А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНИК ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

2-е издание, исправленное

Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям и специальностям

Книга доступна в электронной библиотеке biblio-online.ru, а также в мобильном приложении «Юрайт.Библиотека»

Москва ▪ Юрайт ▪ 2019

УДК 004.056(075.8)
ББК 32.811.4я73
Л79

***Авторы*:**

Лось Алексей Борисович — кандидат технических наук, доцент, заведующий кафедрой компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Нестеренко Алексей Юрьевич — кандидат физико-математических наук, доцент кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Рожков Михаил Иосифович — доктор технических наук, старший научный сотрудник, профессор кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики».

***Рецензенты*:**

Хаметов В. М. — доктор юридических наук, профессор, почетный работник высшего профессионального образования РФ, заведующий кафедрой уголовно-процессуального права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА);

Попов. В. Л. — доктор физико-математических наук, професор Математичекого института имени В. А. Стеклова.

Лось, А. Б.

Л79 Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2019. — 473 с. — (Серия : Бакалавр. Академический курс).

ISBN 978-5-534-10673-2

В учебнике «Криптографические методы защиты информации» изложен курс алгоритмической теории чисел и ее приложений к вопросам защиты информации. Основное внимание уделено строгому математическому обоснованию, эффективной реализации и анализу трудоемкости алгоритмов, используемых в криптографических приложениях. Приведено описание современных криптографических схем и протоколов, использующих изложенные теоретические сведения.

В отличие от существующих пособий по данной тематике учебник содержит в себе изложение, построенное по принципу «от простого к сложному», что позволит освоить рассматриваемый материал без существенного использования дополнительной литературы.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Для студентов, учащихся по специальности «Компьютерная безопасность», магистрантов, обучающихся по специальности «Математические методы защиты информации», а также аспирантов и научных работников.

УДК 004.056(075.8)
ББК 32.811.4я73

ISBN 978-5-534-10673-2

Оглавление

Предисловие

Настоящий учебник предназначен для студентов, изучающих дисциплину «Криптографические методы защиты информации» и обучающихся по специальности «Информационная безопасность».

С момента начала преподавания данной дисциплины в открытых высших учебных заведениях вышел ряд превосходных отечественных учебных пособий по данной теме, к которым мы относим книгу «Введение в криптографию», написанную коллективом авторов под общей редакцией В. В. Ященко, монографии В. И. Нечаева «Элементы криптографии» и О. Н. Василенко «Теоретико-числовые методы в криптографии», учебное пособие «Основы криптографии», написанное А. П. Алферовым, А. Ю. Зубовым, А. С. Кузьминым и А. В. Черемушкиным.

Однако за последнее десятилетие произошел бурный скачок в развитии информационной безопасности. За это время появились новые федеральные законы, регулирующие деятельность в области разработки и применения средств защиты информации, были проведены международные конкурсы, целью которых являлась разработка новых алгоритмов защиты информации. Как следствие, было принято несколько новых национальных стандартов в Российской Федерации, а также в ряде зарубежных стран.

Большое количество актуальной информации, не отраженной в существующих учебных изданиях и доступной лишь в виде разрозненных фрагментов в сети Интернет, послужило причиной для написания настоящего учебника. Мы постарались отразить современное состояние математических и алгоритмических вопросов в различных областях криптографии.

При выборе материала для учебника мы постарались осветить все наиболее значимые математические вопросы, возникающие при разработке и анализе криптографических схем. Мы также рассмотрели вопросы оценки стойкости криптографических схем, свойства используемых криптографических преобразований. В частности, в учебнике приводятся новые результаты по методам построения нелинейных рекуррентных последовательностей с гарантированным периодом выходной гаммы, оценки вероятностей выходных s-грамм фильтрующих схем и генераторов на их основе, а также свойства узлов модульного суммирования и MDS-матриц.

Большое внимание уделено изучению свойств блочных и поточных шифров. Детально рассмотрены разработанные в последнее время новые отечественные криптографические алгоритмы — алгоритм

блочного шифрования «Кузнечик», бесключевая функция хэширования «Стрибог», а также схемы электронной подписи, схемы асимметричного шифрования и протоколы распределения ключей. Изучается ряд зарубежных алгоритмов.

В отдельной главе изложены методы анализа асимметричных схем, стойкость которых основывается на высокой трудоемкости решения ряда теоретико-числовых задач. Описаны методы построения простых чисел, а также известные алгоритмы разложения больших целых чисел на множители и решения задачи дискретного логарифмирования.

В завершение учебника мы рассмотрели действующую нормативную базу Российской Федерации, регулирующую вопросы производства и эксплуатации средств защиты информации. Мы описали принятые к настоящему моменту национальные стандарты в области криптографической защиты информации, а также механизмы создания стандартизированных решений.

Для полного усвоения материала необходимо обладать базовыми знаниями и навыками в следующих дисциплинах: «Теория вероятностей и математическая статистика», «Алгебра», «Теория чисел», «Математическая логика и теория алгоритмов», «Дискретная математика», «Теория информации», «Методы программирования».

Столь большой перечень дисциплин позволит учащемуся не только наиболее полно изучить теоретические вопросы, но и экспериментально решить ряд практических задач, возникающих при исследовании и реализации криптографических алгоритмов. Приводимый учебный материал сопровождается примерами и задачами для самостоятельного решения.

Принятые в настоящее время в Российской Федерации правила лицензирования организаций, занимающихся деятельностью в области защиты информации, требуют большого числа специалистов, имеющих образование по специальности «Информационная безопасность». Мы надеемся, что наш учебник окажется полезным при подготовке таких специалистов, а также будет востребован в их дальнейшей трудовой деятельности.

Указатель обозначений

$\mathbb{N}$	Множество натуральных чисел 1, 2, 3, …
$\mathbb{Z}$, $\mathbb{Z}_m$	Кольцо целых чисел и, соответственно, кольцо вычетов по модулю m
$\mathbb{Q}$, $\mathbb{R}$	Поля соответственно рациональных и действительных чисел
$\mathbb{F}_p$	Конечное простое поле из p элементов, характеристики p, где p — простое число
$\mathbb{F}_q$, $\mathbb{F}_{p^n}$	Конечное поле из $q = p^n$ элементов, характеристики p, где p — простое число
$\mathbb{K}^*$	Мультипликативная группа поля $\mathbb{K}$; например, для конечного простого поля $\mathbb{F}_p$ мультипликативная группа имеет вид $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$
V^n, $\mathbb{F}_2^n$	Пространство векторов длины n с коэффициентами из множества V, т. е. пространство векторов $(a_1, \ldots, a_n)$, где $a_i \in V$, $i = 1, \ldots, n$. Наиболее распространенный случай использования в качестве V конечного поля $\mathbb{F}_2$. В этом случае мы получаем пространство двоичных векторов $\mathbb{F}_2^n$
V^∞	Пространство векторов с коэффициентами из множества V произвольной длины
$GL(m, \mathbb{F}_q)$	Группа квадратных матриц размера $m \times m$ с коэффициентами из поля $\mathbb{F}_q$
$\deg f(x)$	Степень многочлена $f(x)$; так, для многочлена $f(x) = \sum_{i=0}^{s} f_i x^i$, $x_s \neq 0$, выполнено равенство $\deg f(x) = s$
len(a)	Количество элементов в записи вектора a. Если вектор $a = (a_1, \ldots, a_n)$, то $\text{len}(a) = n$. Если a является двоичным вектором, то $\text{len}(a)$ обозначает количество бит в векторе a
$\|\|$	Операция конкатенации двух векторов. Для векторов $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_m)$ выполнены равенство $a\|\|b = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ и равенство $\text{len}(a\|\|b) = n + m$. При этом каждый вектор может быть записан как конкатенация своих координат, т. е. $a = a_1\|\|\cdots\|\|a_n$
$\text{lsb}(d, a)$	Вектор, состоящий из d координат вектора a с наименьшими индексами. Для вектора $a = (a_1, \ldots, a_n)$ выполнено равенство $\text{lsb}(d, a) = (a_1, \ldots, a_d)$
$\text{msb}(d, a)$	Вектор, состоящий из d координат вектора a с наибольшими индексами. Для вектора $a = (a_1, \ldots, a_n)$ выполнено $\text{msb}(d, a) = (a_{n-d+1}, \ldots, a_n)$. Для любого натурального d такого, что $1 \leq d < n$, выполнено равенство $a = \text{lsb}(d, a)\|\|\text{msb}(n-d, a)$

$\oplus$	Операция побитового сложения двух двоичных векторов одинаковой длины. Для двух векторов $a=(a_1, \ldots, a_n)$ и $b=(b_1, \ldots, b_n)$ выполнено равенство $a \oplus b = (a_1 + b_1 \pmod 2), \ldots, a_n + b_n \pmod 2)$
$\lll$	Циклический сдвиг вектора $a=(a_1, \ldots, a_n)$ в сторону старших разрядов, т. е. $a \lll s = (a_{n-s+1}, \ldots, a_n, a_1, \ldots, a_{n-s})$

Глава 1
ИСТОРИЧЕСКИЙ ОЧЕРК

В результате изучения данной главы студент должен:

знать

- криптографическую терминологию;
- основные этапы в развитии криптографии;
- исторических лиц, внесших вклад в развитие криптографии;

уметь

- применять простейшие шифры;
- обосновать сильные и слабые стороны исторических шифров;

владеть

- криптографической терминологией;
- методами вскрытия исторических шифров.

Настоящий учебник, как и большинство книг на эту тему, содержит сведения о современном состоянии науки о шифрах, называемой «криптография» — наука о методах преобразования информации с целью обеспечения ее целостности и конфиденциальности, а также с целью сокрытия самого факта ее передачи.

По мнению ученых и специалистов, криптография возникла одновременно с появлением письменности около V—VII вв. до н. э. и оказала влияние на ход многих исторических событий. В развитие криптографических методов защиты информации внесли свой вклад многие известные математики и политические деятели.

В течение многих веков короли, королевы и полководцы управляли своими странами и командовали армиями, опираясь на имевшиеся в распоряжении средства связи. В то же время, они осознавали последствия того, что произойдет, если их сообщения попадут не в те руки, вражескому государству будут выданы ценные секреты, а жизненно важная информация окажется у противника. Именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров — способов скрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано.

Стремление обеспечить секретность означало, что в государствах существовали соответствующие службы, создающие коды и шифры и отвечающие за обеспечение секретности связи путем раз-

работки и использования надежных средств защиты информации. А в это же самое время потенциальные противники старались раскрыть эти шифры и выведать секреты. Лица, участвовавшие в раскрытии шифров и называемые дешифровальщиками или криптоаналитиками, по мнению современников, являли собой алхимиков от лингвистики — племя колдунов, пытающихся с помощью магии получить осмысленные слова из бессмысленного набора символов.

История кодов и шифров — это многовековая история поединка между создателями шифров и теми, кто старается их раскрыть, интеллектуальная гонка вооружений, которая оказала существенное влияние на ход исторических событий.

Однако утверждать, что развитие криптографии осуществлялось только на государственном уровне, было бы не совсем правильным. С момента появления письменности и начала интенсивного обмена сообщениями люди осознали тот факт, что подчас их содержание не должно стать достоянием посторонних лиц и лиц, для которых оно не предназначено. Простейшим примером может служить переписка влюбленных, по тем или иным причинам вынужденных скрывать свои отношения от окружающих. Во времена господства инквизиции к криптографии прибегали многие известные ученые для сокрытия результатов своих исследований, чтобы избежать преследований и смертной казни. В последнее время часто появляются сообщения о работах по изучению личности великого английского поэта и драматурга Уильяма Шекспира. Одна из наиболее популярных на сегодня точек зрения состоит в том, что это вымышленное лицо, придуманное известным философом и государственным деятелем того времени Фрэнсисом Бэконом, поскольку высокое положение в государстве не позволяло ему заниматься литературным творчеством не только под своим именем, но даже и под псевдонимом. Специалисты утверждают, что найдены зашифрованные записи Бэкона, в которых он подробно описывает данную ситуацию.

Примером трагических событий, связанных с применением криптографии, служит казнь королевы Шотландии Марии Стюарт (конец XVI в.) в результате неудавшегося государственного переворота, который готовили ее сторонники с целью свержения королевы Англии Елизаветы, ее родственницы. Для обмена сообщениями Мария и ее союзники использовали не вполне надежный шифр, который удалось раскрыть приближенным Елизаветы. Оглашенные на суде дешифрованные сообщения явились главным доказательством вины Марии и основанием для вынесения ей смертного приговора. Кроме криптографии сторонники Марии применяли так называемые методы стеганографии — скрытной передачи сообщений, которые они прятали в затычке бочки с пивом.

О случае, когда сокрытия послания оказалось достаточным, чтобы беспрепятственно его передать, отмечал еще древний ученый и историк Геродот. Он поведал историю Гистия, правителя греческого города

Милета, который хотел подтолкнуть своего двоюродного брата и зятя Аристагора к восстанию против персидского царя Дария. Чтобы послание не обнаружили враги, Гистий обрил голову своего вестника, написал на коже текст послания, а затем подождал, пока волосы не отрастут вновь. Вестник, у которого не было ничего явно его компрометирующего, мог путешествовать не беспокоясь. По прибытии на место вестник обрил голову и «вручил» адресату послание.

В своей «Истории» Геродот повествовал о вооруженных столкновениях между Грецией и Персией в V в. до н. э. Он рассматривал эти столкновения как противоборство между свободой и рабством, между независимыми греческими государствами и тиранической Персией. Согласно Геродоту именно искусство тайнописи спасло Грецию от порабощения Ксерксом, царем царей, деспотичным правителем Персии. Наращивание военной мощи Персии видел некто Демарат, грек, изгнанный с родины и живший в персидском городе Сузы. Несмотря на изгнание, он все же оставался лоялен к Греции и поэтому решил предупредить спартанцев о плане вторжения Ксеркса. Проблема заключалась в том, как передать сообщение, чтобы его не могли перехватить персы. Поскольку опасность обнаружения послания была очень велика, то оставался только единственно возможный способ, которым Демарат мог успешно передать свое послание. Он соскоблил воск с двух дощечек для письма, написал прямо на дереве, что собирается делать Ксеркс, а затем снова покрыл воском дощечки с сообщением. По внешнему виду дощечки казались чистыми, без каких-либо записей, поэтому и не вызвали подозрения у персидских солдат. Когда гонец с посланием добрался до места назначения, никто не мог и предположить о наличии послания, пока Клеомена, бывшая женой царя Спарты Леонида I, не догадалась и не сказала, что если они счистят воск, то найдут записанное послание. Так и сделали; после того как был счищен воск, на дощечках обнаружилось послание, которое прочли, а затем передали в другие греческие города. Благодаря этому предупреждению беззащитные на тот момент греки стали сами вооружаться и сумели отразить нападение Ксеркса, которое уже не было внезапным.

Секретная переписка, осуществляемая путем сокрытия имеющегося сообщения, носит название «стеганография», которое происходит из греческих слов *steganos* — «покрытый» и *graphein* — «писать». В течение нескольких тысячелетий во всем мире применялись различные виды стеганографии. Например, древние китайцы писали сообщения на тонкой шелковой ткани, которая затем сворачивалась в крохотный шарик и покрывалась воском, после чего посланец проглатывал этот восковой шарик.

В XVI в. итальянский ученый Джованни Порта показал, как скрыть послание внутри сваренного вкрутую яйца, вначале изготовив чернила из одной унции квасцов и пинты уксуса, а затем записав послание этими чернилами на скорлупе. Раствор проникает сквозь поры скорлупы и оставляет сообщение на поверхности плотного яичного белка,

которое можно прочитать, только разбив яйцо и очистив скорлупу. Стеганография также включает в себя применение невидимых чернил. Еще в I в. н. э. известный ученый древности Плиний показал, как сок некоторых растений может использоваться в качестве таких чернил. После высыхания надпись, сделанная этими чернилами, не видна, но при несильном нагреве она приобретает коричневый цвет.

Многие органические жидкости ведут себя похожим образом: при нагреве, из-за того что в них содержится большое количество углерода, они темнеют. И это не составляет секрета для нынешних шпионов, которые, в случае если у них исчерпались симпатические чернила, используют для этой цели подручные средства.

То, что стеганография смогла просуществовать столь длительное время, показывает, что она, несомненно, обеспечивает определенную секретность, но ей присущ один принципиальный недостаток. Если курьер будет обыскан и у него обнаружат сообщение, то сразу же станет известно и его содержание. Перехват сообщения мгновенно ставит под угрозу всю безопасность. Бдительная стража может тщательно обыскивать всех, кто пересекает границу, счищая с дощечек весь воск, нагревая чистые листы бумаги, очищая сваренные яйца от скорлупы, брея людям головы и так далее, так что случаи обнаружения такого сообщения неизбежны.

В связи с этим, наряду с усовершенствованием стеганографии, происходило развитие криптографии, которая берет начало от греческого слова kryptos, означающего «тайный». Цель криптографии состоит не в том, чтобы скрыть наличие сообщения, а в том, чтобы скрыть его смысл — процесс, известный как шифрование. Чтобы сделать сообщение непонятным, оно зашифровывается по определенному правилу, которое заранее оговаривается между отправителем сообщения и его получателем. Так что адресат, получив сообщение, может применить к нему правило шифрования в обратном порядке, после чего его смысл станет понятным. Преимущество криптографии состоит в том, что если противник перехватит зашифрованное надежным шифром сообщение, то прочитать его ему не удастся. Восстановить исходное сообщение из зашифрованного текста, не зная правил шифрования, может оказаться для противника сложной, а то и вовсе невыполнимой задачей.

Поскольку криптография как наука и как искусство имеет весьма длительную и часто трагическую историю, авторы посчитали, что читателю будет интересно ознакомиться с основными событиями в развитии данного направления.

1900 г. до н. э., Древний Египет. Почти четыре тысячи лет тому назад в древнеегипетском городе Менет-Хуфу на берегу Нила один опытный писец нарисовал иероглифы на могиле дворянина Хнумхотепа II, рассказавшие историю жизни его господина. Сделав это, он стал родоначальником документально зафиксированной истории криптографии.

500 г. до н. э., Иудея. Жители иудейского царства изобрели для написания книг своеобразный простейший шифр, ATBASH, принцип которого основывался на обычном алфавите, только буквы записывались в обратном порядке. На этом «языке» древние евреи писали некоторые книги. А позже ими было изобретено еще несколько способов кодирования записанной информации.

500 г. до н. э., Китай. Основные принципы разведки и контрразведки, включая и методы обработки информации, впервые сформулировал китайский ученый Сун Цзы в своей книге «Искусство войны».

487 г. до н. э., Греция. Греки, по данным историков, создали первое «устройство» для шифрования данных — сциталь. Оно было изобретено в Древней Спарте во времена ее идеолога и политика Ликурга. Для зашифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся получателю сообщения. Последний наматывал его на цилиндр того же диаметра и читал текст по оси цилиндра. Ключом такого шифра являлись диаметр цилиндра и его длина.

Метод дешифрования сциталя впоследствии был изобретен великим Аристотелем, который предлагал наматывать ремень на конус до появления читаемого текста.

IV век до н. э., Греция. Древнегреческий полководец Эней предложил устройство, названное впоследствии диском Энея. Принцип его был прост. На диске диаметром 10—15 см и толщиной 1—2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась катушка с намотанной на ней ниткой достаточной длины. При зашифровании нитка вытягивалась с катушки и последовательно протягивалась через отверстия в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть катушку с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

150 г. до н. э., Ирак. В Уруке, который сейчас известен как Ирак, среди писцов было популярно писать цифры вместо имен при подписании их работ. Вероятно, в большинстве случаев это делалось для того, чтобы сбить с толку читателей, и не имело никаких целей, связанных с безопасностью.

150 г. до н. э., Греция. Греческий писатель Полибий использовал систему сигнализации, которая широко применялась как метод шифрования. Он записывал буквы алфавита в квадратную таблицу и заменял

их координатами: парами чисел (i, j), где i — номер строки, j — номер столбца.

50 г. до н. э., Италия. Юлий Цезарь освоил способ кодирования важных документов путем замены некоторых букв обычного алфавита и применял его для тайной правительственной переписки. Шифр Цезаря был проще ATBASH, но, принимая во внимание тот факт, что большинство людей в то время были неграмотными и читать не умели, оказался пригодным для передачи важных сообщений. Помимо замены ряда собственных букв алфавита, некоторые отдельные слова Цезарь писал на латинском, а некоторые — на греческом, чтобы окончательно сбить с толку злоумышленников. Данный способ шифрования подробно описан им в книге «Записки о галльской войне».

I в. до н. э., Италия. Первым знаменитым западным криптоаналитиком стал венецианец Джованни Соро, который прославился тем, что успешно вскрывал шифры многочисленных европейских княжеств.

200 г., Древний Египет. По данным историка криптографии Девида Кана, шифры применяли для записи на Лейденском папирусе так называемых волшебных рецептов. Предположительно, это были рецепты, чтобы заставить мужчину полюбить женщину или наслать на человека неизлечимую болезнь.

400 г., Индия. Кама Сутра от Ватсайана называет криптографию как умения, которые люди должны знать и практиковать как:

1) искусство понимания написанного в цифрах и написания слов особым способом;

2) искусство говорить, меняя установленный порядок слов.

725 г., арабские страны. Абу Ямади, создатель первого арабского словаря, написал книгу, рассказывающую, как взломать Византийский шифр, написанный в Греции. Его метод атаки базировался на предположении, что послание начинается со слов «во имя Бога», и он расшифровывал остальной текст исходя из этого предположения. Такой же метод атаки применялся во время Второй мировой войны для взлома немецких шифрованных сообщений.

855 г., арабские страны. Арабский ученый Абу Бакр Ахмед бен-Али бен-Вахшия ан-Набати включил описание нескольких классических шифров в свою книгу. Это была первая книга, специально посвященная описанию известных на то время шифров, и называлась она «Книга о большом стремлении человека разгадать загадки древней письменности».

1226 г., Венеция. В архивах Венеции можно отыскать шифр, суть которого заключается в том, что точки и кресты заменяют гласные в нескольких словах, находящихся в разных местах послания.

1250 г., Англия. Роджер Бэкон, английский монах, написал книгу «Секретные произведения искусства, и никакой магии». В ней он описывает несколько простых способов шифрования, таких как, например, использование только согласных букв или «магических изображений».

1327 г., Ватикан. Самый древний шифрованный документ, который хранится в архивах Ватикана, представляет собой небольшой список имен, составленный в 1326—1327 гг., когда в Италии шла борьба между сторонниками Папы Римского и приверженцами императора Священной Римской империи.

1379 г., Ватикан. Габриэль де Лавинд по просьбе папы Климентия VII составил комбинированный алфавит замены и новый способ шифрования — номенклатор, сочетающий в себе элементы шифра замены и кодирования. Этот способ шифрования оставался в общем употреблении среди дипломатов и некоторых штатских в течение последующих 450 лет, несмотря на то что придумывались более стойкие шифры, возможно, из-за удобства его использования.

1392 г., Англия. В книге «О движении планет», написанной англичанином Джефри Чосером, с целью избежать преследования инквизиции используется шифр замены. В некоторых разделах книги Чосер заменил буквы и цифры на другие буквы и цифры.

XIV в., Россия. Уже с XIV в. в Новгороде существовала техника тайного письма. Использовались в основном шифры простой замены. Благодаря торговым связям Новгорода с Германией в России становятся известными многие западные разработки, в том числе новые системы шифрования. Учреждение постоянной почтовой связи России с Европой послужило причиной развития шифрованной переписки.

1412 г., Османская империя. Познания арабов в области криптографии были подробно изложены в произведении Шехаба Калкашанди, которое представляет собой громадную 14-томную энциклопедию Сабхалаша, написанную в 1412 г. В ней дается систематический обзор всех важных областей знания.

Раздел под общим заголовком «Относительно сокрытия в буквах тайных сообщений» содержал две части: одна касалась символических действий и намеков, а другая была посвящена симпатическим чернилам и криптографии. Первый раз за всю историю шифров в энциклопедии приводился список как преобразований перестановки, так и преобразований замены. Более того, в пятом пункте списка впервые упоминался шифр, для которого была характерна более чем одна замена букв открытого текста.

Однако наиболее содержательным разделом труда является первое в истории описание криптоаналитического исследования шифрованного текста. Его истоки, очевидно, следует искать в интенсивном и скрупулезном изучении Корана многочисленными школами арабских грамматиков. Наряду с другими исследованиями они занимались подсчетом частоты встречаемости слов, пытаясь составить хронологию глав Корана, изучали фонетику слов, чтобы установить, являлись ли они подлинно арабскими или были заимствованы из других языков.

Большую роль в обнаружении лингвистических закономерностей, приведших к возникновению криптоанализа, сыграло также развитие лексикографии. Ведь при составлении словаря автору фактиче-

ски приходилось учитывать частоту встречаемости букв, а также то, какие буквы могут стоять рядом, а какие — никогда не встречаются по соседству.

Калкашанди начинает изложение криптоаналитических методов с главного: криптоаналитик должен знать язык, на котором написана криптограмма. Поскольку арабский язык, «самый благородный и самый прекрасный из всех языков», является «одним из наиболее распространенных», то далее дается пространное описание его лингвистических характеристик. Приводятся перечни букв, которые никогда не стоят вместе в одном слове, и букв, которые редко появляются по соседству, а также буквенные комбинации, которые в словах встретить невозможно. Последним идет список букв в порядке «частоты их использования в арабском языке в свете результатов изучения священного Корана».

Автор справедливо отмечает, что «в произведениях, не связанных с Кораном, частота использования может быть иной».

1466 г., Италия. Еще один значительный шаг вперед криптография сделала благодаря труду итальянца Леона Альберти. Известный философ, живописец, архитектор, он в 1466 г. написал труд о шифрах. В этой работе был предложен шифр, основанный на использовании шифровального диска. Диск состоял из неподвижной и подвижной частей. По окружности обеих частей диска наносились знаки алфавита, и подвижная часть диска могла поворачиваться на любой угол. Фиксация подвижной части диска задавала шифр простой замены, а диск мог поворачиваться как при шифровании каждой буквы, так и после шифрования некоторого участка сообщения. Ключом шифрованного сообщения являлась последовательность значений сдвигов диска. Шифр Альберти явился прообразом современных дисковых шифровальных машин.

1473 г., Италия. В рукописи, написанной Арналдусом де Брукселлой, использовался шифр для сокрытия способа создания философского камня.

1518 г., Германия. Богатым на новые идеи в криптографии оказался XVI в. Многоалфавитные шифры получили развитие в вышедшей в 1518 г. первой печатной книге по криптографии под названием «Полиграфия». Автором книги был один из самых знаменитых ученых того времени аббат Иоганнес Тритемий. В этой книге впервые в криптографии появляется квадратная таблица. Алфавиты, используемые для зашифрования, записаны в строки таблицы один под другим, причем каждый из них сдвинут на одну позицию влево по сравнению с предыдущим.

1549 г., Россия. Образуется Посольский приказ. В России появились первые профессиональные тайнописчики, состоящие на государственной службе. На службе в Посольском приказе находились также и люди, создававшие шифры.

1553 г., Италия. Итальянец Джован Батиста Белазо пришел к идее использования в криптографии пароля. Он построил теорию о методах шифрования текста таким образом, чтобы он мог быть расшифрован только с помощью соответствующего пароля.

1555 г., Италия. В 1555 г. в папской курии была учреждена должность секретаря по шифрам.

1557 г., Италия. Папские криптоаналитики вскрыли шифр испанского короля Филиппа II, который тогда воевал с Папой Римским.

1563 г., Италия. Воскресить смешанные алфавиты, которые применял Альберти, и объединить идеи Альберти с идеями Тритемия и Белазо в современную концепцию многоалфавитной замены выпало на долю итальянца Джованни делла Порта.

Ему было 28 лет, когда он в 1563 г. опубликовал книгу «О тайной переписке». По сути, эта книга являлась учебником по криптографии, содержащим криптографические познания того времени. Порта предложил использовать квадратную таблицу с периодически сдвигаемым смешанным алфавитом и паролем и советовал выбирать длинный ключ. Впервые им был предложен шифр простой биграммной замены, в котором пары букв представлялись одним специальным графическим символом. Они заполняли квадратную таблицу размером 20 × 20, строки и столбцы которой занумерованы буквами латинского алфавита.

1564 г., Италия. Белазо публикует описание модификации шифра, идея которого была ранее высказана Кардано, заключающейся в автоматическом выборе ключей для шифрования.

1585 г., Франция. Блез де Виженер написал книгу, описывающую первые криптографические системы с автоматическим выбором ключа для шифрования открытого текста, в которых при выработке ключа следующего письма используется предыдущее открытое или зашифрованное письмо.

1590 г., Франция. Успех в области дешифрования в 1590 г. пришел и к Франсуа Виету, которого в наши дни помнят как человека, которому обязана своим происхождением современная алгебра.

1598 г., Россия. Русский посол в Грузии К. П. Савин для шифрования документов применял шифр перестановки, в котором текст сообщения разбивался на слоги и осуществлялась перестановка букв в слогах.

Начало XVII в., Италия. Нельзя не упомянуть имени итальянца Матео Ардженти, работавшего в области криптографии. В начале XVII в. он составил руководство по криптографии на 135 листах, изданное в переплете из телячьей кожи. В этой книге впервые предложено использовать некоторое слово в качестве мнемонического ключа для смешанного алфавита. Началом смешанного алфавита служило ключевое слово (как правило, без повторяющихся букв), за которым следовали остальные буквы в их естественном порядке.

1623 г., Англия. Сэр Фрэнсис Бэкон описал шифр, который теперь носит его имя, — двухбуквенный шифр, известный сейчас как пятибитное двоичное кодирование. Бэкон применял шифрование совместно

с методами стеганографии путем сокрытия битов шифрованного текста в тексте произвольного письма.

1633 г., Россия. 8 августа 1633 г. вышел Указ Патриарха Филарета об обязательном шифровании дипломатической переписки. Этот день можно считать днем появления официальной российской криптографии.

XVII и XVIII вв., эра «черных кабинетов». XVII и XVIII вв. вошли в историю криптографии как эра «черных кабинетов». В этот период во многих государствах Европы, в первую очередь во Франции, получили развитие дешифровальные подразделения, названные «черными кабинетами». Первый из них был образован по инициативе кардинала Ришелье при дворе короля Людовика XIII. Его возглавил первый профессиональный криптограф Франции Антуан Россиньоль. Достижения этого криптографа действительно неоспоримы. Например, взятие крепости Эден французской армией было ускорено благодаря его работам по дешифрованию секретной переписки противника.

Следует отметить, что некоторые оригинальные идеи, возникшие в криптографии в этот период, связаны с именем самого Ришелье, который использовал, например, для секретной переписки с королем оригинальный шифр перестановки с переменным ключом.

В Англии тоже был свой «черный кабинет». В его работе в XVII в. заметное место занимал Джон Валлис, известный как крупнейший английский математик до Исаака Ньютона. Работы по вскрытию им шифров по указанию парламента привели к назначению Валлиса в 1649 г. в Оксфорд профессором геометрии в возрасте 32 лет. В своем труде «Арифметика бесконечного» он сделал выводы, которые послужили Ньютону стартовой площадкой для разработки интегрального исчисления. Валлис ввел знак для бесконечности и первый путем интерполяции вычислил число π. Кстати, само это обозначение также принадлежит ему.

В Европе получили широкое распространение шифры, называемые номенклаторами, объединявшие в себе простую замену и код. В простейших номенклаторах код состоял из нескольких десятков слов или фраз с двухбуквенными кодовыми обозначениями. Со временем списки заменяемых слов в номенклаторах увеличились до двух или трех тысяч эквивалентов слогов и слов. В царской России XVIII в. закодированное открытое сообщение шифровалось далее простой заменой.

В Германии начальником первого дешифровального отделения был граф Гронсфельд, создавший один из вариантов усовершенствования шифра Виженера. Он взял числовой, легко запоминаемый лозунг. Вместо таблицы Виженера использовался один несмешанный алфавит. При шифровании знаки открытого текста выписывались под цифрами лозунга. Очередная буква открытого текста заменялась буквой алфавита, отстоящей от нее вправо на количество букв, равное соответствующей цифре лозунга.

XVIII в., Россия. В 1702 г. учреждается Походная посольская канцелярия, сосредоточившая в своем ведении важнейшую политическую

переписку. Здесь выполняется вся работа по зашифрованию и расшифрованию переписки Петра I и его приближенных с различными корреспондентами, а также работа по созданию шифров и рекомендаций по их использованию.

В начале 1730-х гг. появляются совершенно новые тайнописные системы — алфавитные и неалфавитные коды, в начале 1740-х гг. — служба перлюстрации переписки иностранных дипломатов.

С конца 1740-х г. начинают употребляться шифры нового типа. Их принципиальным отличием от всех предыдущих систем было помещение в словарь особых знаков, обозначения которых означали, что при расшифровании отдельные участки шифртекста становились пустышками.

Чуть позднее начинает разрабатываться направление, связанное с изменением значности обозначений. Например, может оговариваться, что у некоторых обозначений не пишется первая цифра или несколько цифр (1, 2, 3 вместо 6001, 6002, 6003 и т. п.).

XIX в. Много новых идей в криптографию принес XIX в. Изобретение в середине века телеграфа и других технических видов связи дало новый толчок развитию криптографии. Информация передавалась в виде токовых и бестоковых посылок, т. е. представлялась в двоичном виде. Поэтому возникла проблема «рационального» представления информации, которая решалась с помощью кодов. Коды позволяли передать длинное слово или целую фразу двумя-тремя знаками. Появилась потребность в высокоскоростных способах шифрования и в корректирующих кодах, необходимых в связи с неизбежными ошибками при передаче сообщений. Однако еще до изобретения телеграфа появился ряд интересных шифровальных устройств.

1800 г., США. Приблизительно в 1800 г. была создана шифровальная система, занимающая особое место в истории криптографии. Речь идет о «дисковом шифре» Томаса Джефферсона — первого государственного секретаря США, ставшего позже третьим президентом.

1817 г., США. В 1817 г. американец Десиус Уодсворт сконструировал шифровальное устройство, которое также внесло новую идею в криптографию. Его нововведение состояло в том, что он сделал алфавиты открытого и шифрованного текстов различных длин. Устройство, с помощью которого он это осуществил, представляло собой диск, на котором были расположены два подвижных кольца с алфавитами. Внешний алфавит состоял из 26 букв и 7 цифр (от 2 до 8). Внутренний алфавит состоял лишь из 26 букв. Диск имел подобие неподвижной часовой стрелки, в двух прорезях которой появлялись расположенные друг под другом буквы алфавитов. На внутреннем кольце указывалась буква открытого текста, на внешнем кольце — соответствующая буква шифртекста. Оба кольца могли вращаться и были связаны друг с другом с помощью двух шестерен, одна из которых имела 33 зубца, а другая — 26. Буквы и цифры внешнего кольца были съемными и могли быть собраны в любом порядке. Перед зашифрованием корреспон-

денты договаривались относительно взаимного начального положения обоих колец. Для установки дисков в такое положение шестерни можно было разъединить.

Проследим на примере слова «введение» процесс зашифрования. Сначала внутреннее кольцо поворачивалось до тех пор, пока в прорези стрелки не показывалась буква «в». Стоящая в другой прорези буква внешнего кольца записывалась в качестве первой буквы шифртекста. Затем внутреннее кольцо вращалось до тех пор, пока буква «в» вновь не показывалась в прорези. Это вращение посредством шестеренок передавалось на внешнее кольцо, но из-за различия в числе букв алфавитов оно совершало лишь 26/33 полного оборота, в то время как внутреннее кольцо совершало полный оборот. Значит, второй знак шифртекста располагался во внешнем алфавите на расстоянии семи мест вперед от первого знака, несмотря на то что оба знака представляли одну и ту же букву открытого текста. Если этот процесс зашифрования осуществлять дальше, то шифробозначения для буквы «в» начнут повторяться лишь после того, как будут использованы все 33 буквы и цифры внешнего алфавита. Это объясняется тем, что числа 26 и 33 не имеют общих делителей, благодаря которым такое повторение могло бы произойти раньше. Следующие буквы открытого текста шифруются аналогично.

Такая шифрсистема реализует периодическую многоалфавитную замену. Различие чисел букв алфавитов открытого и шифрованного текстов приводит к существенным отличиям этой системы от предыдущих многоалфавитных систем. Так, в устройстве Уодсворда используется 33 шифралфавита, а не 24 или 26, как в системах Тритемия или Виженера. Важнее то, что эти алфавиты используются не непосредственно один за другим, а в произвольном порядке, который зависит от букв открытого текста. Этот факт служит гораздо более надежной защитой шифра, чем правильная последовательность использования алфавитов, как в системе Тритемия.

Идея Уодсворда была незаслуженно забыта. Славу ее открытия ныне приписывают английскому ученому Чарлзу Бебиджу.

1823 г., Россия. Барон П. Л. Шиллинг фон Канштадт (1786—1837) изобрел новые шифры биграммного типа. Словарь биграммного шифра составляли двузначные буквенные сочетания французского языка, кодовыми обозначениями являлись двух-, трех- или четырехзначные числа, по два для каждой биграммы. Причем шифровались не идущие подряд биграммы открытого текста, а сочетания букв, отстоящих друг от друга на 20—25 символов.

Вторая половина XIX в. Появился весьма устойчивый способ усложнения числовых кодов — гаммирование. Он заключался в перешифровании закодированного сообщения с помощью ключевого числа, которое и называлось гаммой. Шифрование с помощью гаммы состояло в сложении всех кодированных групп сообщения с одним и тем же ключевым числом. Эту операцию стали называть «наложение гаммы».

1853 г., Россия. Управляющим первой секретной экспедицией Канцелярии иностранных дел России бароном Н. Ф. Дризеном разработан первый биклавный шифр. Биклавный шифр представляет собой шифр многозначной замены, состоящий из 26 различных замен с достаточно сложным выбором замены на каждый знак открытого текста, определяемым двумя ключами. При этом отдельным знакам открытого текста соответствуют два знака шифрованного текста. Таким образом, длина шифртекста не соответствует длине открытого текста.

1854 г., Англия. Англичанин Чарльз Уитстон изобрел шифр, который позже стали называть шифром Плейфера. Дело в том, что Лион Плейфер, заместитель председателя Палаты общин, министр почт, председатель Британской ассоциации развития науки, был не только другом Уитстона, но и внешне был похож на него, так что их часто путали. В 1854 г. Плейфер продемонстрировал систему шифрования, которую он назвал «недавно открытый симметричный шифр Уитстона». Это был первый из известных биграммных буквенных шифров. То обстоятельство, что Плейфер популяризировал изобретение Уитстона, сохранило его имя в названии шифра. Этот шифр использовался англичанами в период Первой мировой войны.

1857 г., Англия. Шифр адмирала Фрэнсиса Бифорта (вариант шифра Виженера) был опубликован его братом после смерти Бифорта в виде карты размером 4×5 дюймов.

1859 г., США. Плини Ирл Чейз опубликовал первое описание томографического шифра.

1861 г., Германия. Фридрих Казиски опубликовал книгу, содержащую описание общего метода взлома многоалфавитного шифра с повторяющимся ключом. Тем самым завершилась многовековая эпоха неприступного многоалфавитного шифра.

1865 г., США. В период Гражданской войны в США (1861—1865) южане использовали шифры на основе перестановки столбцов, в то время как войска Конфедерации использовали шифр Виженера, способ взлома которого к тому времени уже был опубликован Казиски.

1872 г., Нидерланды. В 1872 г. Кирхгофс в возрасте 47 лет написал книгу «Военная криптография». В ней сформулированы шесть конкретных требований к шифрам, два из которых относятся к стойкости шифрования, а остальные — к эксплуатационным качествам. Одно из них, сформулированное как «компрометация системы не должна причинять неудобств корреспондентам», стало называться принципом Кирхгофса.

Суть этого принципа состоит в том, что стойкость шифра определяется лишь степенью секретности ключа. Оценка качества шифра должна проводиться при условии, что о данном шифре известно все, кроме используемого для зашифрования информации ключа.

1873 г., Англия. Военное министерство Англии учредило подразделение разведки, состоящее из 27 человек.

1891 г., Франция. Майор Этьен Базери создал свою версию дискового шифратора и после того, как французская армия отказалась

принять его на вооружение, опубликовал устройство своего шифра в 1901 г.

1895 г. Изобретено радио. Важность этого события для криптографии была огромна. Во время войны оно позволяло прослушивать большинство переговоров противника. Таким образом, появилась профессия криптоаналитика, или взломщика зашифрованных сообщений.

1913 г., США. Капитан Паркет Хитт переделал дисковый шифратор в ленточную форму, что привело к созданию шифрмашины М-138-А, использовавшейся США впоследствии во время Второй мировой войны.

1914—1917 гг., Первая мировая война. Осенью 1914 г., в начале Первой мировой войны французы, будучи подготовленными, уже имели станции для прослушивания германских переговоров. Они много усилий потратили на сбор шифрсообщений, хотя и не имели времени и средств для их расшифровки.

Немцы использовали шифр перестановки, который было очень сложно взломать без помощи компьютера. Однако, когда французы смогли найти разные сообщения одинаковой длины, стало возможным сравнительно легко взломать их. Один раз, определив ключ, союзники могли использовать его, чтобы взломать любую германскую передачу в период 8—10 дней, в течение которых применялся данный ключ.

В декабре 1914 г. была создана и начала работу английская дешифровальная служба, получившая название «Кабинет 40».

За период 1914—1916 гг. в России дешифровано 588 австрийских телеграмм, 60 — германских, 606 — болгарских, 225 — турецких, 457 — итальянских и т. д. Причем дешифрование проводилось не только с помощью добытых разведкой шифров и кодов, но и за счет аналитической дешифровальной работы.

В 1915 г. немцы изменили способы шифрования, введя усложненные шифры замены. Данные шифры предусматривали 24 возможных алфавита и комбинации из них. Эти шифры были гораздо более сложными, но французы уже были готовы к этому, постоянно взламывая немецкие сообщения.

В 1916 г. французский офицер Джозеф О. Моборн переделал ленточный шифр Хитта в дисковую форму, что привело к созданию шифровального устройства М-94. Союзники начали использовать «кодовую книгу» в телефонной связи.

Немцы последовательно прослушивали телефонные переговоры, так как вначале шифровались только радиосообщения. После катастрофических людских потерь, являющихся результатом перехвата немцами телефонных переговоров, французский генерал Дубэйл предложил шифрование и таких сообщений.

1917 г., США. В 1917 г. в Америке появился первый криптоаналитик. Им стал Уильям Фредерик Фридман, «отец американского криптоанализа». Сначала вместе с женой Элизабет Фридман работал в специальной лаборатории при правительстве США, а спустя некоторое время открыл свою школу в Ривербэнке. В функции первого криптоаналитика

входило изучение различных вариантов кодирования информации на предмет их взлома. Известно, что системы иногда оказывались несовершенными, и задачей Фридмана стало выявление их уязвимостей.

В тот период появились талантливые ученые и инженеры, ставшие впоследствии известными криптографами. В их числе был Г. О. Ярдли, который вскоре после вступления США в войну в 1917 г. убедил военное министерство в необходимости создания криптографической службы. В 27 лет он был назначен начальником криптографического отдела (MI-8) разведки военного министерства. При отделе было создано учебное отделение по подготовке криптоаналитиков для американской армии. Отдел MI-8 добился больших успехов в дешифровании дипломатической переписки многих развитых стран. В 1919 г. отдел был преобразован в «черный кабинет» с финансированием от военного министерства и госдепартамента в объеме 100 тыс. долл. в год. Одной из главных задач «черного кабинета» было раскрытие японских кодов, некоторые из которых содержали до 25 тыс. кодовых величин.

Значительный успех в криптографии связан с еще одним американцем — Г. Вернамом. У Вернама был редкий склад ума, который позволял ему придумывать оригинальную электрическую цепь и затем переносить ее на чертежный холст, не воспроизводя все требуемые соединения с помощью проводов. В 1917 г. он, будучи сотрудником телеграфной компании, предложил идею автоматического шифрования телеграфных сообщений. Речь шла о своеобразном наложении гаммы на знаки алфавита, представленные в соответствии с телетайпным кодом Бодо пятизначными импульсными комбинациями. Например, буква «а» представлялась комбинацией ($++—— — $++———), а комбинация ($++ — ++$++—++) представляла символ перехода от букв к цифрам. На бумажной ленте, используемой при работе телетайпа, знаку «+» отвечало наличие отверстия, а знаку «—» его отсутствие. При считывании с ленты металлические щупы проходили через отверстия, замыкали электрическую цепь и тем самым посылали в линию импульс тока.

Вернам предложил покоординатно складывать импульсы знаков открытого текста с импульсами гаммы, предварительно нанесенными на ленту. Сложение проводилось по модулю 2. Вернам сконструировал и устройство для такого сложения. Замечательно то, что процесс шифрования оказывался полностью автоматизированным и в предложенной схеме исключался шифровальщик. Кроме того, оказывались слитыми воедино процессы шифрования, расшифрования и передачи информации по каналу связи. Тем самым наряду с традиционной схемой предварительного шифрования, когда по каналу передается предварительно зашифрованное сообщение, было положено начало линейному шифрованию. Главное в его изобретении заключалось в том, что больше не требовалось осуществлять зашифрование и расшифрование секретных сообщений в виде отдельных операций. В 1918 г. два комплекта соответствующей аппаратуры успешно прошли испытания.

1917—1929 гг., США. В период с 1917 по 1929 г. специалистам «черного кабинета» удалось дешифровать более 45 тыс. криптограмм различных стран, в том числе и Японии. Ярдли, желая закрепить успех, подготовил докладную записку Президенту США о мерах по укреплению своей службы. Однако ставший в то время Государственным секретарем Г. Стимсон был шокирован, узнав о существовании «черного кабинета», и полностью осудил его деятельность. Ему принадлежит знаменитая фраза: «Джентльмены не читают писем друг друга». Финансирование «черного кабинета» было прекращено, и Ярдли лишился работы. Он написал книгу «Американский черный кабинет», в которой рассказал о многих успехах по дешифрованию. Книга была издана большими тиражами в ряде стран и произвела эффект разорвавшейся бомбы. Позже Ярдли написал книгу «Японские дипломатические секреты», в которой приводились многие японские телеграммы. Рукопись этой книги была конфискована по решению суда. Последние годы жизни Ярдли не занимался криптографией. Он умер в 1958 г. и был похоронен с воинскими почестями на Арлингтонском национальном кладбище.

Почти половина XX в. была связана с использованием дисковых шифраторов. Различные их конструкции были запатентованы примерно в одно и то же время (в период 1917—1919 гг.) в разных странах: американцем Э. Х. Хеберном, голландцем Х. Ф. Кохом, немцем А. Шербиусом и шведом А. Г. Даммом. Чертежи своей схемы на основе шифрующего диска Хеберн представил в 1917 г., и уже в следующем году был построен первый дисковый аппарат, получивший одобрение ВМС США. В 1921 г. Хеберн основал первую в США компанию по производству шифрмашин, которую через десять лет ждал бесславный конец, связанный с финансовыми трудностями.

1918 г., США. США наняли восемь индейцев из племени чоктоу, чтобы передавать важные сообщения по незащищенным каналам на их родном языке. Так как этот язык чрезвычайно сложный и труден для выучивания, получился простой и эффективный способ шифрования.

1918 г., Германия. Шифрсистема ADFGVX была взята немцами на вооружение уже в конце Первой мировой войны. Это был шифр, который выполнял замену, разбиение на блоки и затем перестановку блоков текста. Он был взломан французским криптоаналитиком лейтенантом Джорджем Пэйнвином.

В том же году 39 летний инженер-электрик Артур Шербиус получил патент на шифровальную машину нового типа «Энигма».

1919 г., Нидерланды. Хьюго Александр Кох запатентовал шифровальную машину роторного типа в Нидерландах. Он передал патентные права на нее Артуру Шербиусу, который и начал ее продажу с 1926 г.

1919 г., Швеция. Арвид Герхард Дамм подал патентную заявку на механическую шифровальную машину роторного типа в Швеции.

Эта машина стала первой из семейства машин, созданных под руководством Бориса Сезара Вильгельма Хагелина, бывшего в то время единственным криптографом, который занимался торговлей и мог вести прибыльный бизнес.

1919 г., Англия. 1 ноября 1919 г. в Англии учреждено Правительственное училище шифровальщиков.

1919—1920 гг., Россия. В России разработаны и применялись шифры: «Пулемет», «Агитатор», «Советский» и др.

1921 г., США. Эдвард Хью Хеберн основал компанию «Электрический код Хеберна», производившую электромеханические шифровальные машины.

1921 г., Россия. Вскрыт немецкий дипломатический шифр, представлявший собой цифровой пятизначный код с перешифровкой гаммой многоразового использования. В августе 1921 г. осуществлено дешифрование первых турецких дипломатических телеграмм.

Дешифрована переписка контрреволюционной организации «Народный союз защиты родины и свободы», использовавшей шифры пропорциональной замены. Также раскрывались шифры и коды монархических организаций.

1923 г., Германия. Артур Шербиус основал компанию «Chiffriermaschinen Aktiengesellschaft» по сборке и продаже машин «Энигма».

1924 г., Германия. Александр фон Крыха изготовил свою кодовую машину, которая позднее использовалась Германским дипломатическим корпусом. Однако она имела криптографическую слабость — малый период. Тестовая криптограмма была взломана американскими криптоаналитиками за 2 ч 41 мин. Тем не менее эта машина продолжала продаваться и использоваться.

1927 г., Швеция. В 1927 году Борис Хагелин возглавил фирму, выкупленную его семьей. Свою следующую машину B-211 он снабдил печатающим устройством, работавшим со скоростью около 200 знаков в минуту. Она была самой портативной печатающей шифровальной машиной до 1934 г. Этот шифратор весил около 17 кг и помещался в деревянном корпусе размером с большой портфель.

1927—1933 гг., США. С введением сухого закона в США начался век криминальной криптографии. По отчету, составленному в середине 1930-х гг. Элизабет Фридман, криптография, использовавшаяся криминальными структурами, была «такой сложности, которая никогда не использовалась никаким правительством даже в самых секретных коммуникациях».

1929 г., США. Лестер Хилл опубликовал книгу «Криптография в алгебраическом алфавите», в которой была предложена операция шифрования блоков открытого текста с помощью матричных операций.

1930-е гг., Англия. Англичане сконструировали шифровальную машину TYPEX, базирующуюся на коммерческом варианте шифратора «Энигма». Эта машина содержала пять роторов, каждый из которых менял буквы алфавита на другие. После того как зашифрованная буква

печаталась, роторы меняли позицию, создавая совершенно новую схему шифрования для следующей буквы.

1930-е гг., США. В этот период времени была создана американская шифровальная машина SIGABA (M-134-C). Историк криптографии Дэвид Канн приписывает ее создание Уильяму Фридману, в то время как Диворс — Франку Роулетту, одному из служащих Фридмана.

Шифровальная машина SIGABA была лучше роторных изобретений Хеберна и Шербиуса, так как она использовала псевдослучайное пошаговое движение составных роторов на каждом шаге шифрования, что было предпочтительнее единообразного пошагового движения роторов в «Энигме». В ней использовалось 15 роторов (10 — для преобразования букв, 5 — вероятно, для контроля пошагового выполнения), в то время как в «Энигме» использовалось только три или четыре.

1930-е гг., Россия. В России велась разработка телефонного шифратора под руководством В. А. Котельникова, ставшего впоследствии академиком, ученым с мировым именем. Ему принадлежит знаменитая теорема дискретизации (или теорема отсчетов), лежащая в основе теории цифровой обработки сигналов. Идея состояла в передаче телефонного сообщения по нескольким (в простейшем случае — по двум) цепям поочередными импульсами в некоторой быстро изменяющейся последовательности. Предлагалось разнести такие линии на значительное расстояние друг от друга с тем, чтобы устранить возможность подключения сразу ко всем одновременно. Подключение же к одной из них позволяло бы слышать лишь отдельные неразборчивые сигналы. В более поздних разработках предлагались различные преобразования непосредственно самой речи. Звуки речи преобразуются телефоном в непрерывный электрический сигнал, который с помощью соответствующих устройств изменяется шифратором по законам электричества. К числу возможных изменений относятся: инверсия, смещение или деление диапазона частот, шумовые маскировки, временные перестановки частей сигнала, а также различные комбинации перечисленных преобразований. Естественно, каждое из указанных преобразований производится под управлением ключа, который имеется у отправителя и получателя. Наиболее просто реализуемым являлось преобразование инверсии. Сложнее реализовались временны́е перестановки. Для их осуществления речевой сигнал в некоторый промежуток времени предварительно записывался на магнитофонной ленте. Запись делилась на отрезки длительностью в доли секунд. Отрезки с помощью нескольких магнитных головок разносились и перемешивались, в результате чего в канале слышалась хаотическая последовательность звуков. Использовалась также движущаяся магнитная головка, которая в зависимости от направления движения считывала сигналы быстрее или медленнее, чем они были записаны на ленте. В результате тон сигналов становился выше или ниже обычного, в канале быстро чередовались высокие и низкие звуки, не воспринимаемые ухом.

Следует отметить, что одной из самых сложных проблем, которые возникали при разработке телефонных шифраторов, была проблема узнавания восстановленной после расшифрования речи.

1931 г., Россия. В начале года созданы объединенные шифровально-разведывательные курсы для подготовки криптографов дипломатического и военного направлений.

1932 г., Россия. Под руководством инженера И. П. Волоска был создан первый опытный образец шифровальной машины на основе принципа наложения комбинаций, так называемой гаммы бесконечного ключа, на комбинации знаков открытого текста. Эта машина называлась ШМВ-1. Из-за своей громоздкости она не пошла в серию, но послужила прототипом для создания новых серийных образцов.

1933—1945 гг., Германия. Шифровальная машина «Энигма» не имела коммерческого успеха, но была принята и усовершенствована, чтобы стать криптографической системой нацистской Германии.

1934 г., Россия. Создана и принята на вооружение шифровальная машина М-100. Несмотря на свою громоздкость (общий вес достигал 141 кг.), данная техника выпускалась серийно и в 1938 г. была успешно испытана в боевых условиях на озере Хасан, в 1939 г. — на Халхин-Голе, в Испании и в 1939—1940 гг. — во время финской войны.

1937 г., США. В США в 1937 г. принят в эксплуатацию первый телефонный шифратор под названием А3. Согласно имеющимся данным именно по такому шифратору президент Рузвельт получил известие о начале Второй мировой войны утром 1 сентября 1939 г.

Шифратор А3 осуществлял инверсию и перестановку пяти поддиапазонов частот. Из 3840 возможных комбинаций фактически использовались лишь шесть, которые менялись 36 раз за каждые 20 с. При этом криптографические слабости компенсировались регулярным изменением частот передачи. Стоит отметить, что такой принцип построения до сих пор находит применение в различных устройствах, например телефонных аппаратах сети GSM.

1937 г., Япония. Японцы изобрели так называемую пурпурную шифровальную машину. Многие машины до этого использовали роторы для изменения позиции букв в алфавите. Вместо этого пурпурная машина использовала телефонные пошаговые переключатели, при этом известные на тот момент времени методы криптоанализа становились неэффективными.

Известно, что код, генерируемый этой машиной, был взломан американским криптографом Фридманом.

1939 г., Англия. Союзники получили первое представление о машине «Энигма», после того как польская разведывательная служба похитила один из аппаратов.

1939 г., США. Выдающиеся результаты в применении математических методов в криптографии принадлежат американскому инженеру Клоду Шеннону. Шеннон получил образование по электронике и математике в Мичиганском университете, где и начал проявлять интерес

к теории связи и теории шифров. В 1940 г. он получил степень доктора по математике, в течение года обучался в Принстонском институте усовершенствования, после чего был принят на службу в лабораторию компании Bell Telephone. К 1944 г. Шеннон завершил разработку теории секретной связи. В 1945 г. им был подготовлен секретный доклад «Математическая теория криптографии», который был рассекречен и издан в 1949 г.

В данной работе излагается теория так называемых секретных систем, служащих фактически математической моделью шифров. Помимо основных алгебраических (или функциональных) свойств шифров, постулируемых в модели, множества сообщений и ключей наделяются соответствующими априорными вероятностными свойствами, что позволяет формализовать многие постановки задач синтеза и анализа шифров. Так, и сегодня при разработке новых классов шифров широко используется принцип Шеннона рассеивания и перемешивания, состоящий в использовании при шифровании многих итераций рассеивающих и перемешивающих преобразований, см. гл. 7.

Разработанные Шенноном концепции теоретической и практической стойкости позволяют количественно оценивать криптографические качества шифров и пытаться строить в некотором смысле идеальные, или совершенные, шифры.

Шенноном также моделируется язык открытых сообщений. А именно, предлагается рассматривать язык как вероятностный процесс, который создает дискретную последовательность символов в соответствии с некоторой вероятностной схемой. Центральной в работах Шеннона является концепция избыточной информации, содержащейся в текстовых сообщениях. Избыточность означает, что в сообщении содержится больше символов, чем в действительности требуется для передачи содержащейся в нем информации. Например, всего лишь десять английских слов — *the, of, and, to, a, in, that, it, is, i* — составляют более 25 % любого английского текста. Легко понять, что их можно изъять из текста без потери информации, так как их легко восстановить по смыслу или контексту.

Фактически Шеннон показал, что успех криптоанализа определяется тем, насколько избыточность, имеющаяся в сообщении, переносится в шифрованный текст. Если шифрование удаляет избыточность, то восстановить текст сообщения по криптограмме становится принципиально невозможно. Задачу дешифрования Шеннон рассматривал как задачу вычисления апостериорных знаний противника о шифре после перехвата криптограммы. Дело в том, что вероятности сообщений и ключей составляют априорные знания противника, которыми он располагает в соответствии с принципом Кирхгофса. После перехвата криптограммы он может (по крайней мере, в принципе, поскольку множества сообщений и ключей конечны) вычислить апостериорные вероятности возможных ключей и сообщений, которые могли быть использованы при составлении данной криптограммы.

1940 г., Англия. При непосредственном участии английского инженера и математика Алана Тьюринга сконструирована машина Bombe (бомба), которая декодировала сообщения, зашифрованные «Энигмой».

1942 г., США. Американцы стали использовать индейцев племени навахо, так же как использовали индейцев из племени чоктоу в Первую мировую войну: они говорили важные сообщения на своем родном языке так, что противник не мог понять их содержание.

1943 г., Россия. Создана новая шифрмашина М-101 «Изумруд». В этом же году в войска было отправлено свыше 90 комплектов М-101. До этого времени использовалась малогабаритная дисковая кодировочная машина К-37 «Кристалл».

1946 г., Великобритания. Был создан Центр правительственной связи Великобритании, который стал наследником правительственной школы кодов и шифров, созданной для радиошпионажа еще в 1919 г. В центре работали специалисты, сумевшие взломать немецкую шифровальную машину «Энигма».

1949 г., Россия. С целью существенного усиления советской криптографической службы создано Главное управление специальной службы (ГУСС).

Вторая половина XX в. Вслед за развитием элементной базы вычислительной техники появились электронные шифраторы, разработка которых потребовала серьезных теоретических исследований во многих областях прикладной и фундаментальной математики, в первую очередь алгебре, теории вероятностей и математической статистике. Сегодня именно электронные шифраторы составляют наибольшую часть средств шифрования. Они удовлетворяют все возрастающим требованиям по надежности и скорости шифрования. Прогресс в развитии вычислительной техники сделал возможным программные реализации криптографических алгоритмов, которые все увереннее вытесняют во многих сферах традиционные аппаратные средства.

1970 г., США. В исследовательской лаборатории IBM доктором Хорстом Фейстелем разработан шифр Люцифер. После нескольких модификаций этот алгоритм трансформировался в алгоритм DES, ставший на долгие годы национальным стандартом США (см. п. 7.4.1).

1976 г., США. Уитфилд Диффи и Мартин Хеллман опубликовали работу «Новые направления в криптографии», знакомящую читателей с идеей открытого криптографического ключа. Они также предложили идею аутентификации, основанной на применении сложной однонаправленной функции.

1977 г., США. Вдохновленные статьей Диффи — Хеллмана американские криптографы Рональд Ривест, Ади Шамир и Леонард Адлеман исследовали возможность реализации на практике криптографических систем с открытым ключом.

После долгих стараний Ривест придумал соответствующий алгоритм, получивший в дальнейшем название схемы RSA. Он тщательно описал его для Шамира и Адлемана и послал им для обсуждения.

Это была практическая реализация шифра с открытым ключом, основывающегося на трудоемкости разложения на множители больших целых чисел. В апреле 1977 г. авторы представили алгоритм шифрования для публикации в научном журнале Scientific American. Статья была опубликована в сентябре того же года и содержала предложение послать полное техническое описание любому, приславшему конверт с обратным адресом. Были получены тысячи подобных запросов со всех концов мира.

Еще один взгляд на возникновение схемы RSA мы излагаем во введении к гл. 10.

1980-е гг., США. Д. Гиффорд предложил схему поточного шифра, которая использовалась с 1984 по 1988 г. агентством Associated Press.

1984 г., США. Пользователями сети USENET использовался шифр ROT-13. Идея заключалась в чередовании букв в алфавите с периодом 13. Так как каждый знал ключ и не было никакой секретности, идея использования данного шифра заключалась в зашифровании сведений так, чтобы на них случайно не наткнулись. По-видимому, это был первый случай применения криптографии обычными гражданами для защиты от проводимой правительством перлюстрации электронных сообщений.

1985 г., США. Тахиром Эль Гамалем была предложена еще одна схема асимметричного шифрования, которая является одним из вариантов метода выработки открытых ключей Диффи — Хеллмана.

1989 г., Россия. В России установлен единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ — алгоритм ГОСТ 28147—89 (в англоязычной литературе просто GOST) (см. п. 7.4.2).

Алгоритм ГОСТ 28147—89 был единственным официально разрешенным для использования алгоритмом шифрования в течение 26 лет.

1990 г., США. Чарльз Беннет и Жиль Брассард опубликовали результаты исследований по квантовой криптографии, суть которых состоит в использовании одиночных фотонов для создания потока ключевых битов с целью последующего зашифрования сообщений методом Вернама.

Следуя законам квантовой механики, квантовая криптография обеспечивает не только секретность, но и помогает определить факт перлюстрации передаваемой информации.

1991 г., США. Американцем Филом Циммерманном выпущена первая версия программы PGP. Данная программа была первой, получившей большое распространение среди обычных пользователей, и использовалась для шифрования почтовых сообщений. Программа PGP использовала для шифрования и аутентификации пользователей схему RSA.

В настоящее время данная программа трансформировалась в пакет GPG, который распространяется в исходных кодах, доступных для скачивания любому желающему. Наличие исходных кодов программы позволяет проверить, что код не содержит закладок.

1992 г., Россия. Нашумевшее дело о так называемых чеченских авизо, когда со счетов Государственного банка России по поддельным платежным документам было похищено более триллиона рублей (в ценах 1992 г.). Разработка и внедрение во всех отделениях расчетно-кассовых центров алгоритмов шифрования для подтверждения подлинности платежных поручений. Идея ведения процедуры подтверждения платежных документов послужила основой для разработки и принятия закона об электронной цифровой подписи.

В том же году была создана Академия криптографии Российской Федерации. Президентом Академии криптографии избран Николай Николаевич Андреев, генерал-полковник в отставке, доктор технических наук, профессор, лауреат Ленинской и Государственной премий. Вице-президентом Академии криптографии избран Владимир Николаевич Сачков, генерал-лейтенант в отставке, доктор физико-математических наук, профессор, лауреат Государственной премии.

2001 г., Россия. Разработка и принятие Федерального закона «Об электронной цифровой подписи», появление удостоверяющих центров, введение понятия сертификата ключа и условий использования электронной цифровой подписи.

2001 г., США. Замена в национальном стандарте США алгоритма DES на новый алгоритм Rijndael, ставший победителем открытого конкурса (см. п. 7.5.1).

2011 г., Россия. Утратил силу Федеральный закон «Об электронной цифровой подписи». Принят Федеральный закон «Об электронной подписи», введены условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью.

2015 г., Россия. Принятие нового алгоритма блочного шифрования «Кузнечик» в качестве национального стандарта Российской Федерации ГОСТ Р 34.12—2015 (см. п. 7.5.1).

Принятие нового национального стандарта Российской Федерации ГОСТ Р 34.13—2015, регламентирующего режимы использования блочных шифров.

На этом очерк по истории криптографии можно завершить. Как очевидно из приведенных выше материалов, на современном этапе развития большинством стран приняты криптографические стандарты, на основе которых разрабатываются защищенные методы хранения и передачи информации.

Дополнительная литература к главе 1

1. *Бабаш А. В., Шанкин Г. П.* История криптографии. Ч. 1. — М. : Гелиос АРВ, 2002.

2. *Бутырский Л. С., Ларин В. А., Шанкин Г. П.* Криптографический фронт Великой Отечественной. — 2-е изд. — М. : Гелиос АРВ, 2013.

3. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации) : учеб. пособие / под ред. В. А. Садовничего. — М. : Высшая школа, 1999.

4. *Русецкая И. А.* История криптографии в Западной Европе в раннее новое время. — СПб. : Центр гуманитарных инициатив. Университетская книга, 2014.

5. *Соболева Т. А.* История шифровального дела в России. — М. : Олма-Пресс, 2002.

6. *Garner M.* Codes, Ciphers and Secret Writing. — Simon & Shuster. — New York, 1972.

7. *Kahn D.* The Codebreakers. — McMillian. — New York, 1967. В русском переводе: *Кан Д.,* Взломщики кодов. М. : Центрполиграф, 2000.

Глава 2
ОСНОВНЫЕ ПОНЯТИЯ И ЗАДАЧИ КРИПТОГРАФИИ

В результате изучения данной главы студент должен:

знать

- основные задачи криптографии;
- формальные модели шифров;
- основные модели осмысленных сообщений;

уметь

- строить формальные модели шифров;
- оценивать число осмысленных сообщений;

владеть

- навыками применения криптографических методов для обеспечения конфиденциальности информации;
- навыками применения криптографических методов для обеспечения целостности информации.

2.1. Задачи криптографии и средства их решения

Криптография (в переводе с греческого — тайнопись) — наука о методах построения шифров, т. е. методах преобразования исходной информации в форму, недоступную для понимания противником. В криптографических исследованиях разрабатываются средства и методы решения следующих задач.

1. *Конфиденциальность*. Защита от ознакомления с содержанием информации (сообщения) лицами, не обладающими правом доступа. При этом:

- не скрывается сам факт передачи сообщения;
- зашифрованное сообщение передается по открытому каналу связи.

Этим криптографические методы отличаются от стеганографических методов, связанных с сокрытием секретного сообщения в «открытом контейнере», например в графическом рисунке или аудиофайле, а также от организационно-технических методов, связанных с защитой канала связи от перехвата передаваемых сообщений (экранирование проводного канала связи от излучений, использование «прыгающих» частот в радиоканалах и др.).

2. *Целостность*. Обеспечение невозможности несанкционированного изменения исходной информации (вставка, удаление или замена части исходных данных). Криптография предоставляет надежные средства обнаружения любых манипуляций с данными.

3. *Аутентификация*. Доказательное подтверждение подлинности сторон и передаваемой информации в процессе информационного взаимодействия. Аутентификация передаваемой информации может проводиться по источнику, содержанию, времени создания и (или) пересылки, а также по другим параметрам.

4. *Невозможность отказа от авторства*. Разработка методов предотвращения возможности отказа от ранее совершенных действий.

2.1.1. Конфиденциальность

Обеспечение *конфиденциальности* информации при ее передаче по открытому, т. е. доступному для контроля злоумышленником, каналу связи в преобразованном виде является традиционной задачей криптографии. Под преобразованием мы понимаем процесс *зашифрования* информации, т. е. ее преобразования с помощью некоторого секретного значения, называемого *ключом*.

При этом процесс зашифрования должен быть обратимым, т. е. допускающим однозначное расшифрование. В общем виде для алгоритмов шифрования и расшифрования используются разные ключи.

Если обозначить алгоритм зашифрования на ключе k_e через E_{k_e}, а процесс расшифрования на ключе k_d, соответственно, D_{k_d}, то должны выполняться соотношения

$$E_{k_e}(x) = y, \quad D_{k_d}(y) = x,$$

где x — открытый текст, подлежащий зашифрованию, а y — шифрованный текст, являющийся результатом операции зашифрования.

Определение 2.1. Совокупность, включающую в себя:
— алгоритмы зашифрования и расшифрования,
— ключевое множество, из которого выбираются ключи зашифрования и расшифрования,
— а также другие используемые криптографические алгоритмы преобразования исходного сообщения,
мы будем называть *шифрсистемой*, или коротко — *шифром*.

В симметричных шифрсистемах знание ключа зашифрования k_e позволяет без существенных затрат вычислить и ключ расшифрования k_d — как правило, эти ключи совпадают. Факт совпадения ключей зашифрования и расшифрования послужил причиной возникновения названия «*симметричные шифрсистемы*».

В несимметричных системах вычисление ключа расшифрования k_d по ключу k_e является сложной математической проблемой. Это позво-

ляет в таких шифрсистемах сделать ключ зашифрования общедоступным (открытым) и держать в секрете только ключ для расшифрования. В этой связи такие криптосистемы называют системами *с открытым ключом*. Отметим, что следуя терминологии, пришедшей к нам из зарубежных публикаций, для асимметричных шифрсистем часто применяется название «*асимметричная схема шифрования*».

Ключ является важнейшим элементом шифрсистемы, и к нему предъявляются следующие требования.

1. Выбор ключа зашифрования k_e должен производиться по случайной равновероятной схеме из ключевого множества K. При этом вероятность выбора ключа k не должна зависеть от шифруемого (защищаемого) открытого текста.

2. Мощность ключевого множества K должна быть достаточно большой, чтобы исключить возможность опробования нарушителем всех возможных значений ключа.

3. При смене ключа зашифрования новый ключ должен выбираться независимым от ранее использованных ключей.

4. Для несимметричных шифрсистем выбор ключей производится с учетом необходимых теоретико-числовых требований к ним.

Не существует единого алгоритма шифрования, удовлетворяющего всем практическим запросам. Это объясняется большим разнообразием:

- типов защищаемой информации;
- потребностей в скорости и объемах передачи защищаемой информации;
- задач по криптографической защите информации.

При исследовании шифрсистем изучается вопрос о возможности раскрытия злоумышленником содержания конфиденциальной информации с использованием любых доступных ему методов. Под *злоумышленником* понимается любой субъект, не имеющий права ознакомления с передаваемой информацией. Злоумышленника также часто называют нарушителем или противником.

При проведении исследований (криптоанализе) действия злоумышленника моделируются. При этом допускается, что с передаваемой по открытым линиям связи информацией противник может совершать как пассивные действия — копирование с целью проведения дальнейших исследований, так и активные — имитацию передачи зашифрованного сообщения или его подмену.

2.1.2. Целостность

Для обеспечения *целостности* передаваемой информации к сообщению $x \in X$ добавляется проверочная комбинация $h = H(k, x)$, называемая *имитовставкой*, или *кодом аутентичности сообщения*. Как правило, имитовставка является значением зависящей от секретного ключа $k \in K$ функции H,

$$H : K \times X \to V_n,$$

которая отображает исходные сообщения произвольной длины в последовательность символов фиксированной длины. Такие функции называют ключевыми функциями хэширования, или коротко — хэш-функциями.

К ключевым хэш-функциям предъявляются в том числе следующие требования:

- невозможность вычисления ее значения $h = H(k, x)$ без знания ключа k;
- невозможность подбора для заданного сообщения x с известным значением $h = H(k, x)$ другого сообщения x' с тем же значением $h = H(k, x')$ без знания ключа k.

Добавим, что более подробно функции хэширования рассматриваются нами в гл. 8.

Для обеспечения целостности по каналу связи передается пара (x, h) — сообщение x и его код аутентичности h. На приемном конце получатель сообщения x вычисляет код аутентичности полученного сообщения и сравнивает его с полученным значением. Несовпадение соответствующих величин свидетельствует о том, что данные были изменены.

Параметры алгоритма вычисления имитовставки выбираются так, чтобы без знания секретного ключа вероятность навязывания противником ложной (искаженной или подделанной) информации была мала. Указанная вероятность служит *мерой имитостойкости* шифра, т. е. способности противостоять активным атакам нарушителя.

2.1.3. Аутентификация

Аутентификация представляет собой установление подлинности взаимодействующих сторон, передаваемых сообщений, сеанса связи и др. и является важной частью задачи обеспечения достоверности получаемой информации.

Применительно к сторонам взаимодействия шифрсистемы аутентификация означает проверку одной из сторон того, что взаимодействующий с ней абонент является законным участником, т. е. тем, за кого он себя выдает. Каждый законный пользователь шифрсистемы должен иметь собственный уникальный *идентификатор* — последовательность символов произвольной длины. В этом случае процедура аутентификации представляет собой проверку соответствия пользователя своему идентификатору.

Собственно проверка осуществляется с помощью протоколов, в процессе выполнения которых стороны формируют запросы и ответы на запросы другой стороны, используя свой секретный ключ. Данный ключ может отличаться от ключей зашифрования/расшифрования и называется *ключом аутентификации*.

В несимметричных шифрсистемах допускается использование двух ключей аутентификации: *секретного ключа аутентификации*, известного только его владельцу и используемого для создания запросов или ответов

на запросы, и *открытого ключа аутентификации*, доступного всем желающим и используемого для проверки созданных запросов или ответов.

Аутентификация информации заключается в проверке ее неизменности в процессе передачи или хранения, т. е. фактически в проверке ее целостности. Наиболее часто используемым механизмом при обеспечении аутентификации взаимодействующих сторон является *электронная подпись*[1]. Помимо этого, электронная подпись позволяет обеспечить невозможность отказа от авторства подписанного сообщения.

Вычисление электронной подписи заключается в преобразовании исходного сообщения с использованием секретного ключа пользователя в некоторую последовательность символов, которая и является электронной подписью. Секретный ключ пользователя должен быть известен только ему и быть персональным, т. е. однозначно связанным с идентификатором пользователя. *Такой ключ часто называют секретным ключом электронной подписи*. Использование персонального ключа позволяет гарантировать, что создать подпись может только владелец секретного ключа.

Проверка правильности электронной подписи должна производиться с использованием *открытого ключа электронной подписи*. Данный ключ должен быть математически связан с секретным ключом пользователя, создавшего электронную подпись, и может быть доступен любому желающему проверить подпись.

С использованием электронных подписей связана задача построения бесключевых функций хэширования H, с помощью которых проводится отображение подписываемого сообщения $x \in X$, представленного в виде последовательности символов произвольной длины, в цифровую комбинацию фиксированной длины

$$H : X \to V_n.$$

Результат применения функции хэширования $h = H(x)$ подписывается с помощью секретного ключа. Функция хэширования, хотя и является открытой, должна обладать свойством односторонности: по значению результирующего значения сложно найти исходное сообщение. Более подробно вопросы строения и использования бесключевых функций хэширования и цифровых подписей рассматриваются нами в гл. 8 и 11.

2.2. Формальные модели шифров

Введем следующие обозначения. Пусть X, K, Y — конечные множества соответственно открытых текстов, ключей и шифрованных текстов такие, что $|X| > 1$, $|K| > 1$, $|Y| > 1$. Пусть

[1] В Российской Федерации ранее было принято использовать название «электронная цифровая подпись». После принятия в 2011 г. Федерального закона «Об электронной подписи» стало применяться более короткое название «электронная подпись».

$$E = \{E_k : k \in K\}, \quad E_k : K \times X \to Y,$$

множество алгоритмов зашифрования, при этом отображение E_k называется *алгоритмом зашифрования* на ключе $k \in K$. Пусть

$$D = \{D_k : k \in K\}, \quad D_k : K \times Y \to X,$$

множество алгоритмов расшифрования, при этом отображение D_k называется *алгоритмом расшифрования* на ключе $k \in K$.

Мы также будем использовать обозначения

$$E_k(X) = \{E_k(x) : \forall x \in X\}, \quad D_k(Y) = \{D_k(y) : \forall y \in Y\}.$$

Следующее определение задает алгебраическую модель шифра (шифрсистемы).

Определение 2.2. Под алгебраической моделью *SA* шифра (шифрсистемы) будем понимать совокупность введенных множеств

$$SA = (X, K, Y, E, D),$$

для которых выполнены свойства:

1) однозначность расшифрования: для любых $x \in X$, $k \in K$ выполняется равенство $D_k(E_k(x)) = x$;

2) для любого $y \in Y$ существуют такие значения $x \in X$, $k \in K$, что $y = E_k(x)$.

При проведении исследований шифров используется также вероятностная модель шифра. Определим исходные (априорные) распределения вероятностей $P(X)$, $P(K)$ на множествах открытых текстов и ключей. Тем самым будем считать заданными:

- вероятность $p(x) \in P(X)$. любого элемента $x \in X$,

$$0 < p(x) \le 1, \quad \sum_{x \in X} p(x) = 1;$$

- вероятность $p(k) \in P(K)$ любого элемента $k \in K$,

$$0 < p(k) \le 1, \quad \sum_{k \in K} p(k) = 1.$$

Определение 2.3. Под вероятностной моделью шифра *SB* понимается совокупность его алгебраической модели и двух вероятностных распределений:

$$SB = SA \cup \{P(X), P(K)\} = (X, K, Y, E, D, P(X), P(K)).$$

Легко видеть, что вероятностная модель представляет собой алгебраическую модель, для которой заданы распределения на множествах открытых текстов X и ключей K. Рассмотрим примеры алгебраических моделей шифра.

2.2.1. Модель шифра простой замены

Пусть $\mathcal{A}, \mathcal{B}$ — два алфавита соответственно открытого и шифрованного текстов такие, что $|\mathcal{A}| = |\mathcal{B}|$. Множество X представляет собой последовательности элементов из алфавита $\mathcal{A}$ произвольной длины, т. е.

$$X = \{x = (x_1, x_2, \ldots), x_i \in \mathcal{A}\}.$$

Аналогично множество Y представляет собой последовательности элементов из алфавита $\mathcal{B}$ произвольной длины, т. е.

$$Y = \{y = (y_1, y_2, \ldots), y_i \in \mathcal{B}\}.$$

Пусть $S(\mathcal{A}, \mathcal{B})$ — множество биективных отображений алфавита $\mathcal{A}$ в алфавит $\mathcal{B}$. Определим $K \subset S(\mathcal{A}, \mathcal{B})$, тогда $k \in K$ представляет собой отображение $k : \mathcal{A} \to \mathcal{B}$, для которого найдется обратное отображение $k^{-1} : \mathcal{B} \to \mathcal{A}$ такое, что

$$k^{-1}(k(a)) = a, \quad \forall a \in \mathcal{A}.$$

Определение 2.4. Шифр простой замены описывается алгебраической моделью $SA = (X, K, Y, E, D)$, в которой множества открытых текстов, шифрованных текстов и ключей X, Y, K определены выше, а алгоритмы шифрования и расшифрования определяются равенствами

$$E_k(x) = (k(x_1), k(x_2), \ldots), \quad D_k(y) = (k^{-1}(y_1), k^{-1}(y_2), \ldots).$$

Пример 2.1

В качестве примера шифра простой замены мы можем привести следующий простой шифр. Сопоставим каждой букве алфавита числовое значение

А	Б	В	…	Э	Ю	Я
0	1	2	…	30	31	32

и определим в качестве алфавита $\mathcal{A} = \mathcal{B} = \mathbb{Z}_{33}$ множество вычетов по модулю 33 (более подробно свойства вычетов рассматриваются нами в гл. 9).

Теперь, выбирая в качестве ключа зашифрования отображение

$$k(a) : \mathbb{Z}_{33} \to \mathbb{Z}_{33}$$

$$k(a) \equiv a + 3 \pmod{33},$$

получим классический шифр Цезаря применительно к буквам русского алфавита. Отметим, что ключом расшифрования является отображение $k^{-1}(b) \equiv b - 3 \pmod{33}$, обратное отображению k.

При сравнительно небольшой мощности алфавита $\mathcal{A}$, что соответствует алфавитам естественных языков, определенный выше шифр

простой замены, несомненно, следует отнести к симметричным шифрам, поскольку знание ключа зашифрования k позволяет легко находить ключ расшифрования k^{-1} (например, полным перебором всех возможных отображений из множества $S(\mathcal{A}, \mathcal{B})$).

В случае, когда алфавит $\mathcal{A}$ обладает большой мощностью, нахождение обратного отображения является сложной задачей. В гл. 7 мы рассмотрим *блочные шифры*, которые являются симметричными шифрами простой замены в алфавите большой мощности. Сейчас же мы приведем еще один пример — несимметричный шифр простой замены с большой мощностью алфавита.

Пример 2.2

Приведем пример несимметричного шифра, который может рассматриваться как шифр простой замены.

Зафиксируем натуральное составное число $m = pq$, являющееся произведением двух простых чисел p, q, и выберем в качестве алфавита $\mathcal{A}$ кольцо $\mathbb{Z}_m$ вычетов по модулю m.

Определим в качестве открытого ключа натуральное число e такое, что НОД$(e(p-1)(q-1)) = 1$ и секретный ключ d, удовлетворяющий условию $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Открытый ключ индуцирует биективное отображение k множества $\mathbb{Z}_m$ в себя следующим образом. Для любого $a \in \mathbb{Z}_m$ определим

$$k(a) \equiv a^e \pmod{m}.$$

Данное отображение задает алгоритм зашифрования. Тогда обратное отображение k^{-1} задается сравнением

$$k^{-1}(c) \equiv c^d \pmod{m}.$$

Легко проверить, что выполнено сравнение

$$k^{-1}(k(a)) \equiv a \pmod{m} \text{ для любого } a \in \mathbb{Z}_m,$$

из которого следует, что отображение k^{-1} определяет алгоритм расшифрования.

Описанную в данном примере шифрсхему принято называть схемой RSA, по первым буквам фамилий авторов — *Rivest*, *Shamir*, *Adleman*. Более подробное изложение данной схемы и ее анализ мы приводим в параграфе 10.1. Как будет показано далее, задача определения обратного отображения k^{-1} является сложной и сводится к разложению числа m на простые сомножители.

2.2.2. Модель шифра перестановки

Пусть $\mathcal{A}$ — алфавит, которому принадлежат символы открытого текста. Зафиксируем некоторое натуральное число n и выберем в качестве множества X множество последовательностей из алфавита $\mathcal{A}$ длины n, т. е.

$$X = \{(x_1, \ldots, x_n),\ x_i \in \mathcal{A}\}. \qquad (2.1)$$

Напомним, что *перестановкой* на множестве $N = \{1, 2, \ldots, n\}$ называется отображение π, ставящее в соответствие вектору $(1, \ldots, n)$ вектор $(\pi_1, \ldots, \pi_n)$, в котором $\pi_1, \ldots, \pi_n$ принимают все возможные значения от 1 до n. В наглядной форме перестановка π может быть записана в виде

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix} \text{ или } \pi = (\pi_1, \pi_2, \ldots, \pi_n).$$

Величину n принято называть *степенью* перестановки.

Действие перестановки π на элементе $\overline{x} = (x_1, \ldots, x_n) \in X$ может быть определено следующим образом:

$$\pi(x_1, \ldots, x_n) = (x_{\pi_1}, \ldots, x_{\pi_n}),$$

т. е. перестановка π переставляет местами элементы вектора $\overline{x}$.

Обозначим символом $\mathcal{S}_n$ множество всех возможных перестановок на множестве N, а символом $\mathcal{S}_n(X)$ множество действий перестановок из $\mathcal{S}_n$ на множестве X.

Рассмотрим операцию композиции, определяемую равенством

$$\pi \cdot \sigma(\overline{x}) = \pi(\sigma(\overline{x})).$$

Относительно введенной операции множество $\mathcal{S}_n(X)$ образует группу, которую называют *группой перестановок*, или *симметрической группой* (см. [2, 4]).

При этом обратной к перестановке π является перестановка π^{-1} такая, что композиция $\pi^{-1} \cdot \pi(\overline{x})$ оставляет вектор $\overline{x} \in X$ неизменным.

Определение 2.5. Шифр перестановки описывается алгебраической моделью

$$SA = (X, K, Y, E, D),$$

в которой множества X, Y определены равенством (2.1) и совпадают. Множество ключей K удовлетворяет условию $K \subseteq \mathcal{S}_n(X)$, а алгоритмы зашифрования и расшифрования определены равенствами

$$E_\pi(x) = (x_{\pi_1}, x_{\pi_2}, \ldots, x_{\pi_n}), \quad D_{\pi^{-1}} = (x_{\pi_1^{-1}}, x_{\pi_2^{-1}}, \ldots, x_{\pi_n^{-1}})$$

для некоторой перестановки $\pi \in K$.

Шифр перестановки является симметричным шифром, поскольку знание перестановки π позволяет эффективно вычислить обратную перестановку π^{-1}. Мы предлагаем читателю в качестве упражнения самостоятельно придумать алгоритм вычисления перестановки π^{-1}.

2.2.3. Модель шифра маршрутной перестановки

Данный шифр относится к классу шифров перестановки и характеризуется простотой выполнения операций шифрования/расшифрования. Один из наиболее распространенных способов шифрования/расшифрования задается некоторым прямоугольником (таблицей) и соответствующим правилом его заполнения. Например, открытый текст записывается в таблицу по строкам, а шифртекст получается в результате выписывания столбцов соответствующей таблицы, или наоборот.

Пример 2.3

Рассмотрим пример на основе таблицы размера 8×5. Открытый текст записываем по строкам, считываем по столбцам.

Порядок записи отражен цифрами в таблице:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40

Шифртекст выписывается так: 1, 6, 11, 16, 21, 26, 31, 36, 2, 7, 12, 17, 22, 27, 32, 37, 3, 8, ... и т. д.

Маршрутная перестановка на основе решетки Кардано

Для построения решетки Кардано исходный квадрат $2n \times 2n$ делится на четыре квадрата размером $n \times n$. В правом верхнем квадрате все ячейки нумеруются числами из множества {1, 2, 3, 4}. Далее исходный квадрат поворачиваем на 90 градусов. В таком случае занумерованные клетки первого квадрата $n \times n$ будут налагаться на клетки второго квадрата такого же размера, находящегося в правом нижнем углу. Переносим номера первого квадрата на соответствующие клетки второго.

Аналогично производится дальнейший поворот исходного квадрата на очередные 90 градусов и перенос номеров в клетки квадрата в левом нижнем углу, а затем и в квадрат в левом верхнем углу. Делаем вырезы по следующему правилу: правый верхний квадрат — вырезы в клетках с номером 1, в правом нижнем — 2, в левом нижнем — 3, в левом верхнем — 4. Накладываем полученную решетку на лист и вписываем в вырезы буквы открытого текста. Затем переворачиваем решетку на 90 градусов и вписываем буквы в открывшиеся окошки. Повторяем так еще два раза.

Так как мы создавали решетку описанным выше способом, при поворотах окошки не попадут друг на друга и при этом весь квадрат $2n \times 2n$

окажется заполненным. Расшифрование происходит с использованием такой же решетки. Длинные тексты шифруются блоками по $4n^2$ знаков.

Пример 2.4

Решеткой Кардано размера 6×6 является таблица, ячейки которой заполнены следующими числами:

1	2	4	1	2	1
2	3	1	4	3	2
1	4	3	3	1	4
4	1	3	3	4	1
2	3	4	1	3	2
1	2	1	4	2	1

Данная таблица состоит из четырех квадратов размера 3×3, вырезы в которых делаются соответственно на цифрах 1, 2, 3 и 4. Места вырезов при повороте исходной решетки на 90, 180 и 270 градусов показаны ниже:

	3		4		
		3			4
					1
2			1		
	2				

	2				
2				3	
			3		
	1			4	
1		1	4		

1				2	
		1			2
1					
4			3		
		4		3	

Упражнение 2.2.1. Расставьте соответствующие номера в незаполненные клетки приведенных выше таблиц.

Упражнение 2.2.2. Найдите открытый текст по шифртексту, который представляет собой заполненную таблицу Кардано из рассмотренного выше примера.

П	И	Р	Е	Е	Ш
З	Р	Р	Д	У	Е
С	Е	А	Е	Т	Н
Т	Т	К	А	Ш	О
Р	А	Н	Е	О	К
И	А	Ф	Р	А	Л

2.2.4. Модель поточного шифра

Одно из наиболее распространенных представлений модели поточного шифра заключается в следующем. Для зашифрования открытого текста, представляющего собой конечную последовательность симво-