательно спланированное взаимодействие двух русских армий.

Первую серьезную ошибку совершил начальник армейского шифровального бюро полковник Андреев, который вплоть до последней минуты перед началом боевых действий воздерживался от рассылки копий новых шифров, предназначенных для использования в период войны.

Когда армии Ранненкампа и Самсонова оказались разделенными Мазурскими болотами и стали связываться друг с другом преимущественно по радио, выяснилось, что в армии Ранненкампа новый шифр

⁷ Соболева Т. А. Указ. соч. С. 27.

получили, а старый уничтожили, а у Самсонова все еще действовал старый. В результате переговоры между армиями были вынуждены некоторое время вести по радио открытым текстом. Результатом стало полное уничтожение армии Ранненкамппа, спаслись лишь немногим более двух тысяч человек.

Хотя в начале войны Россия испытывала большие трудности в обеспечении своих войск всем необходимым, в том числе и средствами связи, уже в первой половине сентября 1914 г. ей удалось полностью снабдить их шифровальными средствами. Принятая шифросистема основывалась на многоалфавитном (полиалфавитном) шифре цифровой замены, метод вскрытия которого в то время уже был известен криптографической службе Австро-Венгрии. Стойкость применявшегося русскими многоалфавитного шифра усугублялась также непростительным упущением при использовании — разрешалось шифрование нескольких букв подряд по одной алфавитной подстановке. Неудивительно, что уже через пять дней после введения в русских войсках этого шифра 19 сентября молодой капитан отделения дешифровальной службы Австро-Венгрии Герман Покорный вскрыл эту систему, поскольку в шифротексте нередко сохранялась структура часто встречающихся в открытом тексте слов, таких как «атака», «дивизия», которые шифровали одной строкой таблицы. Кроме того, русские связисты поначалу вставляли открытый текст в зашифрованный. Вскоре одновременное использование открытых и зашифрованных текстов в сообщениях запретили, но было слишком поздно. В конце сентября 1914 г. криптосистема была взломана окончательно.

Облегчить процесс шифрования — достаточно логичное желание криптографов в мире, где потоки конфиденциальной информации стремительно возрастали. Интересные механические устройства стали появляться еще в начале XIX в. Например, президент США Томас Джефферсон предложил прибор, названный им «дисковым шифром», оказавшийся мощным инструментом шифрования. Его многоалфавитная подстановка была реализована в механизме из 36 дисков, насаженных на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. На ребрах каждого диска выписывались все буквы английского алфавита в произвольном порядке, различном на каждом из дисков. Шифрование осуществлялось группами по 36 символов открытого текста, который выставлялся путем поворота каждого диска в отдельности. В результате на одной линии выстраивался открытый текст, а зашифрованный образовывался путем считывания последовательности букв с любой линии, параллельной выделенной. Обратный процесс производился на анало-

гичном шифраторе: открытый текст отыскивался среди параллельных линий путем прочтения осмысленно возможного варианта. По достоинству изобретение своего президента американцы оценили лишь во время Второй мировой войны, назвав Джефферсона отцом американского шифровального дела.

Оказалось, что использование вращения дисков вокруг оси является наиболее удобным вариантом механических устройств шифрования так называемых дисковых шифраторов.

Одно из самых простых устройств было разработано в конце XIX в. во французской военной академии Сен-Сир, получившее название «Линейка Сен-Сира». Она представляет собой две шкалы с буквами алфавита, одна из которых движется относительно другой в соответствии с буквами ключа. Каждая новая буква ключа устанавливается напротив буквы «а» неподвижной шкалы, определяя тем самым новую подстановку для очередной буквы открытого текста. Таким образом, «линейка Сен-Сира» стала простым механическим воплощением «шифра Виженера», более удобным вариантом шифровального диска, предложенного в свое время Леоном Альберти.

XIX в. можно смело назвать эпохой механизации криптографии. Перечислить все устройства шифрования этого периода достаточно сложно, так как каждая страна создавала свои прототипы приборов, многие из них никогда не использовались, другие же получили широкую известность: шифратор Д. Уодсворта, шифратор Ч. Уитстона⁸.

В XX в. распространение беспроводной связи внесло свои коррективы в требования к секретной связи. Во-первых, возможности криптоанализа в корне изменили отношение к криптостойкости шифров. Условия, о которых впервые высказался Датчман А. Керкхофф, требовали создания надежных шифров, даже если априори противнику известен не только алгоритм шифрования, но и фрагменты открытого и закрытого текстов. Во-вторых, скорость передачи больших потоков информации на огромные расстояния требовала более быстрых процедур шифрования и дешифрования. Необходимость применения электромеханических устройств закономерно привела к рождению нового этапа в криптологии.

Можно предположить, что начало было положено изысканиями Гильберта Вернама. Он предложил использовать особенности телетайпного кода, где кодируемый знак выражается в виде пяти элементов⁹. Каждый из них символизирует наличие («плюс») или отсутствие («минус»)

⁸ Кан Д. Указ. соч. С. 22.

⁹ Сингх С. Указ. соч. С. 47.

электрического тока в линии связи. Таким образом, имеются 32 различные комбинации «плюсов» и «минусов», 26 из них должны соответствовать буквам, а оставшиеся обозначать различные «служебные комбинации» (пробел между словами, переход с букв на цифры и др.). Например, буква «А» выражается комбинацией «++---», букве «М» соответствует «--++-». Закодированное сообщение набивается на перфоленте: «плюсы» представляются отверстиями, а «минусы» их отсутствием. При считывании перфоленты металлические щупы проходят через отверстия, замыкают электрическую цепь и посылают импульсы тока по проводам. А там, где на перфоленте находится «минус», бумага не позволяет этим щупам замкнуть цепь, в результате токовый импульс не передается.

Г. Вернам предложил готовить перфоленту со случайными знаками (так называемую гамму) заранее и затем электромеханически складывать ее импульсы с импульсами знаков открытого текста. Полученная сумма представляла собой шифротекст, предназначенный для передачи по линии связи. Вернам сконструировал специальный механизм, который при шифровании суммировал импульсы электрически. Главное преимущество изобретенного метода заключалось в том, что он впервые сумел соединить два процесса — шифрование и передачу сообщения, привнеся тем самым в шифровальное дело автоматизацию. Другая идея Г. Вернама о возможности создания шифра, не поддающегося вскрытию в том случае, если используется случайная гамма длины, равная длине открытого текста, принесла ему мировую известность.

В 1917 г. компания «AT&T», в которой работал Вернам, передала результаты исследований майору Джозефу Моборну. Д. Моборн, занимавший тогда пост начальника отдела научно-исследовательских и конструкторских разработок войск связи США, был незаурядным криптоаналитиком. В то же время со своей группой криптоаналитиков он пришел к аналогичным выводам в отношении длины случайной гаммы.

Техническое устройство, реализующее в полной мере идеи Г. Вернама и Д. Моборна, создать в начале XX в. так и не удалось по причине невозможности генерации и применения случайной гаммы большой длины, однако изобретение одноразового шифроблокнота используется до сих пор.

Математические выводы о том, что предложенный Г. Вернамом метод шифрования с применением случайной гаммы при длине ключа, равной длине самого сообщения, является единственной абсолютно стойкой системой шифрования, были сделаны значительно позже другим известным американским ученым Клодом Шенноном. В настоящее время программно-аппаратные комплексы, основанные на генерации случай-

ной одноразовой последовательности, успешно используются в государственной связи, например, при проведении горячей линии между США и Россией.

Увы, в XX в. именно войны стали благодатной почвой для многих наук, криптология не стала исключением. Войны, будоражившие Европу с начала XIX в., стали катализатором разносторонних исследований, активизировавшихся в криптографии и криптоанализе. Поэтому неудивительно, что немалое количество изобретений электромеханических устройств за первые 20 лет XIX в. остались только на неоткрытых страницах истории. Другие, напротив, получили мировую известность, несмотря на свою тривиальность и слабую криптостойкость.

Продолжить летопись о шифровальных механизмах можно с изобретений американца Эдварда Хепберна, с 1912 по 1915 гг. им было подано несколько патентных заявок на различные шифровальные приборы.

Один из его механизмов состоял из двух электрических пишущих машинок, соединенных между собой 26 проводами. При нажатии какой-либо клавиши на одной машинке на другой печаталась буква шифротекста. Так как провода оставались подсоединенными к одним и тем же контактам на протяжении всего периода времени, в течение которого набирался открытый текст, то шифрование осуществлялось методом одноалфавитной замены. Несмотря на явные недостатки применяемого метода, изобретение Э. Хепберна было примечательно тем, что преобразование открытого текста в криптограмму выполнялось при помощи электрических импульсов, посылаемых по проводам.

Стремление Э. Хепберна получить устройство, реализующее более надежный шифр, в конце концов привело изобретателя к идее создания дискового шифратора. В 1918 г. этот прибор увидел свет. А в 1921 г. несколько машин приобрели ВМС США, в этом же году была основана фирма «Хепберн электрик код», ставшая первым производителем дисковых шифраторов в США. Но коммерческая деятельность Э. Хепберна потерпела неудачу — в 1926 г. предприятие было объявлено банкротом.

Два других дисковых шифратора, изобретенные в начале XX в., были запатентованы практически одновременно. Хьюго Александр Кох получил патент 7 октября 1919 г., а уже 10 октября был выдан документ на изобретение шведу Арвиду Герхарду Дамму.

Х. Кох увлекался конструированием различных диковинных приспособлений и справедливо полагал, что его новое устройство из области криптографии будет иметь коммерческий успех. Интересно, что сам изобретатель в своем патенте указал на возможность применения различных

материально-энергетических форм для передачи информации внутри своей секретной пишущей машинки. Он говорил, что проникающие лучи света и воздух, а также вода или масло, протекающие по трубкам, могут переносить шифрующий импульс так же хорошо, как и электричество, идущее по проводам. Также им было отмечено, что этот импульс обязательно должен двигаться через диск, а может проходить, например, по трубкам, просверленным в болванках, скользящих между неподвижными пластинами. Х. Кох отдавал предпочтение дисковому механизму, но не создал шифровальной машины в какой-либо из предложенных им в патенте форм. В 1922 г. в связи с тяжелой болезнью он передал все права на свои устройства другому немецкому изобретателю Артуру Шербиусу, имевшему степень доктора наук и ряд патентов, в том числе и в такой далекой от криптографии области, как керамика. А. Шербиус разумно остановился на идее электрической передачи сигнала в шифровальной машине как наиболее перспективной. Хотя его мысли об использовании луча света можно считать началом криптографии XXI в. — квантовой криптографии.

Первый вариант шифровальной машины А. Шербиуса состоял из ряда остроумно выполненных деталей, соединенных в огромную и сложную шифровальную машину. Основой изобретения стали три соединенных проводами узла: клавиатура для ввода каждой буквы открытого текста; шифратор, который зашифровывал каждую букву открытого текста в соответствующую букву шифротекста и индикаторное табло, состоявшее из различных ламп для высвечивания букв шифротекста. Чтобы зашифровать букву открытого текста, оператор нажимает на клавиатуре клавишу с нужной буквой открытого текста, которая посылает электрический импульс через центральный шифратор на противоположную сторону, где на панели с лампочками высвечивается соответствующая буква шифротекста. Шифратор — толстое колесо из резины, пронизанное проводами, являющееся важнейшей частью машины. Провода с клавиатуры входят в шифратор в шести точках, затем несколько раз изгибаются и выходят в шести точках на другой стороне. То, как провода идут внутри шифратора, и определяет, как будут зашифровываться буквы открытого текста. В других модификациях шифровальной машины А. Шербиус использовал для повышения криптостойкости два или три диска. Свое детище он назвал «Энигма» (от греч. *загадка*)¹⁰.

В середине 30-х гг. Гитлер приступил к перевооружению Германии, и эксперты-криптографы вермахта, решив, что «Энигма» обеспечивает

¹⁰ Кан Д. Указ. соч. С. 26.

достаточные гарантии в отношении безопасности связи, начали снабжать ею свои постоянно увеличивающиеся по численности вооруженные силы. На протяжении Второй мировой войны портативная, работавшая от батарей «Энигма» с загорающимися лампочками и в деревянном футляре, имевшая размеры и вес пишущей машинки, активно использовалась в армии, ВМС и ВВС нацистской Германии. Немецкие военные связисты считали ее очень надежной и полагали, что она обеспечивает необходимую безопасность связи. Однако совместными усилиями криптографов антигитлеровской коалиции удалось дешифровывать практически все сообщения, полученные с помощью шифровальной машины «Энигма». В основном заслуга в этом принадлежит английским и польским криптографическим службам.

Если А. Шербиусу удалось реализовать свою идею, то изобретения А. Дамма так и остались на бумаге, так как шифрующий механизм оказался громоздким и сложным. Дамм предложил шифровальное устройство, построенное из двух дисков: шифрдиски вращались над и под неподвижной горизонтальной пластиной. Движением шифродисков управляли зубчатые колеса, позволяющие поворачивать их на различное количество шагов для каждой буквы открытого текста. Тем не менее, единственная в мире компания АВ Cryptograph, которой удалось добиться значительного коммерческого успеха, была основана именно А. Даммом. Борис Цезарь Вильгельм Хагелин¹¹, работавший в фирме АВ Cryptograph, продолжил исследования Дамма. Первым его успехом в 1925 г. стало усовершенствование дискового шифратора, разработанного Даммом. Серия шифровальных устройств Б. Хагелина В-21 и В-211 была принята на вооружение Франции в середине 30-х гг., их сменили С-35 и С-36. Модернизированная модель С-38 была поставлена на вооружение шведской армии и заинтересовала США. Начало войны вынудило продолжить производство устройств С-38 уже в США, где они получили название Converter М-209 (эта версия имела небольшие конструктивные отличия от С-38). Шифровальная машина Converter М-209 массово использовалась армией США (в звене от батальона до дивизии) и на флоте в период Второй мировой войны, а также во время войны в Корее (1950–1953 гг.). Фирма, основанная Б. Хагелином, и по сей день (теперь она называется Crypto AG) является одним из крупнейших мировых производителей криптографической техники.

Для молодой Советской республики ситуация на криптографическом поприще складывалась критическая. В период с 1918 по 1920 гг.

¹¹ Сингх С. Указ. соч. С. 51.

почти все шифровальные сообщения Рабоче-крестьянской Красной армии и советской дипломатии успешно дешифровывались службами других стран.

К началу 30-х гг. положение изменилось к лучшему — для ручного шифрования были внедрены достаточно надежные системы и способы шифрования, но вопрос механизации самих процессов оставался открытым.

Основателем электромеханических шифровальных устройств в СССР по праву признан Иван Павлович Волосок¹². Многие образцы шифровальной и кодировочной техники довоенного и послевоенного периодов сконструированы по его проектам. В советской шифровальной технике за основу был взят принцип наложения комбинаций так называемой гаммы бесконечного ключа на комбинации знаков открытого текста. В итоге получалась нечитаемая криптограмма с гарантированной стойкостью. В качестве носителя знаков гаммы использовалась перфолента, изготовленная с помощью специального устройства, получившего название «Х». Это было оригинальным и удачным изобретением, позволяющим получать шифроленты с гаммой случайной последовательности, что обеспечивало необходимую гарантированную стойкость шифрования любых сообщений. Если вспомнить, то Г. Вернам не смог в полной мере реализовать свое изобретение шифрования телеграфных сообщений именно из-за проблемы генерации случайной гаммы большой длины. Советским инженерам это удалось. И уже в 1932 г. под руководством инженера И. П. Волоска был создан первый опытный образец советской шифровальной машины, получившей название «ШМВ-1». В том же году были разработаны опытные образцы механических шифрующих приспособлений к телеграфным аппаратам, которые не были изготовлены. В силу своей громоздкости и механической ненадежности «ШМВ-1» не пошла в серию, однако послужила прототипом для последующего создания новых серийных образцов. В 1934 г. на вооружение принимается электромеханическая шифровальная машина В-4, получившая впоследствии индекс М-100. Именно с нее начался отсчет создания серии шифровальных машин, обеспечивающих и поныне гарантированную стойкость применяемых шифров.

Шифровальная машина М-100 состояла из трех основных узлов (клавиатура с контактными группами, лентопротяжный механизм с трансмиттером и приспособление, устанавливаемое на клавиатуру пишущей машинки) и семи дополнительных. Общий вес комплекта достигал 141 кг. Дальнейшие усилия разработчиков были направлены на снижение веса

¹² Соболева Т. А. Указ. соч. С. 36.

и габаритов М-100. В итоге в 1943 г. была создана модель М-101 «Изумруд», которая была уменьшена более чем в шесть раз, а по весу — более чем в два. В этом же году в войска было отправлено свыше 90 ее комплектов. К тому времени там уже несколько лет успешно эксплуатировалась малогабаритная дисковая кодировочная машина К-37 «Кристалл», призванная заменить собой документы ручного кодирования в оперативном звене управления (армия — корпус — дивизия).

Надежность советских шифров была настолько высока, что вражеские криптографические службы с 1942 г. прекратили перехватывать наши сообщения, потеряв всякую надежду на их вскрытие.

Начиная с 50-х гг. криптография становится электронной. Это означает широкое применение средств электронной техники для построения систем шифров и их исследования. С 70-х гг. сфера применения криптографии расширяется, она становится гражданской отраслью. Это говорит о том, что криптографические средства начинают применяться для защиты коммерческой информации. Для этих целей 23 ноября 1976 г. в США был принят стандарт шифрования данных DES (Data Encryption Standard) с длиной ключа для коммерческого использования в 56 бит. Криптоалгоритм, принятый как американский стандарт шифрования симметричными ключами, был разработан немецким эмигрантом Хорстом Файстелем, переехавшим в Америку в 1934 г.¹³ Несмотря на постоянное давление со стороны Агентства национальной безопасности (далее — АНБ) США, под пристальным вниманием которых он постоянно находился, Файстелю удалось закончить работу по созданию криптоалгоритма, названного «Люцифер». Криптостойкость алгоритма превзошла все ожидания, поэтому АНБ потребовало принять систему «Люцифер» в качестве стандарта только при ограничении длины ключа в 56 бит. Это, в свою очередь, позволило бы АНБ применить в случае необходимости метод полного перебора для вскрытия криптограмм. С 2000 г. в качестве криптографического стандарта принят AES (Advanced Encryption Standard), который рассматривается в качестве кандидата на международный стандарт шифрования с симметричными ключами.

В 1973 г. английские ученые Джеймс Эллис и Клиффорд Кокс и несколько позже, в 1976 г., американские исследователи Уитфилд Диффи, Мартин Хеллман и Ральф Меркль сломали стереотипы в криптологии (считалось, что в криптографии все научные открытия уже произошли). Они предложили систему шифрования данных без использования секретных каналов связи для передачи ключа другому абоненту. Теперь для

¹³ Сингх С. Указ. соч. С. 58.

переписки достаточно было иметь открытый канал связи в целях обмена ключевой информацией. Такие системы шифрования называли криптосистемами с открытыми ключами.

Началась новая веха в развитии криптографии¹⁴.

Вопрос 2. Криптосистемы с секретным (симметричным) ключом

Современная криптография развивается в двух направлениях. Первое занимается исследованиями и разработками криптосистем с секретными (симметричными) ключами, объектами изучения другого являются криптоалгоритмы с открытыми ключами (асимметричные криптоалгоритмы). Развитие последнего обязано появлению и непрерывному совершенствованию компьютерной техники, что позволило для разработки криптографических методов использовать математический аппарат из таких разделов, как теория вероятности, статистика, алгебра, теория множеств и др.

Разделение криптографических методов на ручные (возможно использование без ЭВМ) и машинные (применяемые только на ЭВМ) произошло во второй половине XX в.

Ручные шифры применялись для преобразования текстов небольшого объема, многие из них используются до сих пор. Машинные криптографические методы изначально предназначались для обработки данных больших объемов на компьютере, причем неважно, буквы это, числа либо другие символы. Очевидно, что машинные шифры не могут заменить ручные, так как вычислительная сложность не позволяет использовать их для ручного шифрования.

Классическая модель криптосистемы с секретным (закрытым) ключом, представленная на рис. 1, практически не изменилась со времен ее изложения К. Э. Шенноном в статье «Communication Theory of Secrecy Systems», опубликованной в журнале «Bell System Technical Journal» в 1949 г.¹⁵

Важная часть такой системы — защищенный канал, по которому секретный (т. е. недоступный криптоаналитику противника) ключ Z , созданный в блоке «источник ключа», передается предполагаемому получателю. Для того чтобы подчеркнуть факт использования одного и того же

¹⁴ Шнайер Б. Прикладная криптография. М., 2017. С. 816.

¹⁵ С момента построения К. Э. Шенноном модели криптосистемы с секретными ключами до настоящего времени она практически не претерпела изменений, поэтому в некоторой литературе встречается название «шенноновская модель».

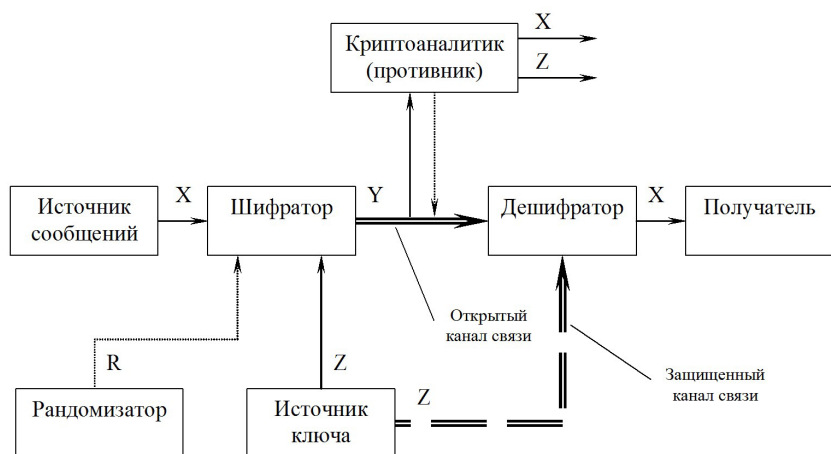


Рис. 1. Классическая модель криптосистемы с секретным ключом
 ключа в шифраторе и дешифраторе сообщений, криптосистемы с секретными ключами называют также одноключевыми или симметричными системами¹⁶.

Ключ Z образует k знаков, выбранных из некоторого алфавита с конечным числом символов (в машинных методах используют двоичный алфавит $\{0, 1\}$). Структурный блок источника сообщений создает открытый текст X , а шифратор образует криптограмму Y как функцию X, Z . Иными словами, в шифраторе по определенному алгоритму происходит шифрование информации X , поступившей из источника сообщений, с использованием секретного ключа.

Таким образом, любая криптосистема работает по следующей схеме: сообщение шифруется с помощью ключа, полученная шифровка передается по обычному открытому каналу связи получателю, в то время как ключ отправляется ему по защищенному каналу, гарантирующему секретность. Имея тот же ключ и криптограмму, получатель выполняет дешифрование и восстанавливает исходное сообщение. В зависимости от целей засекречивания эта схема может несколько видоизменяться. Так, в компьютерной криптографии встречаются случаи, когда отправитель и получатель — одно и то же лицо. Например, можно зашифровать данные, закрыв их от постороннего доступа при хранении, а когда это будет необходимо, расшифровать. В этом случае нередко роль закрытого канала связи играет память. Тем не менее налицо все элементы этой схемы.

¹⁶ Введение в криптографию : учебник / под общ. ред. В. В. Яценко. СПб., 2001. С. 61.

Ручные криптографические методы

Рассмотрим типовые способы криптографического закрытия информации и некоторые простые, основанные на них шифры (криптоалгоритмы).

К. Э. Шеннон выделил два общих принципа, применяемые в практических шифрах, — рассеивание и перемешивание.

Рассеивание — это распространение влияния одного знака открытого текста на много знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. Развитием этого принципа стало распространение влияния одного знака ключа на много знаков шифротекста, что предотвращает восстановление ключа по частям.

Перемешивание — это использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текста.

Добиться выполнения этих принципов нелегко, если учесть, что шифр должен не только затруднять раскрытие, но и обеспечивать легкость шифрования и дешифрования (при известном секретном ключе). Поэтому обычно (особенно в машинных криптоалгоритмах) достаточное рассеивание и перемешивание достигается в *комбинированных шифрах*, т. е. шифрах, реализующихся последовательностью простых криптографических методов, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемешивание.

Существующие ручные шифры подразделяются на два вида преобразований — *подстановки* и *перестановки*.

Подстановки

Моно- и многоалфавитные подстановки — это наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. В моноалфавитных подстановках применяется одна подстановка, в многоалфавитных — не менее двух различных подстановок.

Историческим примером метода моноалфавитной подстановки может служить шифр Гая Юлия Цезаря, пользовавшегося им для того, чтобы содержание его сообщений с арены боевых действий не стало известно противнику.

Представим себе одно из его возможных посланий. Используя подстановку Цезаря, шифротекст мог бы выглядеть так, как показано в правой части рис. 2.

Для того чтобы пользоваться шифром Цезаря, и отправитель и получатель шифровки должны иметь к ней так называемый секретный (тайный) ключ. В нашем примере ключ — это буква под номером «7» (буква «З»).

Отправитель сообщения создает шифротекст, просто складывая 7 с числами, соответствующими каждой букве шифротекста (рис. 3).

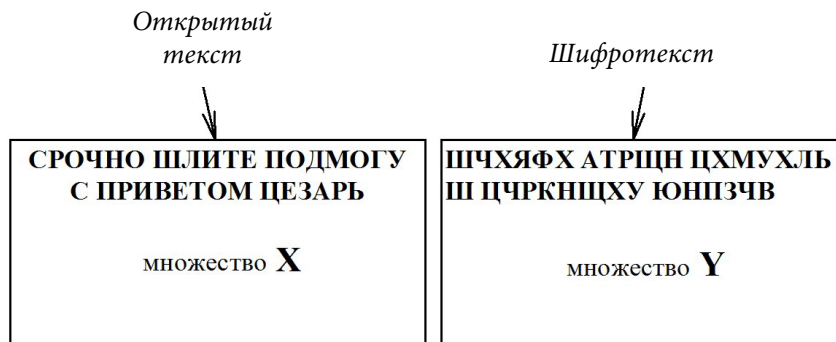


Рис. 2. Пример шифра Гая Юлия Цезаря

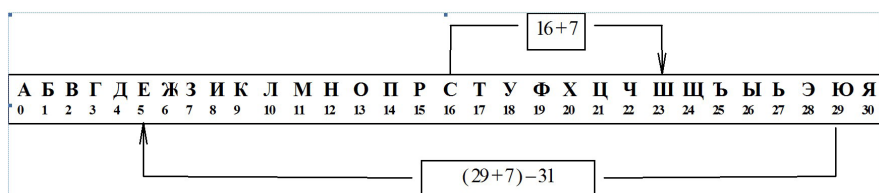


Рис. 3. Пример сдвига в шифре Цезаря с ключом «7»

Так, первая буква открытого текста «С» соответствует числу «16», складывая с «7», получаем число «23», которое соответствует букве «Ш» — первой букве шифротекста на рис. 2.

Обозначим числовой эквивалент элементов открытого текста как множество X , а шифротекста — как множество Y . Число «7», которое мы вычитали (сдвигали) из каждого a_i элемента множества X , чтобы получить шифротекст, называется коэффициентом сдвига K . Теперь представим подстановку Цезаря в математическом виде, а именно: $Y = (X + K) \bmod P$, что означает сложение $X + K$ по модулю P , где P — размер алфавита. Здесь $P = 31$. Такая операция обладает свойством циклического сдвига. В нашем случае, например, складывая 29(Ю) и 7, получим 5(Е). Почему буква Е?

В этом и заключается циклический сдвиг, т. е. если результатом обычного сложения получается число, большее, чем размер алфавита (>31), то недостающее мы восполняем переходом к началу алфавита. При обычном сложении $(29+7)$ получим 36. Вычитая 31 из 36 (размер алфавита P), имеем число 5 или букву Е.

Подстановка Цезаря является самым простым ее вариантом. Она относится к группе *моноалфавитных* подстановок и, как все из этой группы, считается нестойкой к частотному анализу. По этой причине была предложена модификация данного шифра — шифр *Гронсфельда*, который относится уже к *многоалфавитным* подстановкам.

Алгоритм Гронсфельда можно получить, если в преобразовании Цезаря применять для шифрования не постоянный коэффициент сдвига (в нашем примере — цифра 7), а ключ, состоящий из последовательности цифр. Знак в открытом тексте сдвигается на заданное цифрой в ключе значение, а для смещения следующего знака берется очередная цифра ключа.

Для шифрования под сообщением пишут ключ. Если ключ короче сообщения, то его повторяют циклически. Криптограмму получают аналогично шифру Цезаря, но сдвигая каждую букву на соответствующую цифру ключа, например, как при ключе 3712 и русском алфавите (рис. 3). Результат показан на рис. 4.

сообщение	С	О	В	Е	Р	Ш	Е	Н	Н	О	С	Е	К	Р	Е	Т	Н	О
ключ	3	7	1	2	3	7	1	2	3	7	1	2	3	7	1	2	3	7
шифротекст	Ф	Х	Г	З	У	Я	Ж	П	Р	Х	Т	З	Н	Ч	Ж	Ф	Р	Х

Рис. 4. Пример шифра Гронсфельда

Если в шифре Цезаря ключ выбирается случайным образом для преобразования каждого символа открытого текста, т. е. значение ключа применяется только однажды, то можно получить практически нераскрываемый криптоалгоритм.

Для такой системы подстановки используют также термин «одноразовый блокнот» или «шифр Вернама». Суть метода состоит в том, что ключ используется только один раз, при этом каждый символ (бит) шифруется новым случайным символом (битом) ключа. Это требует передачи по секретному каналу ключа, объем которого равен шифруемому затем тексту, однако это дает действительно нераскрываемый шифр. Вместе с тем стойкость шифра теряется при повторном использовании символов (битов) ключа.

Существуют системы, в которых требование шифровать каждый символ отдельным значением ключа снято. Такая схема шифрования основывается на таблице Виженера (рис. 5) и называется *подстановка Виженера*.

Таблица представляет собой квадратную матрицу с числом элементов S , где S — количество символов в алфавите. В первой строке матрицы записываются буквы в порядке очередности их в алфавите,

во второй — та же последовательность букв, но со сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д. Освободившиеся места справа заполняются вытесненными влево буквами, записываемыми в естественной последовательности (принцип циклического сдвига).

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
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
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
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
.																														
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

Рис. 5. Пример таблицы Виженера

Для шифрования текста устанавливается ключ, представляющий собой некоторое слово или набор букв. Далее из полной матрицы (рис. 5) выбирается подматрица шифрования, включающая, например, первую строку и строки матрицы, первым символом (буквой) которой являются последовательно расположенные буквы ключа, например МОРЕ. В итоге получается подматрица, изображенная на рис. 6.

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
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
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
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
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

Рис. 6. Подматрица шифрования, сформированная на основе таблицы Виженера

Процесс шифрования включает следующий порядок действий:

- под каждой буквой шифруемого текста записываются буквы ключа, повторяющие ключ требуемое число раз (рис. 7);

- шифруемый текст в подматрице заменяется буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки подматрицы и буквы ключа, находящейся под ней.

Так, под первой буквой шифруемого текста оказалась буква «М» ключа. В первой строке подматрицы находим букву «З» и выбираем из данной колонки подматрицы букву в той строке, начальный символ которой соответствует букве «М» ключа. Такой буквой оказалась буква «У» (рис. 7).

Далее выполняется замена исходной буквы «З» на «У» в выходном тексте. Выходной текст делится на группы, например, по четыре знака. Для этого алгоритма может быть составлена программа ЭВМ.

<i>Открытый текст</i>	ЗАЩИТА ИНФОРМАЦИИ
<i>Ключ</i>	МОРЕМО РЕМОРЕМОРЕ
<i>Текст после замены</i>	УОИОЭО ШТЯЫЯСМГШО
<i>Шифротекст</i>	УОИО ЭОШТ ЯЫЯС МГШО

Рис. 7. Пример шифрования текста

С одной стороны, раскрыть текст, полученный по данному алгоритму только на основе статистических характеристик языка, очень трудно, так как одни и те же символы открытого текста могут быть заменены различными символами шифрованного текста. С другой стороны, различные символы открытого текста могут быть заменены одинаковыми знаками шифрованного текста.

Для *дешифрования* необходимо знать ключ, который может быть введен пользователем со своего терминала или хранится в памяти ЭВМ в зашифрованном виде. Для шифрования ключа можно также использовать другую систему шифрования.

Расшифровка текста (рис. 8) выполняется в следующей последовательности:

- над буквами шифрованного текста сверху последовательности записываются буквы ключа;
- в строке подматрицы таблицы Виженера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста;
- полученный текст группируется в слова по смыслу.

<i>Ключ</i>	МОРЕ	МОРЕ	МОРЕ	МОРЕ
<i>Шифротекст</i>	УОИО	ЭОШТ	ЯЫЯС	МГШО
<i>Расшифрованный текст</i>	ЗАЩИ	ТАИН	ФОРМ	АЦИИ
<i>Исходный текст</i>	ЗАЩИТА ИНФОРМАЦИИ			

Рис. 8. Пример механизма дешифрования

Один из недостатков шифрования по таблице Виженера — это ненадежность шифрования при небольшой длине ключа и сложность формирования длинных ключей. Так как в ключе не допускается повторения букв (в противном случае шифрование будет неоднозначным), а сам

ключ должен легко запоминаться, последовательность букв, не имеющих определенного смысла, запомнить трудно.

Другой метод многоалфавитной подстановки — *двойной квадрат* (разработан Чарльзом Уитстоном), он более прост, но не менее надежен, чем подстановка Виженера.

Алгоритм шифрует *биграммами*, т. е. происходит замена не одного знака (как в других описанных методах), а двух знаков одновременно. *Двойной квадрат* использует две таблицы, расположенные по горизонтали. Приведем пример использования шифра *двойной квадрат* для русских текстов.

Имеются две таблицы со случайно размещенными в них алфавитами (рис. 9). Для шифрования сообщение разбивают на биграммы. Первая буква биграммы находится в левой таблице, а вторая в правой. Затем в таблице мысленно строится прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины прямоугольника дают буквы шифровки.

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

Рис. 9. Таблицы русского алфавита со знаками в случайном порядке

Применим шифр *двойной квадрат* для следующего открытого текста:
ЗА ЩИ ТА ИН ФО РМ АЦ ИИ

Процесс шифрования рассмотрим на биграмме «ТА». Буква «Т» находится в колонке 4 строки 5 левой таблицы; буква «А» — в колонке 3 строки 2 правой таблицы. Значит, прямоугольник образован строками 5 и 2, а также колонками 4 левой и 3 правой таблиц. Следовательно, шифровке соответствуют буквы, лежащие в колонке 4 строки 2 левой таблицы «Г» и в колонке 3 строки 5 правой таблицы «,». В результате биграмма «ТА» заменяется на биграмму «Г,». Так парами символов шифруется все сообщение:

УД ЖЧ Г, УЖ БК ИУ КС РЖ

Если обе буквы биграммы сообщения находятся в одной строке (биграмма «ЗА»), то и буквы шифровки берутся из этой же строки; первая буква биграммы шифровки — из левой таблицы в столбце, соответствующем второй букве биграммы сообщения; вторая же буква биграммы шифровки — из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Несомненно, шифрование биграммами дает простой и весьма устойчивый к вскрытию шифр. Взлом шифровки двойного квадрата требует больших усилий и длины сообщения более тридцати строк.

Другой метод повышения криптостойкости преобразования состоит в использовании *рандомизации* (от англ. *random* — случайный).

В естественных языках одни буквы встречаются чаще других (в английском это буква «е», в русском — буква «о»). Например, английский текст можно преобразовать в текст, содержащий символы большего алфавита путем замены буквы «е» случайными символами, выбираемыми из «е-группы» символов большего алфавита, а также замены других часто встречающихся английских букв случайными символами, выбираемыми из групп соответствующего размера. В полученном после рандомизации тексте все символы большего алфавита встречаются примерно с одинаковой частотой. Метод замены символов открытого текста случайно выбираемыми символами расширенного алфавита называется *рандомизацией*. Шифрование такого рандомизированного текста делает безрезультатными попытки раскрытия на основе анализа частот отдельных символов. Например, в произведении «Золотой жук» Э. По описывается успешное раскрытие криптограммы знаменитого пирата Кидда именно за счет исследования частоты букв английского алфавита. Однако после дешифрования законный получатель может снять рандомизацию, просто заменяя каждый символ из «е-группы» буквой «е», и т. д., иначе говоря, ему не нужно заранее сообщать, какие именно случайные замены будут сделаны. Такие рандомизированные шифры называют также *шифрами с многократной подстановкой* или *равночастотными шифрами*.

Перестановки

При перестановке перемешивают символы открытого текста, причем конкретный вид перемешивания определяет секретный ключ.

Этот несложный метод криптографического преобразования используется, как правило, в сочетании с другими.

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

Простейшим примером перестановки являются запись исходного текста по строкам некоторой матрицы (таблицы) и чтение его по столбцам этой матрицы. Последовательность заполнения строк и чтения столбцов может быть любой и задаваться ключом. Таким образом, для матрицы размерностью 8x8 (длина блока 64 символа) возможно $1,6 \times 10^9$ ключей, что позволяет на современных ЭВМ путем перебора расшифровать заданный текст. Однако для матрицы размерностью 16x16 (длина блока 256 символов) имеется $1,4 \times 10^{26}$ ключей, и перебор их с помощью современных средств довольно затруднителен.

Повысить сложность, а значит и стойкость перестановки по матрице можно при помощи специальной таблицы, в которую введены некоторые усложняющие элементы. Пример такой таблицы приведен на рис. 10.

КЛЮЧ									
2	6	1	3	8	0	5	9	4	7
д	л	я		№	м	у	д	р	о
	с	т	и	№	н	е		т	№
н	н	ч	е	г	о	№	н		е
н	а		в	и	с	т	н	е	е
№		х	и	т	р	о	с	т	и

Шифруемый текст

– неиспользуемые элементы;
 № – любой символ (буква).

Полученный шифротекст:
ятчх днн№ иеви ртет уе№то лсна о№ееи №№гит дннс мносп

Рис. 10. Пример усложненной перестановки по таблице

Как показано на рисунке, таблица представляет собой матрицу размером 10x10 элементов (размеры могут быть выбраны произвольно), в которую записываются знаки шифруемого текста. Отличие от обычной матрицы заключается в том, что определенное число клеток таблицы не используется (на рисунке они заштрихованы). Количество

и расположение неиспользуемых элементов является дополнительным ключом шифрования. Шифруемый текст блоками по $[m \times n - s]$ элементов ($m \times n$ — размеры таблицы, s — число неиспользуемых элементов) записывается в таблицу. В качестве разделителя между словами указан «N», в действительности им может быть любой символ (буква). Далее процедура шифрования состоит в том, что текст выписывается по столбцам в последовательности, которая определяется ключом. Зашифрованный текст показан на рис. 10.

При расшифровке знаки криптограммы (шифротекста) записываются столбцами таблицы в последовательности знаков ключа и с пропуском неиспользуемых элементов. Затем исходный текст считывается по строкам.

Варьируя размеры таблицы, последовательностью символов ключа, количеством и расположением неиспользуемых элементов, можно получить требуемую стойкость зашифрованного текста.

Еще одним примером применения метода перестановки может быть восьмиэлементная таблица, обладающая рядом маршрутов, носящих название маршрутов Гамильтона (рис. 11).

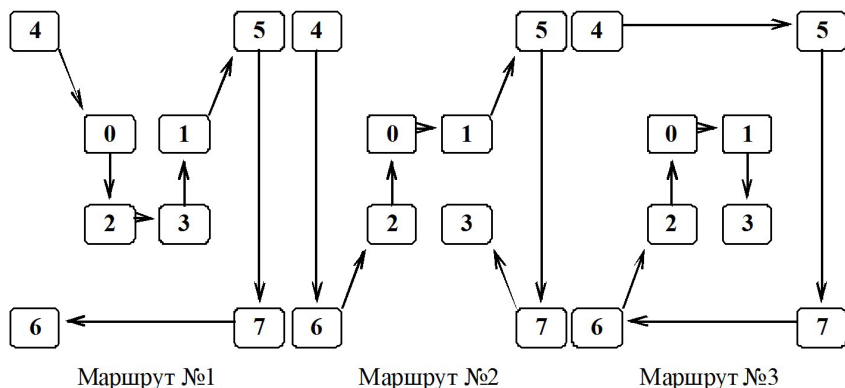
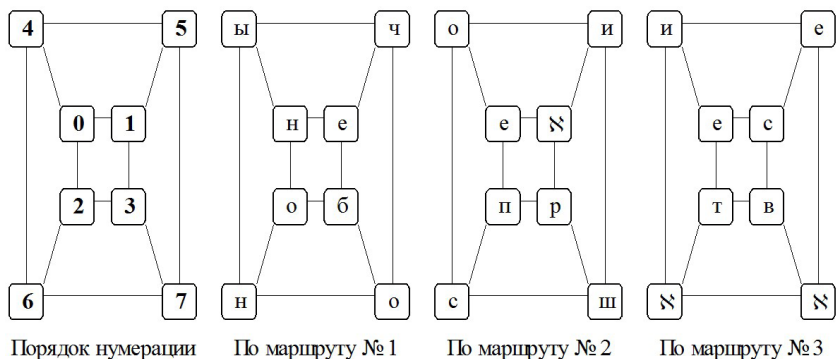


Рис. 11. Пример трех из возможных маршрутов Гамильтона

Их суть заключается в следующем: открытый текст разбивается на блоки по 8 символов в каждом (рис. 12). Элементы каждого блока нумеруются и вносятся в так называемый граф в соответствии с нумерацией элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы вписываются произвольные символы. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом. Марш-

руты (в нашем примере их три) используются в очередности, показанной на рис. 11. При дешифровании в соответствии с известными маршрутами получатель по блокам восстанавливает информацию.



Открытый текст	необычное происшествие		
Текст после перестановки	ынобечон	оспеишир	неиетесв

Рис. 12. Пример шифрования по таблицам Гамильтона

Интересный способ перестановки был изобретен известным математиком Джероламо Кардано. Метод, названный впоследствии перестановкой по маске (решетка Кардано), представляет собой квадратную таблицу, где четверть ячеек прорезана так, что при четырех поворотах они покрывают весь квадрат (рис. 13). Открытый текст разбивается на блоки размерностью квадрата. Вписывание в прорезанные ячейки текста и повороты решетки продолжают до тех пор, пока весь квадрат не будет заполнен, затем берется следующий блок текста, и заполнение квадрата начинается с нового листа. Например, на рис. 13 показаны положения квадрата в процессе шифровки решеткой 4x4. Отверстия в квадрате обозначены белым цветом, а повороты осуществляются по часовой стрелке на указанный угол.

Попробуем зашифровать текст «Я ем альфа и омега». Прежде избавимся от избыточности (устраним пробелы) «Яесмьальфаиомега».

Берем трафарет (4x4) и прикладываем к чистому листу бумаги в клетку. В отверстия квадрата вписываем первые четыре буквы открытого текста «Яесм», после этого трафарет поворачиваем по часовой стрелке на 90 градусов, и в отверстия вносим очередные четыре буквы текста. После полного оборота квадрата (если зашифрован не весь текст) берется следующий блок открытого текста и производится аналогичная процедура, но уже на другом чистом пространстве (рис. 13).

Сдвиг на 0°	Сдвиг на 90°	Сдвиг на 180°	Сдвиг на 270°	Результат																
				<table><tr><td>я</td><td>м</td><td>ф</td><td>ь</td></tr><tr><td>а</td><td>е</td><td>л</td><td>с</td></tr><tr><td>а</td><td>е</td><td>и</td><td>г</td></tr><tr><td>а</td><td>м</td><td>ь</td><td>о</td></tr></table>	я	м	ф	ь	а	е	л	с	а	е	и	г	а	м	ь	о
я	м	ф	ь																	
а	е	л	с																	
а	е	и	г																	
а	м	ь	о																	

Рис. 13. Пример шифрования по маске (решетке Кардано) с квадратом 4x4

В заключение криптограмма записывается в строку по строкам или по столбцам шифр-квадрата. Например, по столбцам получим шифр в конечной форме: яааа меем флиь ьсго.

По указанной причине пробелы в шифре также опускаются.

Число подобных решеток быстро растет с их размером. Так, решетка 2x2 единственна, решеток 4x4 уже 256, а решеток 6x6 свыше 100 тыс.

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

Существуют и другие способы перестановки, которые можно осуществить программным и аппаратным путем. Например, реализованный аппаратным путем блок перестановки, который для преобразования информации использует электрические цепи, по которым она передается параллельным способом. Преобразование текста заключается в «перепутывании» порядка разрядов в цифровой кодограмме путем изменения электрического монтажа схемы в блоке. Для дешифрации на приемном пункте устанавливается другой блок, восстанавливающий порядок цепей.

Машинные криптографические методы

Ранее упоминалось о такой же актуальности ручных шифров, как и машинных. В связи с этим симметричные криптоалгоритмы (обзор будет представлен в этом подразделе) рассматриваются как современные именно с точки зрения хронологии. В отличие от ручных шифров, машинные шифры — это результаты научных исследований XX в.

Машинные шифры предполагают производство электронных вычислений программным, аппаратным или программно-аппаратным способами, а значит, оперируют данными в двоичном виде.

Ярким примером машинных шифров является криптоалгоритм DES (DataEncryptionStandart), который был создан фирмой IBM, и в 1976 г. принят Национальным институтом стандартов и технологий (National Institute of Standards and Technology) в качестве Стандарта Правительства США для шифрования информации почти самой высокой категории — «less-than-top-secret». С тех пор он повторно сертифицировался в качестве такого стандарта каждые пять лет вплоть до 1998 г.¹⁷

Криптоалгоритм DES построен на комбинированном использовании методов гаммирования¹⁸, перестановки и подстановки¹⁹.

Изначально DES создавался блочным шифром²⁰ с блоками фиксированной длины в 64 бита и длиной секретного ключа в 56 битов.

За основу DataEncryptionStandart принят шифр, разработанный Хорстом Фейстелем. Иммигрировавший в США перед Второй мировой войной из Германии, он долгое время не мог найти работу, так как, будучи специалистом в области криптографии, постоянно находился под пристальным вниманием АНБ (США), а вплоть до января 1944 г. — под домашним арестом. Во время военных действий всегда присутствует риск вербовки мигрантов противоположной стороной, поэтому крупные компании, работающие на оборонную промышленность США, в трудоустройстве ему отказывали.

В послевоенные годы Х. Фейстелю удалось предложить компании IBM свой блочный шифр для внедрения в новую серию компьютеров, названный, как упоминалось ранее, впоследствии шифром Люцифера.

¹⁷ Сингх С. Указ. соч. С. 176.

¹⁸ Суть метода гаммирования состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой. Отсюда и название метода — гаммирование.

¹⁹ Все известные современные симметричные стандарты шифрования используют в своих алгоритмах комбинацию из простейших методов, DES не является исключением.

²⁰ Блочные шифры — это последовательность (с возможным повторением и чередованием) основных методов преобразования, которая применяется к следующим друг за другом блокам шифруемого текста. Причем для шифрования используется один ключ, но независимо для каждого блока. В поточных шифрах осуществляется (в отличие от блочных) поэлементное шифрование открытого текста. В общем случае каждый символ открытого текста шифруется, передается и дешифруется независимо от других символов.

Высокая скорость шифрования и проверенная надежность метода позволили выиграть конкурс на принятие его в качестве стандарта симметричного шифрования в США. Однако длина ключа в 128 бит у шифра Люцифера в алгоритме DES была сокращена до 56 бит, так как правительство США посчитало неприемлемым использование высоконадежного метода для коммерческих целей.

Несмотря на интенсивные и тщательные исследования алгоритма DES криптоаналитиками, пока не найдено его уязвимых мест, на основе которых можно было бы предложить метод криптоанализа, существенно лучший, чем полный перебор ключей.

Однако в 1998 г. Национальный институт стандартов и технологий США отказался сертифицировать DES. Это было связано с тем, что уровень развития вычислительной техники сделал возможным вскрытие DES (с длиной секретного ключа 56 бит) относительно дешевыми техническими средствами.

В результате в настоящее время алгоритм DES уже не считается надежным, и в качестве наиболее простой альтернативы ему предлагается алгоритм Triple DES (другое обозначение — 3DES), использующий ключ длиной в 112 бит.

Важным достоинством DES является его высокая производительность. Так, DES быстрее алгоритмов с асимметричными ключами той же криптостойкости, что и DES, в десятки и сотни раз, а в сравнении с Triple DES — примерно в три раза.

Алгоритм Triple DES использует ключ, состоящий из двух ключей DES и имеющий три шага. На первом шаге с помощью первого ключа и алгоритма DES шифруется 64-битный блок открытого текста. Полученная криптограмма на втором шаге шифруется вторым ключом. На последнем шаге результат шифрования, полученный на втором шаге, вновь шифруется с помощью первого ключа и алгоритма DES. Полученный 64-битный блок является криптограммой Triple DES. Таким образом, алгоритм Triple DES требует трехкратного использования DES, отсюда и происходит его название.

В настоящее время DES в классическом виде упоминается лишь в учебниках по криптографии и встречается в лабораторных работах студентов технических специальностей. Но алгоритм, названный в честь его разработчика сетью Фейстеля, используется во многих действующих шифрах (DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA и др.).

Обратимся к особенностям этого алгоритма, рассмотрев его в классическом виде на шифровании блоков открытого текста в 64 бит

и длиной ключа в 56 бит (рис. 14). Алгоритм формируется из ячейки Фейстеля, повторяющейся несколько раз (раундов). Ячейка Фейстеля — это следующая последовательность действий: блок в 64 бит разбивается на два равных — левый L_0 и правый R_0 . Правый блок R_0 и ключ K_1 используются в вычислениях функции F , которая зависит от метода шифрования. Полученный после вычисления функции F результат складывается по модулю два (обозначается $\oplus$) с левым блоком L_0 (остававшийся без изменений) и переносится на место правого блока, исходный блок R_0 — на место левого блока. После чего получившиеся левый L_1 и правый R_1 присоединяются друг к другу. В DES ячейка Фейстеля повторяется 16 раундов. В других методах повторение различно. Блок, полученный на выходе предыдущей ячейки Фейстеля, поступает на вход следующей.

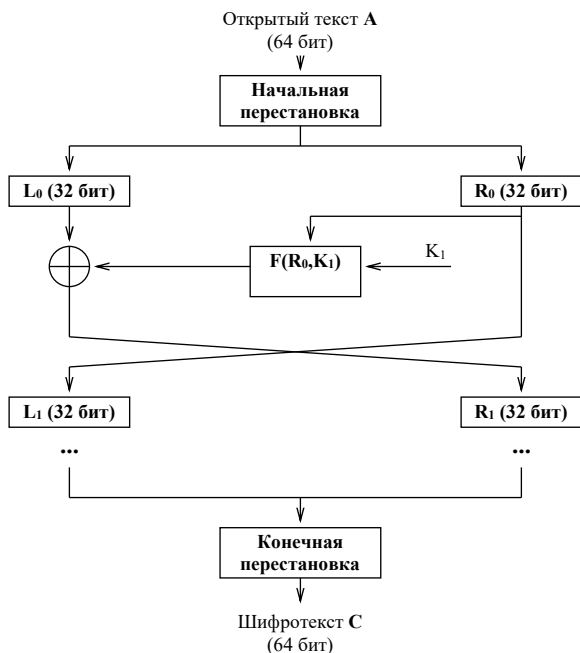


Рис. 14. Сеть блочного шифрования (64 бит) Фейстеля

Следуя примеру США в разработке открытого Национального стандарта шифрования, в 1989 г. Государственный стандарт шифрования данных для сетей ЭВМ приняли в СССР. Он получил обозначение ГОСТ 28147-89 и имел гриф «Для служебного пользования» до конца существования самого СССР. В Российской Федерации он был принят

официально с 1992 г. как Стандарт шифрования данных наряду с другими бывшими стандартами СССР. Стандарт был формально объявлен полностью открытым в мае 1994 г. Стандарт ГОСТ 28147-89 так же, как и DES, является блочным шифром. Длина блока информации составляет также 64 бит, а длина ключа равняется 256 бит, что значительно повысило криптостойкость криптоалгоритма.

Примерно в это же время был разработан и опубликован альтернативный алгоритму DES проект открытого национального стандарта шифрования данных Японии, получивший обозначение FEAL. Это также блочный шифр с блоком данных и ключом в 64 бит каждый. Однако ни он, ни какой-либо другой алгоритм так и не приняты до настоящего времени в качестве национального стандарта шифрования Японии.

В 1990 г. К. Лэй и Дж. Мэсси (Швейцария) предложили проект международного стандарта шифрования данных, получивший обозначение IDEA (International Data Encryption Algorithm)²¹, который международным криптографическим сообществом оценивается довольно высоко и за последние годы усилиями международных организаций по стандартизации (прежде всего европейских) активно выдвигался на роль официального общеевропейского стандарта шифрования данных. Длина ключа алгоритма IDEA равна 128 бит для шифрования блока длиной в 64 бит. Алгоритм будет оставаться стойким к взлому на протяжении нескольких ближайших десятилетий.

Алгоритм IDEA использует три группы операций — побитовое сложение по модулю 2, сложение по модулю 2^{16} , умножение по модулю $2^{16}+1$. Операции производятся над блоками длиной в 16 битов, получающимися в результате деления шифруемого блока на 4 подблока. Алгоритм является циклическим (используется 8 циклов преобразований). Алгоритм IDEA запатентован в США и большинстве европейских стран. Держателем патента выступает компания Ascom-Tech. Алгоритм IDEA быстрее Triple DES, но медленнее DES.

Другой известный алгоритм Skipjack был разработан АНБ (США). В нем применяется ключ длиной в 80 бит и используется 32 цикла на каждую операцию криптографического преобразования.

Криптоалгоритм Skipjack предназначался для того, чтобы по решению суда предоставить правоохранительным органам беспрепятственный доступ к шифруемой информации. В этих целях в специальном микрочипе используется алгоритм Skipjack с двумя ключами. Знания одного из ключей (мастер-ключа) достаточно, чтобы дешифровать любое сооб-

²¹ Шнайер Б. Указ. соч. С. 356.

щение, зашифрованное с помощью этого микрочипа. При изготовлении микросхемы этот мастер-ключ разделялся на две половины, подлежащие хранению в государственных организациях. Если правоохранные органы получают необходимую санкцию в суде, они могут запросить обе половины ключа и считать любую информацию, шифруемую с помощью соответствующей микросхемы. В настоящее время можно утверждать, что идея проекта провалилась. В то же время известно, что АНБ использует алгоритм Skipjack для шифрования собственных сообщений. Это подтверждает высокий уровень криптостойкости алгоритма.

Для быстрого шифрования больших объемов информации Роном Райвестом были разработаны алгоритмы RC2 и RC4 — шифры с переменной длиной ключа. Они быстрее, чем DES, и способны повышать степень защиты за счет выбора более длинного ключа. RC2 — блочный алгоритм, и его можно применять как альтернативу DES. RC4 представляет собой потоковый шифр и работает почти в 10 раз быстрее DES²².

Как уже упоминалось, алгоритм DES отказались сертифицировать вновь в 1998 г., поэтому начались поиски нового стандарта.

После нескольких лет обсуждений 2 октября 2000 г. американский Национальный институт стандартов и технологий утвердил вместо DES новый стандарт блочного симметричного алгоритма шифрования AES (Advanced Encryption Standard)²³. У нового стандарта есть все предпосылки стать международным, поскольку он был принят на основе открытого конкурса, в котором участвовали алгоритмы, предложенные математиками из многих стран (США, Канады, Австралии, Бельгии, Германии, Норвегии, Франции, Южной Кореи, Японии и даже Коста-Рики). Алгоритм Rijndael был подвергнут скрупулезному анализу не только специалистами Национального института стандартов и технологий и АНБ США, но и их конкурентами, среди которых были самые блестящие криптографы и криптоаналитики мира. Однако никому не удалось выявить уязвимые места этого алгоритма.

Rijndael может работать с ключами длиной в 128, 192 и 256 бит, поэтому в обозримом будущем он защищен от атак методом полного перебора всех возможных ключей. Кроме того, алгоритм сочетает в себе высокое быстроедействие и умеренные требования к памяти. Поэтому он может

²² Там же. С. 357.

²³ Известный также как Rijndael, он был разработан бельгийскими криптографами Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen). Название алгоритма образовано из первых букв фамилий его авторов, поэтому в транскрипции с фламандского оно произносится примерно как «рэндал».

быть реализован в самых различных устройствах, включая SIM мобильного телефона и смарт-карты. И наконец, Rijndael не защищен патентами и доступен для свободного использования в любых продуктах.

В 2015 г. принят новый стандарт по протоколам симметричного шифрования в Российской Федерации ГОСТ 34.12.2015 — «Криптографическая защита информации. Блочные шифры». Новый стандарт рассматривает алгоритм блочного шифрования с длиной блока 128 бит (популярное название «Кузнечик») и алгоритм блочного шифрования с длиной блока в 64 бит (популярное название «Магма»).

Криптоалгоритм «Кузнечик» основан на подстановочно-перестановочной сети (SP-сеть — Substitution-Permutation network). Открытый текст разбивается на блоки по 128 бит и генерируется ключ длиной 256 бит (мастер-ключ). Мастер-ключ, разделенный на две половины, формирует два первых раундовых ключа, остальные раундовые ключи вычисляются с помощью известной нам сети Фейстеля, на вход которой подаются первые два раундовых ключа.

Сам метод шифрования «Кузнечик» состоит из полных девяти раундов преобразований и неполного десятого. В каждом раунде SP-сеть включает в себя три этапа шифрования.

1. Операция сложения по модулю двураундового ключа K_i и входного блока данных X .

2. Операция нелинейного преобразования (S -преобразование), представляющая замену одного байта другим в соответствии с таблицей шифрования (рис. 15) и дешифрования (рис. 16).

3. Операция линейного преобразования, заключающаяся в умножении в поле Галуа всех 16 байт блока поочередно, начиная с 15 до 0, на один из коэффициентов ряда (148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194, 16, 133, 32, 148, 1). Сумма 16 байт по модулю 2 записывается на место старшего байта при сдвиге всех остальных в сторону младшего байта.

Десятый раунд включает только первый этап шифрования.

Криптоалгоритм «Магма» заимствован из предыдущего ГОСТ 28147-89 блочного шифрования с разбиением открытого текста на блоки по 64 бит и длиной мастер-ключа в 256 бит. «Магма» основан на сети Фейстеля с повторяющейся ячейкой в 32 раунда (рис. 14). Отличие нового ГОСТ 34.12.2015 от утратившего силу ГОСТ 28147-89 состоит в статически определенной в новом стандарте таблицы перестановки нелинейного биективного преобразования²⁴. При биективном отображении

²⁴ Ершов Ю. Л., Палютин Е. А. Математическая логика : учеб. пособие. 3-е стереотип. изд. СПб., 2004. С. 336.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	252	238	221	17	207	110	49	22	251	196	250	213	35	197	4	77
16	233	119	240	219	147	46	153	186	23	54	241	187	20	205	95	193
32	249	24	101	90	226	92	239	33	129	28	60	66	139	1	142	79
48	5	132	2	174	227	106	143	160	6	11	237	152	127	212	211	31
64	235	52	44	81	234	200	72	171	242	42	104	162	253	58	206	204
80	181	112	14	86	8	12	118	18	191	114	19	71	156	183	93	135
96	21	161	150	41	16	123	154	199	243	145	120	111	157	158	178	177
112	50	117	25	61	255	53	138	126	109	84	198	128	195	189	13	87
128	223	245	36	169	62	168	67	201	215	121	214	246	124	34	185	3
144	224	15	236	222	122	148	176	188	220	232	40	80	78	51	10	74
160	167	151	96	115	30	0	98	68	26	184	56	130	100	159	38	65
176	173	69	70	146	39	94	85	47	140	163	165	125	105	213	149	59
192	7	88	179	64	134	172	29	247	48	55	107	228	136	217	231	137
208	225	27	131	73	76	63	248	254	141	83	170	144	202	216	133	97
224	32	113	103	164	45	43	9	91	203	155	37	208	190	229	108	82
240	89	166	116	210	230	244	180	192	209	102	175	194	57	75	99	182

Рис. 15. Таблица нелинейных замен при шифровании

каждому элементу одного множества соответствует ровно один элемент другого множества, при этом определено обратное отображение, которое обладает тем же свойством. Мастер-ключ для получения раундовых ключей делится на 8 частей по 32 бита, в каждом раунде поочередно используется одна из 8 частей, повторяясь по циклу (три раза с 8-го по первый, последний раз — с первого по 8-й). В каждой ячейке Фейстеля после сложения по модулю 2 блока открытого текста (32 бита) с очередным раундовым ключом результат делится на 8 4-битных блоков, каждый из которых по таблице перестановки нелинейного биективного преобразования заменяется соответственно на другое 4-битное число. Далее после циклического сдвига влево на 11 разрядов результат складывается по модулю 2 со вторым блоком открытого текста (32 бит). Левый и правый блоки меняются местами, затем начинается следующий раунд ячейки Фейстеля.

В настоящее время используются не только криптоалгоритмы «Кузнецик» и «Магма», но и метод шифрования по предыдущему ГОСТ 28147-89.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	165	45	50	143	14	48	56	192	84	230	158	57	85	126	82	145
16	100	3	87	90	28	96	7	24	33	114	168	209	41	198	164	63
32	224	39	141	12	130	234	174	180	154	99	73	229	66	228	21	183
48	200	6	112	157	65	117	25	201	170	252	77	191	42	115	132	213
64	195	175	43	134	167	177	178	91	70	211	159	253	212	15	156	47
80	155	67	239	217	121	182	83	127	193	240	35	231	37	94	181	30
96	162	223	166	254	172	34	249	226	74	188	53	202	238	120	5	107
112	81	225	89	163	242	113	86	17	106	137	148	101	140	187	119	60
128	123	40	171	210	49	222	196	95	204	207	118	44	184	216	46	54
144	219	105	179	20	149	190	98	161	59	22	102	233	92	108	109	173
160	55	97	75	185	227	186	241	160	133	131	218	71	197	176	51	250
176	150	111	110	194	246	80	255	93	169	142	23	27	151	125	236	88
192	247	31	251	124	9	13	122	103	69	135	220	232	79	29	78	4
208	235	248	243	62	61	189	138	136	221	205	11	19	152	2	147	128
224	144	208	36	52	203	237	244	206	153	16	68	64	146	58	1	38
240	18	26	72	104	245	129	139	199	214	32	10	8	0	76	215	116

Рис. 16. Таблица нелинейных замен при дешифровании

В нем таблица нелинейного преобразования не была принудительно задана, что позволяет создавать собственные таблицы преобразований, конфиденциальность которых может способствовать повышению стойкости криптоалгоритма. Для коммерческих организаций участие в создании нелинейного преобразования по ГОСТ 28147-89 предоставляло гарантии отсутствия скрытых функций в криптоалгоритме.

Введение в криптоанализ

Задача стеганографии, как мы знаем, состоит в изобретении метода сокрытия сообщения. Причем обнаружение факта передачи стеганограммы уже означает нестойкость всей стегосистемы.

В криптографии обнаружение криптоаналитиком канала передачи сообщений допускается изначально (см. рис. 1 на стр. 27). Кроме того, при разработке криптоалгоритмов используют допущения О. Керкхоффа²⁵.

1. Криптоаналитик противника имеет полный текст криптограммы.

2. Стойкость шифра должна определяться только секретностью ключа, т. е. весь механизм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.

Если криптограф принимает только эти два допущения, то он разрабатывает систему, стойкую при анализе *на основе только шифрованного текста*.

К современным криптосистемам требования повысились и выражаются в дополнительных допущениях.

3. Если в дополнение к первым двум допущениям криптограф предполагает, что криптоаналитик противника сможет достать (тем или иным способом) несколько отрывков открытого текста и соответствующего ему шифрованного текста, образованного с использованием секретного ключа, принято считать, что система стойкая при анализе *на основе открытого текста*.

4. Криптограф может даже допустить, что криптоаналитик противника способен ввести свой открытый текст и получить правильную криптограмму, образованную с использованием секретного ключа (анализ *на основе выбранного открытого текста*), или предположить, что криптоаналитик противника может подставить фиктивные криптограммы и получить текст, в который они превращаются при расшифровании (анализ *на основе выбранного шифротекста*), или допустить обе эти возможности (анализ *на основе выбранного текста*).

²⁵ Введение в криптографию. С. 90.

Разработчики большинства современных шифров обеспечивают их стойкость к анализу на основе выбранного открытого текста даже в том случае, когда предполагается, что криптоаналитик противника сможет прибегнуть к анализу на основе шифротекста.

Из правил О. Керкхоффа следует, что криптоаналитику могут быть известны все детали процессов шифрования и дешифрования, кроме, разумеется, всего открытого текста X и особенно секретного ключа Z .

Основываясь на модели криптосистемы (рис. 1), К. Э. Шеннон рассмотрел задачу о стойкости криптографических систем с двух точек зрения. Сначала он поставил вопрос о теоретической стойкости: насколько надежна некоторая система, если криптоаналитик противника не ограничен временем и обладает всеми необходимыми средствами для анализа криптограмм. Отвечая на этот вопрос, К. Шеннон вывел два положения криптографии.

Первое положение в вопросе о **теоретической стойкости** заключается в том, что *секретный ключ используется только один раз*, т. е. после зашифрования M знаков открытого текста X нужно заменить секретный ключ Z .

Второе положение состоит в том, что *криптоаналитику доступна только криптограмма Y , и поэтому он может предпринять лишь анализ на основе шифротекста*.

Решение вопроса о теоретической стойкости вносит ясность в криптографию, но приводит к пессимистическому выводу: объем секретного ключа для построения теоретически стойкого шифра недопустимо велик для большинства применений. В связи с этим К. Шеннон рассмотрел также и вопрос о **практической стойкости**: надежна ли система, если криптоаналитик располагает ограниченными временем и вычислительными возможностями для анализа перехваченных криптограмм.

Он показал возможность создания таких практически надежных систем, для которых раскрытие секретного ключа криптоаналитиком противника требует физически нереализуемых затрат. Среднее время работы, необходимое для нахождения (раскрытия) ключа на основе шифротекста определенной длины, Шеннон предложил измерять в удобных единицах, например, в *часах вычислений на конкретной ЭВМ*.

Таким образом, *стойкость большинства практических шифров должна опираться не на теоретическую невозможность их раскрытия, а на практическую сложность такого раскрытия*.

Кроме проблемы создания надежных шифров в системах с симметричными ключами (рис. 1) существует еще одна — *обеспечение защи-*

ты передачи секретных ключей по защищенным каналам получателю, так как если криптоаналитику противника удастся перехватить секретный ключ при его передаче по каналу связи получателю, то все меры по повышению надежности шифра теряют всякий смысл.

Общих методов криптоанализа не существует как для ручных, так и для машинных шифров, а большинство методов вскрытия ручных криптоалгоритмов практически неприменимо в исследовании машинных криптосистем, и наоборот.

Развитие криптографии почти всецело обязано открытиям в математике. Поиски синтеза лингвистики и математики ведутся давно и безуспешно. Такие исследования актуальны не только для криптографии, но и для сжатия, хранения больших объемов данных на современных носителях информации, а также в разработке новых методов синтеза и распознавания речи. Поэтому криптография как объект пристального изучения математиков обычно тоже формулируется в виде математической задачи. Особенность заключается в том, что применение того или иного метода не всегда дает однозначное решение. Исходные данные в криптоанализе сугубо индивидуальны при раскрытии конкретного шифра. Но, как уже упоминалось, всегда считаются известными тип криптоалгоритма и язык открытого текста.

После сбора исходных данных (куда, естественно, входит сама криптограмма), выдвигаются гипотезы (предположения), а затем применяются методы вскрытия для доказательства и извлечения открытого текста. Однако нельзя забывать, что профессионализм (знания в теории чисел, дискретной математики, теории сложности, абстрактной алгебры, статистики, алгоритмического анализа и пр.) и интуиция криптоаналитика играют важную роль.

Процесс криптоанализа всякий раз начинается при подходе к новой системе, и опыт, полученный при раскрытии одной системы шифрования, редко когда может быть применен для раскрытия другой.

Машинные методы криптоанализа не могут полностью заменить человека (особенно при раскрытии ручных шифров), а лишь помогают автоматизировать процесс статистической обработки больших объемов шифротекста.

Можно выделить три направления в методах анализа — методы полного или частичного перебора, специализированные, статистические (частотные).

Различные способы перебора, как правило, применяют для поиска секретного ключа в машинных шифрах. Полный перебор ключа на практике

применяется редко, так как при большой длине ключа это влечет большие вычислительные затраты. Напоминаем, что обязательно должны быть известны метод шифрования и, желательно, длина ключа. Часто выгоднее осуществлять подбор ключа по словарю, в который предварительно заносят наиболее употребительные в качестве паролей слова (или сочетания символов). Недостаток словарного перебора лишь один: если значения секретного ключа нет в словаре, то время потрачено напрасно. Хотя, по исследованиям психологов, большинство выбранных людьми ключей тривиальны.

Специализированные методы разрабатываются индивидуально и основываются на недостатках (погрешностях) того или иного метода шифрования.

Статистические (частотные методы) имеют важное значение при вскрытии ручных и машинных шифров. Их идея проста. Общеизвестно, что у каждого языка речи есть свои особенности построения слогов, слов и предложений. Кроме того, разные символы (буквы) встречаются в сообщениях с определенной частотой, а значит, количество информации, передаваемой разными знаками, неодинаково. Например, ни для кого не секрет, что в русской речи буква «о» употребляется чаще, чем «ь», а буква «и» чаще, чем «щ». То или иное сочетание двух символов (биграммы) также повторяется в тексте неравномерно, некоторые вовсе не встречаются (ТТ; ЪФ; ЧБ, ЯА и др.). Существуют таблицы вероятностей появления отдельных знаков²⁶ и биграмм русского языка (нередко применяются и таблицы вероятности наиболее употребительных слов), которые являются обязательным инструментом криптоаналитика (приложение 1). Безусловно, можно сделать вывод, что в криптограммах должны каким-то образом отражаться закономерности, присутствующие в открытом тексте.

Статистический анализ нельзя назвать универсальным методом, но он значительно облегчает задачу вскрытия шифра, обнаруживая те или иные закономерности, имеющиеся в шифротексте.

Особенностью криптоанализа ручных шифров является зависимость конечного результата от объема исследуемой криптограммы. Увы, но короткие сообщения обычно не поддаются расшифровке, так как в них очень сложно проследить зависимости открытого текста и шифра. Необходимо также учесть, что на практике не всегда верны предположения Керкхофа об известной информации. В приложении 2 приведен занимательный пример криптоанализа шифра князей Барятинских, в котором подробно описывается последовательность вскрытия шифра подстановки.

²⁶ Цымбал В. П. Теория информации и кодирования. Киев, 1977. С. 206.

Об эффективности применения частотного анализа при вскрытии шифров одноалфавитной замены говорят подробные описания на страницах арабских книг IX в. Вместе с тем непосредственное применение частотного анализа для криптоанализа криптограмм, полученных шифрами многоалфавитной подстановки, не дает положительного результата.

Однако анализ шифров многоалфавитной подстановки все же возможен. Например, один из специализированных методов вскрытия шифра Виженера предложил Ч. Бэббидж²⁷. Алгоритм его криптоанализа можно представить в следующем виде.

Этап 1. Определение длины ключа

1. Отыскиваем последовательности букв, которые появляются в шифротексте более одного раза.

Существуют две причины, почему могут возникнуть такие повторения. Первая, и наиболее вероятная, состоит в том, что одна и та же последовательность букв в открытом тексте была зашифрована с помощью одной и той же части ключа. Но есть также определенная, хотя и незначительная, вероятность того, что две разные последовательности букв в открытом тексте, зашифрованные различными частями ключа, случайно образуют идентичные последовательности в шифротексте. Если ограничиться только длинными последовательностями, например, состоящими из четырех или более букв, то вторая причина станет практически нереализуемой и ею можно пренебречь.

2. Определяем величину интервала между повторениями, т. е. находим, через сколько символов криптограммы встречается последовательность. Например, последовательность из четырех символов WGXT повторяется через 20 символов, символы FSOL — через 30 символов, а символы NMRP — через 25 и т. д.

3. Находим множители полученных интервалов, т. е. вычисляем, какие числа делят полученные интервалы нацело. Например, 20 делится нацело на 1, 2, 4, 5, 10, 20; число 30 — на 1, 2, 3, 5, 6, 10, 15, 30; число 25 — на 1, 5, 25.

4. На основе анализа множителей определяем общий множитель для всех повторяющихся последовательностей. Значение найденного множителя будет определять длину ключа. В нашем примере общими множителями являются 1, 2 и 5. Выбор криптографом секретного ключа длиной 1 или 2 маловероятен, поэтому можно предположить, что длина ключа равна 5. Первый этап криптоанализа окончен.

²⁷ Сингх С. Указ. соч. С. 201.

Этап 2. Определение букв ключа

Обозначим ключевое слово в виде $X_1 - X_2 - X_3 - X_4 - X_5$, где X_1 будет первой буквой ключевого слова, X_2 — второй и т. д. Тогда процесс шифрования начнется с шифрования первой буквы открытого текста в соответствии с первой буквой ключевого слова X_1 . Буква X_1 определяет строку матрицы Виженера и тем самым задает одноалфавитную подстановку для первой буквы открытого текста. Когда наступает время для шифрования второй буквы открытого текста, криптограф должен использовать X_2 , чтобы определить другую строку матрицы Виженера, задавая уже иной одноалфавитный шифр замены. Третья буква открытого текста будет зашифровываться в соответствии с X_3 , четвертая — в соответствии с X_4 , а пятая — в соответствии с X_5 . Каждая буква ключевого слова задаст для шифрования свой, отличающийся шифралфавит. Но затем шестая буква открытого текста будет шифроваться в соответствии с X_1 , седьмая — в соответствии с X_2 и так далее по циклу. Другими словами, в нашем случае многоалфавитный шифр состоит из пяти одноалфавитных, причем каждый одноалфавитный шифр отвечает за шифрование 1/5 части всего сообщения.

Как проводить криптоанализ одноалфавитных шифров, нам уже известно. Достаточно выписать все символы криптограммы, соответствующие при шифровании строке матрицы Виженера при ключе X_1 , и применить частотный анализ для полученной последовательности, зашифрованной шифром простой одноалфавитной замены. Аналогичным образом применяется частотный метод для последовательности, соответствующей при шифровании строке матрицы Виженера при ключе X_2 , затем X_3 , X_4 и X_5 .

Таким образом, поиск повторов в шифротексте позволил нам определить длину ключевого слова, в приведенном примере он состоит из пяти символов. Это позволило разделить шифротекст на пять частей, где каждая зашифрована с помощью шифра одноалфавитной замены, который определяется одним символом ключевого слова. С помощью частотного анализа определяем последовательно символы секретного ключа.

Вскрытие современных машинных шифров часто сводится к полному перебору секретного ключа, что связано со сложной комбинацией простых методов криптографии, реализация которых возможна только средствами вычислительной техники. Однако статистические исследования также могут дать важную информацию о машинном шифре, правда, анализ криптограммы в машинных кодах не может определить лингвистические особенности рассматриваемого шифра.

Вопрос 3. Криптосистемы с открытым ключом

В рассмотренных симметричных криптосистемах один и тот же ключ используется для шифрования и дешифрования. Это значит, что первоначально ключ должен быть передан через секретные каналы так, чтобы обе стороны могли иметь его до того, как зашифрованные сообщения будут посылаться по обычным каналам. Это может создавать различного рода неудобства. Однако если вы имеете секретный канал для обмена ключами, тогда зачем вам нужна криптография?

Криптосистемы, не требующие наличия секретного канала связи для предварительного обмена закрытыми ключами, называются криптосистемами с открытыми ключами. Основные концепции криптографии с открытым ключом (или асимметричной криптографии) были разработаны У. Диффи и М. Е. Хеллманом (W. Diffie and M. E. Hellman) и опубликованы ими в 1976 г.²⁸ Первым примером криптографической системы с открытым ключом является алгоритм RSA, названный так по первым буквам фамилий авторов Р. Райвеста, А. Шамира и Л. Адельмана (R. Rivest, A. Shamir, L. Adelman). Алгоритм, разработанный ими в 1977 г., основан на применении так называемых односторонних математических функций, особенностью которых является то, что для нахождения одного из трех параметров, участвующих в вычислениях, необходимо выполнить задачу разложения на простые сомножители (факторизации) очень больших чисел. В основе всех известных алгоритмов с открытым ключом лежит та или иная математическая идея, требующая привлечения огромных вычислительных мощностей для своего решения. Именно наличие такой проблемы не позволяет злоумышленникам определить закрытый ключ по открытому. Математиками доказано, что это трудновыполнимая задача, даже с применением огромных вычислительных ресурсов.

Классическая схема криптосистемы с асимметричными ключами отображена на рис. 17. Главная идея криптографической системы с открытым ключом заключается в том, что каждый пользователь имеет два однозначно взаимосвязанных ключа: публикуемый *открытый ключ* (public key) и *закрытый (секретный) ключ* (private key), сохраняемый втайне. Причем закрытый ключ дешифрует код, созданный с помощью открытого ключа. Открытый ключ может публиковаться и свободно распространяться через коммуникационные сети, а знание открытого ключа не позволяет вам вычислить соответствующий секретный ключ. Такой

²⁸ Шнайер Б. Указ. соч. С. 37.

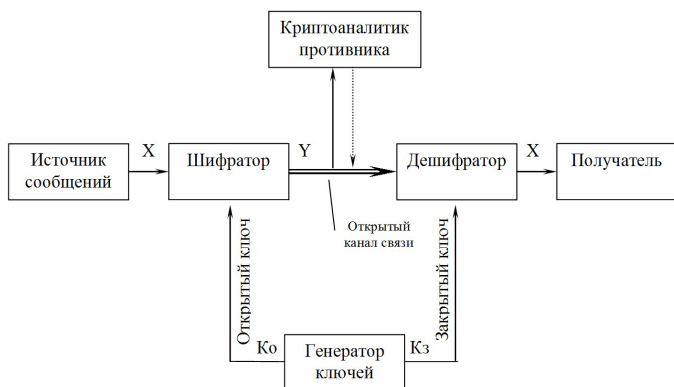


Рис. 17. Схема криптосистемы с открытыми ключами

способ обеспечивает секретность, без необходимости использования специальных каналов связи, обязательных для симметричных криптографических систем.

Абонент X может использовать открытый ключ абонента Y, чтобы зашифровать ему сообщение, а абонент Y использует соответствующий собственный закрытый ключ для расшифровки сообщения от абонента X. Никто не может расшифровать сообщение, адресованное абоненту Y, кроме него самого, потому что только он имеет доступ к закрытому ключу. Что немаловажно, абонент A также не имеет возможности расшифровать сообщение, посланное абоненту Y.

Если ключ для шифрования сообщений распространяется открыто, то любой желающий может воспользоваться им, для того чтобы зашифровать сообщение, адресованное владельцу закрытого ключа. Зашифрованное сообщение можно выслать владельцу ключа даже по незащищенной сети. Для того чтобы расшифровать его, нужно знать закрытый ключ, который известен только адресату. Владения открытым ключом для расшифровки недостаточно, и злоумышленник, перехватив сообщение и не зная закрытого ключа, не сможет его прочесть.

Интуитивно ясно, что закрытый ключ должен быть связан с открытым ключом и теоретически может быть восстановлен по нему. Но практически задача восстановления закрытого ключа по открытому настолько сложна, что может считаться неразрешимой. Например, она может требовать привлечения огромных вычислительных ресурсов.

В другом случае, когда ключ для шифрования сообщений хранится в секрете, а ключ для дешифрования распространяется открыто, получаем вместо схемы шифрования интересную схему аутентификации.

Напомним, что механизмы *идентификации*, *аутентификации* и *авторизации* нужны для подтверждения подлинности субъекта и определения законности прав на действия с объектом. *Идентификация* (именование и опознавание) — процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации. Каждый субъект или объект системы должен быть однозначно идентифицируем. *Аутентификация* (подтверждение подлинности) — это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы, а также целостности и авторства данных при их хранении или передаче для предотвращения несанкционированной модификации. *Авторизация* — это предоставление субъекту прав на доступ к объекту (объектам).

Вернемся к простейшей схеме аутентификации на основе асимметричных криптоалгоритмов. Сообщение, подлинность которого нужно подтвердить, снабжается подписью, содержащей имя автора. Затем автор шифрует сообщение вместе с подписью своим закрытым ключом. Все желающие могут расшифровать сообщение с помощью открытого ключа предполагаемого автора и, посмотрев на подпись, удостовериться в подлинности полученных данных. Но не зная секретного ключа, никто не сможет фальсифицировать подобную подпись. Существуют и более сложные схемы аутентификации, не требующие шифрования всего сообщения с помощью открытого ключа.

Используемый в информационно-вычислительных сетях процесс подтверждения подлинности подсоединившихся пользователей на базе криптографии с открытым ключом обладает одним важным свойством. Он не позволяет отправителю отказаться от факта отправки предъявленного сообщения. Дело в том, что сообщение могло быть зашифровано только отправителем, так как никто, кроме него, не знает закрытого ключа и, следовательно, не может фальсифицировать корректное (проходящее проверку целостности) сообщение.

Недостатком всех известных криптографических алгоритмов с открытым ключом является их медлительность. Они на два-четыре порядка медленнее, чем аналогичные алгоритмы с секретным ключом (в зависимости от алгоритма и реализации). Поэтому широкое распространение получили смешанные схемы, в которых алгоритмы с открытым ключом используются на этапе установления соединения для аутентификации атрибутов сторон и для обмена секретным ключом, который в дальнейшем используется для шифрования и аутентификации сообщений.

Некоторые сведения из математики

Фундаментальным понятием в криптосистемах с открытыми ключами, как уже упоминалось, является определение односторонней функции.

Односторонней (необратимой) называется функция, обладающая двумя свойствами²⁹:

- a) существует полиномиальный алгоритм вычисления $F(x)$;
- b) не существует полиномиального алгоритма инвертирования функции F (т. е. решения уравнения $F(x)=y$ относительно x). Другими словами, можно вычислить $F(x)=y$, если известен x , но нельзя вычислить x , если известен y .

В действительности создание всех криптоалгоритмов с открытыми ключами основано на представлении о *функциях с секретом* (другое название — функции с ловушкой). *Функцией с секретом K* называется функция $F_k: X \rightarrow Y$, зависящая от параметра k и обладающая тремя свойствами:

- a) существует полиномиальный алгоритм вычисления значения $F_k(x)$ для любых k и x ;
- b) не существует полиномиального алгоритма инвертирования функции F_k при неизвестном k ;
- c) существует полиномиальный алгоритм вычисления значения F_k при известном k .

Вопрос о существовании односторонних функций и функций с секретом пока открыт. Для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом. Для них свойство b пока строго не доказано, но считается, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче.

Современные асимметричные криптоалгоритмы базируются на сложности решения следующих математических задач.

1. Задача разложения на множители (факторизации) большого простого числа. Нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Примером метода, основанного на сложности решения задачи факторизации, может служить алгоритм RSA.

2. Задача нахождения дискретного логарифма. С точки зрения вычислительной сложности достаточно легко выполнить операцию возве-

²⁹ Нечаев В. И. Элементы криптографии (Основы теории защиты информации) / под ред. В. А. Садовниченко. М., 1999. С. 76.

дения в степень в конечном поле, но для решения обратной задачи (поиска дискретного логарифма) потребуется практически полный перебор элементов поля. На сложности решения задачи логарифмирования основаны алгоритмы Эль-Гамала, Диффи-Хеллмана.

3. Сложность декодирования в некоторых кодах, исправляющих ошибки, велика: достаточно легко получить кодовое слово (перемножить матрицы), но по кодовому слову найти базовое — задача вычислительно трудная. Этот метод редко используется на практике (известна криптосистема McEliece, применяющая коды Тонна).

Для описания возможных областей применения асимметричных криптоалгоритмов нам потребуется знание некоторых определений и свойств из теории чисел.

Начнем с определения *взаимно простых чисел*. Целые числа a и b называются *взаимно простыми*, если $(a, b) = 1$. Иными словами, это числа, у которых нет общих делителей, отличных от 1 и -1 ³⁰.

Также отметим свойство, что два числа a и b являются взаимно простыми тогда и только тогда, когда найдутся целые числа u и v , такие что $au + bv = 1$.

Следующее определение — это определение *сравнения двух чисел*. Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Говорят, что число a сравнимо с b по модулю m , если a и b при делении на m дают одинаковые остатки и записывают: $a \equiv b \pmod{m}$.

Ясно, что число a сравнимо с b по модулю m тогда и только тогда, когда $a - b$ делится на m нацело. Очевидно, что это бывает тогда и только тогда, когда найдется такое целое число t , что $a = b + mt$. Также можно сказать, что сравнимость a с b по модулю m означает, что a и b представляют один и тот же элемент в кольце $\mathbb{Z}_m$.

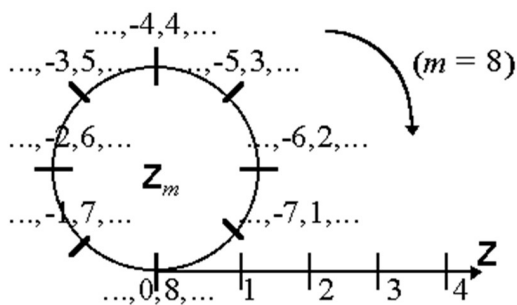


Рис. 18. Классы чисел, сравнимых по модулю 8

³⁰ Виноградов И. М. Основы теории чисел. М., 1972. С. 56.

На рис. 18 представлен пример, который прекрасно поясняет в графическом виде процесс получения классов сравнимых между собой по модулю m . Изображен процесс «наматывания» цепочки целых чисел на колечко с m -делениями, при этом на одно деление автоматически попадают сравнимые между собой числа.

Примеры криптоалгоритмов с открытыми ключами

Здесь в краткой форме опишем два наиболее известных асимметричных алгоритма RSA (название образовано по первым буквам фамилий авторов: R. Rivest, A. Shamir, L. Aldeman) и Эль-Гамала.

Первой в мире криптосистемой стала система RSA, математическая схема которой была разработана в 1977 г. в Массачусетском технологическом институте (США) и запатентована в США в 1982 г. Алгоритм RSA основан на трудности решения задачи разложения на простые сомножители больших целых чисел³¹.

Пусть m и e натуральные числа. Функция f , реализующая схему RSA, устроена следующим образом:

$$f: x \rightarrow x^e \pmod{m}. \quad (1)$$

Для дешифрования сообщения $a = f(x)$ достаточно решить сравнение:

$$x^e \equiv a \pmod{m}. \quad (2)$$

При некоторых условиях на m и e это сравнение имеет единственное решение x . Для описания этих условий необходима функция Эйлера. Эта функция натурального аргумента m обозначается $\varphi(m)$ и равняется количеству целых чисел на отрезке от 1 до m , взаимно простых с m (например, при $m=12$, $\varphi(m)=4$, а при $m=11$, $\varphi(m)=10$). Так $\varphi(1)=1$ и $\varphi(p^r)=p^{r-1}(p-1)$ для любого простого числа p и натурального r . Кроме того, $\varphi(ab)=\varphi(a)\varphi(b)$ для любых натуральных взаимно простых a и b . Эти свойства позволяют легко вычислить значение $\varphi(m)$, если известно разложение числа m на простые сомножители.

Если показатель степени e в сравнении (2) взаимно прост с $\varphi(m)$, то сравнение (2) имеет единственное решение. Для того чтобы найти его, определим целое число d , удовлетворяющее условиям:

$$de \equiv 1 \pmod{\varphi(m)}, \quad 1 \leq d < \varphi(m). \quad (3)$$

Такое число существует, поскольку $(e, \varphi(m))=1$. Здесь и далее символом (a, b) будет обозначаться наибольший общий делитель чисел a

³¹ Введение в криптографию. С. 176.

и b . Классическая теорема Эйлера³² утверждает, что для каждого числа x , взаимно простого с m , выполняется сравнение $x^{\varphi(m)} \equiv 1 \pmod{m}$ и, следовательно,

$$a^d \equiv x^{de} \equiv x \pmod{m}. \quad (4)$$

Следовательно, в предположении $(a, m) = 1$ единственное решение сравнения (2) может быть найдено в виде:

$$x \equiv a^d \pmod{m}. \quad (5)$$

Таким образом, процедура передачи сообщений защищенной схемой RSA заключается в следующем.

1. Выбираются два достаточно больших простых числа p и q , примерно одинаковых по величине, произведение которых является m .

2. Определяется $\varphi(m) = \varphi(pq) = (p-1)(q-1)$.

3. Выбирается e в соответствии с условием $(e, p-1) = (e, q-1)$.

4. Из сравнения (2) находится закрытый ключ d .

5. Публикуются в качестве открытого ключа значения m и e , d остается в секрете.

6. Шифрование исходного сообщения x осуществляется с помощью выражения (1).

7. Дешифрование криптограммы a осуществляется из (3).

Приведем пример шифрования по схеме RSA с небольшими простыми числами $p=211$ и $q=223$, тогда $m=47053$, а $\varphi(m)=46620$. Открытый ключ $e=16813$. Из (3) вычисляем закрытый ключ $d=19837$. В качестве исходного текста возьмем RSA, примем соответствие буквам следующие коды R=18, S=19, A=1, причем каждой букве отводится 5 бит, тогда $x = 1 \cdot 32^2 + 19 \cdot 32^1 + 18 \cdot 32^0 = 1650$.

Криптограмму вычисляем из (1), т. е.:

$$a = x^e \pmod{m} = 1650^{16813} \pmod{47053} = 3071.$$

Дешифрование осуществляется с помощью (5)

$$x = 3071^{19837} \pmod{47053} = 1650.$$

Рассмотрим второй алгоритм с открытыми ключами — схему Эль-Гамала (EGS), криптостойкость которого гарантируется сложностью решения задачи нахождения дискретного логарифма. Алгоритм был разработан в 1984 г. американцем Т. Эль-Гамалем. Этот алгоритм не защищен патентом, что стало одним из доводов, использованных в августе 1991 г. Национальным институтом стандартов и технологий США

³² Там же.

для обоснования выбора алгоритма EGS в качестве основы для национального стандарта DSA (Digital Signature Algorithm) перед комиссией Конгресса США.

Процедура алгоритма достаточно проста: допустим, абоненту А необходимо отправить сообщение абоненту В³³.

1. Задается большое простое число p , которое публикуется (т. е. оно известно обоим абонентам).

2. Абонентом А генерируется в качестве закрытого ключа случайное число x из интервала $(1, p)$, а абонентом В — аналогичное число y из того же интервала.

3. Открытое сообщение S шифруется абонентом А: $S1 = S^x \pmod{p}$, полученная криптограмма $S1$ отправляется абоненту В.

4. Криптограмма $S1$ шифруется абонентом В: $S2 = S1^y \pmod{p}$, полученная криптограмма $S2$ отправляется абоненту А.

5. Абонентом А вычисляется $S3 = S2^{-x} \pmod{p}$ (тем самым устраняется участие закрытого ключа x в криптограмме) и отправляется абоненту В.

6. Криптограмма $S3$ расшифровывается абонентом В из выражения $S = S3^{-y} \pmod{p}$. Результатом является открытое сообщение S .

Залогом криптостойкости алгоритма Эль-Гамала является трудность вычисления дискретного логарифма $\log_S S1$ для вскрытия закрытого ключа x .

Несмотря на то что, по оценке математиков, решить задачу вычисления дискретного логарифма намного сложнее, чем задачу разложения большого целого числа на простые множители (схема RSA), у алгоритмов, подобных схеме Эль-Гамала, вскрытие закрытого ключа одного абонента повлечет угрозу раскрытия всех абонентов криптографической сети. А в схеме RSA пострадает только тот абонент, закрытый ключ которого был подвержен атаке и раскрыт.

Схемы аутентификации на основе криптоалгоритмов с открытыми ключами

Криптосистемы с открытыми ключами в настоящее время предложено применять в трех направлениях:

- 1) как самостоятельные средства защиты передаваемых и хранимых данных;
- 2) как средства аутентификации пользователей и сообщений;
- 3) как средства распределения ключей.

³³ Шнайер Б. Указ. соч. С. 405.

Благодаря разработке средств аутентификации пользователей и сообщений на основе криптосистем с открытыми ключами, стало возможным предотвратить многие действия злоумышленника.

1. *Отказ* — абонент А заявляет, что он не посылал сообщение абоненту В, хотя на самом деле посылал.

2. *Модификация* — абонент В изменяет сообщение и утверждает, что данное (измененное) сообщение посылал ему абонент А.

3. *Подделка* — абонент В формирует сообщение и утверждает, что данное (измененное) сообщение послал ему абонент А.

4. *Активный перехват* — абонент D перехватывает сообщения между абонентами А и В в целях их скрытой модификации.

5. *Маскировка (имитация)* — абонент D посылает абоненту В сообщение от имени абонента А.

6. *Повтор* — абонент D повторяет ранее переданное сообщение, которое абонент А посылал ранее абоненту В.

Рассмотрим классические схемы аутентификации абонентов и сообщений (так называемые схемы аутентификации Шнорра).

Задача *аутентификации абонента* заключается в том, что абонент А доказывает свою подлинность, а абонент В должен ее проверить. Допустим, что абонент А имеет открытый ключ y и закрытый ключ x . Фактически абоненту А необходимо доказать, что он знает x , и сделать это таким образом, чтобы это доказательство можно было проверить, зная только открытый ключ y .

Схема *аутентификации Шнорра*³⁴ позволяет решить эту задачу следующим образом.

1. Выбираются большие простые числа p и q , такие, что q делит $p-1$. А также g таково, что $g^q = 1 \pmod{p}$, $g \neq 1$.

2. В качестве закрытого ключа абонентом А выбирается случайное число x из $\{1, \dots, q-1\}$.

3. Абонентом А вычисляется $y = g^x \pmod{p}$ и публикуется открытый ключ y .

4. Абонентом А выбирается случайное число k из множества $\{1, \dots, q-1\}$, вычисляется $r = g^k \pmod{p}$, затем r посылается абоненту В.

5. Абонентом В выбирается случайное e из множества $\{1, \dots, 2^t-1\}$, где t — некоторый параметр, и отправляется абоненту А.

6. Абонентом А вычисляется $s = (k + xe) \pmod{q}$ и отправляется абоненту В.

³⁴ Введение в криптографию. С. 13.

7. Абонентом В проверяется соотношение $r = g^s y^e \bmod p$ и, если оно выполняется, доказательство принимается, иначе — отвергается.

Схема аутентификации сообщений выполняет функцию *электронной подписи* (ЭП), которая по сути является подписью документа в электронном виде. Причем электронная подпись имеет ряд свойств.

1. Подписывать документ может только обладатель закрытого ключа, т. е. подделать подпись невозможно.

2. Проверить подлинность подписи может любой абонент, знающий открытый ключ.

3. При возникновении споров отказаться от подписи невозможно, так как ее нельзя подделать.

4. Подписанные электронные документы можно, не опасаясь ущерба, пересылать по любым каналам связи.

Теперь рассмотрим *схему электронной подписи Шнорра*, обладающей всеми этими свойствами.

1. Выбираются большие простые числа p и q , такие, что q делит $p-1$. А также g таково, что $g^q = 1 \pmod p$, $g \neq 1$.

2. В качестве закрытого ключа подписывающим выбирается случайное число x из $\{1, \dots, q-1\}$.

3. Подписывающим вычисляется $y = g^x \bmod p$ и публикуется открытый ключ y .

4. Подписывающим выбирается случайное число k из множества $\{1, \dots, q-1\}$, вычисляется $r = g^k \bmod p$.

5. Подписывающим вычисляется $e = h(r, m)$, где m — подписываемое сообщение; h — *хэш-функция*, позволяющая после преобразования сообщения любой длины получить последовательность одинаковой длины.

6. Подписывающим вычисляется $s = (k + xe) \bmod q$ и отправляется сообщение m с подписью (e, s) получателю.

7. Получателем вычисляется соотношение $r' = g^s y^e \bmod p$ и проверяется, выполняется ли равенство $e = h(r', m)$. Если да, то подпись принимается, в противном случае — отвергается.

Кроме представленных схем аутентификации Шнорра существует ряд ее модификаций, а также другие схемы, в том числе основанные на алгоритме RSA³⁵.

Заслуживает внимания еще одно направление использования асимметричных криптоалгоритмов — *электронные деньги*. Исследования в этой области ведутся на протяжении последних 30 лет, и безуспешно.

³⁵ Шнайер Б. Указ. соч. С. 410.

Как правило, под *электронными деньгами* понимают электронные платежные средства, обеспечивающие неотслеживаемость.

Для работы с электронными деньгами разрабатываются специальные криптографические протоколы, называемые протоколами электронных платежей. В таком протоколе задействованы три участника, которых мы будем называть банк, покупатель и торговое предприятие (далее — ТП). Покупатель и ТП, каждый имеют счет в банке, и покупатель желает заплатить ТП за товар или услугу.

В платежной системе используются три основные транзакции:

- снятие со счета;
- платеж;
- депозит.

В транзакции *снятия со счета* покупатель получает подписанную банком электронную банкноту на затребованную сумму. При этом счет покупателя уменьшается на эту сумму. В транзакции *платежа* покупатель передает банкноту ТП и указывает сумму платежа. ТП, в свою очередь, передает эту информацию банку, который проверяет подлинность банкноты. Если банкнота подлинная, банк проверяет, не была ли она потрачена ранее. Если нет, то банк заносит банкноту в специальный регистр, зачисляет требуемую сумму на счет ТП, уведомляет ТП об этом, и если достоинство банкноты выше, чем сумма платежа, возвращает покупателю сдачу (через ТП). С помощью транзакции *депозита* покупатель может положить сдачу на свой счет в банке.

Безопасность банка основывается на невозможности подделать его подпись для создания фальшивой банкноты или, другими словами, на невозможности, получив набор подлинных электронных банкнот, подделать подпись еще хотя бы для одной банкноты. Для неотслеживаемости покупателя необходимо, чтобы банк, получив банкноту в транзакции платежа, не мог установить, кому она была выдана. То же относится и к «сдаче». Это парадоксальное требование удовлетворяется с помощью схемы так называемой затемненной (слепой) подписи: в транзакции снятия со счета банк подписывает не банкноту, а некоторую «абракадабру», из которой покупатель восстанавливает подписанную банкноту. Таким образом, неотслеживаемость гарантируется тем, что банк просто не знает, что именно он подписал. Реализация идеи электронных денег основана на тех же свойствах аутентификации, что были указаны выше, с той лишь разницей, что теперь участников в схеме уже трое. Хотя существуют и варианты автономных систем электронных наличностей, одна из них использует схему

аутентификации абонента Шнорра. В данном случае протокол электронных платежей не предполагает третьего участника в схеме платежа — так называемые децентрализованные (пиринговые) платежные системы. На основе пиринговых платежных систем построено большинство современных криптовалют.

Из этого следует, что все электронные платежные системы (централизованные и децентрализованные) используют асимметричные криптоалгоритмы для аутентификации своих участников и формирования электронных подписей электронных денег.

В последнее время большое внимание уделяется алгоритмам ЕСС (Elliptic Curve Cryptography)³⁶, основанным на применении конструкций, называемых *эллиптическими кривыми*.

По современным оценкам сложности при уровне надежности алгоритмов ЕСС, соответствующим криптостойкости алгоритмов, основанным на задаче дискретного логарифмирования с длиной ключа 512 бит, можно ограничиться эллиптической кривой, точки которой описываются парами целых чисел, каждое из которых имеет длину 160 бит. Это позволяет сократить общую длину записи секретного ключа с 512 бит до 320, что, в свою очередь, уменьшает сложность вычислений (а значит и время) в 2,4 раза. Таким образом, эллиптические алгоритмы представляют особый интерес для приложений, связанных с микропроцессорными картами, когда необходимо разгрузить процессоры при операциях электронной подписи, а также минимизировать объем памяти для хранения ключа.

Отметим, что в России также приняты национальный стандарт ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и на его основе и межгосударственный стандарт ГОСТ Р 34.10-2018. В представленных стандартах описывается метод формирования и проверки электронной цифровой подписи, использующий операции в группе точек эллиптической кривой, определенной над конечным простым полем. Электронная цифровая подпись под заданной документированной информацией или сообщением в электронной форме позволяет беспрепятственно отправлять подписанные данные по незащищенным телекоммуникационным каналам без опасения ее подделки. Примечательно, что в данных стандартах указаны в качестве допустимых синонимов электронной цифровой подпи-

³⁶ Там же. С. 420.

си такие формулировки, как цифровая подпись, электронная подпись. Определение синонимов позволяет согласовать терминологию указанных выше технических стандартов и Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Процесс создания и проверки электронной подписи использует функцию хеширования (см. выше схему электронной подписи Шнорра), алгоритм и процедуры вычисления которой описаны в ГОСТ Р 34.11-2012 (на его основе — ГОСТ Р 34.11-2018).

ТЕМА 2. СТЕГАНОГРАФИЯ

Вопрос 1. История стеганографии

Не менее древняя история повествует о развитии направлений в стеганографии. Именно в этой области человеческой деятельности были реализованы самые дерзкие и фантастические идеи.

Методы *лингвистической стеганографии* связаны непосредственно с сокрытием информации в текстовых документах. Обычно после применения лингвистических методов стеганограмма имеет вид документа, который может нести любую отвлекающую смысловую нагрузку для читающего и неочевидную полезную информацию для истинного получателя.

Лингвистические стеганограммы подразделяются на две основные категории: *условное письмо* и *семаграммы*.

Существуют три вида условного письма: жаргонный код, пустышечный шифр, геометрическая система.

В *жаргонном коде* слова имеют двойное значение: одно общепринятое, а другое известно только посвященным. Стеганограмма представляет собой текст, который должен иметь как можно более неприметное и правдоподобное содержание.

Сначала он может содержать лишь упоминание об обоюдно известных событиях и лицах: «Я посетил человека, с которым Вы обедали на прошлой неделе». А далее может идти отрезок текста, понятный только адресату, например, один преступник сообщает об аресте другого: «Этот человек попал в больницу», вместо слова «тюрьма» используя слово «больница».

Строгих математических методов обнаружения жаргонного кода не существует, как, впрочем, и для раскрытия других лингвистических стеганограмм. Поэтому акцент делается на профессионализме исследователя, который должен уделять повышенное внимание искусственным оборотам и тяжелым фразам.

В работе Д. Кана «Взломщики кодов»¹ приведен следующий интересный случай со вскрытием жаргонного кода времен Первой мировой войны. У одного английского цензора вызвали подозрения слишком крупные ежедневные телеграфные заказы на сигары (главным образом из портовых городов Англии) от «двух голландских дельцов». Однажды из Портсмута они заказали 10 тыс. сигар «Корона». На следующий день из Плимута они потребовали крупную партию более дешевых сигар. Затем в течение одной ночи в заядлых курильщиков превратились все жители Ньюкасла. Казалось, все население прибрежных районов Англии внезапно почувствовало непреодолимую тягу к курению. По предложению цензора была осуществлена проверка, в результате которой «двое голландских дельцов» оказались немецкими разведчиками, а их заказы — условным письмом, в котором заказ на 5 тыс. сигар для Ньюкасла означал, что в этом порту находятся 5 крейсеров. 30 июля 1915 г. оба немецких разведчика были расстреляны.

На этом примере виден недостаток данного метода, заключающийся в том, что жаргонный код почти всегда удается вскрыть сразу после обнаружения. Более того, прослеживается такая закономерность, что чем менее подозрительно внешнее содержание жаргонного кода, тем легче он поддается вскрытию. А чем больше жаргонный код перегружен всякими правдоподобными подробностями, тем больше он содержит данных для раскрытия его подлинного смысла.

Другим видом условного письма является *пустышечный шифр*. При его применении в тексте имеют значение лишь некоторые определенные буквы или слова. Например, читается каждое пятое слово или первая буква каждого слова, в то время как все остальные буквы или слова служат в качестве «контейнера» для сокрытия значимого текста. Стеганограммы, созданные на основе пустышечного шифра, обычно выглядят еще более искусственно, чем жаргонный код.

Слабая стойкость пустышечного шифра к криптоанализу ограничивает область его применения, хотя простота метода привлекает обывателей для его использования в частной переписке.

Примером могут служить письма американского солдата, посланные во время Второй мировой войны, в которых он пытался (правда, неудачно) сообщить о своем месте службы семье².

Пользуясь заранее условленной системой переписки со своими родителями, молодой солдат пытался довести до их сведения, что находится

¹ Кан Д. Взломщики кодов. М., 2000. С. 64.

² Там же. С. 77.

в Тунисе. Для этого в пяти письмах домой он использовал в качестве второго инициала своего отца сначала «Т», затем «У», «Н», «И» и «С». К несчастью, эти письма были получены в другом порядке, а беспечный солдат забыл проставить на письмах даты. Обезумевшие родители написали ему, что они перерыли весь свой атлас, но нигде не смогли найти «Нутси».

В 1943 г. подобные попытки настолько участились, что руководству ВМС США пришлось предупредить моряков о том, что пользование «семейными кодами» может привести к суровому наказанию.

Третьим видом условного письма является *геометрическая система*. При ее применении имеющие значение слова располагаются на странице в определенных местах или в точках пересечения геометрической фигуры заданного размера.

Известен случай, когда в период Второй мировой войны пленные немецкие офицеры-подводники в своих письмах домой посылали тайные сообщения, делая небольшие пробелы после каждой значимой буквы. Один бдительный английский цензор заметил, что эти маленькие пробелы попадают в самых неестественных местах, даже в середине слогов. Оказалось, что в своих скрытых посланиях немцы сообщали о тактике, применявшейся англо-американскими союзниками в борьбе с немецкими подводными лодками, а также об их технических недостатках.

Вторую категорию лингвистической стеганографии составляют *семаграммы* — тайные сообщения, в которых шифрообозначениями являются любые символы, кроме букв и цифр. Эти сообщения могут быть переданы, например, в рисунке, содержащем точки и тире для чтения по коду Морзе.

Однажды в Нью-Йоркском цензурном отделении перевели все стрелки в предназначенной для отправки партии часов, опасаясь, что их положение может заключать в себе какое-то сообщение.

Исследование сообщений, скрытых лингвистическими средствами, или, точнее, подозрительных в этом отношении, является весьма сложным процессом.

Иногда криптоаналитик не может даже сказать, скрывается ли некое содержательное сообщение за неуклюже составленным или просто безграмотным текстом. И даже если он совершенно уверен, что такое сообщение там спрятано, найти его часто просто невозможно. Обычно в распоряжении цензора имеется всего одно сообщение, а вероятные слова, на которые можно опереться при криптоанализе, отсутствуют.

В начале Второй мировой войны американской цензуре даже рекомендовалось не работать над предполагаемой криптограммой свыше по-

лучаса, исходя из того, что если за это время криптоаналитик не вскрыл ее, он вообще никогда ее не прочтет. Эти непрочитанные сообщения представляли собой трудную проблему для цензоров. В них могла содержаться важная секретная информация, и тогда их не следовало отправлять дальше по адресу. Но пока подозрительное послание не было дешифровано, вина его отправителя оставалась недоказанной. Тем не менее иногда письма специально задерживали или видоизменяли, чтобы предполагаемая тайная информация не дошла до адресата.

технологическая стеганография сводилась к применению различного рода невидимых чернил. В XX в. появились методы технического направления, например, микроточка.

Невидимые чернила бывают двух видов: органические жидкости и симпатические химикалии (чернила).

К *органическим жидкостям* можно отнести мочу, молоко, уксус и фруктовые соки, которые становятся зримыми в результате незначительного нагревания. Несмотря на давнюю известность и слабую стойкость, они настолько удобны, что применялись даже во время Второй мировой войны.

Симпатические чернила представляют собой химические растворы, бесцветные после высыхания, но образующие видимое соединение после обработки другим химикалием (реагентом). Например, если разведчик пишет железным купоросом, то текст невидим, пока его не обработают раствором цианата калия, после чего образуется берлинская лазурь (вещество, обладающее красивым цветом). Искусство изготовления хороших чернил для тайнописи состоит в том, чтобы найти вещество, которое реагировало бы с минимальным количеством химикалий (лучше всего — с одним).

Основная трудность при применении симпатических чернил была связана с невозможностью обеспечить быструю обработку огромного количества информации, которую приходилось передавать разведчикам. Тогда немцы применили способ тайнописи, который директор ФБР Д. Гуввер назвал «шедевром немецкой разведки». Это так называемая *микроточка* — крошечная фотография, на которой с достаточной ясностью воспроизводился текст письма.

Известие, полученное в феврале 1940 г. от двойного агента («Ищите точки, множество маленьких точек»), привело сотрудников ФБР в состояние паники. Они начали лихорадочно разыскивать повсюду признаки появления маленьких точек. Лишь в августе 1941 г. один лаборант внезапно заметил слабое свечение на поверхности конверта, найденного у человека, подозреваемого в связях с немецкой разведкой. В результате была

обнаружена первая микроточка, замаскированная под знак препинания машинописного шрифта. Микроточки позволили немцам решить проблему передачи большого количества информации. Вскоре в Германию хлынул поток разведывательных данных, замаскированных под сотни точек в телеграммах, любовных письмах, деловых сообщениях, семейных посланиях, а иногда в виде кусочков тонкой фотопленки, наклеенных под марками.

Вопрос 2. Современные стеганографические методы

Достаточно полная классификация стеганографических методов приведена на рис. 19. Многие исследователи полагают, что стеганография зародилась до появления письменности, другие утверждают обратное. Для изучения прикладных аспектов данный спор не имеет существенного значения, поэтому перейдем к разновидностям методов.

Стеганография подразделяется на *лингвистическую, технологическую и компьютерную*.



Рис. 19. Классификация стеганографических методов

Лингвистическая стеганография

В настоящее время широко применяются как классические методы лингвистической стеганографии (до компьютерной эпохи), так и новые

интересные разработки, использующие особенности хранения и передачи информации в электронном виде.

В лингвистической стеганографии скрытие осуществляется в текстах, что определяет выбор файл-контейнеров для встраивания скрываемых сообщений — это файлы различных форматов, содержащие текстовую информацию.

Для применения ранее известных методов, например пустышечного или жаргонного кодов, необходимо подобрать текстовые файлы в электронном виде для скрытия. При этом расширяются возможности индивидуальной модификации того или иного метода.

Разберем уже известный нам пустышечный код. Выписав первые буквы слов текста, определяемого как пустышка, можно прочесть скрываемый текст. Однако акростих не применялся в качестве стеганографии со времен Древней Греции. Современные способы пустышечного кода используют сложные варианты формирования стегопути для встраивания скрываемых текстов. Так, можно в первом слове указать на первую букву стегопути, во втором — на третью букву, в третьем слове четвертая буква будет являться частью стегопути. Таким образом, стегопуть будет представлен набором цифр, указывающих на номер буквы в словах пустышечного текста, совокупность выписанных букв будет скрытым сообщением. Сложность запоминания стегопути можно компенсировать современными средствами шифрования или скрытия другим способом компьютерной стеганографии, например, цифровой, методы которой будут рассмотрены ниже. Нетрудно заметить, что этот пример близок к алгоритму книжного шифра. Благодаря разнообразию современных способов передачи информации стегоконтейнер и стегопуть передаются раздельно.

Жаргонный код применяется не одно тысячелетие. Нередко в криминальных структурах требуется скрыть передаваемое сообщение либо сформировать сообщение в устной или письменной формах со скрытым смыслом, понятным только определенным лицам. Примитивность жаргонного кода компенсируется мобильностью выбора новых слов с двойным смыслом. Например, при распространении наркотических средств у слов *лошадь*, *слон*, *гертруда*, *перец*, *хлеб*, *черный* второе значение — героин. Марихуана — это *дым*, *шишки*, *молоко*, *пластилин*. Безобидные выражения «Приди ко мне, Гертруда», «Детишкам нужен пластилин», «Купи мне, пожалуйста, молока», «Захвати по дороге мне белого хлеба» — могут скрывать совсем другой смысл. Сленг постоянно меняется — *шира*, *ширка*, *карандаш*, *боинг*, *снаряд*, *машина*, *насос*, *сучок*, *шар*, *лайба*, *агрегат* — неполный перечень слов, скрытый смысл которых указывает на шприц.

Знаки и символы также могут скрывать информацию (семаграммы). Дизайн страницы веб-сайта для «посвященных» может указывать на принадлежность ресурса, например, какому-то тайному обществу. Не секрет, что символы «666», «SSS» — знаки антихриста, «69» — иньянь, «999» — опийный наркоман, «Л.О.Н.» означает «люблю общество наркоманов», а «АУЕ» — «арестантский уклад един». Но семаграммы могут нести информацию не только о принадлежности к тому или иному кругу лиц, сообществу, но и передавать короткую (от одного бита) важную информацию, предположим, предупреждающую об опасности. Заранее договорившись об условных знаках, символах, группа пользователей средствами социальных сетей, почтовых серверов, форумов, чатов может предупреждать друг друга о тревоге, сборе и пр.

Потоки текстовой информации в глобальной сети Интернет не поддаются счислению, а значит ручной стегоанализ носит эпизодический характер. Поэтому применяется автоматическая фильтрация трафика специальным программным обеспечением, которое реализует специфические алгоритмы поиска скрытых сообщений. Так как в настоящее время и в ближайшем будущем не предвидится интеллектуальных систем стегоанализа, способных поспорить с когнитивной деятельностью человека, все вышеперечисленные методы лингвистической стеганографии при правильных протоколах скрытия могут быть признаны надежными.

Особенности хранения данных в электронном виде дают возможность создавать новые методы лингвистической стеганографии. В электронном виде существует возможность осуществлять пользователю деятельность с большими объемами текстовой информации, внушительные электронные библиотеки могут помещаться в современных гаджетах. Разумеется, существуют различные средства автоматизации, обработки и поиска текстовой информации. Возникла потребность в разработке программных средств автоматизации процесса скрытия информации в области лингвистической стеганографии. Задача автоматизированных методов скрытия предполагает бинарное кодирование скрываемых сведений и алгоритм встраивания полученного двоичного кода в текстовый контейнер. Как правило, количество скрываемых данных значительно меньше контейнера (приблизительно в соотношении 1/200, т. е. на 200 символов пустышечного кода можно скрыть один байт информации). Но при обработке больших объемов информации в электронном виде автоматизация стеганографии оправдывает себя. Ниже приводятся способы лингвистической стеганографии, предназначенные для про-

граммной реализации, однако в некоторых случаях они могут использоваться для ручного скрытия.

Один из таких — метод произвольного интервала³, в котором количественное значение пробелов определяет код «0» или «1». Например, один пробел между словами — «1», а два — «0». Пробелы можно устанавливать не только между словами выровненного текста, но и в концах строк⁴. Простота метода является его единственным достоинством. К основным недостаткам можно причислить передачу малого объема информации на единицу пустышечного текста из-за применения бинарного кодирования, а также неустойчивость к ручному и автоматическому форматированию текста, устраняющему избыточность пробелов.

Устойчивость к редактированию демонстрируют синтаксические и семантические методы лингвистической стеганографии.

В синтаксических методах формирование стегопути основывается на изменении пунктуации или стиля и структуры текста.

Применяя двоичное кодирование скрываемого текста, в синтаксических методах встраиваются биты последовательности. Стегопуть определяется особенностями русского языка. Например, при перечислениях можно заменить разделитель-запятую на союз «и»: он является автором романов, рассказов, очерков — он является автором романов, рассказов и очерков. Появление запятой означает встроенный бит «1», а союз соответствует «0». Средством кодирования могут быть и сокращения с аббревиатурами. Как и в предыдущем методе, для сокрытия небольшого количества информации потребуются значительные объемы текста.

Соккрытие информации путем изменения структуры предложений можно отнести к непопулярным, так как трудозатраты для передачи единицы информации выше, чем у других методов: «Когда я спал, они что-то натворили. / Они что-то натворили, когда я спал». Изменением структуры предложения скрыт один бит информации.

При рассмотрении семантических методов наибольший интерес вызывает метод синонимических замен. В работе И. А. Большакова⁵ пред-

³ Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев, 2017. С. 19.

⁴ Текин В. Текстовая стеганография. URL: <http://www.iso27000.ru/chitalnyi-zai/steganografiya/tekstovaya-steganografiya> (дата обращения: 17.01.2022).

⁵ Большаков И. А. Два метода синонимического перефразирования в лингвистической стеганографии. URL: <https://www.dialog-21.ru/media/2496/bolshakov.pdf> (дата обращения: 17.01.2022).

лагается сформировать словари синонимов. Сохраняя синтаксическую структуру предложения и порядок слов, во всем тексте ищут слова, входящие в синонимические группы словаря синонимов. После проверки допустимости замены соответствующий синоним оставляется в группе потенциальных замен. После определения всех возможных синонимических замен в пустышечном тексте становится известным объем встраиваемой информации. Сами же замены выполняются в соответствии с кодируемой информацией. Необходимо отметить, что рассматриваются не только синонимы слов, но и словосочетаний, например: надеяться, возлагать надежды, питать надежду; наконец, в конечном счете, в конце концов; в течение нескольких дней, за несколько дней; сокращений — Соединенные Штаты Америки, Соединенные Штаты, США; экс-президент, бывший президент; замминистра, заместитель министра. Таким образом, словарь синонимов значительно расширяется, поэтому для этого метода скрытия требуется разработка программного обеспечения для автоматизации процесса поиска стегопути и встраивания стегосообщения. При встраивании закодированной информации исходные слова кодируются — «1», а их синонимы или синонимические фразы — «0».

Насколько применимы методы лингвистической стеганографии в настоящее время, зависит от интеллектуальных и технических возможностей пользователя. Однако существует несколько интересных протоколов, простота в применении и достаточность в стойкости стегоконтейнеров которых заслуживает внимания. Рассмотрим один из протоколов передачи конфиденциальной информации в чате методом лингвистической стеганографии.

1. Абонентам А и Б до передачи известны ник (ключ), ключи друг друга и чат-канал для формирования стегоканала. Отметим, что в глобальной сети присутствует большое множество чатов, форумов, созданных в социальных сетях групп и пр., к тому же время открытия стегоканала и ники абонентов, все это — неизвестная противнику информация, что уже является сложной задачей для стегоанализа.

2. Абонент А отправляет в локальную очередь секретное сообщение М, информирующее о готовности к сеансу связи. Это может быть любая фраза, о которой заранее договариваются абоненты. Например, «Привееет! Наконец я с вами!».

3. Абонент Б подтверждает готовность его принять сообщением N: «Мы все приветствуем тебя».

4. Используя общий протокол, передают скрытое сообщение. Скрытое можно отправлять любым методом лингвистической стеганографии,

причем после открытия стегоканала абонент А передает скрытое сообщение в разговоре со всеми пользователями чата, что затрудняет противнику возможность распознать адресата.

5. Абонент А отправляет в локальную очередь секретное сообщение Z, информирующее о закрытии сеанса связи, например: «Всем пока, моя бабушка испекла пирожки».

6. Абонент Б подтверждает сообщением W («До следующей встречи!») закрытие сеанса связи.

Повысить стойкость протокола позволяет совместное использование методов шифрования и стеганографии.

Технологическая стеганография

К методам технологической стеганографии относятся методы, которые основаны на использовании химических или физических свойств различных материальных носителей информации. В литературе можно встретить понятие технической стеганографии, которое является синтезом методов, основанных на использовании химических или физических свойств различных материальных носителей информации, и современных информационных технологий, например, техническая стеганография на основе технологий создания голограммы или кинеграммы. Известные исторические факты применения технологической стеганографии рассмотрены выше. В настоящее время технологическая стеганография не имеет широкого практического применения.

Компьютерная стеганография

В компьютерной стеганографии исследуются методы скрытия в процессах хранения, передачи и обработки цифровой информации. Стремительное развитие стеганографических методов в этом направлении не позволяет утвердительно предоставить полную их классификацию. Компьютерную стеганографию можно разделить на два направления: использование особенностей файловых систем и свойств компьютерных форматов и цифровую стеганографию. В последнее время, возможно, в отдельное направление компьютерной стеганографии выделится сетевая стеганография, а в ближайшем будущем при появлении квантовых компьютеров вслед за квантовой криптографией мы будем наблюдать новые методы квантовой стеганографии. В рамках методов, использующих особенности файловых систем и свойств компьютерных форматов, рассмотрим встречающиеся в глобальной сети Интернет, в том числе среди криминальных структур, при скрытой передаче данных.

Задача *компьютерной стеганографии* состоит в следующем: исходными данными является *файл-контейнер*, предназначенный для сокрытия тайных сообщений, так называемых *встроенных (скрытых) сообщений*. Требуется таким образом встроить сообщение в контейнер, т. е. сформировать такой *стегоконтейнер* (стеганограмму), который полностью бы соответствовал назначению файла-контейнера и содержал в неявном для органов чувств человека виде встроенное сообщение⁶. Большинство известных методов компьютерной стеганографии используют особенности оцифровки графической, аудио- и видеoinформации. Самые популярные из них — алгоритмы сокрытия информации в графических файлах, например, формата *.bmp или *.jpeg. Эти методы основаны на особенностях зрительного и слухового восприятия человека.

Модель *стеганографической системы*⁷ представлена на рис. 20.

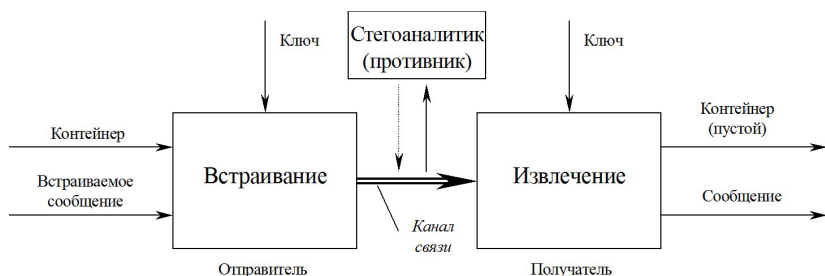


Рис. 20. Обобщенная модель стеганографической системы

Важным элементом в модели, как видно из рисунка, является ключ. Именно он должен обеспечивать сокрытие сообщения в контейнере. Ключ — это то главное, что тщательно скрывает отправитель и на раскрытие которого направляет, в частности, свои усилия *стегоаналитик*⁸.

⁶ Рассматриваемые термины в компьютерной стеганографии были предложены и утверждены на конференции Information Hiding: First Information Workshop в 1996 г.

⁷ Стеганографическая система (стегосистема) — это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

⁸ Стегоаналитик — специалист (в некоторых случаях определяется как противник отправителя и получателя), который, использует методы стегоанализа в целях обнаружения, извлечения или изменения встроенного в стегоконтейнер сообщения.

Использование особенностей файловых систем и свойств компьютерных форматов

Метод использования зарезервированных для расширения полей компьютерных форматов данных применяется для сокрытия незначительных объемов данных. Как правило, разработчики компьютерных форматов файлов в служебных областях оставляют несколько зарезервированных байтов для дальнейшей возможной модификации форматов файлов. Зарезервированные поля компьютерных форматов не используются при эксплуатации файлов, а значит, могут быть контейнерами для сокрытия нескольких байтов информации. Заносить и считывать скрытую информацию позволяет специальное программное обеспечение, например, побитное считывание можно осуществить программой WinHex. Надежность метода низкая, так как специальное программное обеспечение позволяет осуществлять поиск подобных скрытых сообщений в автоматическом режиме (предлагается использовать только совместно с шифрованием скрываемой информации).

Методы сокрытия информации в текстовых файлах, которые рассматривались в лингвистической стеганографии, можно дополнить способами сокрытия с применением скрытых (непечатаемых) символов форматирования, использованием инструментов цвета и уплотнения символов (например, в файлах с форматами текстового процессора MS Word — знаки конца абзаца, неразрывный пробел и др.). Система сокрытия должна включать словарь скрытых знаков форматирования, которые будут использоваться в стегоалгоритме, и стегопуть, определяющий правило внесения в контейнер специальных знаков форматирования двойного значения. В качестве простейшего способа можно использовать скрытый знак форматирования «неразрывный пробел», а стегопуть определяет правила внесения «неразрывного пробела» после буквы, несущей двойной смысл. Так как пробелы можно устанавливать только после каждого слова, то необходимо в *пустышечном тексте* выискивать слова, оканчивающиеся на нужную букву. Еще недавно были популярны способы пустышечного кода, где буква (слово), несущая двойной смысл, определялась номером в строке, например, каждая пятая буква третьего слова несла скрытую информацию.

Как видно из примеров, такие стеганографические приемы подкупают своим разнообразием. Недостатки метода — слабая производительность и низкая степень скрытности. Второй недостаток частично можно устранить, применяя различные алгоритмы шифрования. Существует свободное программное обеспечение для реализации данного метода.

Несмотря на кажущуюся простоту и низкую степень скрытности, не нужно при выборе данного подхода забывать постулат о соизмеримости ценности скрываемой информации и затрат на ее защиту. Например, применение шрифта белого цвета на белом фоне в качестве стеганографического метода иногда бывает вполне оправданным решением. В наш информационный век в телекоммуникационных сетях вращается такое количество данных, что отфильтровать их потоки при известных источниках и получателях и даже с применением специального программного обеспечения проблематично. При этом все лингвистические методы стеганографии могут быть вскрыты, как правило, только в ручном режиме, и для их обнаружения иногда достаточно проведения статистического анализа.

Другой ряд методов, основанных на сокрытии информации в текстовых контейнерах и применении скрытых знаков форматирования, предполагает сокрытие не букв, а их двоичных кодов. Назовем такие вариации бинарным методом. Рассмотрим один из таких вариантов с применением регистра букв. Разрабатывается программное обеспечение, переводящее предварительно скрываемую информацию в двоичный код, а затем в пустышечном тексте формирующее стегопуть по правилу: буквой верхнего регистра в тексте кодируется «1», а буквой нижнего регистра — «0». Например, скрываемая информация «10010100» в тексте «revolution» отобразится «RevOlUtion». Следующий метод предполагает «игру» пробелами в окончании строк, причем количество пробелов есть число в десятичной системе, при переводе которого в двоичный вид читаем скрытое сообщение.

Общеизвестен метод подмены знаков русских символов (кодируемых двоичным знаком «0») на латинские идентичного начертания (кодируемых двоичным знаком «1»)⁹.

В дополнение к перечисленным методам сокрытия в текстовых файлах немаловажным является контейнер, который может быть выбранным, навязанным или случайным. Существует достаточное количество мониторов, осуществляющих фильтрацию трафика на предмет поиска стегоконтейнеров. Решение задачи выбора стегоконтейнера определяется прежде всего неприметностью для программ-мониторов. Поэтому в последнее время на рынке программного обеспечения можно увидеть программы лингвистической стеганографии, формирующие контейнеры для сокрытия информации в виде спама, как менее всего вызывающие подо-

⁹ Бондарчук С. С., Давыдова Е. М., Костюченко Е. Ю. Встраивание цифровых водяных знаков для обеспечения защиты информации. URL: <https://cyberleninka.ru/article/n/vstraivanie-tsifrovyyh-znakov-dlya-obespecheniya-zaschity-informatsii/viewer> (дата обращения: 15.01.2022).

зрение среди пользователей и среди программ стегоанализа, например, сайт <https://www.spammimic.com/>.

Методы удаления идентифицирующего файл заголовка предполагают предварительное шифрование данных одним из криптоалгоритмов и отдельную отправку идентифицирующего заголовка зашифрованного файла от самой криптограммы.

Чтобы устранить недостаток, заключающийся в необходимости заранее передать получателю идентифицирующий заголовок, данный способ применяют в комбинации с каким-либо методом цифровой стеганографии. Например, отправка и идентифицирующего заголовка, и криптограммы в графических стегоконтейнерах. Метод реализован в таком программном обеспечении, как WhiteNoiseStorm, S-Tools.

В методах сокрытия в системных или неиспользуемых областях электронных накопителей информация записывается обычно в неиспользуемые места электронных носителей, причем существует возможность скрывать данные не только в служебных областях файловой системы (например, на нулевой дорожке), но и искусственно создавать неиспользуемые области (сознательная маркировка некоторой области диска как поврежденной). Файловая система никогда не будет применять те области носителя информации, которые отмечены как поврежденные, поэтому, записывая сведения в такие области, можно быть уверенным в ее сохранности. Вместе с тем производительность метода незначительная, ведь относительно незаметно можно скрыть только небольшие объемы информации. Для обнаружения факта сокрытия не требуется сложных методов стегоанализа, достаточно иметь стандартные утилиты для работы с носителями информации, но простота способа применения позволяет оставить его в арсенале методов защиты информации.

В продолжение списка похожих методов предлагаем рассмотреть способ сокрытия данных в остатках кластеров, принадлежащих различным файлам. Размер кластера на современных носителях информации от нескольких килобайт до нескольких десятков килобайт позволяет скрыть достаточно внушительный объем данных без какого-либо специального программного обеспечения. Этот метод использует принцип записи файла в целом количестве кластеров. Всегда можно создать файл-контейнер с информацией, в котором часть последнего кластера, принадлежащего этому файл-контейнеру, будет незанятой, а значит, может быть использована для сокрытия информации. При просмотре такого файла стандартными программными средствами заметить скрытую в последнем кластере информацию невозможно.

Цифровая стеганография

В криминальных структурах широко распространена именно цифровая стеганография. Во-первых, это обусловлено широким спектром методов цифровой стеганографии и программным обеспечением, их реализующих. Во-вторых, в качестве контейнеров используются аудио-, видео- и графические файлы, обращение которых в глобальных сетях в большом количестве значительно увеличивает шанс оставаться вашему стегоконтейнеру незамеченным. В-третьих, комбинация цифровой стеганографии совместно с современными способами шифрования представляет надежный скрытый способ передачи больших объемов данных на любые расстояния благодаря развитым информационно-телекоммуникационным сетям. Посредством цифровой стеганографии можно решить следующие задачи:

- защита конфиденциальной информации от несанкционированного доступа;
- преодоление систем мониторинга и управления сетевыми ресурсами;
- камуфлирование программного обеспечения;
- защита авторского права на некоторые виды интеллектуальной собственности.

В чем отличие этого направления стеганографии от других? Определение цифровой стеганографии гласит, что это наука о способах сокрытия одних битовых последовательностей в других, имеющих аналоговую природу. Причем скрыть необходимо не только незаметно, но и надежно¹⁰. Цифровая стеганография является разделом компьютерной стеганографии, где все методы предусматривают обработку бинарных данных. Отсюда вывод — особенность цифровой стеганографии заключается в аналоговой природе цифрового (бинарного) контейнера. Ранее приводились примеры таких контейнеров — аудио-, видео- и графические файлы. Звук и изображение связаны с органами слуха и зрения человека, которые воспринимают информацию в непрерывном (аналоговом) виде. Устройства (аудиомагнитофоны, видеоманитофоны) воспроизведения звука и видеоизображения до недавнего времени подразумевали аналоговую запись информации. Перечисленные файлы хранят информацию (музыку, песни, мультфильмы, фотографии и многое другое) в двоичном виде, которая изначально имела аналоговую природу. В работе «Цифровая стеганография» указано, что аналоговая природа цифровых данных предполагает приведение непрерывных сигналов в оцифрованный вид.

¹⁰ Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М., 2016. С. 7.

Соккрытие информации обусловлено избыточностью оцифрованной аудио- и визуальной информации. Направления цифровой стеганографии представлены на рис. 21¹¹.

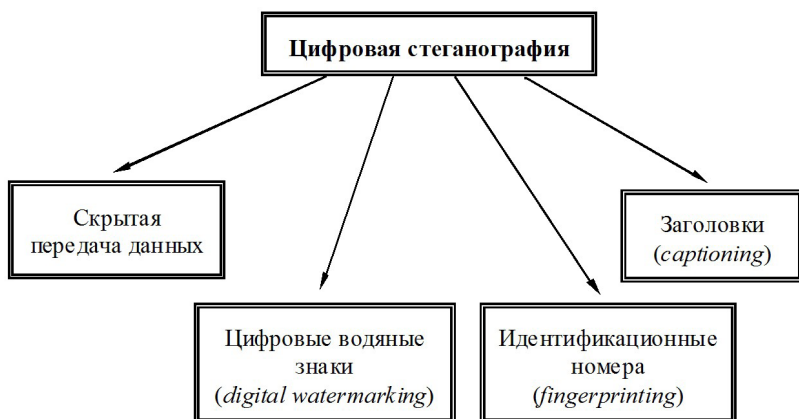


Рис. 21. Классификация направлений цифровой стеганографии

При восприятии видимого диапазона света человеческий глаз не успевает наблюдать за всеми изменениями плотности потока энергии световой волны, воспринимая лишь усредненные значения, которые называются интенсивностью света. При сохранении, например, цифровых фотографий фиксируется интенсивность света в какой-то момент времени в виде матрицы чисел. А цифровой аудиопоток записывается как числовая матрица с информацией об интенсивности звукового сигнала в последовательно идущие моменты времени. Небольшое изменение интенсивности света, записанного в двоичном виде в файлах, человеческий глаз не заметит, т. е. изменение информации в младших, незначачих рядах числовой матрицы не повлияет на восприятие аудио- или визуальной информации человеком. На этом принципе основываются методы цифровой стеганографии.

Идентификационные номера (fingerprinting) предназначены для защиты от незаконного использования объектов авторского права или смежных прав. Наказание за нарушение авторских и смежных прав предусматривается в ч. 2 ст. 146 УК РФ. Не последнее место в раскрытии и расследовании подобных преступлений играет компьютерная экспертиза, в задачу которой в том числе входит доказательство факта тиражирования копий носителей с определенного оригинала. Так, при изъятии партии контрафактной

¹¹ Там же. С. 13.

продукции на DVD-дисках очень сложно определить, с какого именно оригинального DVD-диска выполнены все эти копии. Идентификационные номера — это уникальная двоичная последовательность, например, встраиваемая в музыкальные произведения известного исполнителя, записанная в двоичном виде на DVD-диск. Тогда в случае незаконного тиражирования вся контрафактная продукция будет содержать тот же уникальный номер, что и оригинал. Это значительно упрощает поиск источника изъятой контрафактной продукции. Факт встраивания *fingerprinting* злоумышленнику может быть известен, однако технология предусматривает невозможность извлечения этой уникальной информации.

Заголовки (captioning) применяются не столько в целях сокрытия, сколько для размещения разнородной информации в одном файле. Например, размещение в одном файле графической, текстовой и аудиоинформации может потребоваться в медицинской области, когда у вас представлен компьютерный файл с рентгеновским снимком, просматривая который, в случае необходимости можно вывести историю болезни пациента или аудиозапись с его жалобами на здоровье. Защита медицинской тайны и персональных данных требует предварительного шифрования информации. При обычном просмотре компьютерного файла наблюдается только обезличенный рентгеновский снимок, а при вводе секретного ключа просматривается информация ограниченного доступа. Captioning можно использовать в геоинформационных системах, где разнородные данные могут скрываться в слоях электронной топографической карты местности.

Цифровой водяной знак (digital watermarking) (далее — ЦВЗ) является защитой от присвоения авторства (плагиата) мультимедийной информации. Метод основан на встраивании в защищаемый объект невидимых меток. Метками в двоичном виде может быть самая разнообразная информация (персональные данные автора объекта интеллектуальной собственности, дата и др.). В случае причинения обладателю интеллектуальных прав крупного ущерба предусматривается уголовная ответственность (ч. 1 ст. 146 УК РФ). В отличие от скрытой передачи данных, факт существования ЦВЗ общеизвестен. Возможно даже наличие устройства (декодера, встроенного в DVD-носитель) для обнаружения ЦВЗ. Например, профессиональный фотограф устанавливает ЦВЗ на свои фотографии, сохраненные в цифровом виде. При обнаружении фактов неправомерного использования другими лицами результатов своей интеллектуальной деятельности доказательством авторства будет служить цифровой водяной знак, встроенный в каждую фотографию правообладателя, т. е., по сути, ЦВЗ выполняет функцию электронной подписи для

мультимедийной информации. Разумеется, злоумышленник, зная и имея возможность считать ЦВЗ, попытается удалить или модифицировать интересующую его встраиваемую цифровую метку.

При разработке методов скрытия ЦВЗ необходимо предусматривать их защиту от различного рода искажений. Также нужно учитывать, для чего правообладатель использует ЦВЗ. Отсюда следует деление ЦВЗ на робастные, хрупкие и полухрупкие. *Робастные* методы встраивания должны обеспечивать устойчивость ЦВЗ при любых деструктивных естественных и искусственных воздействиях на него (внешние помехи, изменения формата файла, злонамеренное искажение). *Хрупкие* ЦВЗ должны изменяться при любом воздействии на контейнер (например, цифровую фотографию). Преследуемая цель при этом — определение факта модификации контейнера, вида и местоположения этого изменения. Внедрение хрупких ЦВЗ в мультимедийную продукцию позволит упростить обнаружение факта монтажа цифровых фотографий при криминалистической экспертизе. *Полухрупкие* ЦВЗ обладают смешанными свойствами робастных и хрупких. Например, ЦВЗ может быть устойчив к помехам и хрупким по отношению к монтажу цифровой фотографии. Перспективность использования ЦВЗ в настоящее время обеспечивает большое разнообразие коммерческих предложений на данном сегменте рынка, а также широкий спектр методов и устройств внедрения ЦВЗ.

Рассмотрим простейшие примеры встраивания данных. Первоначально необходимо определить *стегопуть* — это последовательность таких битов, изменение которых не повлечет заметных искажений контейнера. Далее осуществляется встраивание заранее сформированного ЦВЗ в соответствии со стегопутем. Допустим, генерируется ключ, который является маской для вставки ЦВЗ в стегопуть, или перед битом стегопути вставляется бит ЦВЗ.

Скрытая передача данных — основное направление цифровой стеганографии. Доступность информационно-коммуникационных технологий значительно расширила возможности криминального мира, в том числе в передаче больших объемов конфиденциальной информации в преступных целях. В настоящее время эти структуры вооружены надежными техническими методами и средствами защиты информации, позволяющими решать поставленные перед ними задачи шифрования данных и их сокрытия от правоохранительных органов. Охота за специалистами в области кибербезопасности ведется не только силовыми ведомствами разных стран, но и в среде организованной преступности. Даже применение несложных способов цифровой стеганографии в комбинации с крип-

тографическими методами может предоставить злоумышленникам надежный канал передачи конфиденциальной информации.

Раскрыть суть сокрытия данных поможет метод цифровой стеганографии, использующий для встраивания менее значащие биты цифровых изображений. Например, имеются цифровая фотография (стегоконтейнер) и текст (сообщение) конфиденциального характера (представленный в двоичном виде), которые нужно спрятать. Фотография, как и любое цифровое изображение, состоит из пикселей (picture element). Количество пикселей по горизонтали и вертикали представляет собой матрицу, разрешение которой определяется их общим количеством. Допустим, для цветной фотографии используется цветовая модель для излучаемых объектов RGB (Red Green Blue), где цвет каждого пикселя кодируется смешением трех аддитивных составляющих: красного, зеленого и синего (трех байт). Если в каждом из трех байт цвета пикселя изменить младший значащий бит (least significant bit (LSB)), то интенсивность света пикселя изменится не более чем на 1%. Человеческий глаз не в состоянии заметить такие ничтожные изменения плотности потока энергии световой волны, а значит скрываемое сообщение можно распределить по младшим значащим битам цвета пикселей цифровой фотографии без опасения появления визуальных дефектов. Таким образом, возможно сокрытие больших объемов данных в графических изображениях, приблизительно 1/8 размера графического файла.

Как правило, оценка количества информации, допустимого для встраивания в графический файл, определяется специальным программным обеспечением. Предложенный метод сокрытия прост в применении, но и не сложен в обнаружении противником стегосообщения. Чтобы усложнить вскрытие, предлагается сформировать стегопуть из младших бит цвета пикселей, встраивание же проводить лишь в некоторые из них в соответствии с ключом. Ключ генерируется как псевдослучайная последовательность и сохраняется втайне. Количество встраиваемой информации при этом сокращается, а стеганоанализ существенно усложняется. Способ встраивания скрываемой информации в младшие значащие биты также применяется в аудиофайлах, добиваясь невосприимчивости органом слуха человека изменений в оцифрованном звучании.

В настоящее время существует достаточно много программного обеспечения в области цифровой стеганографии. В глобальной сети Интернет можно найти обзоры интересных компьютерных программ по стеганографии и стеганоанализу. Рассмотрим возможности, на наш взгляд, удобной и имеющей профессиональный функционал компьютерной программы

OpenPuff (разработчик EmbeddedSW). OpenPuff — это портативное программное обеспечение с собственной переносимой структурой (без установки разделов реестра, файлов *.ini), т. е. использование программы не требует инсталляции и не оставляет следов на компьютере (рис. 22).

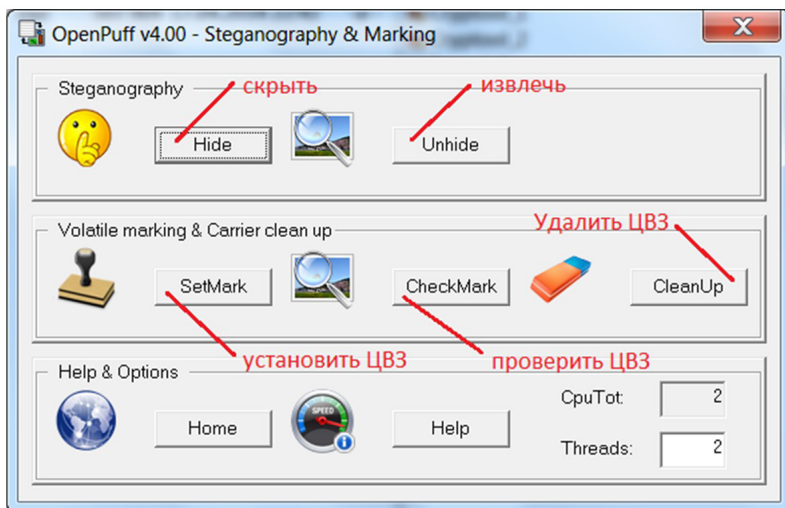


Рис. 22. Основное окно программы OpenPuff v4.00

В программе OpenPuff поддерживается большое количество форматов файлов: изображения (BMP, JPG, PCX, PNG, TGA); аудио (AIFF, MP3, NEXT/SUN, WAV); видео (3GP, MP4, MPG, VOB); Flash-поддержка Adobe (FLV, SWF, PDF) (рис. 23).

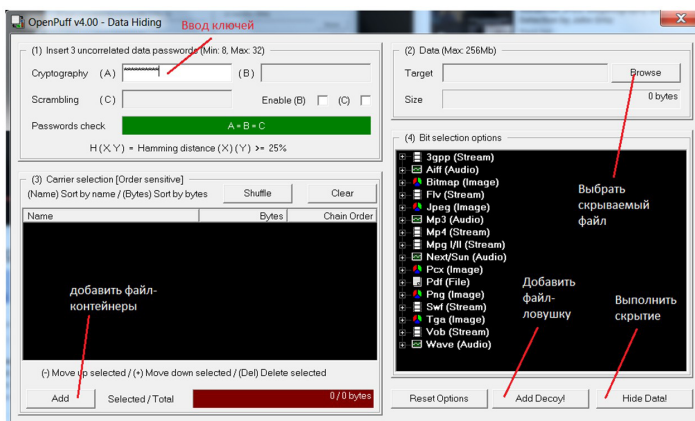


Рис. 23. Окно сокрытия данных программы OpenPuff v4.00

Программа OpenPuff является мощным инструментом, обеспечивающим многоуровневую защиту скрываемых данных. Используется предварительное шифрование скрываемого современными криптоалгоритмами. Встроенный защищенный генератор псевдослучайных чисел (CSPRNG) применяется для скремблирования и защиты от ряда методов стеганоанализа, а инструмент ловушек, т. е. встраивание двух текстов, один из которых, отвлекающий, затруднит доказательство факта причастности к сокрытию того или иного сообщения. Причем большие объемы данных могут быть распределены по нескольким стегоконтейнерам разных форматов.

Программа OpenPuff поддерживает два основных режима: сокрытие данных в файле и подписывание файла (ЦВЗ). Максимальный размер ЦВЗ — 32 бита. Программа самостоятельно определяет стегопуть для встраивания ЦВЗ, в зависимости от формата выбранного файл-контейнера (рис. 24).

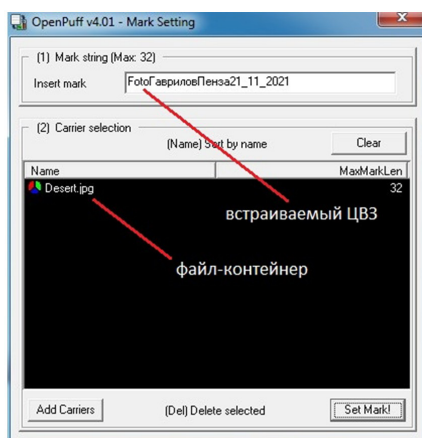


Рис. 24. Окно генерации ЦВЗ программы OpenPuff v4.00.

ТЕМА 3. УПРАВЛЕНИЕ КЛЮЧАМИ

Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в информационных системах (далее — ИС), где количество пользователей составляет десятки и сотни, управление ключами — серьезная проблема.

Под *ключевой информацией* понимается совокупность всех действующих в ИС ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то завладевший ею злоумышленник получает неограниченный доступ ко всем данным.

Управление ключами — информационный процесс, включающий в себя три элемента:

- 1) генерацию ключей;
- 2) накопление ключей;
- 3) распределение ключей.

Рассмотрим, как они должны быть реализованы для того, чтобы обеспечить безопасность ключевой информации в ИС.

Вопрос 1. Генерация ключей

В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, это датчики псевдослучайных чисел (далее — ПСЧ)¹. Однако степень случайности их генерации должна быть достаточно высокой. Идеальными генераторами являются устройства на основе «натуральных» случайных процессов. В частности, появились серийные образцы генерации ключей на основе *белого радиошума*. Другие случайные математические объекты — десятичные знаки иррациональных чисел (например, экспонента), которые вычисляются с помощью стандартных математических методов.

¹ Шнайер Б. Прикладная криптография. М., 2002. С. 370.

В ИС со средними требованиями защищенности вполне приемлемы программные генераторы ключей, которые вычисляют ПСЧ как сложную функцию от текущего времени и (или) числа, введенного пользователем.

Вопрос 2. Накопление ключей

Под *накоплением* ключей понимается организация их хранения, учета и удаления.

Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание.

Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован.

В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей.

Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие информацию, называются *мастер-ключами*. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть и не хранил их на каких-либо материальных носителях.

Важное условие безопасности информации — периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно. Вопрос обновления ключевой информации связан и с третьим элементом управления ключами — распределением ключей.

Вопрос 3. Распределение ключей

Это самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

- 1) оперативность и точность распределения;
- 2) скрытность распределяемых ключей.

В последнее время замечен сдвиг в сторону использования крипто-систем с открытым ключом, в которых проблемы распределения ключей не существует. Тем не менее распределение ключевой информации в ИС требует новых эффективных решений.

Распределение ключей между пользователями реализуется двумя разными подходами.

1. Путем создания одного или нескольких центров распределения (удостоверяющих центров) ключей — так называемый *централизованный подход*. Его недостаток состоит в том, что в центре распределения известно, кому и какие ключи назначены, и это позволяет читать все сообщения, циркулирующие в ИС. Возможные злоупотребления существенно влияют на защиту информации.

2. Прямой обмен ключами между пользователями ИС. В этом случае проблема заключается в том, чтобы надежно удостоверить подлинность субъектов.

В обоих случаях должна быть гарантирована подлинность сеанса связи. Это можно обеспечить двумя способами:

1. *Механизм запроса-ответа*, который состоит в следующем: если пользователь А желает быть уверенным, что сообщения, которые он получает от В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент (запрос). При ответе пользователь В должен выполнить некоторую операцию над этим элементом. Это невозможно осуществить заранее, так как неизвестно, какое случайное число придет в запросе. После получения ответа с результатами действий пользователь А может быть уверен, что сеанс является подлинным. Такой механизм вполне может быть реализован с помощью схемы аутентификации Шнорра, описанной выше.

2. *Механизм отметки времени («временной штемпель»)*. Он подразумевает фиксацию времени для каждого сообщения. В этом случае каждый пользователь ИС может знать, насколько «старым» является прошедшее сообщение.

В обоих случаях следует использовать шифрование, чтобы быть уверенным, что ответ послан не злоумышленником и штемпель отметки времени не изменен.

При использовании отметок времени возникает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса. Ведь сообщение с «временным штемпелем» в принципе не может быть передано мгновенно. Кроме этого, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

В реальных ИС (например, в системах оплаты кредитных карт) применяется именно второй механизм установления подлинности и защиты от подделок. Используемый интервал составляет от одной до нескольких минут. Много способов кражи электронных денег основано на вставке в этот промежуток подложного запроса на их снятие.

В качестве примера прямого обмена ключами может быть рассмотрен механизм *открытого распределения ключей*. Он решает задачу выработки общего закрытого (секретного) ключа для сеанса связи любой пары пользователей ИС.

Алгоритм открытого распределения ключей Диффи-Хеллмана был предложен в 1976 г. и назван так в честь его создателей. Он предполагает независимое генерирование каждым из пары связывающихся абонентов своего случайного числа, преобразование его посредством некоторой процедуры, обмен преобразованными числами по открытому каналу связи и вычисление общего секретного ключа на основе информации, полученной в процессе связи от партнера. Каждый такой ключ существует только в течение одного сеанса связи или даже его части.

Таким образом, открытое распределение ключей позволяет каждой паре пользователей системы самим выработать свой общий закрытый ключ, упрощая тем самым процедуру распределения секретных ключей.

Алгоритм Диффи-Хеллмана выглядит следующим образом².

1. Задается пара открытых ключей p и D .
2. Абонентом А генерируется в качестве закрытого ключа случайное число x из интервала $(1, p)$, а абонентом В — аналогичное число y из того же интервала.
3. Закрытый ключ x шифруется абонентом А: $S1 = D^x \pmod{p}$, полученная криптограмма $S1$ отправляется абоненту В.
4. Закрытый ключ y шифруется абонентом В: $S2 = D^y \pmod{p}$, полученная криптограмма $S2$ отправляется абоненту А.
5. Общий ключ для абонентов А и В вычисляется как $S = S1^y = S2^x$, полученная криптограмма $S2$ отправляется абоненту А.

Хотя описанный алгоритм позволяет обойти проблему скрытой передачи ключа, необходимость аутентификации остается. Без дополнительных средств ни один из абонентов не может быть уверен, что он обменялся ключами именно с тем, который ему нужен. Опасность имитации в этом случае остается.

Использование блуждающих ключей. Как уже отмечалось, проблема распределения ключей является наиболее острой в крупных ИС. Отчасти она решается (точнее, снимается) за счет использования открытых ключей. Но наиболее надежные криптосистемы с открытым ключом типа RSA достаточно трудоемки, а для шифрования мультимедийных данных и вовсе непригодны.

² Там же. С. 50.

Оригинальные решения проблемы «блуждающих ключей» активно разрабатываются специалистами. Эти системы являются некоторым компромиссом между системами с открытыми ключами и обычными алгоритмами, для которых требуется наличие одного и того же ключа у отправителя и получателя.

Идея метода достаточно проста. После того, как ключ использован в одном сеансе по некоторому правилу, он сменяется другим. Это правило должно быть известно и отправителю, и получателю. Зная правило, после получения очередного сообщения получатель тоже меняет ключ. Если правило смены ключей аккуратно соблюдается и отправителем, и получателем, то в каждый момент времени они имеют одинаковый ключ. Постоянная смена ключа затрудняет раскрытие информации злоумышленником.

Основная задача в реализации этого метода — выбор эффективного правила смены ключей. Наиболее простой путь — генерация случайного списка ключей. Смена ключей осуществляется в порядке списка. Однако очевидно, что список придется каким-то образом передавать.

Другой вариант — использование математических алгоритмов, основанных на так называемых *перебирающих последовательностях*. На множестве ключей путем одной и той же операции над элементом получается другой элемент. Последовательность этих операций позволяет переходить от одного элемента к другому, пока не будет перебрано все множество.

Наиболее доступным считается использование полей Галуа. За счет возведения в степень порождающего элемента можно последовательно переходить от одного числа к другому. Эти числа принимаются в качестве ключей.

Ключевой информацией в данном случае является исходный элемент, который перед началом связи должен быть известен и отправителю, и получателю.

Надежность таких методов должна быть обеспечена с учетом известности злоумышленнику используемого правила смены ключей.

Интересной и перспективной задачей является реализация метода блуждающих ключей не для двух абонентов, а для достаточно большой сети, когда сообщения пересылаются между всеми участниками.

Вопрос 4. Пример программной реализации управления ключами

В операционной системе Astra Linux (Smolensk) 1.6 есть специализированное графическое приложение для создания и централизованного хранения ключей. Оно называется «Цифровая подпись KGpg».

Это приложение разработано как часть рабочего окружения KDE (KDE Applications / KDE Utilities) и является графическим интерфейсом (GUI) к консольной утилите GnuPG (GPG)³.

Для запуска приложения «Цифровая подпись KGpg» необходимо в стартовой меню-панели Fly (Пуск) перейти в «Утилиты» и запустить соответствующую утилиту. На рис. 25 представлено основное окно программы.

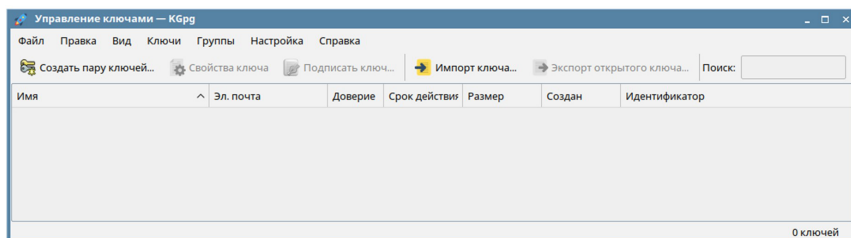


Рис. 25. Основное окно программы «Цифровая подпись KGpg»

С помощью KGpg можно управлять ключами шифрования, а также производить операции шифрования/расшифровки текста и файлов. Приложение поставляется с параметрами «по умолчанию», обеспечивающими большинству пользователей приемлемый уровень безопасности и комфорта.

Полноценная работа с программой возможна только при наличии хотя бы одного ключа. При первом запуске KGpg предлагает создать ключ. Далее, используя соответствующее диалоговое окно, можно создавать, редактировать и удалять ключи. Ключ можно сформировать стандартный, просто введя имя и электронную почту, а при желании использовать большее количество опций можно задействовать «Режим эксперта» (при этом запустится консоль для создания ключа из командной строки). Длина ключа может иметь одно из значений: 1024, 2048, 4096. При создании ключа доступны следующие алгоритмы: Gost R 34.10-2012, Gost R 34.10-2001, RSA и RSA, RSA, DSA и ElGamal. При использовании алгоритма RSA и RSA становится доступным выбор возможных применений ключа: проверка подлинности, защитное преобразование, подпись (рис. 26).

³ GPG / GnuPG (GNU Privacy Guard) — консольная утилита для шифрования информации и создания электронных цифровых подписей с помощью различных алгоритмов (RSA, DSA, AES и др.). Утилита создана как свободная альтернатива проприетарному PGP (Pretty Good Privacy) и полностью совместима со стандартом IETF OpenPGP (может взаимодействовать с PGP и другими OpenPGP-совместимыми системами).

Создание ключа — KGrg

Создание пары ключей

Имя:
Петров А.Е.

Эл. адрес (необязательно):
rae@mvd.ru

Комментарий (необязательно):
Начальник

Срок действия:
6 месяцев

Размер ключа:
2048

Алгоритм:
GOST R 34.10-2012

Возможные применения

- ☐ Сертификация
- ☐ Проверка подлинности
- ☐ Защитное преобразование
- ☐ Подпись

Режим эксперта Да Отмена

Рис. 26. Окно создания ключа KGrg

После того, как ключ создан, он выводится в главном окне программы — появляется возможность экспортировать открытый и закрытый ключи (рис. 27).

Управление ключами — KGrg

Файл Правка Вид Ключи Группы Настройка Справка

Создать пару ключей... Свойства ключа Подписать ключ... Импорт ключа... Экспорт открытого ключа... Поиск:

Имя	Эл. почта	Доверие	Срок действия	Размер	Создан	Идентификатор
Петров А.Е.	rae@mvd.ru		17.04.2022	256 /	19.10.2021	190CE86E108F64AF
Петров А.Е.	rae@mvd.ru				19.10.2021	190CE86E108F64AF

0 ключей

Рис. 27. Созданные ключи в окне программы «Цифровая подпись KGrg»

Другой известный пакет программ для обмена сообщениями по электронной почте, получивший название PGP (Pretty Good Privacy)⁴, разработан американским программистом Ф. Циммерманом. Основная идея Циммермана состояла в создании качественной и надежной программы шифрования для электронной почты, базирующейся на использовании наиболее сильных криптоалгоритмов, опубликованных в то время (на рубеже 80–90-х гг.) в открытой литературе. Пакет PGP в первых его версиях вместе с исходными текстами программ был распространен в 1991 г. по сетям электронной почты практически во всем мире и использовался многими программистами в разработках средств защиты информации. Пакет PGP удачно совместил в себе возможности шифрования сообщений симметричными блочными алгоритмами распределения симметричных ключей с помощью асимметричного алгоритма шифрования RSA, а также создания электронных подписей сообщений.

⁴ Сингх С. Книга кодов: тайная история кодов и их «взлома». М., 2007. С. 217.

Таблица 1. Распределение вероятностей букв в русском тексте

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	пробел
Вероятность	.062	.014	.038	.013	.025	.072	.007	.016	.062	.010	.028	.035	.026	.053	.090	.023	0.175
Буква	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
Вероятность	.040	.045	.053	.021	.002	.009	.004	.012	.006	.003	.014	.016	.014	.003	.006	.018	

Таблица 2. Логарифмы распределения вероятностей биграмм в русском тексте

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	%		
А	2	7	8	6	7	7	7	4	7	7	7	8	8	3	7	6	7	8	2	6	6	7	7	5	5	0	0	6	7	9	7	9	7	
Б	7	1	1	0	1	6	2	2	6	0	5	6	3	5	7	2	7	5	0	7	0	3	4	1	0	5	5	2	2	0	3	5	13	
В	8	0	5	0	4	8	0	3	7	1	6	7	5	6	8	4	6	6	6	6	0	3	0	1	3	0	0	2	0	0	4	8	38	
Г	6	0	1	1	6	5	0	0	6	0	4	5	4	4	8	0	7	0	6	0	0	1	2	3	0	0	0	2	0	0	4	8		
Д	8	1	6	3	4	8	1	0	7	0	4	7	1	7	8	4	7	0	6	0	0	1	3	4	0	0	0	4	0	0	4	5	7	
Е	5	5	6	7	8	6	6	4	7	7	8	8	9	6	5	8	8	9	3	3	6	5	6	5	6	0	1	1	5	5	9	73		
Ж	6	0	0	0	6	7	2	1	7	0	5	0	2	7	1	0	1	2	1	3	0	0	0	0	0	0	0	2	0	0	0	2	8	
З	8	4	6	2	6	4	1	1	6	1	5	5	6	6	7	1	5	0	0	6	0	0	2	1	0	0	2	2	0	0	4	6	14	
И	6	6	7	6	6	8	5	7	7	7	6	8	8	5	5	7	8	8	1	5	7	7	7	7	6	3	0	0	0	6	7	9	64	
Й	0	0	3	0	3	0	0	0	0	0	3	6	5	4	0	0	0	6	6	0	0	0	1	2	3	0	0	0	0	0	0	8	11	
К	8	1	5	1	1	6	5	2	7	1	2	7	0	5	8	0	7	6	6	7	0	0	6	0	1	1	0	0	0	0	0	7	29	
Л	8	4	1	2	1	8	6	1	8	0	4	4	1	6	7	0	0	3	3	6	3	0	0	3	1	1	0	8	0	7	8	6	31	
М	7	5	7	2	2	8	0	1	7	0	4	4	7	6	8	5	1	3	1	6	1	0	0	0	0	0	0	3	0	0	6	8	32	
Н	9	0	3	3	6	8	1	1	9	0	6	0	1	7	8	0	5	7	6	5	2	5	3	0	0	0	0	5	0	4	6	7	50	
О	2	8	8	8	6	7	7	6	8	7	8	7	6	7	8	8	3	2	5	6	7	6	5	0	1	5	2	5	9	8	9	89		
П	7	0	0	0	0	8	0	4	7	0	3	6	1	4	8	4	9	4	5	6	2	0	1	0	0	0	0	5	3	0	4	4	28	
Р	9	1	6	4	4	8	6	0	8	0	5	2	6	6	8	4	2	6	6	7	3	5	4	2	4	2	0	4	0	1	6	7	48	
С	6	4	6	2	5	7	2	0	7	0	7	8	6	6	8	7	5	6	9	6	7	3	5	1	5	5	0	0	6	1	3	8	7	43
Т	8	2	7	1	4	8	0	0	8	0	6	4	5	5	6	9	3	8	8	4	6	0	0	0	4	0	2	1	8	0	1	5	8	60
У	3	4	6	6	7	6	5	3	3	6	5	5	6	0	6	7	7	7	1	5	5	0	6	3	6	3	6	0	0	7	4	8	19	
Ф	6	0	0	0	5	0	0	6	0	0	2	2	0	6	0	4	0	3	5	4	0	0	0	0	0	0	0	0	0	0	2	4		
Х	4	3	3	0	4	0	0	3	0	1	1	0	5	6	0	5	3	1	3	0	0	2	0	0	0	1	0	0	0	0	0	8	6	
Ц	5	0	6	0	0	6	0	0	7	0	0	0	0	3	0	0	0	3	0	0	0	0	4	0	0	0	0	0	0	0	5	6		
Ч	7	0	1	0	0	8	0	7	0	6	1	0	6	2	0	1	0	7	3	0	0	0	1	3	0	0	3	0	0	0	4	12		
Ш	5	0	0	0	6	0	0	7	0	3	3	4	0	3	4	0	3	0	3	4	0	0	0	0	0	0	4	0	0	0	5	3		
Щ	6	0	0	0	7	0	0	6	0	0	0	0	2	0	0	2	0	0	4	0	0	0	0	0	0	0	4	0	1	0	1	3		
Ъ	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	1	
Ы	1	4	7	3	5	7	1	5	1	7	5	5	6	4	2	1	5	5	5	6	0	0	7	0	5	4	1	0	0	0	1	8	18	
Ь	0	1	0	0	0	3	0	7	1	0	6	0	4	7	1	0	0	6	4	0	0	0	0	1	6	1	0	0	0	6	2	8	12	
Э	0	0	4	0	0	1	0	0	0	2	6	5	2	1	0	2	0	1	7	0	4	3	0	0	0	0	0	0	0	0	1	4		
Ю	0	5	0	2	0	1	2	0	4	1	0	0	0	0	0	3	7	0	0	0	6	1	7	0	1	7	0	1	0	3	0	7	6	
Я	0	1	5	2	5	6	2	3	0	4	2	3	6	5	0	1	4	4	7	0	0	4	4	3	0	4	0	0	6	4	9	18		
	7	8	9	7	8	7	5	8	8	3	8	6	8	9	9	9	8	9	8	7	7	6	7	8	5	1	1	8	2	6	0	138		

Алгоритм шифра князей Барятинских

Приводим алгоритм криптоанализа шифра, обнаруженный в библиотеке Уварова на листе рукописи XVII в. и названного в дальнейшем шифром Князей Барятинских. Исследования проводились Н. В. Энговатовым. Результаты были опубликованы им в труде «Тайнопись князей Барятинских и вопросы дешифровки древнерусских криптограмм»¹. Фрагмент рукописи содержится в рисунке. Предлагаем отрывок работы Н. В. Энговатова.

Дешифровку криптограмм необходимо начинать с анализа ее шифра. Он сводится к установлению графических особенностей знаков тайнописи, т. е. включает в себя также систематизацию криптографических средств. Какие-либо сопоставления знаков одной криптограммы со знаками других на раннем этапе дешифровки могут только внести путаницу.

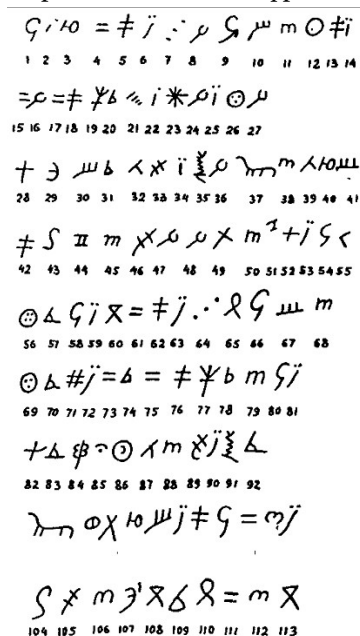


Рис. Тайнопись XVII в.
с занумерованными знаками

Необходимость предварительной систематизации знаков криптограмм диктуется многими причинами. Не исключено, что один и тот же знак мог выступать в разных начертаниях, что могло быть связано со стремлением к нарочитому усложнению шифра. В этом шифре могло также существовать несколько различных по начертанию знаков для передачи одного и того же звукового значения (как это имеет место в общеславянских азбуках). Кроме того, при беглости почерка, которым выполнена наша криптограмма, произвольно возникает вариант начертаний одного и того же знака. Для облегчения дальнейших рассуждений мы занумеровали знаки указанной криптограммы и будем теперь ссылаться на соответствующие индексы.

При систематизации знаков тайнописи нужно обратить внимание на повторяю-

¹ Энговатов Н. В. Тайнопись князей Барятинских и вопросы дешифровки древнерусских криптограмм // Археологический ежегодник за 1962 г. М., 1962. URL: https://rusneb.ru/catalog/000202_000006_1135333/ (дата обращения: 15.01.2022).

щиеся в криптограмме отрывки, под которыми могли скрываться идентичные словосочетания, слова или морфемы. В исследуемой криптограмме имеются следующие повторяющиеся написания: знаки 1–20 и 58–78, а также 89–102 и 33–45. Некоторые расхождения для части знаков указанных отрывков следует, вероятно, отнести на счет расхождений окончаний слов, но для большинства знаков приходится признать предположительную идентичность.

С учетом вариантов начертаний знаков, представленных в двух указанных параллельных местах пометки, нужно произвести предварительную систематизацию знаков шифра. При этом выясняется, что данный вид тайнописи представлен 25 типами знаков, некоторые из них имеют варианты начертания. Кроме этого, знаки 51 и 55 из-за их фрагментарности затруднительно соотнести с другими выделенными знаками шифра.

Предварительный опыт нашей систематизации позволяет сделать вывод о буквенном характере криптограммы. Славяно-русские тайнописи вообще носят буквенно-звуковой характер. Приняв мысль о буквенно-звуковом характере шифра, мы сталкиваемся с необходимостью установить звуковое значение букв исследуемой тайнописи. Это можно производить несколькими способами. В частности, дешифровку криптограммы можно было бы производить на основе статистического анализа, вскрыв присущие и другим текстам особенности употребления знаков. Например, о двух первых по употребительности знаках можно почти безошибочно сказать, что они (как это характерно вообще для русских текстов) являются буквами для гласных звуков «о», «а», «и». Однако не исключено, что из-за недостаточного объема криптограммы все эти статистические закономерности проступают в ней недостаточно последовательно. Поэтому статистический метод следует привлекать в данном случае осторожно.

Другим вспомогательным методом предварительного установления звукового значения тайнописных букв является сопоставление со знаками уже известных шифров. М. Н. Сперанский обнаружил, что совокупность знаков исследуемой тайнописи несопоставима с какой-либо известной разновидностью древнерусских шифров. Однако не лишено основания его предположение о вероятной связи букв исследуемой криптограммы со знаками шифров более раннего времени. Предполагать специально для нашего случая, что писец совершенно не учитывал предшествующее тайнописание, будет едва ли благоразумным. Поэтому приходится склоняться к мысли, что шифр криптограммы составлен

из **нескольких тайнописей** раннего периода. Здесь следует помнить и о такой особенности русских тайнописей XVII в., как отказ от древних типов литорейных шифров и создание более сложных видов тайнописи. С учетом этих обстоятельств и нужно подходить к шифру нашей криптограммы.

В частности, некоторые знаки этого шифра напоминают обычные начертания кириллицы букв (например, Ъ), а другие знаки можно трактовать как упрощенные или усложненные знаки кириллицы. Так, имеются знаки, напоминающие перевернутое «от», лигатуру «оу», зеркальное «е». В состав шифра вошли, очевидно, знаки, сформированные по принципу «полусловицы», с ее недописанными начертаниями обычных кириллических букв. Один из знаков, в частности, напоминает недописанную букву «юс большой». Не исключено также, что тайнописец, используя начертания некоторых кириллических букв, изменил звуковые значения этих знаков. Это касается дважды встретившихся в криптограмме букв «пси» и «кси», обычно малоупотребительных в кириллице. Часть знаков шифра не имеет соответствий в кириллических начертаниях.

К их числу относятся три знака:

- 1) в виде трех точек;
- 2) в виде двух черточек;
- 3) в виде четырех черточек. Подобным способом обозначались знаки в «мудрой литорей», где кириллические буквы из разряда единиц заменялись соответствующим числом точек, а из разряда десятков — соответствующим числом черточек. Поэтому указанные знаки соответствовали бы в «мудрой литорей»:

- 1) три точки — букве «г» (цифра 3);
- 2) две черточки — букве «к» (цифра 20);
- 3) четыре черточки — букве «м» (цифра 40).

Учитывая высказанные общие соображения, приступим непосредственно к дешифровке криптограммы. Поскольку те знаки нашего шифра, которые имеют чрезвычайно характерные литорейные начертания, едва ли возникли в результате простой случайности, проверим, не соответствуют ли они в исследуемой криптограмме своим литорейным значениям.

Для начала дешифровки наиболее удобен текст, включающий параллельные отрывки: знаки 1–9 и 58–66. Поэтому начнем дешифровку сразу с этих двух мест. Знаки 7 и 64 указанных отрывков — варианты одного и того же знака, составленного из трех точек и соответствующего знаку «г» «мудрой литорей». Можно предположить то же значение и для

указанных знаков нашей криптограммы. Вместе с тем знаки 4 и 61 исследуемых отрывков соответствуют составленному из двух черточек литорейному знаку «к».

В результате этих предварительных соображений мы получаем для отрывков из знаков 4–7 и 61–64 такое чтение: К — — Г и К — — Г.

Поскольку наша криптограмма — это запись на рукописи, имеющая, видимо, близкое отношение к аналогичным припискам на книгах, естественно предположить под дважды встретившимся написанием «К — — Г» слово «книга». С таким предположением согласуется позиция и последовательность букв «к» и «г» в указанных отрывках. Само же слово «книга» часто встречается в приписках такого рода².

Кроме этого, приходится предположить, что два непрочитанных знака могли быть в указанном месте буквами «н» и «и», соответствуя чтению «книг(а)». В частности, знак перед буквой «г» (6, 63) по начертанию близок к кирилловскому «Ѣ», с которым его и можно отождествить. В то же время этот знак относится к наиболее употребительным буквам криптограммы, так как встретился в ней 14 раз (т. е. больше любого другого). Учитывая, что по употребительности на первом месте в русских текстах стоят гласные «о», «а», «и», мы можем уверенно предположить для указанного знака значение «и». При этом чтение исследуемых отрывков принимает вид — К — ИГ и К — ИГ.

Предположив для непрочитанного знака значение «н», мы придем к чтению: КНИГ и КНИГ.

Предположив в указанных случаях чтение «книг», мы получим значения четырех букв криптограммы — «к», «н», «и», «г». Правильность их значений может быть подтверждена только в ходе дальнейшей дешифровки, но пока эти значения приходится принять условно. Знаки 2 и 59 наших параллельных отрывков соответствуют уже установленному значению «и», что дает чтение: — И — КНИГ — — И — И — КНИГ — —.

Так как знаки 8 и 65, стоящие после основы «книг», различаются по начертанию, следует предположить в указанных местах разные падеж-

² В данном случае применен метод искусственной билингвы. При использовании этого метода исходят из того а) что на каких либо предметах с определенным назначением обычно пишут, кому принадлежал (принадлежит) этот предмет, например, надписи на топорах типа «топор такого-то» или б) что надпись, которую предстоит расшифровать (озвучить), начинается с определенной традиционной формулы (титул, имя и т. п.). Так, отправным пунктом дешифровки египетского письма (которое по отношению к нашему времени может рассматриваться как тайнопись) явилась идентификация имени Птолемея на Розетском камне. (Подр. см.: *Гриневиц Г. С. Пра-славянская письменность. Результаты дешифровки*. Т. 2. М., 1999. С. 131).

ные формы от слова «книга». Стоящие перед словом «книга» написания из трех знаков также различаются только конечными знаками 3 и 60. Об этом слове, находящемся перед написанием «книг», нам известно следующее:

1) оно выступает в противопоставленных по конечному знаку формах;

2) обозначено всего лишь тремя буквами;

3) второй звук обозначен буквой «и»;

4) основа состоит из написания, представленного двумя буквами;

5) конечный знак, по-видимому, относится к окончаниям.

Соблазнительно было бы видеть в указанном слове прилагательное или местоимение в их падежных формах Его краткость (три буквы) заставляет остановиться на местоимениях с короткими основами.

Если учесть также частое употребление в многочисленных пометках на книгах (вплоть до настоящего времени) традиционного словосочетания «сия книга», то нетрудно убедиться в том, что в исследуемом случае это словосочетание, видимо, и выступает. Если это так, то знаки 1 и 58 должны иметь значение «с», а отрывки читаются так: СИ — КНИГ — — и СИ — КНИГ — —.

Однако если знаки 1 и 58 имеют значение «с», то это же самое значение относится и к знакам 9 и 66. Наши отрывки, следовательно, читаются: СИ — КНИГ — С и СИ — КНИГ — С.

Едва ли в написании падежных окончаний слова «книга» входила буква «с». Но если она не входила в окончание, то в исследуемых случаях падежные окончания этого слова отмечены единственным знаком. Таким образом, при анализе падежных форм словосочетания «сия книга» следует исходить из наблюдений над знаками 1–8 и 58–65: СИ — КНИГ — и СИ — КНИГ —.

Иными словами, формы слова «сия» состоят для исследуемых мест из написаний в три знака, а форма слова «книга» — из написаний в пять знаков. Поскольку в этих параллельных случаях выступают разные падежные формы словосочетания, всем упомянутым условиям отвечают только формы именительного и винительного падежей единственного числа — «сия книга» и «сию книгу».

Учитывая это, обратим внимание на употребительность знаков окончания слова «книга», т. е. знаков «а», «у» (КНИГа — КНИГу). По нашим подсчетам, буква «а» более чем в два раза употребительней буквы «у» («у», «оу»). В сгоревшей рукописи «Слово о полку Игореве» буква «а» была употреблена 1059 раз, а «у» — всего 492 раза. Это соотношение

сохраняется и для более поздних текстов. Так, в «Повести о Сухане» на 324 буквы «а» приходится 141 буква «у».

Обратившись к данным криптограммы, мы установим, что знаки типа «8» в криптограмме встречались 7 раз, а графемы типа знака 65 — всего лишь два раза, т. е. в 3,5 раза реже знаков типа 8.

Принимая во внимание эту статистическую особенность употребления знаков, мы придем к выводу, что знак 8 в качестве более употребительного соответствует букве «а», а знак 65 как менее употребительный — букве «у». Эти соображения дают основание для чтения: СИ — КНИГА и СИ — КНИГУ.

Предположение, что во втором случае знак 65 имеет значение «у», поддерживается начертаниями этого знака, являющегося ничем иным как опрокинутой кириллической лигатурой «оу».

Учитывая, что форма местоимения «сей» должна согласовываться с формами существительного «книга», мы приходим к необходимости предположить для первого случая чтение «сия», а для второго «сию»: СИЯ КНИГА С и СИУ КНИГУ С.

Знак 3 для «я» внешне похож на кириллическую букву «ю», но на самом деле является заимствованным из «полусловицы» недописанным «а» йотированным, т. е. соответствует предполагаемому значению «я». Знак 60 также, по-видимому, заимствован из «полусловицы», так как представляет собой недописанное начертание «юса»  или .

Таким образом, произведенная дешифровка двух отрывков криптограммы дала нам значения 9 букв тайнописи: «а», «г», «и», «к», «н», «с», «у», «ю», «я». Если установленные значения этих графем верны, то дальнейшая дешифровка криптограммы не представляет серьезных трудностей.

На основе дешифрованного отрывка можно сделать вывод о том, что криптограмма относится к распространенному виду пометок о принадлежности книги или об авторстве лица, произведшего запись. Следует ожидать появления в начале заметки после слов «СИЯ КНИГА» имени владельца. Обратим внимание на место в записи, занятое знаками 21–27 и читающееся с учетом известных уже букв: — И — АИ — А. Первый знак этого написания (21) состоит из четырех черточек, т. е. соответствует букве «м» «мудрой литореи». Приняв это значение, мы получим: МИ — АИ — А. Видимо, под этим написанием скрывается имя: «Михаила». Действительно, знак 23 является усложнением кириллического «х» при помощи двух дополнительных черточек, а за знаком 26 остается после этого предположить значение «л», если оно в дальнейшем подтвердится. Прочтение имени «Михаила» дает дополнительно знаки «м», «х», «л».

На основе установленных значений приступим к дешифровке отрывка текста, представленного после слов «сия книга» и «сию книгу» двумя параллельными отрывками (знаки 9–20 и 66–78). Судя по составу знаков, указанные отрывки скрывают один и тот же текст, читающийся:

(СИЯ КНИГА) С — — Л НИКАКН — — (МИХАИЛА)

(СИЮ КНИГУ) С — — Л — НИК — КИ — —

Написание «кн — —» приходится признать в обоих случаях каким-то самостоятельным словом. В первом случае после него стоит имя «Михаила», отграничивающее конец слова «кн — —», а начало того же слова примыкает к написанию «с — — лника». Признав за написанием «кн — —» значение самостоятельного слова, мы будем вынуждены считать написание «с — — лника» также самостоятельным. Поэтому начнем дешифровку указанных отрывков с написаний: С — — Л — НИКА и С — — Л — НИК—.

Конечный знак написания «с — — л — ник —», несомненно, не мог обозначать согласный, поскольку окончаний, состоящих из одного согласного, среди падежных форм имен существительных не имеется. Поэтому приходится предположить для знака 74 значение гласного или редуцированного гласного. Поскольку знаки «а», «у», «я», «ю» нам известны, этот знак мог быть буквами «о», «е», «ы», «ъ», «ь» или «ять». Однако следует принять во внимание, что в написании «с — — л — ник —» дважды употреблен знак для этого гласного звука (70, 74); подставим его вероятные значения сразу для двух мест этого написания. Получим следующие варианты:

С — — ЛОНИКО, С — — ЛЕНИКЕ, С — — ЛЫНИКЫ, С — — ЛЬНИКЪ, С — — ЛЪНИКЪ, С — — ЛЪНИКЪ. Из этих вариантов, вероятно, приемлемы только два:

С — — ЛЬНИКЪ и С — — ЛЪНИКЪ.

Не исключено, что исследуемый шифр не различал «ь» и «ъ». Во всяком случае, мы условно принимаем для указанных знаков в одних случаях значение «ь», а в других — «ъ». Вероятно, дальнейшая дешифровка поможет выяснить уместность такого допущения, а пока мы останавливаемся на чтении указанного написания: С — ЛЬНИКЪ. При этом анализируемое написание в двух рассматриваемых случаях читается: С — — ЛНИКА и С — — ЛЬНИКЪ. Пропуск «ь» в первом варианте написания вполне понятен, так как в XVII в. подобное опущение редуцированного звука в такой позиции не может вызвать удивления.

Продолжая дешифровку, обратим внимание на второй знак написания «С — — ЛЬНИКЪ», являющийся перевернутым кириллическим «т», мы приходим к чтению:

(СИЯ КНИГА) СТ — ЛНИКА КН — — (МИХАИЛА)

(СИЮ КНИГУ) СТ — ЛЬНИКЪ КН — —

Поскольку непрочитанный знак в слове «ст — лник», несомненно, обозначает гласный, приходится выбирать пока еще неизвестные нам значения гласных — «е», «ять», «о», «ы»: СТЕЛЬникъ, стЬлЬникъ, стьльникъ, стольникъ.

Вероятно, не вызовет возражения наше предположение о том, что из этих вариантов наиболее удовлетворителен один: СТОЛЬНИКЪ.

В отличие от других гипотетических вариантов, слово «стольникъ» действительно существовало в русском языке XVII в. Независимо от этих комбинаторных соображений, тот знак, которому мы приписали значение «о», является по начертанию опрокинутой буквой кириллицы «от». Таким образом, в параллельных местах криптограммы выступает в разных падежных формах одно и то же слово: СТОЛНИКА и СТОЛЬНИКЪ.

Приступим к дешифровке стоящего после этого слова написания «КН — —». Поскольку здесь мы видим самостоятельное слово, обращает на себя внимание, что последний знак этой группы соответствует редуцированному «ъ» или «ь»: КН — Ъ или КН — Ь. В том или ином случае непрочитанный знак 19, 77 не мог обозначать гласный. Поэтому приходится принять для него значение какого-либо согласного звука. Следует учитывать также малочисленность слов, которые могли начинаться в XVII в. с группы согласных «кн». Для исследуемого случая словом, удовлетворяющим всем этим условиям, можно, по-видимому, признать чрезвычайно употребительное в тот период сокращенное написание слова «князь» — КНЗЬ.

При этом знакам 19 и 77 придается значение буквы «з». На основе сделанных наблюдений приступим к дешифровке конца криптограммы (знаки 104–113), который читается: С — — — Ю — УК — Ю. Предпоследний знак в этом отрывке — опрокинутое «от», т. е. буква «о», на один вариант которой мы уже указывали выше. Подобный же знак употреблен и в начале рассматриваемого отрывка (знак 106). Таким образом, конец пометки читается: С — О — Ю — УКОЮ. Было бы заманчивым видеть в написании «— УКОЮ» слово «рукою» для чего следует предположить за знаком 109 значения «р», что мы и делаем: с — о — ю «рукою». При этом предшествующее слово читается как «с — о — ю», а его предпо-

следний знак является зеркальным вариантом кириллического «Е». Предположив за знаком 107 значение «е», приходим к чтению: с — оею рукою. После этого не остается иной возможности, как читать знак 105 в слове «с — оею» как: «СВОЕЮ РУКОЮ». Кстати, отметим, что словосочетание «своею рукою» вообще характерно для приписок на книгах, в том числе и для тайнописных пометок.

Опираясь на полученные результаты, приступим к дешифровке группы знаков 79–93, стоящей после слов «сию книгу стольникъ кнзь» и означающей по аналогии с началом надписи имя собственное: ОСИ — Ъ. Поскольку неизвестный знак в этом написании мог быть только буквой для согласного (он стоит перед «ъ»), принимаем для него значение «п», так как остальные буквы не дают удовлетворительного чтения: ОСИПЪ.

Таким образом, в криптограмме, кроме стольника князя Михаила, упоминается стольник князь Осип. Следует ожидать после этих имен также отчеств этих князей, так как это были весьма значительные лица. В связи с этим остановимся на группе знаков 28–36, стоящих после имени Михаила и читающихся: ПЕТЪРВИ — А. За неизвестным знаком этого слова приходится предполагать значение «ч», что позволяет читать отчество: ПЕТЪРВИЧА. Пропуск буквы «о» объясняется, вероятно, ошибкой тайнописца. По-видимому, после отчества Михаила должно было стоять также обозначение княжеского рода, к которому принадлежал этот стольник. Поскольку та же самая группа знаков повторяется и после имени Осипа, оба князя, очевидно, принадлежали к одному княжескому роду. Его название следует видеть в знаках 37–47 и 93–103 нашей криптограммы, которые читаются: — ОРЯТНСКОВА и — ОРЯТИНСКОЙ. Отсутствие «и» в первом варианте фамилии нужно, видимо, отнести к дефектам листа, на котором дошла до нас криптограмма. Этот знак находился у края листа; соседний с ним знак 55 сохранился фрагментарно.

Первый знак в написании фамилии нам пока не встречался. Однако княжеские фамилии XVII в. хорошо известны. К нашему случаю подходит только одна. Мы имеем в виду Барятинских, писавшихся по своему калужскому родовому поместью «Борятино» — Барятинскими. С учетом этой справки рассматриваемые отрывки читаются: БОРЯТНСКОВА и БОРЯТИНСКОЙ.

Вплоть до XVII в. среди Барятинских не было Осипов. В XVII в. это имя носил Осип Федорович Барятинский, имевший племянника Михаила Петровича. Старший брат Осипа Петр Федорович упоминается в 1658 г.

среди «дворян московских», а о самом Осипе известно, что в 1674 г. он был стольником и воеводой в Великих Луках, а в 1682 г. руководил переписью Великого Новгорода.

Учитывая эти соображения, приступим к дешифровке отрывка (знаки 84–92), предположительно содержащего отчество Осипа. Этот отрывок читается: — — — РОВИЧЬ. Первый знак этого слова (84) следует, по всей видимости, считать буквой «Ф» — Ф — — РОВИЧЬ. Исходя из позиционных и других соображений, знак 86 нужно идентифицировать с буквой «Д» — Ф — ДРОВИЧЬ. В результате мы приходим к необходимости признать неизвестный знак в отчестве Осипа буквой для гласного звука. Но едва ли это было «Е», имеющее несхожее с этим знаком начертание. Приходится склониться к тому, что неизвестный знак обозначал звук «е», хотя в русскую орфографию знак для «ё» вошел значительно позже конца XVII в. Тайнописное «Е», вероятно, передавало соответствующий дифтонг «ио», «ео» в слове «Феодорович», «Феодорович (Фёдорович).

Таким образом, после прочтения этой группы знаков текст криптограммы выглядит так: «Сия книга столника кнзь Михаила Петъровича Борятнскова... сию книгу стольник кнзь Осип Федорович Борятинской своею рукою». Непрочитанный отрывок скрывает, очевидно, глагольную форму и читается АРО — ПИС — ЛЪ. Знак 51, стоящий над строкой, может быть выносным написанием, обязанным влиянию кириллицы. Эта выносная буква, на наш взгляд, сопоставима с вариантными начертаниями тайнописного «с», т. е. отрывок читается: А РОСПИС — ЛЪ. Непрочитанный знак (55) дошел до нас в виде фрагмента на краю листа. Оставшиеся неповрежденными его элементы не препятствуют идентификации знака с тайнописным «А». В связи с этим оставшийся отрывок читается как А РОСПИСАЛЪ.

В результате указанных выше допущений исследуемая криптограмма прочитана нами следующим образом:

СИЯ КНИГА СТОЛНИ
КА КНЗЬ МИХАИЛА
ПЕТЪРВИЧА БОРЯТ
НСКОВА А РОСПИСА
ЛЪ СИЮ КНИГУ СТО
ЛЬНИКЪ КНЗЬ ОСИ
ПЪ ФЕДРОВИЧЬ
БОРЯТИНСКОЙ
СВОЕЮ РУКОЮ

Но на этом история шифра князей Бяратинских не закончилась. Отечественный ученый Г. С. Гриневич выдвинул гипотезу и в дальнейшем доказал, что исследуемый текст несет в себе еще один смысл — смысл иного содержания. Тем самым был обнаружен метод шифрования, неизвестный ранее в научных кругах, названный им в дальнейшем «тайнопись двакарты»³. Для его подробного изучения мы адресуем вас к указанному источнику.

³ Гриневич Г. С. Указ. соч. С. 131.

ОГЛАВЛЕНИЕ

Введение.....	3
ТЕМА 1. КРИПТОГРАФИЯ	
Вопрос 1. История криптографии	8
Вопрос 2. Криптосистемы с секретным (симметричным) ключом	26
Вопрос 3. Криптосистемы с открытым ключом	52
ТЕМА 2. СТЕГАНОГРАФИЯ	
Вопрос 1. История стеганографии	65
Вопрос 2. Современные стеганографические методы.....	69
ТЕМА 3. УПРАВЛЕНИЕ КЛЮЧАМИ	
Вопрос 1. Генерация ключей	86
Вопрос 2. Накопление ключей.....	87
Вопрос 3. Распределение ключей	87
Вопрос 4. Пример программной реализации управления ключами	90
ПРИЛОЖЕНИЯ.....	94

Учебное издание

Симаков Александр Александрович,
Кургузов Антон Владимирович

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Редактор Е. А. Жукова

Корректор Л. И. Замулло

Технические редакторы М. Ю. Чалкова, П. В. Ярославцева

ИД № 03160 от 02 ноября 2000 г.

Подписано в печать: 22.12.2022. Формат 60×84/16. Бумага офсетная № 1.

Усл. печ. л. 6,3. Уч.-изд. л. 5,2. Тираж 210 экз. Заказ № 323.

