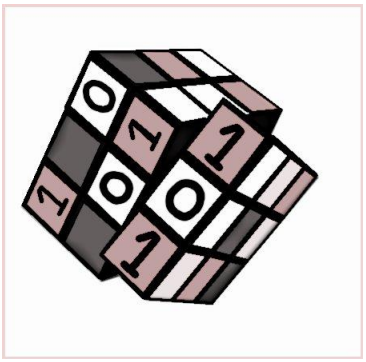
А.П.Алексеев, В.В.Орлов

Стеганографические и криптографические методы защиты информации

Учебное пособие



Рекомендовано Методическим советом ГОУ ВПО «Поволжский государственный университет телекоммуникаций и информатики» в качестве учебного пособия по дисциплине «Информатика» для студентов ПГУТИ обучающихся по специальностям: 210400, 210401, 210402, 210403, 210404, 210405, 210406, 210302, 090106
Протокол заседания комиссии Методического совета ПГУТИ
№ 11 от 23 декабря 2006г.

Самара,
2010 г.

УДК 004.056
А 47

Стеганографические и криптографические методы защиты информации; учебное пособие/ Алексеев А. П. Орлов В.В./ ИУНЛ ПГУТИ - 2010 - 330 с.

ISBN 978-5-904029-12-8

Рецензенты:
декан факультета телекоммуникаций и радиотехники ПГУТИ д.т.н., профессор Карташевский В.Г.,
заведующий кафедрой «Защита информации» СамГУ Осипов М.Н.

В учебном пособии в компактной форме описаны основные принципы защиты информации. В книге содержится большое число методических указаний на выполнение лабораторных и практических работ по криптографии и стеганографии. Оптический диск, прилагаемый к этой книге, содержит необходимые программы и начинённые контейнеры, из которых студенты в процессе выполнения лабораторных работ должны суметь извлечь скрытую там информацию.

Книга предназначена для студентов и преподавателей. Преподаватели с помощью этого учебного пособия смогут «беззаботно» провести два семестра занятий. Студенты смогут получить практические навыки в шифровании, дешифровании и создании скрытых каналов связи.

Учебное пособие ориентировано на студентов телекоммуникационных специальностей 210400…210406, 210302, изучающих информатику, на студентов специальностей 210403 и 090106, изучающих защищенные системы связи.

ISBN 978-5-904029-12-8

Введение

Познание бесконечности
требует бесконечного времени.
А. и Б. Стругацкие

Защищать передаваемую (или хранимую) информацию от несанкционированного использования приходится во многих случаях. Это требуется при решении государственных, дипломатических, военных задач, в работе бизнеса (коммерции), при исследовании новых научно-технических проблем, при разработке оригинальных технологических процессов и устройств. Защищать информацию требуется при документообороте в государственных организациях и при ведении приватной частной переписки. Необходима защита интеллектуальной собственности аудио, кино, фото продукции. Развитие современных телекоммуникационных технологий (спутниковое телевидение, сотовая телефония, дистанционное управление удаленными объектами) невозможно представить без защиты передаваемой информации. Необходима защита данных, хранимых на персональном компьютере.

Защищать информацию можно путем шифрования передаваемых сообщений (криптографические методы), либо путем создания скрытого канала связи (методы стеганографии). Нередко криптография и стеганография используются совместно (комплексно) для увеличения степени защиты информации. Современные тенденции науки показывают необходимость шифрования сообщения перед их скрытой передачей или хранением.

В настоящее время уже произошло становление криптографии, как самостоятельной науки с собственной теорией, с серийно выпускаемыми аппаратными и программными средствами шифрования. Что касается стеганографии, то сейчас идет накопление и обобщение материала, создание обобщающей теории, решение малоисследованных прикладных задач. При этом некоторые приемы, разработанные в криптографии, с успехом применяются и в стеганографии.

Стеганографические методы позволяют скрыть информацию в различных объектах (контейнерах): в текстовых документах (электронные статьи, книги, отчеты, письма), в графических файлах (рисунки, баннеры, фотографии), видео файлах (клипы, фильмы, анимация), в звуковых файлах (музыкальные произведения, речь, природные звуки), на HTML-страницах, в субтитрах фильмов, в сообщениях, передаваемых с помощью SMS, MMS, чатов, мессенджеров и блогов. Текстовые сообщения можно скрытно размещать в неиспользуемых областях Flash-памяти, жестких и оптических дисков.

Число разновидностей контейнеров, которые можно использовать на практике, велико. Если принять во внимание, что каждый вид контейнера может существовать в разных форматах, а для сокрытия информации могут

использоваться разнообразные методы (алгоритмы), то остановится очевидным многомерность стеганографических задач. Отсюда вытекает большой простор для творчества криптографов и сложность положения криптоаналитиков.

Графические форматы BMP, JPEG, GIF, PNG при внедрении информации имеют свои особенности. Такое же положение существует со звуковыми файлами форматов WAV, MP3, WMA, APE, FLAC, OGG, AAC, CDA. Каждый из форматов видео (MPEG, MOV, WMV, RM, DIVX) требует разработки собственных методов внедрения и извлечения скрываемой информации.

Мощным средством сокрытия информации могут стать методы пространственного разделения информации. При этом сообщение можно разделить (раздробить) на слова, буквы и даже биты, а затем распределить (распылить) по разным контейнерам. Для повышения степени защиты распыляемое сообщение должно быть предварительно зашифровано одним из криптостойких шифров. Понятно, что работа криптоаналитика в подобных ситуациях многократно усложняется.

Еще большей стойкостью обладают методы защиты информации, основанные на пространственно-временном распылении информации. Для их реализации зашифрованное сообщение распыляется по нескольким контейнерам, но каждый из контейнеров доступен для обработки лишь в короткий промежуток времени, который известен только доверенным лицам.

Таким образом, для преодоления пространственно-временной защиты криптоаналитику потребуется не только решить традиционную криптографическую задачу, но суметь среди множества контейнеров отыскать нужные, извлечь из них информацию и расположить её в соответствующем порядке. Не следует забывать, что криптоаналитик должен еще угадать (вычислить, установить) время, в которое демонстрируется истинный контейнер, а не его близнец. Учитывая тот факт, что криптоаналитику заранее не известны серверы, на которых размещается скрываемая информация, то ему придется непрерывно контролировать (сканировать и анализировать) всю глобальную Сеть. Задача становится практически не решаемой, за приемлемое время. Такую задачу сложно решить так же, как трудно отыскать иголку в стоге сена. Хотя бесконечная изобретательность криптоаналитиков позволяет надеяться на решение многих задач. Кстати, иголка из стога сена может быть извлечена с помощью мощного магнита.

В данном учебном пособии рассматриваются классические шифры и шифры, разработанные авторами. Даются основные сведения о стеганографии. Во второй части приводится большое число лабораторно-практических работ, позволяющих получить представление о современных стеганографических методах защиты информации.

Особенностью этого пособия является его ориентация на учебный процесс. Здесь приводятся самые необходимые сведения из теории и большое число методических разработок, нацеленных на практическое освоение методов защиты информации.

Оптический диск, прилагаемый к этой книге, содержит необходимые программы и начинённые контейнеры, из которых нужно суметь извлечь скрытую там информацию.

Учебное пособие подготовлено для проведения занятий по дисциплинам: «Информатика» для студентов специальностей 210400 – 210406 и «Стеганография» для студентов специальности 210403.

Основная часть книги была многократно апробирована на лекционных и практических занятиях, опубликована в центральной печати (журналы «Информатика и образование», «Инфокоммуникационные технологии», доклады конференций), обсуждена на семинарах. Одно из технических решений защищено патентом.

В настоящее время имеется несколько отечественных публикаций методического характера для дисциплин, связанных с использованием криптографии. По сведениям авторов данная работа является первой, в которой для студентов подготовлены лабораторные работы, направленные на освоение методов стеганографии.

Авторы понимают, что рассматриваемые в данной работе вопросы неисчерпаемы, требуют подготовки публикаций объемом в сотни и тысячи раз больше, чем данная книга. Однако, учитывая мысль, что «жизнь коротка, а искусство вечно», было решено подготовить в короткое время компактную публикацию. Книга поможет многим сделать первый шаг в освоении стеганографии.

Разделы 1.3, 1.4, 2.7, 3.11 написаны Орловым В.В.
Разделы 1.5, 2.2, 2.3, 3.9, 3.10 написаны при участии
Макарова М.И.
Разделы 1.4, 3.3, 3.12 написаны при участии Жеренова Ю.В.
Раздел 2.3, 4.2 написан при участии Батаева А.Ф.
Раздел 3.8. написан Алениным А.А.
Раздел «Ресурсы Internet» подготовлен Царевой О.В.
Общее редактирование выполнено Алексеевым А.П.

Авторы искренне благодарны Царевой О.В., которая сумела устранить в рукописи большое число ошибок разного характера.

1. Криптографические методы защиты информации

Мне известны системы шифров,
которыми пользовались во время войн
за Сардинию и Савойю, во время
англо-французской осады Севастополя,
во время боксерского восстания в Китае
и во время последней русско-японской войны.
Ярослав Гашек

Методы криптографии нацелены на превращение открытого текста в нечитаемый текст, который сложно понять без секретного ключа, известного только доверенным лицам.

Шифры можно классифицировать по разным признакам. Например, по способу использования ключей их можно разделить на симметричные и асимметричные (с открытым ключом). В симметричных шифрах один и тот же ключ используется для шифрования и дешифрования.

В асимметричных криптосистемах шифрование производят с помощью открытого (всем известного) ключа, а дешифрование – с помощью другого секретного ключа.

1.1. Классические симметричные шифры

Криптографические методы защиты информации можно использовать в качестве элементов (составных частей) стеганографических методов сокрытия информации. Перед тем как скрыть текстовую информацию в каком-либо контейнере её следует зашифровать. Этим создается еще один уровень (барьер, бастион) защиты информации, который усложняет криптоанализ.

Большинство классических криптографических методов уже не имеют практической ценности и представляют лишь учебный (методический) интерес. Хотя в сочетании со стеганографией любой метод шифрования может стать мощным средством защиты информации. Кроме того, изучение классических методов криптографии может натолкнуть специалиста по стеганографии на интересные свежие идеи.

1.1.1. Шифр атбаш

Всякая задача становится простой,
после того как вам её объяснили.
Конан Дойл

Порой священные иудейские тексты шифровались методом замены букв открытого текста на другие буквы. Вместо первой буквы алфавита записывалась последняя буква, вместо второй — предпоследняя и т. д. Этот древний шифр назывался атбаш.

Следующая таблица иллюстрирует идею этого шифра.

Таблица 1.1.1

Буквы открытого текста	А	Б	В	Г	Д	Е
Буквы криптограммы	Я	Ю	Э	Ь	Ы	Ъ

Приведем пример шифровки, составленной с помощью шифра атбаш. Открытый текст «ГДЕ АББА» превращается в криптограмму «ЬЫЪ ЯЮЮЯ».

Секретным ключом для этого шифра является таблица замен (табл. 1.1.1).

1.1.2.Шифр Цезаря

Вместо хвоста – нога,
А на ноге – рога.
Леонид Дербенёв

Известен факт шифрования переписки Юлия Цезаря (100—44 до н. э.) с Цицероном (106—43 до н. э.).

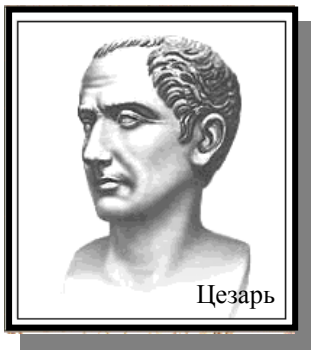


Рис. 1.1.2.1. Юлий Цезарь

Шифр Цезаря реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей от нее в алфавите на фиксированное число букв. В своих шифровках Ю.Цезарь заменял букву исходного открытого текста буквой, отстоящей от исходной буквы впереди на три позиции.

Приведем таблицу замен для этого шифра.

Таблица 1.1.2.1

Буквы открытого текста	А	Б	В	Г	Д	Е
Буквы криптограммы	Г	Д	Е	Ё	Ж	З

Фраза «ГДЕ АББА», зашифрованная эти шифром, трансформируется в символы «ЁЖЗ ГДДГ».

1.1.3. Квадрат Полибия

Вглядевшись, она как в тумане увидела
еще одну панель с буквами алфавита от A до Z
и тут же вспомнила, что нужно ввести шифр.
Дэн Браун

В Древней Греции (II в. до н.э.) был известен шифр, который создавался с помощью квадрата Полибия. Таблица для шифрования представляла собой квадрат (матрицу) с пятью столбцами и пятью строками, которые нумеровались цифрами от 1 до 5. В каждую клетку такой таблицы записывалась одна буква. В результате каждой букве соответствовала пара цифр, и шифрование сводилось к замене буквы парой цифр.

Идею квадрата Полибия проиллюстрируем таблицей с русскими буквами. Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (квадрат 6 х 6). Заметим, что порядок расположения символов в квадрате Полибия является секретной информацией (ключом).

Таблица 1.1.3.1

	1	2	3	4	5	6
1	**А**	**Б**	**В**	**Г**	**Д**	**Е**
2	**Ё**	**Ж**	**З**	**И**	**Й**	**К**
3	**Л**	**М**	**Н**	**О**	**П**	**Р**
4	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**
5	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**
6	**Э**	**Ю**	**Я**	**,**	**.**	**-**

Зашифруем с помощью квадрата Полибия фразу «ГДЕ АББА»:

14 15 16 11 12 12 11,

а затем слово «КРИПТОГРАФИЯ»:

26 36 24 35 42 34 14 36 11 44 24 63

Из примеров видно, что в шифрограммах первым указывается номер строки, а вторым — номер столбца. В квадрате Полибия столбцы и строки можно маркировать не только цифрами, но и буквами. В этом случае криптограмма будет состоять из пар букв.

1.1.4. Аффинные криптосистемы

Это только вначале трудно.
Потом будет ещё труднее.
Измайлов А.М., Чебуров В.В.

При шифровании буквы открытого текста нумеруются числами, например, для кириллицы числами в диапазоне от 0 до 32. Затем каждая буква открытого текста заменяется буквой, порядковый номер которой вычисляется с помощью линейного уравнения и вычисления остатка от целочисленного деления.

Аффинные криптосистемы задаются при помощи двух чисел a и b. Для русского алфавита эти числа выбираются из условия $a \geq 0$, $b \leq 32$. Максимальное число символов в используемом алфавите обозначаются символом γ. Причем числа a и $\gamma = 33$ должны быть взаимно простыми. Если это условие не будет выполняться, то две разные буквы могут отображаться (превращаться) в одну.

Каждый код буквы открытого текста μ заменяется кодом буквы криптограммы по следующему правилу. Вначале вычисляется число $\alpha = a \cdot \mu + b$, а затем выполняется операция целочисленного деления числа α на число $\gamma = 33$, то есть $\alpha = \beta(\mathrm{mod}\ (\gamma))$. В качестве кода символа шифрограммы используется остаток от целочисленного деления β.

Для определенности выберем такие числа: $a = 5$ и $b = 3$.

Фрагмент процедуры, иллюстрирующей порядок шифрования, приведен в таблице.

Таблица 1.1.4.1

Буква открытого текста	А	Б	В	Г	Д	Е	…	Я
Код буквы открытого текста μ	0	1	2	3	4	5	…	32
Код буквы криптограммы β	3	8	13	18	23	28	…	31
Буква криптограммы	Г	З	М	С	Ц	Ы	…	Ю

Предположим, что нужно зашифровать сообщение «ГДЕ АББА». В результате получим: «СЦЫ ГЗЗГ».

В ранее рассмотренных нами шифрах каждой букве открытого текста соответствовала одна определенная буква криптограммы. Подобные шифры называются шифрами одноалфавитной замены.

В следующей таблице приведены результаты шифрования фразы «ГДЕ АББА» разными одноалфавитными шифрами.

Таблица 1.1.4.2

Шифр	Криптограмма
Шифр атбаш	ЬЫЪ ЯЮЮЯ
Шифр Цезаря	ЁЖЗ ГДДГ
Квадрат Полибия	14 15 16 11 12 12 11
Аффинные криптоситстемы	СЦЫ ГЗЗГ

Анализ последней таблицы показывает, что одинаковые буквы открытого текста заменяются одинаковыми символами в криптограмме. Нужно обратить особое внимание на четыре последних символа криптограмм. Четвертый и седьмой символы во всех криптограммах одинаковые. Одинаковыми являются пятый и шестой символы криптограмм. Эта же закономерность наблюдается в открытом тексте.

Этот недостаток одноалфавитных шифров замены позволяет взломать шифрограммы большой длины без знания секретного ключа.

1.1.5. Шифр Виженера

- Ключ! - замычал инженер,
клацая зубами.
И.Ильф, Е.Петров

Длинные сообщения, полученные методом одноалфавитной замены, раскрываются с помощью таблиц относительных частот. Для этого определяется частота появления каждого символа в шифровке и делится на общее число символов в криптограмме. Затем с помощью статистической таблицы относительных частот определяется, какая замена была сделана при шифровании.

Повысить криптостойкость позволяют шифры многоалфавитной замены (иначе их называют шифрами многозначной замены). При этом каждому символу открытого алфавита ставят в соответствие не один, а несколько символов шифровки (алфавита замены).

Ниже приведен фрагмент ключа многоалфавитной замены:

Таблица 1.1.5.1

А	Б	В	Г	Д	Е
18	7	5	19	21	2
12	4	90	35	83	15
48	14	22	10	99	32

С помощью многоалфавитного шифра сообщение «ГДЕ АББА» можно зашифровать несколькими способами:

19—83—32—48—4—7—12,

10—99—15—12—4—14—12 и т. д.

Для каждой буквы исходного алфавита создается некоторое множество символов замены. При этом в алфавите замен не должно быть одинаковых символов. Многоалфавитные шифры изменяют картину статистических частот появления букв и этим затрудняют вскрытие шифра без знания ключа (без знания конфигурации таблицы многоалфавитной замены).

Рассмотрим шифр многоалфавитной замены, который был описан в 1585 г. французским дипломатом Блезом де Виженером. Шифрование производится с помощью, так называемой таблицы Виженера. Здесь показана часть таблицы для того, чтобы изложить лишь идею метода.

Каждая строка в этой таблице соответствует одному шифру простой замены (типа шифра Цезаря). При шифровании открытое сообщение записывают в строчку, а под ним помещают ключ. Если ключ оказывается короче сообщения, то ключ циклически повторяют. Шифровку получают, находя символ в матрице букв шифрограммы. Символ шифрограммы находится на пересечении столбца с буквой открытого текста и строки с соответствующей буквой ключа.

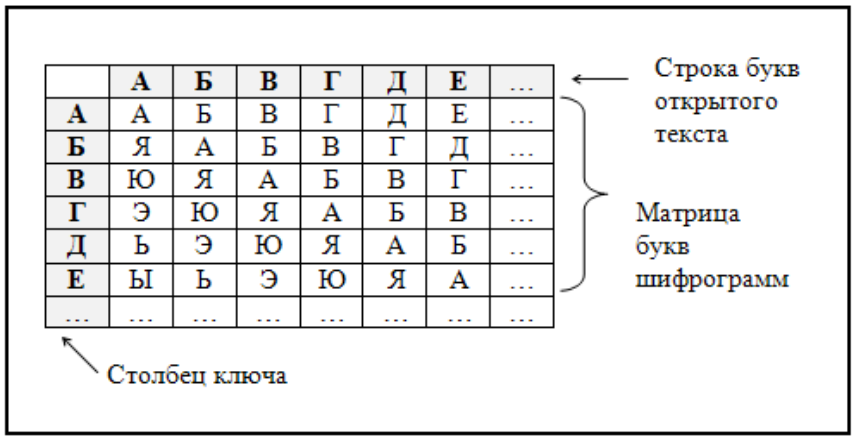


Рис. 1.1.5. 1. Фрагмент таблицы Виженера

Предположим, что нужно зашифровать сообщение «ГДЕ АББА». В качестве ключа выберем слово «ДЕВА». В результате получим:

Таблица 1.1.5.2

Сообщение	Г	Д	Е	А	Б	Б	А
Ключ	Д	Е	В	А	Д	Е	В
Шифровка	Я	Я	Г	А	Э	Ь	Ю

В результате преобразований получится шифровка «ЯЯГ АЭЬЮ». Нужно обратить пристальное внимание на последние четыре символа криптограммы. В отличие от шифров одноалфавитной замены здесь одинаковые буквы открытого текста зашифрованы разными буквами шифровки.

1.1.6. Система Плейфейра

Система Плейфейра позволяет формировать многоалфавитные шифры. Рассмотрим основную идею этой системы.

Шифрование производится с помощью квадрата (или прямоугольника), в который занесены буквы соответствующего национального алфавита. Буквы записываются в квадрат или прямоугольник в произвольном порядке. Этот порядок записи букв и конфигурация таблицы являются секретным ключом. Для определенности возьмем прямоугольную таблицу размером 8х4, в качестве букв алфавита – кириллицу, а буквы расположим в алфавитном порядке. Так как число русских букв 33, а число клеток – 32, то исключим из таблицы букву Ё.

Таблица 1.1.6

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

Предположим, что требуется зашифровать слово КРИПТОГРАФИЯ.

Рассмотрим правила шифрования.

1. Открытый текст делится на блоки по две буквы. Буквы в одном блоке не должны быть одинаковыми. Произведем разделение исходного слова на блоки по две буквы:

КР-ИП-ТО-ГР-АФ-ИЯ.

2. Если буквы шифруемого блока находятся в разных строках и столбцах, то в качестве заменяющих букв используются буквы, расположенные в углах прямоугольника, охватывающего буквы открытого текста. Например, блок КР заменяется символами ИТ.

3. Если буквы открытого текста попадают в одну строку, то шифрограмма получается путем циклического сдвига вправо на одну клетку. Например, блок ИП будет преобразован в ЙИ. Еще один пример к этому правилу. Если, предположим, требуется преобразовать блок КН, то получится ЛО.

4. Если обе буквы открытого текста попадают в один столбец, то для шифрования осуществляют циклический сдвиг на одну клетку вниз.

Например, блок ЖЦ будет преобразован в символы ОЮ, а блок ТЪ в символы ЪВ.

В соответствии с описанными правилами слово КРИПТОГРАФИЯ будет преобразовано в криптограмму ИТЙИЦКАУДРПШ.

1.1.7. Система Хилла

- Что он делает?
- Считает, да цифры пишет,
таких чудных цифр я отроду не видал.
Эдгар По

Рассмотрим криптографическую систему Хилла, в которой шифрование осуществляется с использованием математических преобразований: вычислений с помощью приемов линейной алгебры.

Данный шифр для отдельно взятой буквы можно считать многоалфавитным. Однако пары букв шифруются везде одинаково. Поэтому в широком смысле понятия криптографическую систему Хилла следует отнести к одноалфавитным шифрам.

Система Хилла некоторыми операциями сильно напоминает аффинную криптосистему.

Первоначально открытый текст методом замены следует преобразовать в совокупность чисел. Предположим, что шифруется текст, написанный с использованием 26-ти латинских букв. Выберем следующий алгоритм замены букв на числа: латинские буквы A, B, C, D, …, Z будем заменять соответственно числами 1, 2, 3, 4,…, 26. Другими словами: пронумеруем буквы в порядке их расположения в алфавите, и при замене будем использовать их порядковые номера. В данном случае выбран такой алгоритм замены, но понятно, что он может быть любым.

Предположим, что нужно зашифровать немецкое слово ZEIT. Заменим буквы в соответствии с их порядковыми номерами в алфавите четырьмя числами: 26 – 5 – 9 – 20.

Далее следует выбрать некоторое число $d \geq 2$. Это число показывает, порядок разбиения открытого текста на группы символов (определяет, сколько букв будет в каждой группе). С математической точки зрения число d показывает, сколько строк должно быть в векторах-столбцах. Примем $d = 2$. Это означает, что числа 26 – 5 – 9 – 20 нужно разбить на группы по два числа в каждой группе и записать их в виде векторов-столбцов:

$$P1 := \begin{bmatrix} 26 \\ 5 \end{bmatrix} \qquad P2 := \begin{bmatrix} 9 \\ 20 \end{bmatrix}$$

Далее следует записать матрицу исходного текста:

$$M := \begin{bmatrix} 26 & 9 \\ 5 & 20 \end{bmatrix}$$

Шифрование выполняется путем вычисления следующих выражений:

$$C1 = M \cdot P1 \text{ и } C2 = M \cdot P2$$

В результате расчетов получится:

$$C1 = \begin{bmatrix} 721 \\ 230 \end{bmatrix} \qquad C2 = \begin{bmatrix} 414 \\ 445 \end{bmatrix}$$

Окончательный результат шифрования получается путем целочисленного деления элементов векторов-столбцов C1 и C2 по модулю 26 (нахождение остатка от целочисленного деления).

$$C11 := \begin{bmatrix} \mathrm{mod}(C1_0, 26) \\ \mathrm{mod}(C1_1, 26) \end{bmatrix} \qquad C11 = \begin{bmatrix} 19 \\ 22 \end{bmatrix}$$

$$C21 := \begin{bmatrix} \mathrm{mod}(C2_0, 26) \\ \mathrm{mod}(C2_1, 26) \end{bmatrix} \qquad C21 = \begin{bmatrix} 24 \\ 3 \end{bmatrix}$$

В результате шифрования по каналу связи будет оправлена последовательность чисел: 19 – 22 – 24 – 3. Для ранее выбранного ключа замены это будет соответствовать шифрограмме SVXC. Данный пример иллюстрирует тот факт, что системы шифрования часто базируются на математических преобразованиях.

Заметим, что приведенные здесь вычисления выполнены с помощью математической системы Mathcad.

1.1.8. Метод гаммирования

Слова – лишь символы и знаки
того ручья с бездонным дном,
который в нас течет во мраке
и о совсем журчит ином.
Игорь Губерман

При шифровании методом гаммирования (иначе его называют аддитивным методом) вначале открытый текст кодируют, преобразуя каждую букву в число.

Затем к каждому числу прибавляют секретную гамму (псевдослучайную числовую последовательность). Технически добавление гаммы к открытому тексту в криптографических системах осуществляется поразрядно (поточный шифр). Процедуру добавления гаммы удобно реализовать с помощью двоичных чисел. При этом на каждый бит открытого текста накладывается бит секретной гаммы.

Генератор гаммы выдает последовательность битов: $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_n$. Этот поток битов и поток битов открытого текста $p_1, p_2, p_3, \ldots, p_n$ подвергаются поразрядно логической операции Исключающее ИЛИ. В результате получается поток битов криптограммы:

$$c_i = p_i \oplus \gamma_i.$$

При дешифровании операция Исключающее ИЛИ выполняется над битами криптограммы и тем же самым потоком гаммы:

$$p_i = c_i \oplus \gamma_i.$$

Благодаря особенностям логической операции Исключающее ИЛИ на приемной стороне операция вычитания заменяется данной логической операцией. Сказанное иллюстрируется примером.

Предположим, что P = 10011001, а G = 11001110. В результате зашифрованный байт C будет иметь следующий вид:

Таблица 1.1.8.1

P	1	0	0	1	1	0	0	1
G	1	1	0	0	1	1	1	0
C	0	1	0	1	0	1	1	1

На приемной стороне будет повторно выполнена логическая операция Исключающее ИЛИ:

Таблица 1.1.8.2

C	0	1	0	1	0	1	1	1
G	1	1	0	0	1	1	1	0
P	1	0	0	1	1	0	0	1

Из этих таблиц видно, что переданный и принятый байты одинаковые.

В ЭВМ преобразование открытого текста в числа происходит естественным путем, так как каждый символ кодируется двоичным числом. Вид этого преобразования может быть разным. Для определенности будем считать, что сообщение в ЭВМ кодируется с помощью кодовой таблицы CP - 1251.

Будем считать, что секретная гамма добавляется к открытому тексту по правилу сложения по модулю два без переносов в старшие разряды (логическая операция Исключающее ИЛИ). Результаты всех преобразований поместим в таблицу.

Таблица 1.1.8.3

Открытый текст	Г	Д	Е	А	Б	Б	А
Десятичное число	195	196	197	192	193	193	192
Двоичное число	11000011	11000100	11000101	11000000	11000001	11000001	11000000
Гамма (десятичная)	32	18	36	11	61	23	3
Гамма (двоичная)	00100000	00010010	00100100	00001011	00111101	00010111	00000011
Криптограмма (двоич.)	11100011	11010110	11100001	11001011	11111100	11010110	11000011
Криптограмма (десят.)	227	214	225	203	252	214	195
Криптограмма	г	Ц	б	Л	ь	Ц	Г

Для наглядности результат шифрования (шифрограмма) переведен с помощью таблицы CP-1251 в буквы. Из таблицы видно, что открытый текст был записан прописными буквами, а криптограмма содержит как прописные, так и строчные буквы. Естественно, что при реальном (а не учебном) шифровании набор символов в шифрограмме будет еще богаче. Кроме русских букв будут присутствовать латинские буквы, знаки препинания, управляющие символы.

1.1.9. Метод перестановок

Множество современных методов шифрования можно разделить на четыре большие группы: методы **замены** (подстановки), **перестановок, аддитивные** (гаммирования) и **комбинированные** методы.

В разделах 1.1.1-1.1.7 были рассмотрены шифры замены (подстановок). В разделе 1.1.8 рассмотрен аддитивный метод.

Рассмотрим основные идеи метода перестановок.

В шифрах **перестановок** все буквы открытого текста остаются без изменений, но перемещаются с их исходных позиций на другие места. Следующая простейшая «шифровка» получена методом перестановки двух соседних букв РКПИОТРГФАЯИ. В этом «секретном» сообщении не сложно узнать слово КРИПТОГРАФИЯ.

Более сложный алгоритм перестановок сводится к разбиению сообщения на группы по три буквы. В каждой группе первую букву ставят на третье место, а вторую и третью буквы смещают на одну позицию влево. В результате получится криптограмма: РИКТОПРАГИЯФ.

Рассмотрим примеры шифрования сообщения методом **перестановок.**

Идея этого метода криптографии заключается в том, что запись открытого текста и последующее считывание шифровки производится по разным путям некоторой геометрической фигуры (например, квадрата).

Для пояснения идеи возьмем квадратную таблицу (матрицу) 8 □ 8. Будем записывать открытый текст в эту матрицу последовательно по строкам сверху вниз, а считывать криптограмму по столбцам последовательно слева направо.

Предположим, что требуется зашифровать сообщение:

НА ПЕРВОМ КУРСЕ ТЯЖЕЛО УЧИТЬСЯ ТОЛЬКО ПЕРВЫЕ ЧЕТЫРЕ ГОДА ДЕКАНАТ.

Таблица 1.1.9.1

Н	А	_	П	Е	Р	В	О
М	_	К	У	Р	С	Е	_
Т	Я	Ж	Е	Л	О	_	У
Ч	И	Т	Ь	С	Я	_	Т
О	Л	Ь	К	О	_	П	Е
Р	В	Ы	Е	_	Ч	Е	Т
Ы	Р	Е	_	Г	О	Д	А
_	Д	Е	К	А	Н	А	Т

В таблице символом «_» обозначен пробел.

В результате преобразований получится шифровка:

НМТЧОРЫ_А_ЯИЛВРД_КЖТЬЫЕЕПУЕЬКЕ_КЕРЛСО_ГАРСОЯ_ЧОНВЕ__ПЕДАО_УТЕТАТ

Как видно из примера, шифровка и открытый текст содержат одинаковые символы, но они располагаются на разных местах.

Ключом в данном случае является размер матрицы, порядок записи открытого текста в матрицу и порядок считывания шифрограммы. Естественно, что ключ может быть другим. Например, запись открытого текста по строкам может производиться в таком порядке: 48127653, а считывание криптограммы может происходить по столбцам в следующем порядке: 81357642.

Будем называть порядок записи в строки матрицы ключом записи, а порядок считывания шифрограммы по столбцам – ключом считывания. Тогда правило дешифрирования криптограммы, полученной методом перестановок, можно в общем виде записать так.

Чтобы дешифровать криптограмму, полученную с помощью матрицы *n x n*, нужно криптограмму разбить на группы символов по *n* символов в каждой группе. Крайнюю левую группу записать сверху - вниз в столбец, номер которого совпадает с первой цифрой ключа **считывания**. Вторую группу символов записать в столбец, номер которого совпадает со второй цифрой ключа считывания и т.д. Открытый текст считывать из матрицы по строкам в соответствии с цифрами ключа **записи.**

Рассмотрим пример дешифрации криптограммы, полученной методом перестановок. Известно, что при шифровании использованы матрица 6x6, ключ записи 352146 и ключ считывания 425316. Текст шифрограммы таков:

ДКАГЧЬОВА_РУААКОЕБЗЕРЕ_ДСОХТЕСЕ_Т_ЛУ

Разобьем шифрограмму на группы по 6 символов:

ДКАГЧЬ ОВА_РУ ААКОЕБ ЗЕРЕ_Д СОХТЕС Е_Т_ЛУ

Затем первую группу символов запишем в столбец 4 матрицы 6х6, так как первая цифра ключа **считывания** – 4 (см. рисунок 1.1.9.1,а). Вторую группу из 6 символов запишем в столбец 2 (см. рисунок 1.1.9.1,б), третью группу символов – в столбец 5 (см. рисунок 1.1.9.1,в), пропустив две фазы заполнения матрицы, изобразим полностью заполненную матрицу (см. рисунок 1.1.9.1, г).

Считывание открытого текста в соответствии с ключом записи начинаем со строки 3, затем используем строку 5 и т.д. В результате дешифрования получаем открытый текст:

ХАРАКТЕР ЧЕЛОВЕКА СОЗДАЕТ ЕГО СУДЬБУ

Естественно, что описанная процедура дешифрования криптограммы производится компьютером автоматически с помощью заранее разработанных программ.

	1	2	3	4	5	6
1				Д		
2				К		
3				А		
4				Г		
5				Ч		
6				Ь		

а)

	1	2	3	4	5	6
1		О		Д		
2		В		К		
3		А		А		
4		_		Г		
5		Р		Ч		
6		У		Ь		

б)

	1	2	3	4	5	6
1		О		Д	А	
2		В		К	А	
3		А		А	К	
4		_		Г	О	
5		Р		Ч	Е	
6		У		Ь	Б	

в)

	1	2	3	4	5	6
1	С	О	З	Д	А	Е
2	О	В	Е	К	А	_
3	**Х**	**А**	**Р**	**А**	**К**	**Т**
4	Т	_	Е	Г	О	_
5	Е	Р	_	Ч	Е	Л
6	С	У	Д	Ь	Б	У

г)

Рис. 1.1.9.1. Порядок дешифрации методом перестановок

1.1.10. Перестановки по сложным траекториям

Он доказывал,
что кто-то должен присматривать за обществом,
что взлом шифров агентством –
вынужденная необходимость, залог мира.
Дэн Браун

В методе перестановок запись открытого текста может происходить по различным траекториям. Например, может быть использована ромбовидная таблица. Зашифруем с ее помощью афоризма У.Коллинза «Никогда не доверяйте тем подчиненным, которые не находят у начальства никаких изъянов».

Таблица 1.1.10.1

1	2	3	4	5	6	7	8	9	10	11	12	13
						Н						
					И	К	О					
				Г	Д	А	_	Н				
			Е	_	Д	О	В	Е	Р			
		Я	Й	Т	Е	_	Т	Е	М	_		
	П	О	Д	Ч	И	Н	Е	Н	Н	Ы	М	
,	_	К	О	Т	О	Р	Ы	Е	_	Н	Е	_
	Н	А	Х	О	Д	Я	Т	_	У	_	Н	
		А	Ч	А	Л	Ь	С	Т	В	А		
			Н	И	К	А	К	И	Х			
				И	З	Ъ	Я	Н				
					О	В	_					
						_						

Пусть ключ считывания будет таким: 5-13-2-7-1-4-12-3-11-6-10-8-9

В результате чтения текста по столбцам получится следующая криптограмма:

Г_ТЧТ ОАИИ_ П_ННК АО_НР ЯЬАЪВ _,ЕЙД ОХЧНМ
ЕНЯОК АА_ЫН _АИДД ЕИОДЛ КЗОРМ Н_УВХ О_ВТЁ
ЫТСКЯ _НЕЕН Е_ТИН

Очевидно, что наличие пробелов и знаков препинания в криптограмме облегчает криптоанализ. Поэтому пробелы и знаки препинания перед шифрованием часто удаляют. Хотя это может привести к серьезным смысловым ошибкам. Например, как понять такой текст: «Зачёт поставить нельзя незачёт»? Изменение положения запятой в предложении меняет смысл на противоположный.

На следующем рисунке показано несколько геометрических фигур (треугольник, прямоугольник, ромб, параллелограмм, трапеция, пятиугольник, шестиугольник, восьмиугольник). Эти фигуры можно использовать для записи открытого текста по строкам и считывания шифрограммы по столбцам.

Естественно, что не только эти фигуры можно использовать для шифрования. Есть возможность использовать и более сложные формы.

Траектории записи открытого текста в указанные фигуры и считывания получающейся криптограммы также можно усложнить.

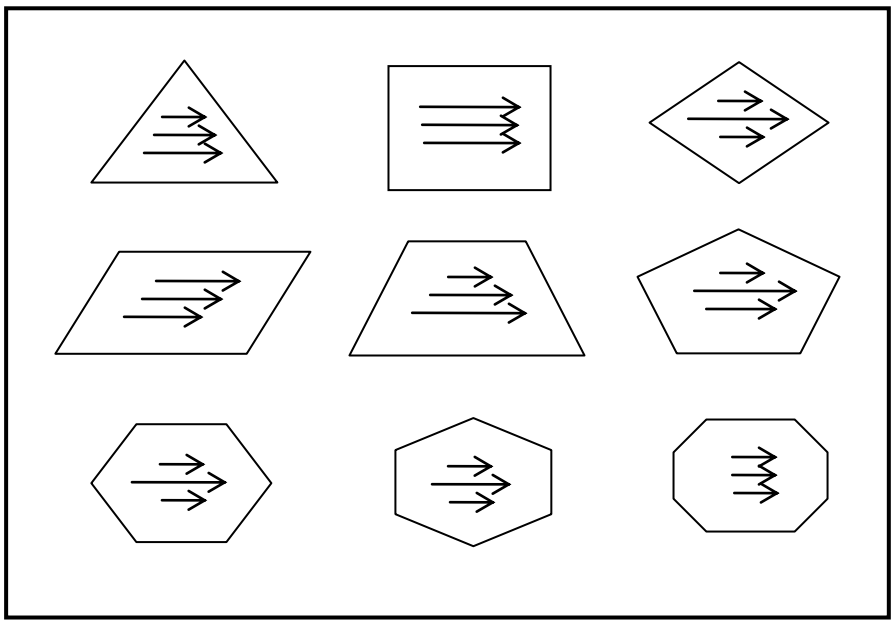


Рис. 1.1.10.1. Примеры геометрических фигур

На следующем рисунке показано несколько примеров различных траекторий записи открытого текста.

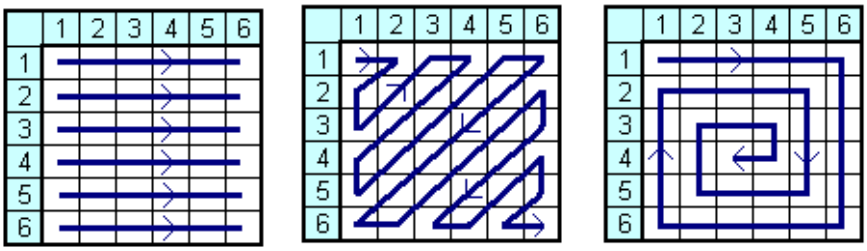


Рис. 1.1.10.2. Примеры траекторий

Предполагается, что в этих трех случаях считывание криптограмм будет производиться по столбцам.

Казалось бы, что, чем сложнее траектория, тем труднее произвести криптоанализ. Однако это не всегда так. Следует отдать предпочтение первой траектории (запись по строкам). При записи «змейкой» и «по спирали» в криптограммах будут проступать фрагменты открытого текста. При записи «змейкой» останутся не перетасованными две пары символов в столбце 1 и две пары символов в столбце 6.

Особенно неудачен последний вариант. При использовании траектории «спираль» шесть символов в столбце 6 и четыре символа в столбце 5 останутся не перемешанными.

Например, зашифруем фразу: «Температура в норме: тридцать шесть и шесть». Запишем открытый текст по спирали в матрицу 6x6.

Таблица 1.1.10.2

	1	2	3	4	5	6
1	Т	Е	М	П	Е	Р
2	И	Д	Ц	А	Т	А
3	Р	Ш	Е	С	Ь	Т
4	Т	И	Ь	Т	Ш	У
5	Е	Ь	Т	С	Е	Р
6	М	Р	О	Н	В	А

Считаем криптограмму в соответствии с ключом: 3-1-6-4-2-5. В результате получится шифрограмма, которой отчетливо проступает буквосочетание «РАТУРА».

МЦЕЬТОТИРТЕМ**РАТУРА**ПАСТСНЕДШИЬРЕ**ТЬШЕ**В

И всё же сложные траектории можно использовать для формирования криптограммы. Например, в ромбовидной таблице запись открытого текста можно осуществить по следующей траектории (рис. 1.1.10.3). При этом считывать криптограмму нужно по столбцам.

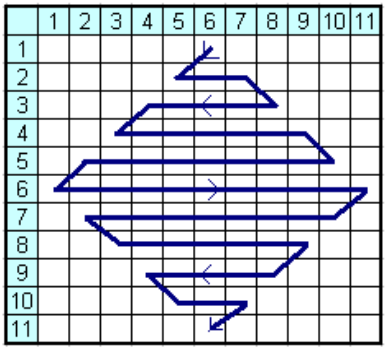


Рис. 1.1.10.3. Пример траектории

1.2. Асимметричные системы

…возможно всё,
на невозможное просто требуется
больше времени.
Дэн Браун

Алгоритмы шифрования с открытым ключом используют так называемые **необратимые или односторонние функции**. Эти функции обладают следующим свойством: при заданном значении аргумента *x* относительно просто вычислить значение функции *f(x).* Однако, если известно значение функции *y = f(x),* то нет простого пути для вычисления значения аргумента *x*.

Все используемые в настоящее время криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований.

1. Разложение больших чисел на простые множители (алгоритм **RSA**, авторы — Райвест, Шамир и Адлеман — **R**ivest, **S**hamir, **A**dleman).

2. Вычисление логарифма или возведение в степень (алгоритм **DH**, авторы — Диффи и Хелман).

3. Вычисление корней алгебраических уравнений.

Рассмотрим простейший пример «необратимых» функций.

Легко в уме найти произведение двух простых чисел 11 и 13. Но попробуйте быстро в уме найти два простых числа, произведение которых равно 437. Подобные трудности возникают и при использовании вычислительной техники для отыскания двух простых сомножителей для очень большого числа: найти сомножители можно, но потребуется много времени.

Таким образом, в системе кодирования RSA, основанной на разложении на множители, используются два разных ключа: один для шифрования сообщения, а второй — отличный от первого, но связанный с ним — для дешифрования. Ключ шифрования (открытый, несекретный ключ) основан на произведении двух огромных простых чисел, а ключ дешифрования (закрытый, секретный ключ) — на самих простых числах.

Заметим, что операцию разложения простого числа на множители порой называют **факторизацией.**

Термин «необратимые» функции неудачен. Правильнее было бы их назвать быстро (или просто) необратимые функции. Однако этот термин устоявшийся, и с неточностью приходится мириться.

В 40-х годах XX в. американский инженер и математик Клод Шеннон предложил разрабатывать шифр таким образом, чтобы его раскрытие было эквивалентно решению сложной математической задачи. Причем сложность задачи должна быть такой, чтобы объем необходимых вычислений превосходил вычислительные возможности современных ЭВМ.

В асимметричных системах приходится применять длинные ключи (2048 бита и больше). Длинный ключ увеличивает время шифрования открытого сообщения. Кроме того, генерация ключей становится весьма длительной. Зато пересылать открытые ключи можно по незащищенным (незасекреченным, открытым) каналам связи. Это особенно удобно, например, для коммерческих партнеров, разделенных большими расстояниями. Открытый ключ удобно передавать от банкира сразу нескольким вкладчикам.

В **симметричных** алгоритмах используют более короткие ключи, поэтому шифрование и дешифрование происходят быстрее. Но в таких системах рассылка ключей является сложной процедурой. Передавать ключи нужно по закрытым (секретным) каналам. Использование курьеров для рассылки секретных ключей дорогая, сложная и медленная процедура.

1.2.1. Алгоритм RSA

Сейф Биггломана представляет
собой гипотетический сценарий,
когда создатель сейфа прячет
внутри его ключ, способный его открыть.
Дэн Браун

Рассматриваемый алгоритм шифрования разработали Rivest, Shamir, Adleman (RSA).

Опишем пример использования такой криптосистемы.

Пусть абонент А (например, банкир) и абонент В (например, вкладчик) решили организовать между собой секретную передачу информации.

Каждый из абонентов независимо друг от друга выбирает два больших простых числа, находит их произведение, функцию Эйлера от этого произведения и выбирает случайное число, меньшее вычисленного значения функции Эйлера и взаимно простое с ним.

Напомним, что **простое число** — это целое положительное число, большее единицы, не имеющее других делителей, кроме самого себя и единицы. **Взаимно простые числа** — целые числа, не имеющие общих (простых) делителей.

Порядок создания ключей проиллюстрируем с помощью таблицы. Для наглядности числа выбраны малой величины. Фактически эти числа имеют около 100 десятичных разрядов.

Таблица 1.2.1.1

Действия	Абонент А (банкир)	Абонент В (вкладчик)
1. Выбор двух простых чисел p и q	$p = 7; q = 13$	$p = 11; q = 23$
2.Вычисление произведения $r = p \cdot q$	$r = 7 \cdot 13 = 91$	$r = 11 \cdot 23 = 253$
3. Расчет функции Эйлера $\varphi(r) = r–p–q+1$	$\varphi(r) = 72$	$\varphi(r) = 220$
4. Выбор случайного числа s, взаимно простого с $\varphi(r)$ из интервала $0 < s < \varphi(r)$	$s = 5$	$s = 31$
5. Расчет **секретного** ключа t с помощью соотношения $s \cdot t = 1(\mathrm{mod}\,\varphi(r))$	$5 \cdot t = 1(\mathrm{mod}(72))$ $t = 29$	$31 \cdot t = 1(\mathrm{mod}(220))$ $t = 71$
6. Публикация **открытых** ключей s, r	$s = 5$, $r = 91$	$s = 31$, $r = 253$

Использованная в таблице запись $\alpha = \beta(\mathrm{mod}(\gamma))$ означает, что при целочисленном делении числа α на число γ остаток равен β.

Например, 7 = 1(mod(3)).

Функция Эйлера — арифметическая функция $\varphi(r)$, значение которой равно количеству положительных чисел, не превосходящих r и взаимно простых с r.

Предположим, что абонент А решил послать сообщение абоненту В. Вначале методом замены каждый символ сообщения заменяется (шифруется) числом. Допустим, что требуется переслать первую букву открытого сообщения, которая предварительно зашифрована методом замены числом 2.

Абонент А шифрует число 2 открытым (опубликованным) ключом абонента В. Для шифрования передаваемое число 2 возводится в степень $s = 31$, т. е.

$$m = 2^{31} = 2147483648.$$

Затем находят остаток от деления числа m на величину $r = 253$, в результате которого получается число 167, то есть:

$$2^{31} = 167 \text{ (mod(253))}.$$

Напомним, что числа s и r являются открытым ключом абонента В.

В линию передается число 167, которое является шифром исходного числа 2.

Получив шифрограмму (167), абонент В использует свой секретный ключ $t = 71$. Для дешифрации он возводит полученное число 167 в степень 71 и находит остаток от деления на число 253. Математически это записывается так:

$$167^{71} \equiv 2(\text{mod}(253)).$$

В данном случае остаток от деления равен 2, значит, шифрация и дешифрирование произошли правильно. Было передано число 2, и это же число было принято после всех преобразований.

Предположим, что абонент В решил ответить абоненту А и направить ему букву, зашифрованную числом 3.

Абонент В использует открытый (опубликованный) ключ абонента А ($s = 5$, $r = 91$) и выполняет шифрующее преобразование числа 3. Математически это записывается так:

$$3^5 \equiv 61(\text{mod}(91)).$$

В линию отправляется число 61. Получив это число, абонент А восстанавливает (дешифрирует) исходный текст с помощью своего секретного ключа $t = 29$:

$$61^{29} \equiv 3(\text{mod}(91)).$$

В результате дешифрации на приемной стороне получено число 3, которое отправил абонент В.

Процесс передачи букв между абонентами иллюстрирует следующая таблица.

Передача			Число	Прием		
Букв	Число	Шифрование		Дешифрование	Число	Букв

а			линии			а
M	2	$2^{31} = 167(\mathrm{mod}(253))$	167	$167^{71} = 2(\mathrm{mod}(253))$	2	M
L	3	$3^{5} = 61(\mathrm{mod}(91))$	61	$6129 = 3(\mathrm{mod}(91))$	3	L

Таблица 1.2.1.2

Первая строка приведенной таблицы поясняет процесс передачи буквы M от абонента A к абоненту B. Вторая строка показывает, как передается буква L от абонента B к абоненту A. В данном случае считается, что буква M кодируется числом 2, а буква L – числом 3.

В приведенных примерах был рассмотрен порядок передачи одного символа с каждой стороны. Понятно, что таким образом последовательно передается целое сообщение, но преобразование над каждым символом происходит по рассмотренной схеме. Заметим, что для использования этого метода необходимо сообщение предварительно преобразовать в набор чисел, например, с помощью кодовой таблицы.

Достоинством шифрования с открытым ключом является исключение необходимости передачи секретного ключа по закрытым каналам связи, например, с помощью курьера.

Однако у этого метода есть существенный недостаток. Используя опубликованный ключ, сообщение может прислать любой абонент, выдавая себя за другого абонента.

В подобных случаях требуется **аутентификация** — подтверждение авторства присланного документа. Для этих целей разработан способ шифрования, который называется **электронной подписью.**

Суть этого метода шифрования заключается в том, что сообщение шифруется не только опубликованным открытым ключом, но и собственным секретным ключом абонента, отправляющего сообщение.

Рассмотрим пример.

Предположим, что абонент B (вкладчик) решил послать сообщение, состоящее из числа 41, абоненту A (банкиру). Вначале вкладчик шифрует сообщение открытым ключом банкира:

$$41^{5} \equiv 6(\mathrm{mod}(91)).$$

В результате шифрования получено число 6.

Дальше вкладчик повторно шифрует это сообщение **своим секретным ключом** 71:

$$6^{71} \equiv 94(\mathrm{mod}(253)).$$

Шифрограмма 94 отправляется банкиру.

Банкир, получив секретное сообщение, использует вначале открытый ключ вкладчика:

$$94^{31} \equiv 6(\mathrm{mod}(253)).$$

Затем банкир использует свой секретный ключ:

$$6^{29} \equiv 41(\mathrm{mod}(91)).$$

В результате абонент А (банкир) получает сообщение, состоящее из числа 41.

При использовании электронной подписи никто другой не сможет прислать банкиру сообщение (например, поручение перевести деньги) от имени абонента В, так как на передаче нужно обязательно использовать секретный ключ вкладчика, который известен только абоненту В.

Цифровая подпись используется не только для заверения текстовых или финансовых документов. Эта же информационная технология применяется для указания авторства разработанной программы.

1.3. Шифрование с помощью графических матриц

Основная идея защиты информации с помощью графических матриц заключается в следующем.

Для шифрования передаваемой информации буквы (точнее, символы) представляют в виде графических матриц, состоящих из белых и черных точек. При шифровании точки в графических матрицах переставляются или заменяются другими в соответствии с выбранным ключом. Зашифрованная путем перестановки и замены пикселей информация дробится на биты, которые распыляются по множеству контейнеров [19].

Одним из возможных применений этого шифра является скрытная передача информации с помощью сайта, содержащего большое число фотографий (или аудио файлов, Web-страниц). При этом противник не знает, какие фотографии являются контейнерами и в какой последовательности передаваемая информация распылена по контейнерам.

Для формирования практически равновероятной смеси битовых последовательностей изображения символов формируются из одинакового числа белых и черных пикселей. Это позволяет формировать на выходе шифратора последовательность двоичных сигналов с равномерным распределением.

Значительно усложняет стегоанализ распыление имеющейся битовой последовательности по нескольким контейнерам. Причем распыление происходит не детерминировано, а по случайному закону в соответствии с секретным ключом.

Необходимо отметить следующий момент, касающийся криптоанализа. Многие методы криптоанализа основаны на создании и использовании модели открытого текста (учет повторения отдельных символов, создание таблиц частот встречающихся отдельных символов, биграмм, триграмм…). Автоматический криптоанализ предполагает использование цепей Маркова. В результате автомат, а не человек определяет: получен открытый текст или он нечитаемый (бессмысленный набор символов).

Однако модель открытого текста трудно применить для взлома сообщения, зашифрованного с помощью рассматриваемого шифра. Здесь символы представлены с помощью графических матриц и для силового взлома криптограммы следует использовать автомат распознавания образов. Задача

становится принципиально неразрешимой, когда вместо традиционных символов используются графические матрицы с равновероятным распылением белых и черных точек.

Наибольшая степень защиты достигается в том случае, когда вместо символов даже слегка напоминающих символы открытого текста, используется пёстрая, псевдослучайная мозаика. Автомат не будет знать, что искать. Лишь при утечке сведений о таблице замен, которая связывает символы открытого текста и секретные псевдослучайные графические матрицы, появляется возможность произвести автоматический криптоанализ.

Однако для полного криптоанализа потребуется преодолеть еще несколько уровней защиты информации. Первый уровень – это традиционная криптографическая защита (сообщение должно быть предварительно зашифровано одним из криптостойких способов). Второй уровень – нужно определить размер графической матрицы, порядок расположения информативных, маскирующих, пограничных пикселей. Затем нужно определить, какой вид преобразования матрицы осуществлен в данном случае (сдвиг влево – вправо, вверх – вниз, перестановка столбцов, строк…), и каковы количественные характеристики этого преобразования. Третий уровень защиты состоит в решении комбинационной задачи по собиранию битов из пространственно распределенных контейнеров. При этом неизвестно, какие контейнеры содержат информацию и в какой последовательности распылены биты.

Рассмотрим примеры формирования изображения различных символов с помощью графических матриц (см. рис.1.3.1).

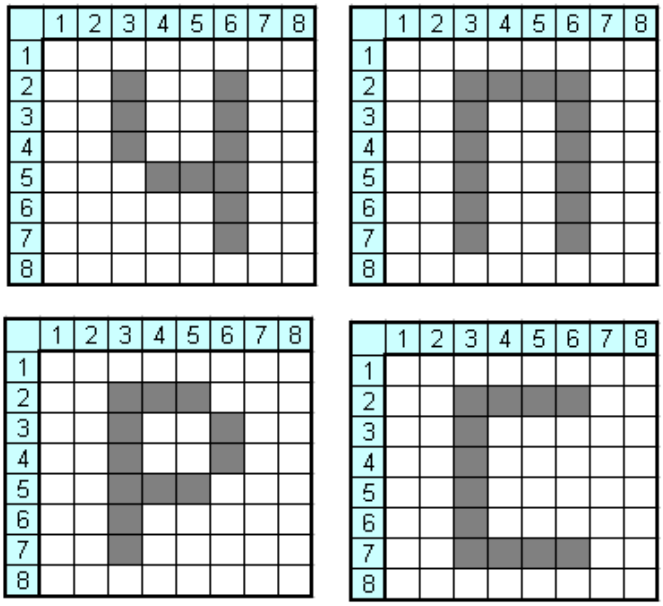


Рис.1.3.1. Четыре графические матрицы
с изображением букв «Ч», «П», «Р» и «С».

В данном случае выбрана матрица 8 x 8.

Следующая матрица имеет большее число пикселей: 10 x 10 (см. рис.1.3.2).

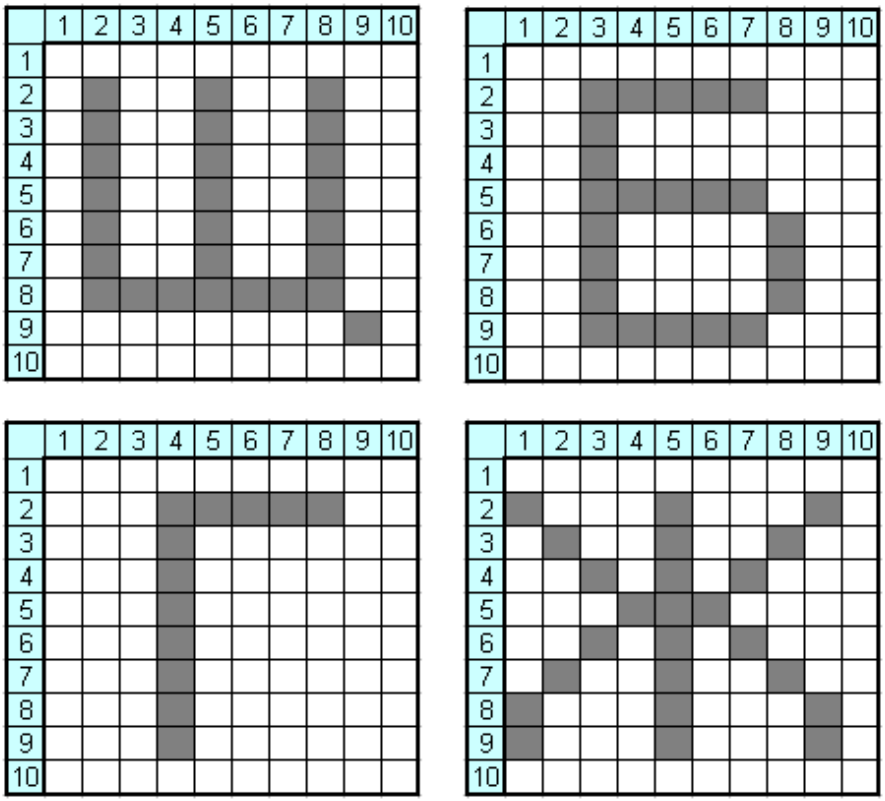


Рис. 1.3.2. Четыре графические матрицы
с изображением букв «Щ», «Б», «Г» и «Ж»

Анализ приведенных изображений показывает, что для формирования разных символов требуется разное число информативных пикселей. Буква «Щ» содержит 29 черных точек, буква «Б» - 23, буква «Г» - 12, буква «Ж» - 24. Понятно, что такое заметное количественное различие графических матриц дает некоторую зацепку для криптоаналатиков. Например, они могут попытаться восстановить передаваемые символы путем подсчета числа чёрных пикселей в каждой графической матрице.

Улучшить ситуацию можно за счет формирования рамки вокруг изображения символов (рис.1.3.3). При этом общее число черных точек во всех графических матрицах должно быть одинаковым.