Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра информационных технологий
и систем безопасности

Т.М. Татарникова

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум

РГГМУ
Санкт-Петербург
2013

УДК 621.391.037.372

Татарникова Т.М. Криптографические методы защиты информации. Лабораторный практикум. – СПб.: РГГМУ, 2013. – 64 с.

Рецензент: И.М. Лёвкин, д-р техн. наук, проф. СПбГУСЭ.

Лабораторный практикум предназначен для выполнения лабораторных работ по курсу «Криптографические методы защиты информации» и содержат описание основных типов шифров, их свойств и криптографических алгоритмов, некоторые методы криптоанализа простейших шифров, основы математического моделирования в криптографии и контрольные вопросы для закрепления пройденного материала.

Предназначено для подготовки специалистов по направлению «Информационная безопасность».

Tatarnikova T.M. Cryptographic methods of information protection. Laboratory practical. – St. Petersburg, RSHU Publisher, 2013. – 64 pp.

Laboratory practical is intended for laboratory work in the course of «cryptographic methods of information security» and contain a description of the main types of ciphers, their properties, and cryptographic algorithms, some methods of cryptanalysis of simple ciphers, the basics of mathematical modeling in cryptography and control questions to consolidate the material.

Intended for training specialists in the field of «Information Security».

ВВЕДЕНИЕ

Защита конфиденциальных сообщений в открытых сетях требует применения криптографических методов.

Криптография является самым мощным в настоящее время средством защиты информации и представляет самостоятельную прикладную науку, основанную на глубоких математических знаниях.

Криптографические методы позволяют обеспечить конфиденциальность данных, устанавливать подлинность отправителя и контролировать целостность передаваемых сообщений.

Базовая модель криптографии, представленная на рис. 1 предполагает существование противника, имеющего доступ к открытому каналу связи и перехватывающего путем подслушивания все сообщения, передаваемые от отправителя к получателю. Подслушивание со стороны противника называется пассивным перехватом сообщений. Кроме того, противник может активно вмешивается в процесс передачи информации – модифицировать передаваемые сообщения, навязывать получателю свои собственные сообщения из канала. Такие действия называются активным перехватом сообщений.

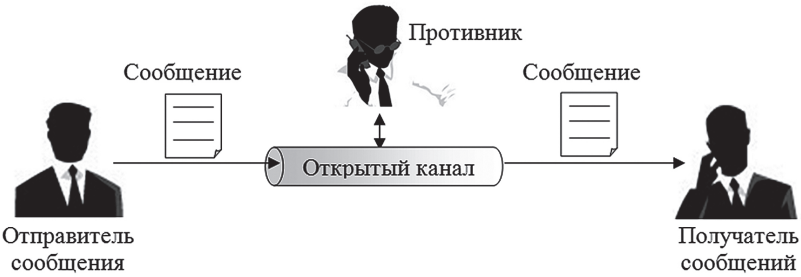

Рис. 1. Базовая модель криптографии

Способы противодействия противнику основаны на применении методов шифрования. Все современные методы шифрования делятся на одноключевые или симметричные и двухключевые или асимметричные.

В симметричных криптографических системах ключи, используемые на передающей и приемной сторонах, полностью идентичны. Такой ключ несет в себе всю информацию о засекреченном сообщении и поэтому не должен быть известен никому, кроме двух участвующих в разговоре сторон. Противник, наблюдая зашифрованное сообщение (шифротекст), не может прочитать сообщение. Отсюда возникает задача для противника – получение открытого сообщения по наблюдаемому шифротексту, а именно задача сводится к раскрытию секретного ключа шифрования/дешифрования. Действия, предпринимаемые противником с целью раскрытия секретного

ключа, называется атакой. Секретный канал, используемый для передачи секретного ключа от отправителя к получателю, должен исключать возможность утечки информации.

В асимметричных криптографических системах для шифрования и дешифрования применяются различные ключи. Для шифрования информации, предназначенной конкретному получателю, используют уникальный открытый ключ получателя-адресата. Соответственно для дешифрования получатель использует парный секретный ключ. Для передачи открытого ключа от получателя к отправителю секретный канал не нужен. Вместо секретного канала используется аутентичный канал, гарантирующий подлинность источника передаваемой информации (открытого ключа отправителя). Аутентичный канал является открытым и доступен противнику.

С помощью криптографических методов решается задача целостности информации. Целостность – это гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений. Целостность предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и т.д. Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям.

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, то есть установления подлинности автора и отсутствия изменений в полученном документе. Эта задача также решается криптографическими методами, основанными на применении электронной цифровой подписи – ЭЦП. Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. ЭЦП решает проблему возможного спора между отправителем и получателем, в том числе и в суде, при наличии юридической базы для ее применения.

В настоящее время криптографические методы нашли широкое применение не только для защиты информации от несанкционированного доступа, но и в качестве основы многих новых электронных информационных технологий – электронного документооборота, электронных денег, тайного электронного голосования и др.

Лабораторный практикум содержит необходимый материал для выполнения лабораторных работ по курсу «Криптографические методы защиты информации» и включает способы решения задач конфиденциальности, аутентификации и целостности информации.

Лабораторная работа №1.
КРИПТОАНАЛИЗ ШИФРА ПРОСТОЙ ЗАМЕНЫ

Цель работы: Выполнить криптоанализ текста, зашифрованного шифром простой замены с применением неперебoрного метода вскрытия шифротекста.

1.1. Описание объекта исследования

Самым простым из известных исторических шифров является шифр подстановки, который использовал Юлий Цезарь при переписке в военных походах.

В шифре Цезаря каждая буква алфавита заменяется буквой, которая находится на три позиции дальше в этом же алфавите. Рассмотрим на примере.

Открытый текст: meet me after the toga party
Шифрованный текст: PHHW PH DIWHU WKH WRJD SDUMB

Алфавит считается «циклическим» поэтому после Z идет A. Определить преобразование, можно перечислив все варианты, как показано ниже.

Открытый текст: abcdefghijklmnopqrstuvwxyz
Шифрованный текст: DEFGHIJKLMNOPQRSTUVWXYZABC

Если каждой букве назначить числовой эквивалент (a = 1, b = 2, c = 3 и т.д.), то алгоритм можно выразить формулами (1.1–1.3). Каждая буква открытого текста *m* заменяется буквой шифрованного текста *C*:

$$C = E(m) = (m+3) \bmod (26). \tag{1.1}$$

В общем случае сдвиг может быть любым, поэтому обобщенный алгоритм Цезаря записывается формулой:

$$C = E(m) = (m+k) \bmod (26), \tag{1.2}$$

где *k* принимает значение в диапазоне от 1 до 25, назовем *k* ключом шифрования.

Алгоритм дешифрования записывается формулой:

$$m = D(C) = (C-k) \bmod (26). \tag{1.3}$$

Если известно, что определенный текст был шифрован с помощью шифра Цезаря, то с помощью простого перебора всех вариантов раскрыть шифр просто – для этого достаточно перебрать 25 возможных вариантов ключей k. На рис. 2 показаны результаты применения этой стратегии к указанному выше в рассматриваемом примере сообщению. В данном случае открытый текст распознается в третьей строке.

Шифрованный текст:	PHHW	PH	DIWHU	WKH	WRJD	SDUMB
$k = 1$	oggv	og	chvgt	vjg	vqic	rctva
$k = 2$	nffu	nf	bgufs	uif	uphb	qbsuz
$k = 3$	meet	me	after	the	toga	party
$k = 4$	ldds	ld	zesdq	sgd	snfz	ozqsx
$k = 5$	kccr	kc	ydrcp	rfc	rmey	nyprw
$k = 6$	jbbq	jb	xcqbo	qeb	qldx	mxoqv
$k = 7$	iaap	ia	wbpan	pda	pkcw	lwnpu
$k = 8$	hzzo	hz	vaozm	ocz	ojbv	kvmot
$k = 9$	gyyn	gy	uznyl	nby	niau	julns
$k = 10$	fxxm	fx	tymxk	max	mhzt	itkmr
$k = 11$	ewwl	ew	sxlwj	lzw	lgys	hsjlq
$k = 12$	dvvk	dv	rwkvi	kyv	kfxr	grikp
$k = 13$	cuuj	cu	gvjuh	jxu	jewq	fqhjo
$k = 14$	btti	bt	puitg	iwt	idvp	epgin
$k = 15$	assh	as	othsf	hvs	hcuo	dofhm
$k = 16$	zrrg	zr	nsgre	gur	gbtn	cnegl
$k = 17$	yggf	yg	mrfqd	ftq	fasm	bmdfk
$k = 18$	xppe	xp	lqepc	esp	ezrl	alcej
$k = 19$	wood	wo	kpdob	dro	dyqk	zkbdi
$k = 20$	vnnc	vn	jocna	cqn	cxpj	yjach
$k = 21$	ummb	um	inbmz	bpm	bwoi	xizbg
$k = 22$	tlla	tl	hmaly	aol	avnh	whyaf
$k = 23$	skkz	sk	glzkx	znk	zumg	vgxze
$k = 24$	rjjy	rj	fkyjm	ymj	ytlf	ufwyd
$k = 25$	qiix	qi	ejxiv	xli	xske	tevxc

Рис. 2. Криптоанализ шифра простой замены (шифра Цезаря) методом перебора всех вариантов ключей

Применение метода последовательного перебора всех возможных вариантов оправдано, если выполняются три важные характеристики данного шифра:

– известны алгоритмы шифрования и дешифрования;
– необходимо перебрать небольшое количество вариантов;
– язык открытого текста известен и легко узнаваем.

Алгоритм, для которого требуется перебрать слишком много ключей, делает криптоанализ на основе метода последовательного перебора практически бесполезным.

В этом случае для криптоаналитика существует другая линия атаки. Если криптоаналитик имеет представление о природе открытого текста (например, о том, что это несжатый текст на английском языке), можно использовать известную информацию о характерных признаках, присущих текстам на соответствующем языке. Методика криптоанализа текста, зашифрованного шифром простой замены с применением неперебороного метода вскрытия шифротекста состоит из следующих этапов.

На первом этапе можно определить относительную частоту (вероятность) $p(C)$ появления в тексте различных букв и сравнить их со среднестатистическими данными для букв соответствующего языка, представленных в табл. 1 для русского языка и в табл. 2 для английского языка.

Выяснить значения 3–4 букв текста и выполняется сравнение рангов символов шифртекста с рангами символов в русском языке. Далее необходимо заменить эти три или четыре символа в шифртексте на символы русского языка с теми же рангами.

Таблица 1

$p(C)$ появления символов в среднестатистическом тексте для русского языка

Буква	$p(C)$	Буква	$p(C)$	Буква	$p(C)$
О	0,090	М	0,026	Й	0,010
Е	0,072	Д	0,025	Х	0,009
Ф	0,062	П	0,023	Ж	0,007
И	0,062	У	0,021	Ш	0,006
Н	0,053	Я	0,018	Ю	0,006
Т	0,053	З	0,016	Ц	0,004
С	0,045	Ы	0,016	Щ	0,003
Р	0,040	Б	0,014	Э	0,003
В	0,038	Ь,Ъ	0,014	Ф	0,002
Л	0,035	Г	0,013		
К	0,028	Ч	0,012		

Таблица 2

$p(C)$ появления символов в среднестатистическом тексте для английского языка

Буква	$p(C)$	Буква	$p(C)$	Буква	$p(C)$
E	0,131	N	0,071	H	0,053
T	0,104	R	0,068	D	0,038
A	0,082	I	0,063	L	0,034
O	0,080	S	0,061	F	0,029
C	0,028	P	0,020	X	0,002
M	0,025	W	0,015	J	0,001
U	0,024	B	0,014	Q	0,001
G	0,020	V	0,009	Z	0,001
Y	0,020	K	0,004		

На втором этапе, продолжая анализ частоты появления букв и применяя метод проб и ошибок, необходимо воспользоваться особенностями языка. Например, для русского языка это удвоение букв, окончания слов, короткие слова типа «как», «или», союзы и т.п.

1.2. Порядок выполнения работы

1. Использовать результаты сравнения статистических характеристик символов шифртекста и русского языка для определения предварительных значений нескольких символов в шифртексте.
   1.1. Выполнить частотный анализ символов зашифрованного текста.
   1.2. Выписать символы из шифртекста с частотой большей 0,04 и произвести ранжирование их в порядке убывания частоты.
   1.3. Сравнить ранги символов шифртекста с рангами символов в русском языке.
   1.4. Выбрать 3–4 наиболее частых символа в шифртексте и русском языке с одинаковыми рангами.
   1.5. Заменить три или четыре символа в шифртексте на символы русского языка с теми же рангами. Проверить совпадение рангов замененных символов в шифртексте и соответствующих символов в русском языке. Например, буква «о» самая частая буква в русском языке – она же должна оказаться самой частой буквой в шифртексте.
2. Использовать результаты грамматического анализа шифртекста и на его основе произвести полное дешифрование текста.
   2.1. Выполнить предварительный анализ и расшифровку коротких слов (предлогов, местоимений, союзов междометий и т.п.) с использованием результатов, полученных в п. 1.5.

2.2. Для идентификации остальных символов шифртекста воспользоваться особенностями русского языка (удвоения букв, окончания слов и т.п.).

1.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы.

- Результаты частотного анализа шифрованного текста для первых символов, имеющих частоту большую 0,04.
- Ранжирование наиболее часто встречающихся символов в порядке убывания.
- Таблица ранжирования символов, имеющих в расшифрованном тексте частоту большую 0,04, и сравнения с ранжированием наиболее частых символов русского языка.
- Примеры особенностей русского языка, использованных при дешифровании.
- Два-три варианта замены символов в шифртексте на символы русского языка с теми же рангами (попытки криптоанализа).
- Таблица замены наиболее часто встречающихся символов шифртекста на соответствующие им по рангу символы в русском языке.
- Ответ на контрольный вопрос, номер которого соответствует номеру варианта задания.
- Выводы по проделанной работе.

1.4. Контрольные вопросы

1. Что такое энтропия языка?
2. Что понимается под избыточностью сообщения?
3. Что такое шифр простой замены?
4. В чем состоит обобщение шифра Цезаря?
5. Опишите краткую историю возникновения шифра Цезаря.
6. Объясните принцип дешифрования шифра простой замены.
7. Объяснить, почему при вскрытии шифра простой замены используется не полное ранжирование по частоте всех символов русского языка, а лишь 3-4 наиболее частых символов, как в п. 1.4?
8. Какими характеристиками должен обладать шифр, чтобы была возможность применить метод частотного анализа?
9. Какие виды криптоанализа Вам известны?
10. Охарактеризуйте базовую модель криптографии.
11. Какие основные разновидности шифров простой замены применялись в прошлом?
12. Сформулируйте правила шифрования/дешифрования шифра Цезаря.

1.5. Литература

1. *Бабаш А.В., Шанкин Г.П.* История криптографии. Учебное пособие. – М.: «Гелиос АРВ», 2001.
2. *Бескид П.П., Татарникова Т.М.* Криптографические методы защиты информации. Часть 1. Основы криптографии. Учебное пособие. – СПб.: изд. РГГМУ, 2010. – 95 с.

Лабораторная работа №2.
ШИФРЫ ПЕРЕСТАНОВКИ НА ПРИМЕРЕ ШИФРА КАРДАНО

Цель работы: Разработать алгоритмы шифрования и дешифрования сообщений с применением решетки Кардано.

2.1. Описание объекта исследования

В XVI веке Джероламо Кардано, итальянский математик, врач и философ, изобрел шифр, основанный на простой и в то же время надежной перестановке букв сообщения.

Для шифрования используется квадрат с прорезанными в нем несколькими ячейками, получившей название решетки Кардано (рис. 3). Ячейки прорезались таким образом, чтобы при повороте решетки вокруг своего центра на 90°, потом на 180°, а затем на 270° в прорезях поочередно появлялись все позиции исходной решетки и, причем только по одному разу. При шифровании решетка накладывалась на листок для послания сначала в исходном положении – выписывалась слева направо сверху вниз первая порция (четверть) послания. Затем решетка поворачивалась на 90°, скажем, по часовой стрелке – выписывалась вторая четверть сообщения и т.д. (рис. 4).

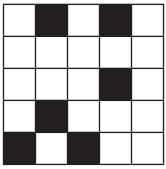

Рис. 3. Решетка Кардано

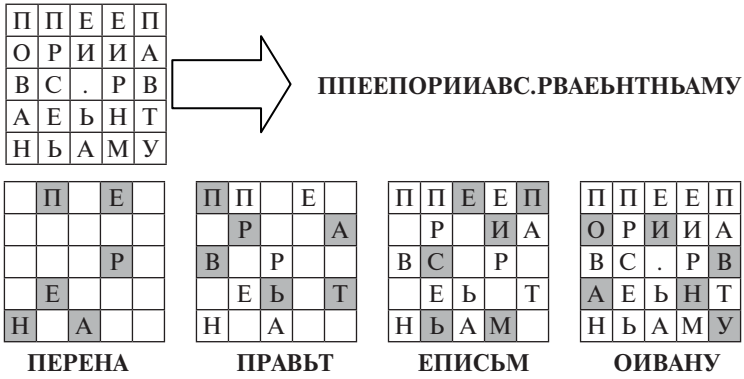

Рис. 4. Шифрование решеткой Кардано

Для дешифрования необходимо иметь точную копию той решетки, которой пользовался шифровальщик, и повторять с ней те же самые повороты. Решетка была удобна для хранения, предельно проста в обращении и при этом давала неплохую стойкость шифра – не зная, как именно расположены прорези на квадрате размером $N \times N$ человеку, перехватившему послание, теоретически нужно было перебрать $4^{N^2/4}$ вариантов. Например, для квадрата 6×6 это число уже равняется 262144, то есть несет 18 бит информации. Если бы не существовало способа восстанавливать поэтапно расположение прорезей, учитывая особенности фонетики национального языка, то дешифрование квадрата 10×10 еще недавно было на грани возможностей современных ЭВМ, поскольку информация о прорезях такого квадрата составляет уже около 50 бит.

Подобные шифры, не модифицирующие буквы сообщения, а только меняющие их расположение, называются перестановочными.

2.2. Порядок выполнения работы

1. Компьютеры в лаборатории объединены в локальную сеть. С каждого компьютера на рабочем месте имеется доступ к диску общего пользования «Y:\Student:». Загрузите программу с именем «Криптография\сетка_вар_xx», где xx – номер варианта.
2. Дешифровать текст, заданный в варианте, восстанавливая при этом решетку-ключ (необходимо восстановить прорезанные ячейки в решетке).
3. Разработать алгоритм шифрования решеткой Кардано.
4. Сформировать решетку-ключ размером 10×10 ячеек.
5. Зашифровать заданный в варианте текст, поворачивая решетку по часовой стрелке.
6. Шифрование производится без пробелов и знаков препинания.
7. Сформировать отчет по лабораторной работе с описанием всех вышеизложенных пунктов.

2.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- В первой части отчета по лабораторной работе, связанной с дешифрованием сообщения необходимо предоставить:
  - Вариант задания – зашифрованное сообщение.
  - Восстановленная решетка Кардано.
  - Дешифрованное сообщение.
- Во второй части отчета по лабораторной работе, связанной с зашифрованием сообщения необходимо предоставить:
  - Вариант задания – открытый текст.

– Алгоритм шифрования квадратом Кардана.
– Разработанная по алгоритму решетка-ключ для шифрования.
– Зашифрованный текст.

- Ответ на контрольный вопрос, номер которого соответствует номеру варианта задания.
- Выводы по проделанной работе.

2.4. Контрольные вопросы

1. Сколько бит информации необходимо для перебора и раскрытия шифрованного текста, состоящего из 140 символов?
2. Классифицируйте шифр Кардано и объясните, по каким признакам Вы отнесли шифр к определенному классу.
3. Сравните два шифра «Квадрат Полибия» и «Решетка Кардано». В каком из этих шифров выше стойкость и почему.
4. Разработайте алгоритм криптоанализа шифра Кардано.
5. Что более целесообразно для надежной защиты информации: архивация открытого текста с последующей шифрованием или шифрование открытого текста с последующей архивацией?
6. Найдите максимальное количество прорезей в решетке размером $N \times N$.
7. Какие еще шифры перестановки Вам еще известны?
8. Какое максимальное количество прорезей можно сделать в квадрате размером $N \times N$ для получения решетки Кардано?
9. Какой вид криптоанализа применим для вскрытия шифртекста, зашифрованного решеткой Кардано?

2.5. Литература

1. *Бабаш А.В., Шанкин Г.П.* История криптографии. Учебное пособие. – М.: «Гелиос АРВ», 2001.
2. *Бескид П.П., Татарникова Т.М.* Криптографические методы защиты информации. Часть 1. Основы криптографии. Учебное пособие. – СПб.: изд. РГГМУ, 2010. – 95 с.

Лабораторная работа №3.
ПОТОЧНЫЕ ШИФРЫ

Цель работы: Разработать генератор гаммы на базе линейного рекуррентного регистра сдвига и выполнить шифрование путем наложения гаммы на открытый текст.

3.1. Описание объекта исследования

Главной отличительной чертой поточных шифров является побитная обработка информации. Как следствие, шифрование и дешифрование в таких схемах может обрываться в произвольный момент времени, как только выясняется, что передаваемый поток прервался, и также восстанавливаться при обнаружении факта продолжения передачи. Подобная обработка информации может быть представлена в виде автомата, который на каждом такте:

– генерирует по какому-либо закону один бит шифрующей последовательности;
– каким-либо обратным преобразованием накладывает один бит открытого потока на данный шифрующий бит, получая зашифрованный бит.

В арифметике по модулю 2, к которой относятся любые преобразования над битами, существуют только две обратимые операции: исключающее ИЛИ (XOR, оно же сложение по модулю 2) и отрицание NOT. Обратимой называется функция, у которой, зная результат и все операнды, кроме одного, можно восстановить этот неизвестный операнд. Очевидно, что в процессе шифрования потока можно применять только обратимые операции, иначе на приемной стороне получатель не сможет однозначно восстановить исходный текст по принятому сообщению, даже зная правильный ключ. Следовательно, как бы много мы не создавали шифрующих бит на один бит исходного текста, все их придется накладывать на данный бит путем комбинации из операций XOR и отрицаний. Но отрицания можно вносить внутрь операции XOR:

$$\text{для } \forall\ a \text{ и } b: \mathrm{NOT}\left(a\ \mathrm{XOR}\ b\right) = a\ \mathrm{XOR}\left(\mathrm{NOT}\ b\right) = \left(\mathrm{NOT}\ a\right)\mathrm{XOR}\ b.$$

Следовательно, как бы ни была сложна композиция из шифрующих бит и исходного бита, ее всегда можно разделить, то есть представить в виде:

$$P\ \mathrm{XOR}\ F\left(g_1, g_2, g_3\right),$$

где P – исходный бит (открытый); g_i – шифрующие биты; F – некоторая функция, содержащая в качестве операции исключающее ИЛИ и отрицание.

Очевидно, что логичнее сразу произвести это преобразование над промежуточными битами g_i и получить в результате только один шифрующий бит g. В результате вся формула шифрования примет универсальный вид:

$$c = p \text{ XOR } g, \tag{3.1}$$

где c – зашифрованный бит.

Все современные поточные шифры действуют по данной схеме. Бит шифрования, получающийся на каждом новом шаге автомата, как впрочем, и целый набор таких бит, принято обозначать символом γ (гамма), а сами поточные шифры получили из-за этого второе название – шифры гаммирования. Общая схема шифрования поточным шифром приведена на рис. 5.

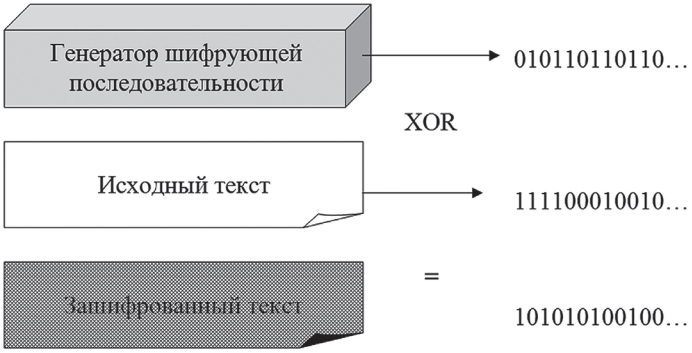

Рис. 5. Шифрование поточным шифром в общем виде

Три основных компонента, над которыми вычисляется функция, порождающая гамму:

– ключ;
– номер текущего шага шифрования;
– близлежащие от текущей позиции биты исходного и/или зашифрованного текста.

Самыми простыми схемами, используемыми в качестве базовых при построении поточных шифров являются линейные регистры сдвига (ЛРС). ЛРС представляет собой несколько (от 20 до 100) ячеек памяти, в каждой из которых может храниться один бит информации. Совокупность бит, находящихся в данный момент в ЛРС, называется состоянием. Для выработки очередного бита шифрующей последовательности, т.е. гаммы, ЛРС производит один цикл преобразований, называемый тактом, по следующему алгоритму:

1. Первый (скажем, самый правый) бит из последовательности поступает на выход ЛРС – это очередной бит гаммы.

2. Содержимое всех промежуточных ячеек памяти сдвигается на одну позицию вправо.
3. В пустую ячейку памяти, появившуюся в результате сдвига у левого края ЛРС, помещается бит, который вычисляется, как операция XOR над значениями из ячеек ЛРС с определенным номером.

Направление сдвига не играет никакой роли. Схема ЛРС представлена на рис. 6.

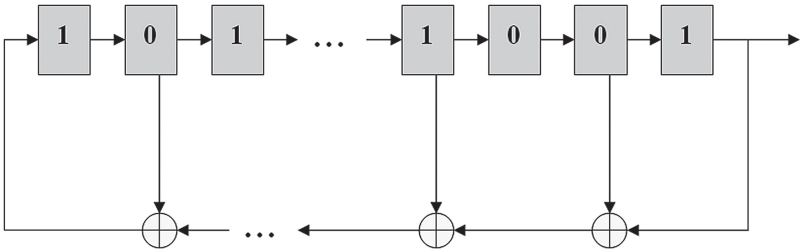

Рис. 6. Общий вид ЛРС

Число бит, охваченных в ЛРС обратной связью, называется разрядностью. При использовании в качестве простейшего шифра перед началом процесса в ячейки памяти ЛРС помещают побитно ключ. Как следствие, бит гаммы, порождаемый на каждом такте зависит от ключа и от номера данного такта в общей процедуре шифрования. Пример работы ЛРС разрядности с отводами обратной связи от нулевого и второго битов при установке ключа «011» представлен на рис. 7.

При достаточно долгой работе ЛРС неизбежно возникает его зацикливание – количество возможных вариантов состояний ЛРС конечно, а следовательно, по выполнении определенного числа тактов его ячейках создается комбинация бит, которая в нем однажды уже оказывалась. С этого момента кодирующая последовательность начнет циклически повторяться с фиксированным периодом. Если представить множество состояний ЛРС и переходов между ними в виде графа, то в зависимости от номеров ячеек, порождающих обратную связь, могут получиться совершенно различные топологии. Некоторые из них приведены на рис. 8.

Цикл «000» характерен для всех графов из-за строения ЛРС. На рис. 8*а* кроме «нулевого» цикла существуют еще два цикла из 3-х состояний и из 4-х. На рис. 8*б* цепочка сходится к циклу из 3-х состояний и уже никогда оттуда не выходит. И, наконец, на рис. 8*в* все возможные состояния кроме «нулевого», объединены в один замкнутый цикл.

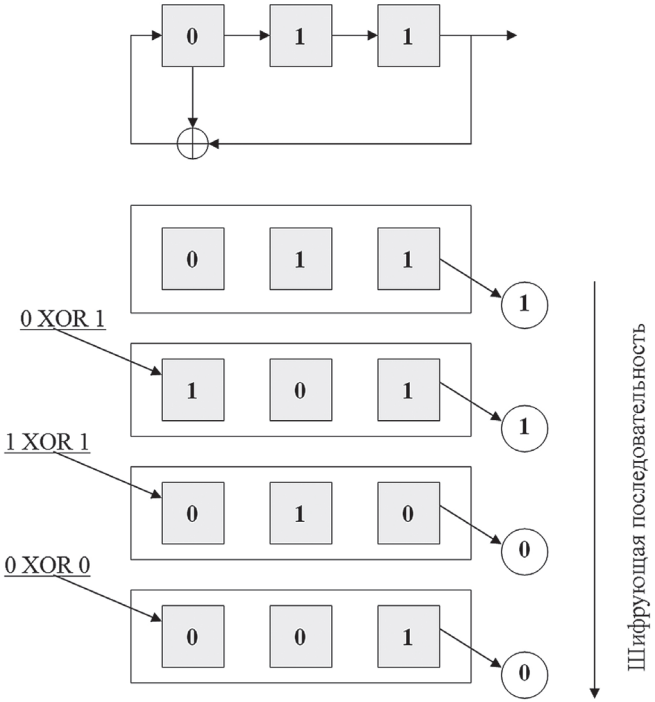

Рис. 7. Пример работы ЛРС

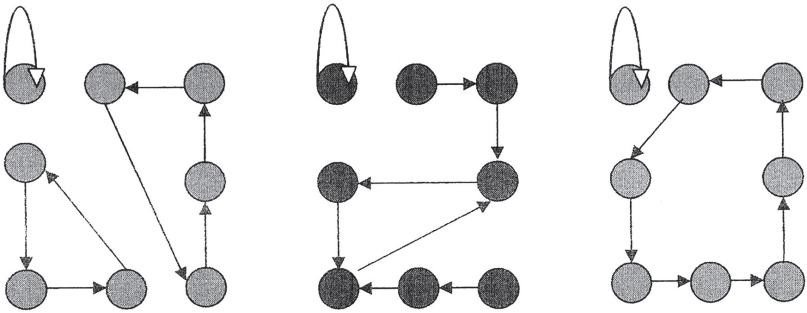

Рис. 8. Графы линейного регистра сдвига

3.2. Порядок выполнения работы

1. Закодировать сообщение ASCII кодом (таблица ASCII приведена в приложении).
2. Разработать генератор гаммы с применением ЛРС и получить шифрующую последовательность равную длине открытого текста.

3. Зашифровать открытый текст путем наложения шифрующей последовательности (гаммы) на открытый текст.
4. Сформировать документ, в который записать зашифрованный текст и схему ЛРС с ключом.
5. Отправить документ по локальной сети лаборатории адресату.
6. Полученный по сети от другого источника документ, предназначенный Вам дешифровать.

3.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- Схема линейного регистра сдвига.
- Цикл шифра гаммирования.
- Открытый текст.
- Граф ЛРС.
- Зашифрованный текст.
- Схема ЛРС для дешифрования.
- Последовательность наложения шифра гаммирования на зашифрованный текст.
- Дешифрованный текст.
- Ответ на контрольный вопрос, соответствующий номеру варианта.
- Выводы по проделанной работе.

3.4. Контрольные вопросы

1. В чем слабость шифра гаммирования с неравновероятной гаммой?
2. Почему наложение на открытый текст гаммы, представляющей собой периодическую последовательность небольшого периода, не дает надежной защиты?
3. Какая функция называется обратимой? Назовите известные Вам обратимые операции.
4. Приведите общую схему образования поточного шифра.
5. Приведите сравнительный анализ шифра гаммирования и шифра Виженера.
6. Покажите известные Вам схемы порождения гаммы.
7. Перечислите разновидности поточных шифров и их отличительные особенности.
8. Перечислите свойства, которыми должна обладать шифрующая последовательность на основе гаммы.
9. Дайте общую характеристику поточного шифра.

3.5. Литература

1. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003.
2. *Бескид П.П., Татарникова Т.М.* Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности. Учебное пособие. – СПб.: изд. РГГМУ, 2010. – 103 с.

Лабораторная работа №4.
ШИФРЫ МНОГОБУКВЕННОЙ ЗАМЕНЫ НА ПРИМЕРЕ ШИФРА ХИЛЛА

Цель работы: Выполнить шифрование и дешифрование сообщений.

4.1. Описание объекта исследования

Одним из интересных представителей многобуквенных шифров является шифр, разработанный математиком Лестером Хиллом в 1929 году. Лежащий в его основе алгоритм заменяет каждые m последовательных букв открытого текста m буквами шифрованного текста. Подстановка определяется m линейными уравнениями, в которых каждому символу присваивается числовое значение (a = 0, b = 1, c = 2, ..., z = 25). Например, при $m = 3$, получаем следующую систему уравнений:

$$C1 = \left(k_{11}p_1 + k_{12}p_2 + k_{13}p_3\right) \bmod 26$$
$$C2 = \left(k_{21}p_1 + k_{22}p_2 + k_{23}p_3\right) \bmod 26$$
$$C3 = \left(k_{31}p_1 + k_{32}p_2 + k_{33}p_3\right) \bmod 26$$

Эту систему уравнений можно записать в виде произведения вектора и матрицы в следующем виде:

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{11} & k_{12} & k_{13} \\ k_{11} & k_{12} & k_{13} \end{pmatrix} \times \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

или в виде:

$$C = KP,$$

где C – вектор длины 3, представляющий шифрованный текст; P – вектор длины 3, представляющий открытый текст; K – матрица размерности 3×3, представляющая ключ шифрования.

Все операции выполняются по модулю 26.

Рассмотрим пример шифрования и дешифрования. Пусть матрица K:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Первые три буквы открытого текста представлены вектором (15 0 24), таким образом, K(15 0 24) = (275 819 486) mod 26 = (11 13 18) = LNS.

Продолжая вычисления, получим для данного примера шифрованный текст вида: LNSHDLEWTRW.

Для расшифровки необходимо воспользоваться матрицей, обратной *K*. Обратной по отношению к матрице *K* называется такая матрица K^{-1}, для которой выполняется равенство $KK^{-1} = K^{-1}K = I$, где I – это единичная матрица (матрица, состоящая из нулей всюду, за исключением главной диагонали, проходящей с левого верхнего угла в правый нижний, на которой предполагаются единицы). Обратная матрица существует не для всякой матрицы, однако когда обратная матрица имеется, для нее обязательно выполняется приведенное выше равенство. В данном примере обратной матрицей является следующая:

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Это проверяется следующими вычислениями:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

В результате применения матрицы K^{-1} к шифрованному тексту получается открытый текст. В общем виде криптосистема Хилла записывается соотношением:

$$C = E_k(P) = KP,$$
$$P = D_k(C) = K^{-1}C = K^{-1}KP = P, \qquad (4.1)$$

где C – шифрованный текст; P – открытый текст; K – ключ шифрования; E_k – функция шифрования; D_k – функция дешифрования.

Преимущество шифра Хилла состоит в том, что он полностью маскирует частоту вхождения отдельных букв – чем больше размер матрицы, тем больше шифрованном тексте скрывается информации о различиях в значениях частоты появления других комбинаций символов. Так, шифр Хилла с матрицей 3×3 скрывает частоту появления не только отдельных букв, но и двухбуквенных комбинаций.

Хотя шифр Хилла устойчив к попыткам криптоанализа в тех случаях, когда известен только шифрованный текст, этот шифр легко раскрыть при наличии известного открытого текста. Рассмотрим шифр Хилла с матрицей $m \times m$. Предположим, что нам известно m пар отрывков открытого и соответствующего шифрованного текстов, каждый длины m. Обозначим такие пары $P_j = (p_{1j}, p_{2j}, ..., p_{mj})$ и $C_j = (C_{1j}, C_{2j}, ..., C_{mj})$, чтобы выполнялось условие

$C_j = KP_j$ для всех $1 \leqslant j \leqslant m$ и некоторой неизвестной ключевой матрицы K. Теперь определим две такие матрицы $X = (p_{ij})$ и $Y = (C_{ij})$ размера $m \times m$, что $Y = XK$. Тогда, при условии что для матрицы X существует обратная матрица, K можно определить по формуле $K = X^{-1}K$. Если же получить матрицу, обратную матрице X невозможно, то необходимо сформировать другую матрицу X с дополнительными парами соответствия открытого и шифрованного текстов, до тех пор, пока не будет найдена обратная матрица.

Рассмотрим пример. Предположим, что открытый текст «friday» шифрован с помощью шифра Хилла с использованием матрицы 2×2, в результате чего получен шифрованный текст PQCFKU. Таким образом, известно, что $K(5\ 17) = (15\ 16)$, $K(8\ 3) = (2\ 5)$ и $K(0\ 24) = (10\ 20)$. Используя первые две пары символов открытого и шифрованного текстов, получаем:

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K$$

Вычисляем матрицу, обратную матрице X:

$$\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}$$

Таким образом, можно получить значение ключа:

$$\begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

4.2. Порядок выполнения работы

1. С помощью любого математического пакета сформируйте матрицу-ключ, у которой имеется обратная ей матрица.
2. Зашифруйте открытый текст.
3. Передайте зашифрованное сообщение вместе с ключом по локальной сети лаборатории адресату и получите переданное Вам шифрованное сообщение с ключом
4. Вычислить матрицу обратную полученной в качестве ключа к полученному сообщению.
5. Дешифровать полученное сообщение.

4.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- Открытый текст собственного задания.
- Матрицу-ключ к собственному заданию с вычислениями, доказывающими, что у данной матрицы существует обратная ей матрица.

- Зашифрованный текст собственного задания.
- Шифрованный текст адресованного Вам сообщения полученного по локальной сети лаборатории.
- Матрица-ключ для дешифрования.
- Вычисления над матрицей-ключом для получения обратной матрицы с последующей дешифрацией полученного сообщения.
- Дешифрованное сообщение.
- Ответы на контрольные вопросы.
- Выводы о проделанной работе.

4.4. Контрольные вопросы

1. Предположим, что шифр Хилла используется для зашифрования открытого текста, представленного в виде двоичной последовательности. Сколько ключей имеет такой шифр?
2. К какому виду шифров относится шифр Хилла: поточным или блочным, докажите правильность своих рассуждений.
3. Приведите сравнительный анализ шифра Хилла и шифра Плейфейера.
4. Дайте математическое определение обратной матрицы.
5. Что такое стойкость шифра?
6. Оцените стойкость шифра Хилла при наличии достаточного числа пар соответствия открытого и шифрованного текстов.
7. Дайте характеристику шифру Хилла.
8. В каких современных шифрах применяются идеи, подобные шифру Хилла?
9. Перечислите недостатки шифра Хилла.

4.5. Литература

1. *Столингс В.* Криптография и защита сетей. Принципы и практика. 2-е изд. – М.: Вильямс, 2001.
2. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. Учеб. пособие. – М.: Гелиос-АРВ, 2001.

Лабораторная работа №5.
ПОЛИАЛФАВИТНЫЕ ШИФРЫ

Цель работы: ознакомиться с полиалфавитными шифрами на примере шифров Виженера и Вернама.

5.1. Описание объекта исследования

Одна из возможностей усовершенствования простого многоалфавитного шифра заключается в использовании нескольких многоалфавитных подстановок, применяемых в ходе шифрования открытого текста в зависимости от определенных условий. Семейство шифров, основанных на применении таких методов шифрования, называется *полиалфавитными шифрам*. Подобные методы шифрования обладают следующими свойствами:

– используется набор связанных многоалфавитных подстановок;
– имеется некоторый ключ, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Самым широко известным и одновременно простым алгоритмом такого рода является шифр Виженера. Блез де Виженер – французский дипломат, криптограф и алхимик. Шифр, называемый в настоящее время шифром Виженера, в XIX веке был ошибочно ему приписан.

Шифр Виженера – метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

В табл. 3 представлено современное табло Виженера. Все 26 шифров располагаются по горизонтали, и каждому из шифров соответствует своя ключевая буква, представленная в крайнем столбце слева. Алфавит, соответствующий буквам открытого текста, находится в первой сверху строке таблицы. Процесс шифрования прост – необходимо по ключевой букве *x* и букве открытого текста *y* найти букву шифрованного текста, которая находится на пересечении строки *x* и столбца *y*. В данном случае такой буквой является буква *V*.

Чтобы зашифровать сообщение, нужен ключ, имеющий ту же длину, что и само сообщение. Обычно ключ представляет собой повторяющееся нужное число раз ключевое слово, чтобы получить строку подходящей длины. Например, если ключевым словом является *deceptive,* сообщение «we are discovered save yourself» шифруется следующим образом:

Ключ:	deceptivedeceptivedeceptive
Открытый текст:	we are discovered save yourself
Шифрованный текст:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Таблица 3

Таблица Виженера

ABCDEFGHIJKLMNOPQRSTUVWXYZ	
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HIJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
R	RSTUVWXYZABCDEFGHIJKLMNOPQ
S	STUVWXYZABCDEFGHIJKLMNOPQR
T	TUVWXYZABCDEFGHIJKLMNOPQRS
U	UVWXYZABCDEFGHIJKLMNOPQRST
V	VWXYZABCDEFGHIJKLMNOPQRSTU
W	WXYZABCDEFGHIJKLMNOPQRSTUV
X	XYZABCDEFGHIJKLMNOPQRSTUVW
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Расшифровать текст также просто – буква ключа определяет строку, буква шифрованного текста, находящаяся в этой строке, определяет столбец, и в этом столбце в первой строке таблицы будет находиться соответствующая буква открытого текста.

Преимущества этого шифра заключается в том, что для представления одной и той же буквы открытого текста в шифрованном тексте имеется много различных вариантов – по одному на каждую из неповторяющихся букв ключевого слова. Таким образом, скрывается информация, характеризующая частоту употребления букв. Но и с помощью данного метода все же не удается полностью скрыть влияние структуры открытого текста на структуру шифрованного.

Если выбрать ключевое слово равное по длине открытого текста, но отличающееся от открытого текста по статистическим данным, то шифр станет более стойким. Такая система шифрования была предложена инженером

компании AT&T Гилбертом Вернамом в 1918 г. Его система оперирует не буквами, а двоичными числами. Кратко ее можно выразить формулой:

$$C_i = p_i \otimes k_i, \tag{5.1}$$

где p_i – i-я двоичная цифра открытого текста (ASCII код); k_i – i-я двоичная цифра ключа (шифр-блокнот); C_i – i-*я* двоичная цифра шифрованного текста; $\otimes$ – операция XOR.

Таким образом, шифрованный текст генерируется путем побитового выполнения операции XOR для открытого текста и ключа. Благодаря свойствам этой операции для расшифровки достаточно выполнить подобную операцию:

$$p_i = C_i \otimes k_i. \tag{5.2}$$

Сутью этой технологии является способ выбора ключа. Вернам предложил использовать закольцованную ленту, что означает повторение ключевого слова, так что система на самом деле предполагала работу хоть и с очень длинным, но все же повторяющимся ключом. Несмотря на то, что такая схема в силу очень большой длины ключа значительно усложняет задачу криптоанализа, схему тем не менее, можно взломать, имея в распоряжении достаточно длинный фрагмент шифрованного текста, известные или вероятно известные фрагменты открытого текста либо и то, и другое сразу.

Офицер армейского корпуса связи Джозеф Моборн предложил такие улучшения схемы шифрования Вернама, которые сделали эту схему исключительно надежной. Моборн отказаться от повторений и предложил случайным образом генерировать ключ, по длине равной длине сообщения. Такая схема, получившая название ленты однократного использования (или схемы с одноразовым блокнотом), взлому не поддается. В результате ее применения на выходе получается случайная последовательность, не имеющая статистической взаимосвязи с открытым текстом. Поскольку в этом случае шифрованный текст не дает никакой информации об открытом тексте, нет способа и взломать шифр. Сложность практического применения этого метода заключается в том, что и отправитель, и получатель должны располагать одним и тем же случайным ключом и иметь возможность защитить его от посторонних. Поэтому, несмотря на все преимущества шифра Вернама перед другими шифрами, на практике его используют редко.

5.2. Порядок выполнения работы

1. Для шифрования с помощью таблицы Виженера составить аналогичную таблицу ширования для русского алфавита.

2. Выбрать ключ шифрования и зашифровать предложенный вариант сообщения.
3. Сформировать документ, в который записать зашифрованное сообщение и ключ.
4. Отправить документ по локальной сети лаборатории адресату-получателю.
5. Для зашифрования методом Вернама каждой букве открытого текста поставить в соответствие ASCII код (таблица ASCII приведена в приложении).
6. Каждую цифру ключа перевести в двоичный код.
7. Зашифровать предложенный преподавателем открытый текст шифром Вернама.
8. Сформировать документ, в который записать зашифрованный текст и содержимое шифр-блокнота и отправить документ по локальной сети лаборатории адресату-получателю.
9. Полученные по сети документы адресованные Вам и выполнить их дешифрование.

5.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- В первой части отчета по лабораторной работе представить результаты шифрования:
  - Вариант открытого текста и ключ для шифрования с помощью шифра Виженера.
  - Таблица Виженера для русского алфавита.
  - Зашифрованное методом Виженера сообщение.
  - Ключ-лента в цифровом виде.
  - Цепочка ASCII кодов открытого текста.
  - Результат шифрования методом Вернама: операция XOR открытого текста и ключа.
- Во второй части отчета по лабораторной работе представить результаты дешифрования:
  - Результат операции XOR полученного по сети ключа и зашифрованного сообщения методом Вернама в цифровом виде.
  - Дешифрованные тексты методом Виженера и методом Вернама.
- Ответы на контрольные вопросы.
- Выводы по работе.

5.4. Контрольные вопросы

1. Какой шифр называется совершенным?
2. Какие атаки используются в криптоанализе?

3. В чем отличие теоретической и практической стойкости шифра?
4. Определите основные этапы по вскрытию шифра Виженера.
5. Приведите сравнительный анализ шифра Виженера и шифра Вернама.
6. Основой какого современного шифра является шифр Вернама?
7. От чего зависит стойкость шифра Виженера?
8. От чего зависит стойкость шифра Вернама?
9. Какой из шифров известен как шифр одноразовых блокнотов?

5.5. Литература

1. *Бабаш А.В., Шанкин Г.П.* История криптографии. Учебное пособие. – М.: «Гелиос АРВ», 2001.
2. *Бескид П.П., Татарникова Т.М.* Криптографические методы защиты информации. Часть 1. Основы криптографии. Учебное пособие. – СПб.: изд. РГГМУ, 2010. – 95 с.

Лабораторная работа №6.
РЕШЕНИЕ ЗАДАЧИ КРИПТОАНАЛИЗА ШИФРА ПРОСТОЙ ЗАМЕНЫ

Цель работы: по предлагаемой методике решить задачу криптоанализа шифра простой замены.

6.1. Описание объекта исследования

Разберем предлагаемый метод криптоанализа на примере. Рассмотрим шифртекст (рис. 9):

1	**С**	**З**	**Я**	**И**	**Г**	**Н**	**Д**	**Л**	**В**	**С**	**З**	**Л**	**П**	**В**	**У**
2	**И**	**У**	**Л**	**З**	**Х**	**Г**	**З**	**Т**	**Э**	**Ф**	**Б**	**Д**	**А**	**Т**	**И**
3	**Г**	**К**	**П**	**З**	**Т**	**С**	**И**	**П**	**З**	**Н**	**Ф**	**Э**	**Л**	**К**	**И**
4	**Э**	**М**	**У**	**О**	**У**	**Д**	**Т**	**Ж**	**Г**	**З**	**Д**	**И**	**М**	**И**	**С**
5	**Э**	**М**	**И**	**Г**	**С**	**З**	**Ф**	**П**	**Л**	**З**	**М**	**Д**	**Ф**	**Г**	**Д**
6	**С**	**И**	**П**	**Э**	**Л**	**Э**	**Ц**	**З**	**Ю**	**В**	**С**	**З**	**Е**	**З**	**Л**
7	**З**	**Г**	**Э**	**Г**	**И**	**У**	**М**	**В**	**П**	**Т**	**Э**	**Г**	**Д**	**Э**	**З**
8	**У**	**М**	**И**	**Г**	**З**	**Ф**	**Т**	**Э**	**Г**	**З**					

Рис. 9. Шифртекст

При раскрытии будем иметь в виду следующие отличительные признаки шифра однобуквенной замены:

– в шифротексте встречается большое число сплошных повторений;
– диаграмма встречаемости шифробозначений – рельефная и соответствует диаграмме открытого текста.

Проведем предварительный анализ шифротекста.

Подчеркнем в шифротектсте наиболее характерные неслучайные повторения и представим в табл. 4.

Таблица 4

Характерные неслучайные повторения

Повторение	Количество
ВСЗ	2
МИГ	2
ТЭГ	2
ИУ	2

Прежде всего необходимо отметить, что в тексте явно имеется значимо завышенное число повторений.

Наличие большого числа повторений свидетельствует о том, что для зашифрования использовался шифр простой замены.

Для раскрытия шифра простой замены производится разбиение шифртекста на шифробозначения, выполним маркировку шифробозначений (ШО) и маркировку пар ШО.

В результате получим следующий шифртекст (рис. 10):

1	С	З	Я	И	Г	Н	Д	Л	В	С	З	Л	П	В	У
2	И	У	Л	З	Х	Г	З	Т	Э	Ф	Б	Д	А	Т	И
3	Г	К	П	З	Т	С	И	П	З	Н	Ф	Э	Л	К	И
4	Э	М	У	О	У	Д	Т	Ж	Г	З	Д	И	М	И	С
5	Э	М	И	Г	С	З	Ф	П	Л	З	М	Д	Ф	Г	Д
6	С	И	П	Э	Л	Э	Ц	З	Ю	В	С	З	Е	З	Л
7	З	Г	Э	Г	И	У	М	В	П	Т	Э	Г	Д	Э	З
8	У	М	И	Г	З	Ф	Т	Э	Г	З					

Рис. 10. Маркированный шифртекст

Подсчитаем частоты встречаемости ШО и запишем их в порядке убывания частот:

З-16	С-7	В-4	Ж-1
Г-11	М-6	К-2	0-1
И- 11	П-6	Н-2	Х-1
Э-10	Т-6	А-1	Ц-1
Д-7	У-6	Б-1	Ю-1
Л-7	Ф-5	Е-1	Я-1

Подсчитаем частоты встречаемости маркированных пар шифробозначений:

– биграммы ШО с частотой встречаемости 4: ГЗ, ИГ, СЗ;
– биграммы ШО с частотой встречаемости 3: ЛЗ, МИ, ТЭ, ЭГ;
– биграммы ШО с частотой встречаемости 2: ВС, ГД, ЗЛ, ЗТ, ЗФ, ИП, ИУ, ПЗ, СИ, УМ, ЭЛ, ЭМ.

Далее необходимо разбить все ШО на гласные и согласные с учетом основных свойств открытого текста – сочетаемости и чередования, повторяемости букв в русском языке. Работа начинается с самых частых ШО. При этом самые частые надо раскрашивать, чтобы наглядно видеть их взаимосвязи.

Рассмотрим самой частое ШО – «З». По шифртексту оно распределено равномерно, в отдельных местах чередуется через одно, два или три ШО. В маркировке пар ШО – в сочетаниях, оно встречается чаще всех других ШО. Причем сочетается как с частыми ШО («Г», «Л», «С», «Т»), так и с

ШО средней и низкой повторяемости («М», «Ф», ..., «Ю», «Я»). Все это дает основание полагать, что за этим ШО скрывается гласная буква (причем, скорее всего, буква «О»).

По свойствам открытого текста чаще встречаются сочетания гласных и согласных букв, чем согласных с гласными или гласных с гласными. Значит можно предположить, что все ШО, которые часто встречаются с ШО «З», скорее всего, скрывают согласные буквы. Поэтому ШО «Г», «С», «Л», «Т», «Ф», «П», часто сочетающиеся с ШО «З», будем считать согласными буквами (табл. 4). Дальнейший анализ подтвердит эти предположения.

Но если «Г» – согласная буква, то «И» – гласная, т.к. эти ШО сочетаются между собой 4 раза (табл. 4). Далее ШО «Э» хорошо сочетается с «Т» и «Г». Значит, видимо, что «М» и «У» – согласные буквы.

Разнесем полученные результаты по шифртексту, как на рис.11.

1	С	З	Я	И	Г	Н	Д	Л	В	С	З	Л	П	В	У
2	И	У	Л	З	Х	Г	З	Т	Э	Ф	Б	Д	А	Т	И
3	Г	К	П	З	Т	С	И	П	З	Н	Ф	Э	Л	К	И
4	Э	М	У	О	У	Д	Т	Ж	Г	З	Д	И	М	И	С
5	Э	М	И	Г	С	З	Ф	П	Л	З	М	Д	Ф	Г	Д
6	С	И	П	Э	Л	Э	Ц	З	Ю	В	С	З	Е	З	Л
7	З	Г	Э	Г	И	У	М	В	П	Т	Э	Г	Д	Э	З
8	У	М	И	Г	З	Ф	Т	Э	Г	З					

Рис. 11. Размеченный шифртекст

Из группы ШО высокой повторяемости неопределенным осталось ШО «Д». Изучив сочетаемость этого ШО в шифртексте, можно сделать вывод, что оно чаще встречается с согласными буквами и, кроме того, по тексту оно чередуется как гласная буква. Скорее всего, за этим ШО скрывается гласная буква.

В пользу этого предположения говорит также то, что в группе ШО высокой повторяемости должно быть четыре гласные буквы, а пока выявлено только три. Значит «Д» – гласная.

Продолжая процесс, определяем, что «В», «Ж», «О» – гласные буквы, а «Е», «К» «Н», «Ц», «Ю», «Я» – согласные. Окончательные результаты разбиения шифробозначений на гласные и согласные приведены в табл. 5 и рис. 12.

Таблица 5

Группа ШО высокой повторяемости

Гласная/Согласная	–	⌣	–	–	–	⌣	⌣	⌣	⌣	⌣	⌣	⌣
Шифробозначение	3	Г	И	Э	Д	Л	С	М	П	Т	У	Ф
Частота	16	11	11	10	7	7	7	6	6	6	6	5

	⌣	–	–	–	⌣	⌣	–	⌣	–	⌣	–	⌣	⌣	–	⌣
1	**С**	**З**	**Я**	**И**	**Г**	**Н**	**Д**	**Л**	**В**	**С**	**З**	**Л**	**П**	**В**	**У**
	–	⌣	⌣	–		⌣	–	⌣	–	⌣		–		⌣	–
2	**И**	**У**	**Л**	**З**	**Х**	**Г**	**З**	**Т**	**Э**	**Ф**	**Б**	**Д**	**А**	**Т**	**И**
	⌣	⌣	⌣	–	⌣	⌣	–	⌣	–	⌣	⌣	–	⌣	⌣	–
3	**Г**	**К**	**П**	**З**	**Т**	**С**	**И**	**П**	**З**	**Н**	**Ф**	**Э**	**Л**	**К**	**И**
	–	⌣	⌣	–	⌣	–	⌣	–	⌣	–	–	–	⌣	–	⌣
4	**Э**	**М**	**У**	**О**	**У**	**Д**	**Т**	**Ж**	**Г**	**З**	**Д**	**И**	**М**	**И**	**С**
	–	⌣	–	⌣	⌣	–	⌣	⌣	–	–	⌣		⌣	⌣	–
5	**Э**	**М**	**И**	**Г**	**С**	**З**	**Ф**	**П**	**Л**	**З**	**М**	**Д**	**Ф**	**Г**	**Д**
	⌣	–	⌣	–	⌣	–	⌣	–	⌣	–	⌣	–	⌣	–	⌣
6	**С**	**И**	**П**	**Э**	**Л**	**Э**	**Ц**	**З**	**Ю**	**В**	**С**	**З**	**Е**	**З**	**Л**
	–	⌣	–	⌣	–	⌣	⌣	–	⌣	⌣	–	⌣	–	–	–
7	**З**	**Г**	**Э**	**Г**	**И**	**У**	**М**	**В**	**П**	**Т**	**Э**	**Г**	**Д**	**Э**	**З**
	⌣	⌣	–	⌣	–	⌣	⌣	–	⌣	–					
8	**У**	**М**	**И**	**Г**	**З**	**Ф**	**Т**	**Э**	**Г**	**З**					

Рис. 12. Шифртекст с разделением на гласные и согласные

При этом не определены самые редкие ШО: «А, «Б», «Х».

Можно попробовать определить их, но при этом велика вероятность ошибки. Кроме того, т.к. они встречаются редко, то их определение не имеет существенной роли для раскрытия шифра простой замены.

Следующий этап – соотнесение ШО их буквам открытого текста:

- ШО «З». Исходя из частоты встречаемости и очень высокой сочетаемости с другими ШО логично предположить, что за самым частым ШО «З» скрывается буква О».
- ШО «Г». Оно также очень часто участвует в сочетаниях – «ГЗ», «ИГ», «ЭГ», «ГД» и т.д. По свойствам открытого текста, видимо, это буква «Н».
- ШО «Д». Оно дважды сочетается с другими гласными буквами («З», «Д», «И», и «Д», «Э»), скорее всего, оно скрывает букву «И».

Среди частых пар ШО только одна типа «согласная несогласная» – это пара «УМ». Кроме того, в шифртексте встречается и одна пара «МУ». Исходя из свойств русского текста, можно предположить, что за парой «МУ» скрывается сочетание «СТ». Поэтому ШО «У» соответствует «С», а ШО «М» – «Т».

По свойствам русского открытого текста среди самых частых букв должно быть 4 гласных: «О», «И», «Е», «А». Мы соотнесли ШО для двух из них («З» – «О», «Д» – «И») и у нас осталось еще два частых ШО «И» и «Э»,

которые скрывают гласные буквы. Значит ШО «И» и «Э» скрывают буквы «А» и «Е». Не совсем ясно, как их правильно сопоставить. Здесь необходимо опробовать оба варианта:

«И» → «А», «Э» → «Е»;

«И» → «Е», «Э» → «А».

Путем опробования несложно установить, что верен первый вариант «И» → «А», «Э» → «Е». Результат начального этапа показан в таблице.

При этом в конце текста, в строках 7 и 8 (рис. 13) получилась следующая группа букв «ЕНИЕОСТАНО..ЕНО». Так как подряд следуют три гласные буквы «ИБО», то логично предположить, что это конец одного слова и начало другого. Получаем: «ЕНИЕ ОСТАНО..ЕНО». Здесь нетрудно угадать слово «ОСТАНОВЛЕНО». После чего дальнейшее раскрытие не представляет никакого труда. В 5-й строке читается «ТАНКОВ ПРОТИВНИКА» и т.д. В итоге получаем следующий текст, приведенный на рис. 13.

1	**К**	**О**	**М**	**А**	**Н**	**Д**	**И**	**Р**	**У**	**К**	**О**	**Р**	**П**	**У**	**С**
2	**А**	**С**	**Р**	**О**	**Ч**	**Н**	**О**	**Л**	**Е**	**В**	**Ы**	**И**	**Ф**	**Л**	**А**
3	**Н**	**Г**	**П**	**О**	**Л**	**К**	**А**	**П**	**О**	**Д**	**В**	**Е**	**Р**	**Г**	**А**
4	**Е**	**Т**	**С**	**Я**	**С**	**И**	**Л**	**Ь**	**Н**	**О**	**И**	**А**	**Т**	**А**	**К**
5	**Е**	**Т**	**А**	**Н**	**К**	**О**	**В**	**П**	**Р**	**О**	**Т**	**И**	**В**	**Н**	**И**
6	**К**	**А**	**П**	**Е**	**Р**	**Е**	**Х**	**О**	**Ж**	**У**	**К**	**О**	**Б**	**О**	**Р**
7	**О**	**Н**	**Е**	**Н**	**А**	**С**	**Т**	**У**	**П**	**Л**	**Е**	**Н**	**И**	**Е**	**О**
8	**С**	**Т**	**А**	**Н**	**О**	**В**	**Л**	**Е**	**Н**	**О**					

Рис. 13. Дешифрованный текст

По результатам раскрытия шифра можно составить следующую таблицу зашифрования (табл. 5).

Таблица 5

Соответствие ШО буквам открытого текста

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

Необходимо подчеркнуть, что изложенные этапы раскрытия шифра простой замены основаны на статистических свойствах открытого текста и для реальных текстов возможны какие-либо отклонения от приведенных частот встречаемости. Поэтому при раскрытии шифра простой замены возможны ошибки и иногда необходим перебор нескольких вариантов.

Здесь разобран пример раскрытия шифра простой замены для текста на русском языке. Однако данная методика сохраняется при раскрытии шифра

простой замены для текстов на других языках. При этом используются те же свойства открытого текста: повторяемость букв, сочетаемость букв, чередование гласных и согласных, но с учетом устойчивых статистических характеристик для конкретного языка.

Изложенная методика основана на опыте криптоаналитика и позволяет максимально сократить ошибки и перебор вариантов. Возникающие трудности по раскрытию шифра простой замены обычно связаны с отклонениями от данной методики.

6.2. Порядок выполнения работы

1. Провести предварительный анализ шифротекста и выявить отличительные признаки шифра однобуквенной замены. Для простоты в качестве алфавита открытого и шифрованного текста выбраны 30 русских букв. Буквы «Е», «Ё», «И», «Й», «Ъ» и «Ь» отождествлены.
2. Определить ШО, скрывающие гласные и согласные буквы. Итогом этого этапа должно стать разделение всех ШО на две группы – на группу гласных букв и группу согласных.
3. Выполнить «начитку» текста, в результате которой каждому шифробозначению соотносится буква открытого текста. Итогом этого этапа является вскрытие текста.
4. Построить таблицу зашифрования, которая представляет собой результат проведения криптоанализа.

6.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- Исходный шифртекст.
- Таблица характерных неслучайных повторений.
- Таблица маркировки шифробозначений и маркировки пар шифробозначений.
- Таблица частот встречаемости шифробозначений в порядке убывания частот.
- Список частот встречаемости маркированных пар шифробозначений.
- Рассуждения по разбивке ШО на гласные и согласные.
- Рассуждения по соотнесению шифробозначений скрываемым буквам открытого текста.
- Полученный расшифрованный текст.
- Таблица зашифрования.
- Ответы на контрольные вопросы.
- Выводы о проделанной работе.

6.4. Контрольные вопросы

1. Можно ли рассматривать множество возможных открытых и шифрованных текстов как множество шифрвеличин и шифробозначений шифра замены.
2. Какие шифры называются шифрами простой замены.
3. Что является ключом шифра простой замены. Каково максимально возможное число ключей шифра простой замены.
4. Какое сообщение проще расшифровать – длинные или короткие?
5. Возможно ли вскрытие шифра простой замены при условии, что известны только статистические данные о языке сообщения и его алфавит?
6. Какие особенности русского языка используются при криптоанализе шифра простой замены?
7. Существуют ли шифры, не являющиеся ни шифрами замены, ни шифрами перестановки?
8. Приведите известные методы криптоанализа.
9. Какой метод криптоанализа применяется в случае, когда известно, что сообщение зашифровано шифром простой замены?

6.5. Литература

1. *Белов Е.Б., Зубов А.Ю., Погорелов Б.А., Проскурин Г.В., Черемушкин А.В., Шанкин Б.П., Шурупов А.Н.* Криптографические методы защиты информации. Учебно-методическое пособие. Ч.2. – М.: ИКСИ, 2003.
2. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003.

Лабораторная работа №7.
ИЗУЧЕНИЕ МЕТОДОВ И СРЕДСТВ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННЫХ МАССИВОВ

Цель работы: Получение практических навыков проведения мероприятий по контролю целостности информационных массивов.

7.1. Описание объекта исследования

Информация, хранимая в технических средствах, может подвергаться случайному или умышленному несанкционированному изменению. Одним из способов проверки целостности информации является хранение эталонных копий, используемых для сравнения. Преимущество этого метода состоит в том, что не только обнаруживаются любые возможные изменения, но и возможно 100 % быстрое восстановление исходного состояния информации. Однако такая процедура при необходимости частых проверок целостности данных большого объема приводит к существенным временным задержкам, так же существенно (в два раза) увеличивается требуемый для хранения информации объем памяти, а в случае сжатия информации требуются еще и дополнительные преобразования, поэтому этот метод применяется только в специальных случаях. Более технологичным является способ, основанный на вычислении некоторых контрольных сумм. Вычисляются по заданному алгоритму контрольные суммы для массивов данных (например, файлов, каталогов), находящихся в исходном состоянии. Эти вычисленные контрольные суммы записываются в таблицы, которые затем используются для проверки целостности информации. В этом случае проверка целостности состоит в вычислении по заданному алгоритму контрольной суммы для данного блока информации и сопоставления полученного значения с эталонным значением контрольной суммы. Выигрыш состоит в том, что, во-первых, теперь нет необходимости проводить сравнение двух больших массивов данных и иметь существенный дополнительный объем памяти, а во-вторых, появляется больше возможностей по нейтрализации угроз преднамеренного синхронного изменения исходного массива и его контрольной копии. Целостность проверяется путем сравнения, например, 64-битовых, 128-битовых или 256-битовых контрольных сумм. Такие контрольные суммы называются защитными контрольными суммами (ЗКС).

При фиксации исходного состояния для информационных массивов вычисляются их образы, имеющие функциональную зависимость от всех, или некоторой части символов информационного массива. Таким образом, при изменении составляющих информационного массива изменяются (или должны изменяться) и вычисляемые при проверке их информационные образы.

В зависимости от объемов хранимых информационных массивов, существующих технических ограничений и характера воздействия на хранимую информацию могут выбираться различные способы получения эталонных образов информации. При этом такие образы могут иметь большую, равную или меньшую длину, чем исходная информация, а функциональная зависимость символов образа от символов исходной информации может быть известной или содержать скрываемые (секретные) составляющие. Последнее особенно актуально в случае, когда имеет место целенаправленное умышленное воздействие на хранимую информацию. В случае, когда объемы хранимой информации являются достаточно большими, а допустимое время проверки ограничено – применяют функциональные преобразования, дающие образы исходной информации меньшей длины, чем длина защищаемого информационного массива. Такие преобразования принято называть хэш-функциями, процесс получения образа информации – хэшированием, а значение хэш-функции – хэш-образом.

Таким образом, хэш-функция представляет собой криптографическую функцию от сообщения произвольной длины, значение которой зависит сложным образом от каждого бита сообщения. Хэш-функции можно разделить на два класса:

- Бесключевые хэш-функции – имеют один вход (сообщение).
- Ключевые хэш-функции – имеют два входа (сообщение и секретный ключ).

Хэш-функция реализуется, как правило, в виде некоторой итеративной процедуры, которая позволяет вычислить для сообщения M произвольной длины, так называемый хэш-код $H(M)$ фиксированного размера m (обычно m оставляет 128–256 бит). Этот код и является эталонной характеристикой сообщения M.

К хэш-функциям предъявляют следующие основные требования:

– вычислительно неосуществимо нахождение сообщения M, хэш-функция которого была бы равна заданному значению H;
– вычислительно неосуществимо нахождение двух разных сообщений M_1 и M_2 с равными значениями хэш-функции, т.е. сообщений, удовлетворяющих условию $H(M_1) = H(M_2)$.

В силу того, что размерность хэш-образа меньше размерности аргумента хэш-функции, могут иметь место случаи, когда хэш-образы от различных аргументов равны: $H(M) = H(M_2)$, где M_1 и M_2 – информационные массивы, $M_1 \neq M_2$; H – хэш-функция. Такие случаи называют коллизиями хэш-функции. Множество аргументов хэш-функции, хэш-образы которых равны, называются кластерами. При этом следует иметь в виду, что преобразование (случайное или умышленное) контролируемого информационного массива $M\backslash$ в массив M_2, принадлежащий одному и тому же кластеру, что и M_2,

является принципиально необнаруживаемым при контроле с использованием данной хэш-функции. Для хэш-функции с n-битным выходным значением вероятность того, что две произвольные последовательности символов будут иметь равные хэш-образы, равна 2^{-n}.

Хэш-функция должна обладать устойчивостью к коллизиям, т.е. должно быть трудно найти два случайных сообщения, M и M', для которых $H(M) \sim H(M')$. Если это требование не выполняется, то можно провести вскрытие методом, основанным на парадоксе дней рождения. Этот парадокс состоит в ответе на следующий вопрос: какова должна быть численность группы случайно выбранных людей, чтобы с вероятностью 0,5 в этой группе нашлось два человека, у которых дни рождения совпадают. Оказывается, что численность этой группы должна составлять всего примерно 19 человек. Дело в том, что вероятность совпадения дней рождения для случайной пары составляет $p' = 1/365$, а в группе из n человек имеется $C_n^2 = n(n-1)/2 \approx n^2/2$ разных пар. Вероятность того, что хотя бы у одной из этих пар будет иметь место совпадение дней рождения, составляет $p \approx p'n^2/2$, откуда для $p = 0{,}5$ получаем $n \approx \sqrt{1/p'}$.

64-битовые хэш-функции слишком малы, чтобы противостоять вскрытию методом, основанным на парадоксе дней рождения. Более практичны однонаправленные хэш-функции, выдающие 128-битовые хэш-значения. При этом, чтобы найти два документа с одинаковыми хэш-значениями, для вскрытая методом, основанным на парадоксе дней рождения придется хэшировать 2^{64} случайных документов, что, впрочем, недостаточно, если нужна длительная безопасность. NIST в своем Стандарте безопасного хэширования (Secure Hash Standard, SHS), использует 160-битовое хэш-значение. Это еще сильнее усложняет вскрытие методом, основанным на парадоксе дней рождения, для которого понадобится 2^{80} хэшированый.

Для разработки вычислительно стойких хэш-функций, как и шифров, используются два общих принципа: рассеивания и перемешивания. Рассеиванием называется распространение влияния одного знака открытого текста на много символов значения хэш-функции или шифртекста, а перемешиванием – преобразование, нарушающее взаимосвязи статистических характеристик входного и выходного текста.

В зависимости от решаемой задачи в качестве алгоритмов защитного контрольного суммирования (АЗКС) могут быть использованы различные алгоритмы, обеспечивающие влияние каждого входного бита данных на значение контрольного кода. Например, могут быть использованы алгоритмы, зависящие от секретного ключа, достоинством которых является сравнительная простота построения при обеспечении высокой скорости вычисления контрольных сумм и стойкости к преднамеренным искажениям данных. Наиболее общим и важным случаем АЗКС являются хэш-функции, которые не используют секретных параметров и в то же

время обеспечивают малую вероятность необнаружения преднамеренного модифицирования информации, основанного на анализе свойств хэширующего преобразования.

В современных автоматизированных системах обработки информации во многих случаях предпочтительно применение блочных шифров. В этом случае сообщение M можно представить в виде конкатенации n блоков одинакового размера: $M = M_1|M_2|...|M_n$. Пусть каждый блок имеет длину b бит. Если длина сообщения не является кратной b, то последний блок дополняется по некоторому заранее оговоренному правилу до длины b. Например, последний блок дописывается двоичным вектором (1000...0). Если длина последнего блока равна b, то к сообщению присоединяется дополнительный 6-битовый блок (1000...0).

Типовая хэш-функция вычисляется путем последовательного шифрования двоичных блоков M_i сообщения M соответствии со следующим итеративным выражением (7.1).

$$H_i = E\left(H_{i-1}, M_i\right),$$

где E – базовая функция шифрования.

На рис. 14 приведена типовая схема образования блочной хэш-функции. Здесь H_0 – специфицированное начальное значение хэш-функции; H_n – значение хэш-функции, принимается за эталонную характеристику.

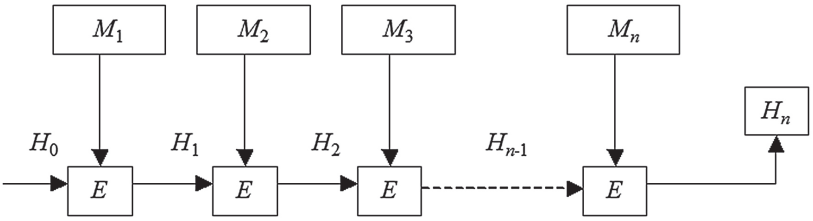

Рис. 14. Типовая схема вычисления блочной хэш-функции

В алгоритмах вычисления хэш-функций в качестве базовых функций шифрования обычно используются стойкие блочные шифры, а также односторонние криптографические функции. В этом случае обеспечивается влияние каждого бита сообщения на значение получаемой хэш-функции.

Рассмотрим основные приемы построения базовых функций хэширования.

Идея создания функций $y = f(x)$, для которых вычисление аргумента x по значению y будет вычислительно неосуществимым, состоит в том, что преобразование может быть сделано необратимым, если текущие значения вычислять в зависимости от значений на предыдущем шаге.

Одним из перспективных способов повышения стойкости алгоритмов является задание неопределенности хода преобразования информации. Эта идея может быть реализована путем введения случайных данных в преобразуемое сообщение. Если в механизме преобразования используются операции или процедуры, зависящие от преобразуемых данных, то в этом случае сами операции будут изменяться случайно. Введение элементов случайности в процедуру преобразования преследует цель затруднить использование общего принципа криптоанализа блочных шифров, основанного на попытках выявления статистических свойств алгоритма шифрования, например, путем подбора специальных исходных текстов.

При создании блочных алгоритмов необходимо использовать нелинейные преобразования с хорошими свойствами рассеивания и перемешивания (или комбинацию линейных и нелинейных преобразований). Достоинством линейных преобразований является простота реализации, малое время их выполнения и удобство использования секретного ключа в качестве параметра преобразования. Однако на основе одних только линейных преобразований очень сложно обеспечить высокую стойкость. Одним из способов достижения хорошего рассеивания и перемешивания состоит в построении составного шифра, который включает ряд последовательно используемых простых шифров, каждый из которых вносит небольшой вклад в рассеивание или в перемешивание. Большое число современных блочных шифров используют многократное повторение некоторого набора операций преобразований, называемого раундом шифрования.

7.2. Описание лабораторной установки

Лабораторная установка представляет собой рабочую станцию (IBM совместимый компьютер семейства Pentium) с установленной операционной системой (ОС) Windows, рабочими папками (директориями), содержащими рабочие файлы и программой обеспечения лабораторной работы «Янтарь».

Режимы работы программы:

– работа с файлами, отчетами и журналом;
– ввод дополнительной информации о контролируемых объектах;
– фиксация контрольных сумм;
– проверка целостности;
– сравнение файлов-отчетов;
– сведения о программе.

Результатом работы программы являются контрольные суммы задаваемых файлов, которые отображаются в специальном «окне вывода». Результаты могут быть сохранены в текстовый файл-отчет.

После вызова программы разворачивается окно, представленное на рис. 15.

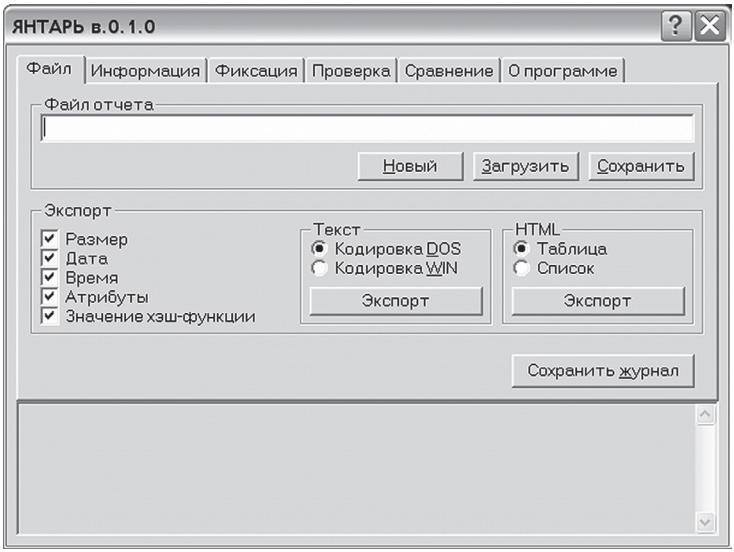

Рис. 15. Программа «Янтарь». Работа с файлами

Рассмотрим, какие функции предоставляют режимы работы программы.

Работа с файлами-отчетами и журналом. Данный режим позволяет:

– создать новый файл-отчет;
– загрузить существующий файл-отчет для последующей работы с ним;
– сохранить файл-отчет;
– экспортировать файл-отчет в текстовый формат или в формат .html;
– сохранить текущий журнал в файле.

Ввод дополнительной информации о контролируемых объектах. После выбора данного режима разворачивается окно, показанное на рис. 16.

Введенная информация будет отображаться в файле-отчете. *Фиксация контрольных сумм.* После выбора режима фиксации контрольных сумм разворачивается окно, показанное на рис. 17.

Данный режим позволяет вычислить контрольные суммы заданных файлов по заданным алгоритмам. Выбор списка файлов происходит в соответствующем окне, которое разворачивается после выбора опции «Добавить». Убрать файлы из списка можно, выделив их в окне «Список файлов» и выбрав опцию «Убрать». При выборе опции «Обновить» происходит перерасчет контрольных сумм по заданным алгоритмам для всех файлов из списка. Для задания алгоритмов хэширования их следует отметить в левой части окна (выбранные алгоритмы будут выделены другим цветом, например, на рис. 17 выбранные алгоритмы – SHF2, GOST3411, MD5, SHA).

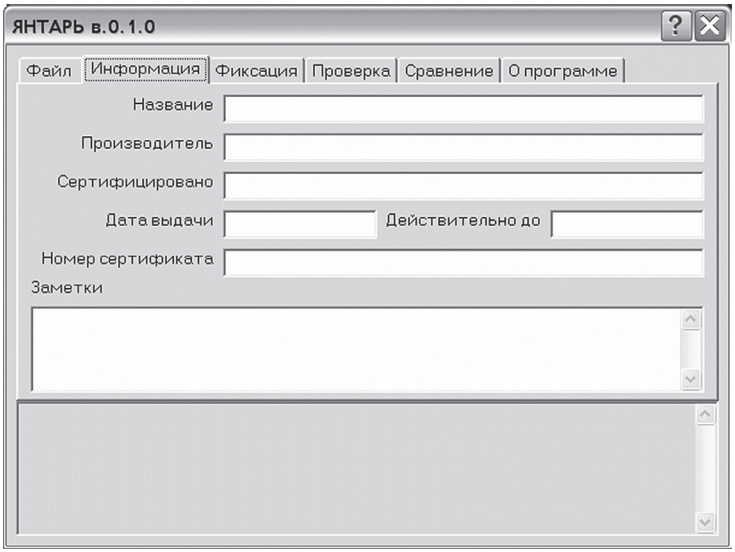

Рис. 16. Режим ввода дополнительной информации

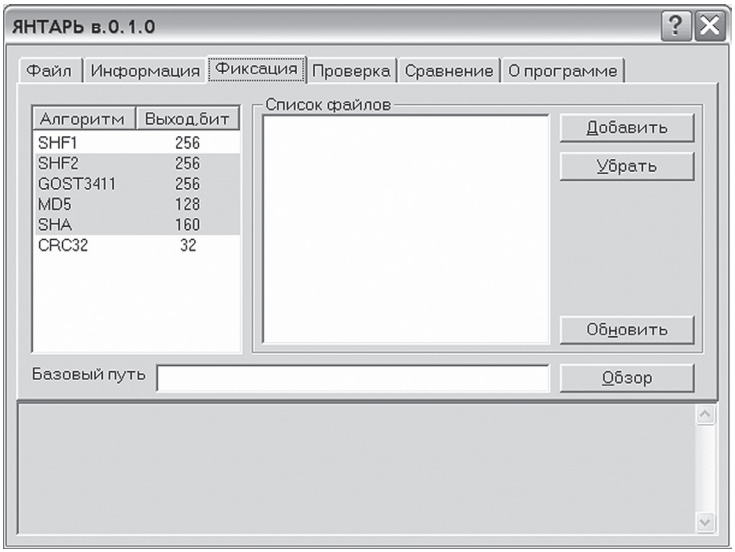

Рис. 17. Режим фиксации контрольных сумм

В списке файлов отображаются не только имена файлов, но и пути к ним. Путь к файлу считается относительно базового пути. Базовый путь можно выбрать в диалоговом окне, нажав кнопку «Обзор».

Пример. Даны следующие файлы:

c:\windows\help\access.chm

d:\home\readme.txt

Если в качестве базового пути указать c:\windows\, то в списке файлов заданные файлы будут иметь вид:

help\access.chm

d:\home\readme.txt

Если в качестве базового пути указать d:\home\, то в списке файлов заданные файлы будут иметь вид:

c:\windows\help\access.chm

readme.txt

Проверка целостности. После выбора режима проверки целостности разворачивается окно, показанное на рис. 18.

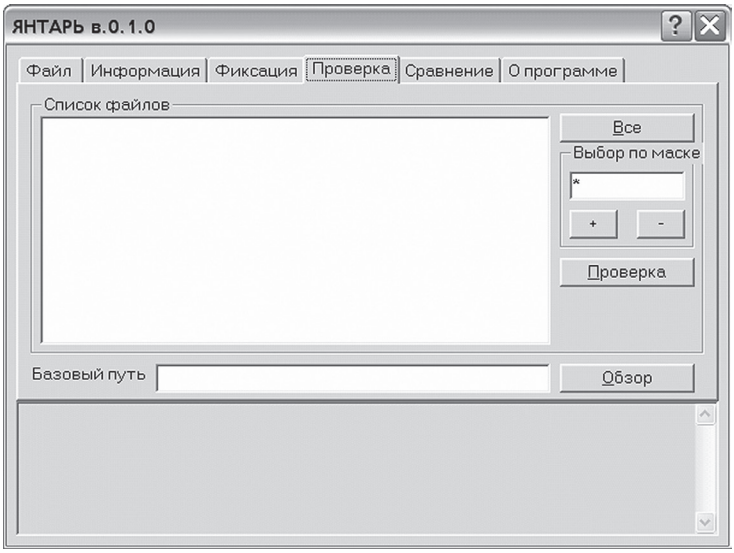

Рис. 18. Режим проверки целостности

В этом окне происходит проверка целостности заданных файлов. Поле «Список файлов» содержит файлы, выбранные в режиме фиксации контрольных сумм. В режиме проверки целостности редактировать список файлов нельзя. Файлы, подлежащие проверке целостности, можно выбрать из списка следующими способами:

- Опция «Все». Отметить все файлы в списке можно простым нажатием на кнопку «Все».
- Выбор по маске. Задайте маску в маленьком поле справа и нажмите «+» или «–». «+» отмечает как выбранные все файлы, соответствующие

маске, «–» убирает выделение со всех файлов, соответствующих маске.

Примеры масок: *, *.exe, c*.txt и т.п.

- Ручной выбор.

Для запуска проверки выбранных файлов необходимо выбрать опцию «Проверка». Результаты проверки отображаются в поле в нижней части окна.

Сравнение файлов-отчетов. После выбора данного режима разворачивается окно, показанное на рис. 19.

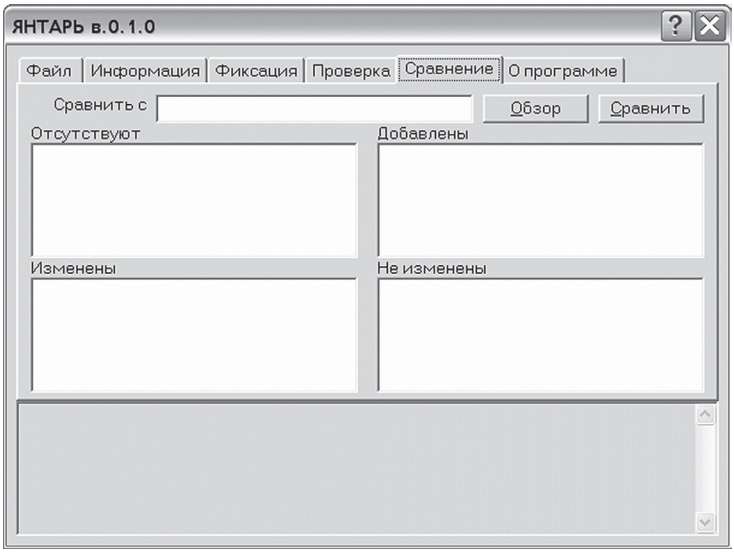

Рис. 19. Режим сравнения файлов-отчетов

Выбрать файл-отчет для сравнения с текущим можно, нажав кнопку «Обзор». После нажатия кнопки «Сравнить» происходит сравнение двух отчетов, и результаты сравнения выводятся на экран.

В поле «Отсутствуют» отображаются файлы, которые отсутствуют в текущем отчете, но присутствуют в отчете, выбранном для сравнения. В поле «Добавлены» отображаются файлы, которые присутствуют в текущем отчете, но отсутствуют в отчете, выбранном для сравнения. В поле «Изменены» отображаются файлы, которые присутствуют в обоих отчетах, но характеристики этих файлов не совпадают. В поле «Не изменены» отображаются файлы, которые присутствуют в обоих отчетах и они идентичны.

7.3. Порядок выполнения работы

1. Создайте папку с рабочими файлами. Например, pl.txt, p2.txt, и т.д.
2. Выполнить фиксацию эталонных контрольных сумм файлов. Для этого:

2.1. Активизировать программу amber.exe.
2.2. Перейти в режим ввода дополнительной информации о контролируемых объектах. Для этого выбрать закладку «Информация». В поле «Название» ввести текст «Лабораторная работа» и номер лабораторной работы. В поле «Производитель» ввести свою фамилию, инициалы и номер группы. Остальные поля можно не заполнять.
2.3. Перейти в режим фиксации контрольных сумм. Для этого выбрать закладку «Фиксация». Выбрать в левой части окна алгоритмы, по которым будут вычисляться контрольные суммы заданных файлов (определяются номером варианта по таблице 9). Задать базовый путь, нажав кнопку «Обзор». 2.4. Задать список файлов, нажав кнопку «Добавить». Список файлов выбирать по своему усмотрению. В списке должно быть от 10 до 20 файлов. После задания файлов автоматически подсчитываются их контрольные суммы по выбранным алгоритмам.
2.4. Перейти в режим работы с файлами-отчетами и журналом. Для этого выбрать закладку «Файл». Сохранить отчет, нажав кнопку «Сохранить». Экспортировать полученные результаты в текстовый файл, нажав кнопку «Экспорт» под группой «Текст». Кодировку текста выбрать по своему усмотрению. Полученные результаты необходимо включить в отчет по лабораторной работе.

3. Проверить файлы на целостность:
3.1. В режиме работы с файлами-отчетами и журналом (закладка «Файл») загрузить отчет, сформированный в п. 2. Для этого нажать кнопку «Загрузить» и в открывшемся диалоге выбрать нужный файл.
3.2. Перейти в режим проверки целостности (закладка «Проверка»). Выполнить проверку всех файлов. Результаты проверки отображаются в нижней части окна.
3.3. Перейти в режим работы с файлами-отчетами и журналом. Сохранить журнал, нажав кнопку «Сохранить журнал». Полученные результаты включить в отчет по лабораторной работе.
3.4. Нарушить целостность одного из файлов, фиксация контрольных сумм которого производилась в п. 2, предварительно сделав резервную копию этого файла. Это можно сделать, например, с помощью текстового редактора.
3.5. Повторить проверку на целостность файлов из отчета, сформированного в п. 2.5. Полученные результаты включить в отчет по лабораторной работе.

4. Исследовать свойства хэш-функций (изменение 1 бита):
4.1. С помощью программы «Янтарь» подсчитать контрольную сумму выбранного файла. Алгоритм хэширования определяется номером варианта (см. табл. 9). Результат сохранить в файле.

4.2. Создать резервную копию выбранного файла. С помощью текстового (или другого подходящего) редактора изменить выбранный файл таким образом, чтобы измененным оказался 1 бит. С помощью программы «Янтарь» подсчитать контрольную сумму этого файла. Результат сохранить в файле, сравнить с результатом, полученным в п.2, выводы включить в отчет по лабораторной работе. Восстановить выбранный файл из резервной копии.

5. Исследовать свойства хэш-функций (перестановка блоков информации):
   5.1. С помощью программы «Янтарь» подсчитать контрольную сумму выбранного файла. Алгоритм хэширования определяется номером варианта (см. табл. 9). Результат сохранить в файле.
   5.2. Создать резервную копию выбранного файла. С помощью текстового (или другого подходящего) редактора переставить местами два байта в выбранном файле. С помощью программы «Янтарь» подсчитать контрольную сумму этого файла. Результат сохранить в файле, сравнить с результатом, полученным в п. 1, выводы включить в отчет по лабораторной работе. Восстановить выбранный файл из резервной копии.

7.4. Содержание отчёта

Отчет по лабораторной работе содержит следующие элементы:

- Номер варианта и параметры задания в соответствии с табл. 6.
- Результирующие файлы по пунктам задания 2–5.
- Ответы на контрольные вопросы.
- Выводы о полученных результатах.

Таблица 6

№ варианта	№ задания		
	2.1	2.3	2.4
1	SHF1	SHA	GOST3411
2	SHF2	CRC32	MD5
3	GOST3411	MD5	SHF1
4	MD5	SHF1	SHF2
5	SHA	SHF2	CRC32
6	CRC32	GOST3411	SHA
7	MD5	SHF2	SHA
8	CRC32	SHF1	MD5
9	GOST3411	CRC32	SHF2

7.5. Контрольные вопросы

1. Дайте определение хэш-функции.
2. Почему изменение одного бита в конце сообщения приводит к разным хэш-функциям?
3. Почему перестановка двух слов в тексте, которая не меняет смысл текста и его объем влияет на полученные значения хэш-функций?
4. Какие основные требования предъявляются к хэш-функциям?
5. Что такое коллизии хэш-функции?
6. Какова вероятность того, что две произвольные последовательности символов будут иметь равные хэш-образы для хэш-функции с n-битным выходным значением?
7. Какими свойствами обладают хэш-функции?
8. Дайте определение однонаправленной функции.
9. Что означают принципы рассеивания и перемешивания, реализованные в алгоритмах получения хэш-образов файлов?

7.6. Литература

1. *Молдовян Н.А., Молдовян А.А., Еремеев М.А.* Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004.
2. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001.

Лабораторная работа №8.
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПО АСИММЕТРИЧНОЙ СХЕМЕ ШИФРОВАНИЯ

Цель работы: ознакомление с криптографическими средствами обеспечения конфиденциальности данных на примере шифра RSA.

8.1. Описание объекта исследования

Для решения задачи распределения ключей была выдвинута концепция двухключевой (или асимметричной) криптографии (рис. 20).

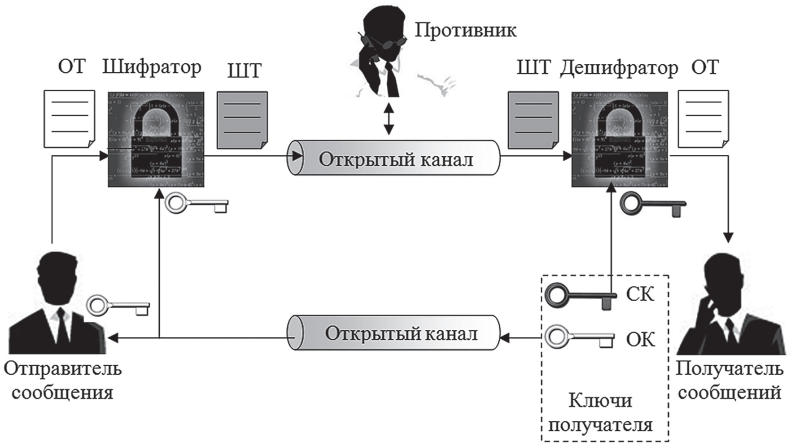

Рис. 20. Двухключевая криптосистема шифрования

В такой схеме для шифрования и дешифрования применяются различные ключи. Для шифрования информации, предназначенной конкретному получателю, используют уникальный открытый ключ (ОК) получателя-адресата.

Соответственно для дешифрования получатель использует парный секретный ключ (СК). Для передачи открытого ключа от получателя к отправителю секретный канал не нужен. Вместо секретного канала используется аутентичный канал, гарантирующий подлинность источника передаваемой информации (открытого ключа отправителя). Аутентичный канал является открытым и доступен всем, в том числе и противнику.

Асимметричные шифры не имеет смысла использовать для защищенного хранения документов. Их прерогатива – защита сообщений, электронной почты, прикрепленных к посланиям файлов и т.п.

Все криптосистемы с открытым ключом используют представление сообщений в виде целых чисел и преобразование этих целых чисел в

криптограммы, представляющие собой также целые числа, поэтому математической основой всех систем с открытым ключом является, прежде всего, теория чисел.

Для ознакомления с асимметричными системами шифрования разберём алгоритм RSA, названного так по первым буквам фамилий авторов этого алгоритма: R. Rivest, A. Shamir, L. Adleman. Алгоритм основан на трудноразрешимых задачах факторизации и дискретного логарифмирования. Перейдем к детальному рассмотрению схемы шифрования.

Первый этап – *создание пары ключей* – состоит из следующих операций.

1. Выбираются два больших простых числа p и q.
2. Вычисляется n, равное $(p \cdot q)$.
3. Выбирается произвольное число e ($e < n$), такое, что наибольший общий делитель НОД $(e, (p-1) \cdot (q-1)) = 1$, т.е. e должно быть взаимно простым с числом $(p-1) \cdot (q-1)$.
4. Методом Евклида решается в целых числах уравнение $e \cdot d + (p-1) \cdot (q-1) \cdot y = 1$.
   Здесь неизвестными являются переменные d и y – метод Евклида как раз и находит множество пар (d, y), каждая из которых является решением уравнения в целых числах.
5. Пара чисел (e, n) – публикуется как открытый ключ. Число d хранится в секрете – это и есть закрытый ключ, который позволяет читать все послания, зашифрованные с помощью пары чисел (e, n).

Второй этап – собственно *шифрование* с помощью открытого ключа.

1. Отправитель разбивает свое сообщение на блоки, равные $k = [\log_2(n)]$ бит, где квадратные скобки обозначают взятие целой части от дробного числа. Подобный блок может быть интерпретирован как число из диапазона $(0; 2^k - 1)$.
2. Для каждого типа числа (назовем его m_i) вычисляется выражение $c_i = ((m_i)^e) \bmod n$. Блоки c_i и есть зашифрованное сообщение. Их можно без опасения передать по открытому каналу, поскольку операция возведения в степень по модулю простого числа является тот самой трудноразрешимой математической задачей.

Третий этап – *дешифрование* послания с помощью секретного ключа. Частный случай теоремы Эйлера утверждает, что если число n представимо в виде произведения двух простых чисел p и q, то для любого x имеет место равенство:

$$\left(x^{(p-1)(q-1)}\right) \bmod n = 1. \qquad (8.1)$$

Для дешифрования RSA-сообщения воспользуемся формулой (8.1). Возведем обе ее части в степень $(-y)$: $\left(x^{(-y)(p-1)(q-1)}\right) \bmod n = 1^{(-y)} = 1$. После умножения обеих частей равенства на x получим:

$$\left(x^{(-y)(p-1)(q-1)+1}\right) \bmod n = 1 \cdot x = x. \tag{8.2}$$

Величина d была подобрана с помощью алгоритма Евклида так, что $e \cdot d + (p - 1) \cdot (q - 1) \cdot y = 1$, то есть $e \cdot d = 1 + (-y) \cdot (p-1) \cdot (q-1)$. Следовательно, в выражении (8.2) можно заменить показатель степени на число $(e \cdot d)$. Получаем:

$$\left(x^{(e \cdot d)}\right) \bmod n = \left(x^{(-y)(p-1)(q-1)+1}\right) \bmod n = 1 \cdot x = x. \tag{8.3}$$

То есть для того чтобы прочесть сообщение $c_i = ((m_i)^e) \bmod n$, достаточно возвести его в степень d по модулю n:

$$\left(\left(c_i\right)^d\right) \bmod n = \left(\left(m_i\right)^{(e \cdot d)}\right) \bmod n = m_i. \tag{8.4}$$

Общий вид RSA системы приведен на рис. 21.

За время существования криптосистемы RSA были обнаружены алгоритмы взлома схемы при частных случаях его параметров. Поэтому в настоящее время принцип выбора простых чисел p и q – основы криптосхемы – пополнился рядом дополнительных ограничений:

- числа $(p + 1)$ и $(q + 1)$ должны содержать в своем разложении на множители большие простые делители;
- числа p и q должны очень близко совпадать по порядку длины;
- секретный ключ не должен в результате процедуры создания ключей оказаться очень маленьким. Если подобное условие случайно выполнилось, придется «перевыбирать» случайное число e и повторить процедуру вычисления d;
- каждый абонент сети должен использовать уникальное значение n.

В современной криптографии порогом раскрываемости RSA считается длина n в 512 бит. Эта величина находится на «грани доверия». Кроме нее используются криптосхемы с ключами в 768, 1024, 2048 бит.

Рассмотрим работу схемы RSA на небольших числах. Естественно, из-за малых значений p и q дополнительные требования на их выбор не выдержаны. Пусть $p = 5$, а $q = 11$, тогда значение $n = 55$. В качестве открытого ключа e выбираем число 7, таким образом, весь открытый ключ имеет вид ($e = 7$, $n = 55$). Вычилим закрытый ключ d: уравнение $e \cdot d + (p - 1) \cdot (q - 1) \cdot y = 1$ приобретает вид $7 \cdot d + 40 \cdot y = 1$ и имеет в целых числах решение $d = 23$, $y = -4 = 51$. Таким образом, закрытым ключом является число 23.

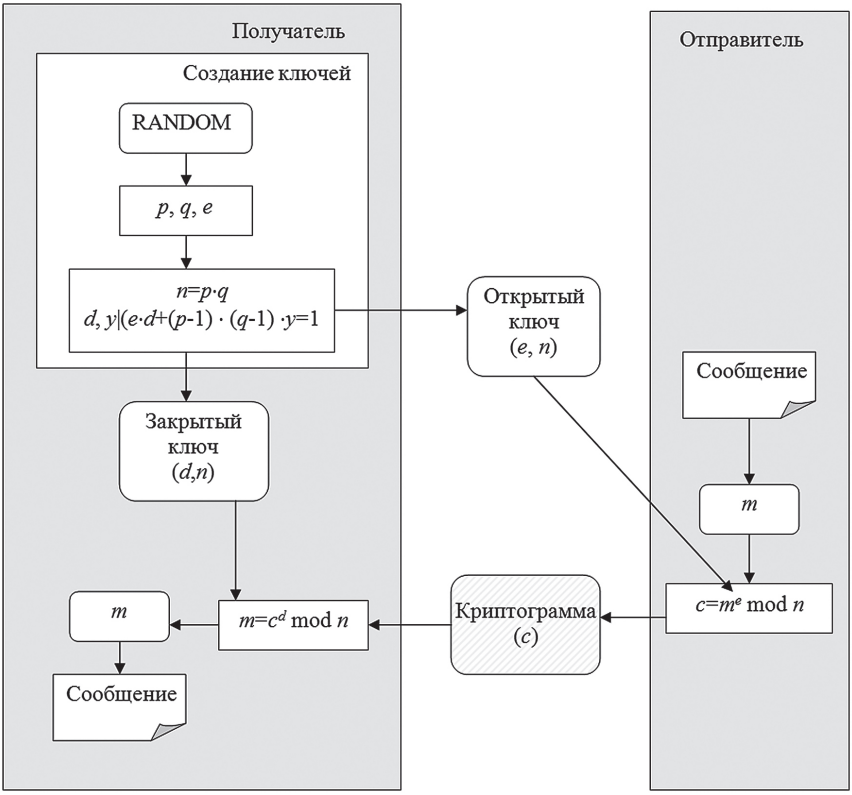

Рис. 21. Криптосистема RSA

Пусть произвольный отправитель хочет передать абоненту комбинацию бит 100111_2, ее числовой эквивалент: 39_{10}. Возведем 39 в степень открытого ключа $e = 7$ по модулю $n = 55$: $(39^7 \bmod 55) = 19$. Число 19 является шифрограммой и передается по открытому каналу связи. Получатель по приходу сообщения возводит его в степень $d = 23$: $(19^{23} \bmod 55) = 39$. Исходное послание восстановлено.

8.2. Порядок выполнения работы

Последовательность выполняемых действий включает следующие шаги:

1. Сформировать два простых числа p и q длиной 2 десятичных знака.
2. Вычислить модуль $n = p \cdot q$.
3. Вычислить функцию Эйлера от модулю n: $\varphi(n) = (p - 1)(q - 1)$.
4. Выбрать случайный открытый ключ e длиной 2 десятичных знака.
5. Вычислить закрытый ключ $d = e^{-1} \bmod \varphi(n)$.

6. Зашифровать заданное сообщение M: $C = M^e \bmod n$, где C – зашифрованное сообщение (криптограмма).
7. Расшифровать полученную криптограмму: $C^d \bmod n = M'$. Убедиться, что $M' = M$.
8. Результаты оформить в виде табл. 7.

Таблица 7

Результаты шифрования и дешифрования

M_i	M^e	C	C^d	M'

8.3. Содержание отчета

Отчет по лабораторной работе содержит следующие элементы:

- Исходные данные.
- Результаты шифрования и дешифрования в виде табл. 7.
- Ответ на контрольный вопрос.
- Выводы о полученных результатах.

8.4. Контрольные вопросы

1. Какие числа называются простыми?
2. Определите назначение открытого и секретного ключей в системе RSA.
3. Почему схема RSA называется асимметричной?
4. Какие особенности системы RSA необходимо учитывать при ее практическом использовании?
5. Какое число является простым?
6. Какому требованию должны удовлетворять простые делители модуля в системе RSA?
7. Нужен ли секретный канал связи при шифровании алгоритмом RSA? Обоснуйте ответ.
8. Для какого процесса (шифрование или дешифрование) используется открытый ключ в системе RSA?
9. Для какого процесса (шифрование или дешифрование) используется секретный ключ в системе RSA?

8.5. Литература

1. *Молдовян Н.А.* Практикум по криптосистемам с открытым ключом. – СПб.: Петербург-БХВ, 2010. – 304 с.
2. *Татарникова Т.М.* Криптографические методы защиты информации. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации. Учеб. пособие. – СПб.: изд. РГГМУ, 2010. – 104 с.
3. *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.

Лабораторная работа №9.
АУТЕНТИФИКАЦИЯ ДОКУМЕНТОВ НА ОСНОВЕ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

Цель работы: ознакомиться с процедурами формирования и проверки электронно-цифровой подписи (ЭЦП). Получить практические навыки формирования открытого и закрытого ключей ЭЦП по алгоритму RSA.

9.1. Описание объекта исследования

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, то есть установления подлинности автора и отсутствия изменений в полученном документе. Обычной «бумажной» подписью традиционно заверяется подлинность документа. Стойкость подписи, то есть невозможность ее подделки посторонними лицами обеспечивается двумя основными условиями: во-первых, ее уникальностью, основанной на индивидуальных особенностях почерка, а во-вторых, физической целостностью бумажного документа, на котором произведена подпись. При этом подпись не может быть подделана даже тем лицом, которое проверяет ее подлинность.

Однако при передаче электронных документов по компьютерным сетям или хранении на машинных носителях воспользоваться данными условиями невозможно, в том числе и при передаче факсимильных сообщений (ФАКС), поскольку они допускают простую подделку.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- *активный перехват* – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- *маскарад* – абонент *C* посылает документ абоненту *B* от имени абонента *A*;
- *ренегатство* – абонент *A* заявляет, что не посылал сообщения абоненту *B*, хотя на самом деле послал;
- *подмена* – абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A*;
- *повтор* – абонент *C* повторяет ранее переданный документ, который абонент *A* посылал абоненту *B*.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, а также частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является электронная цифровая подпись – ЭЦП.

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. ЭЦП решает проблему возможного спора между отправителем и получателем, в том числе и в суде, при наличии юридической базы для ее применения.

Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
– не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
– гарантирует целостность подписанного текста.

Одновременно с этими ЭЦП должна представлять собой относительно небольшое количество дополнительной цифровой информации (цепочку данных), которые можно передавать по сетям вместе с подписываемым текстом, то есть она должна удовлетворять следующим четырем основным требованиям:

– цифровая подпись должна быть уникальной, то есть никто, кроме автора, не может создать такую же подпись, включая лиц, проверяющих ее подлинность;
– каждый пользователь сети, законный или незаконный, может проверить истинность цифровой подписи;
– подписавший не может отказаться от сообщения, заверенного его цифровой подписью;
– как реализация, так и проверка цифровой подписи, должны быть достаточно простыми.

Чтобы удовлетворить всем перечисленным требованиям цифровая подпись, в отличие от «бумажной», должна зависеть от всех бит сообщения и изменяться даже при изменении одного бита подписанного сообщения. Для реализации цифровой подписи на основе симметричных криптосистем необходимо участие доверенного лица – арбитра. Реализация цифровой подписи без арбитра возможна только на основе использования асимметричных систем.

Система ЭЦП включает две процедуры:

– процедуру постановки подписи;
– процедуру проверки подписи.

В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

При формировании ЭЦП отправитель, прежде всего, вычисляет хэш-функцию hash(M) подписываемого текста M. Вычисленное значение хэш-функции hash(M) представляет собой один короткий блок информации h, характеризующий весь текст M в целом. Затем число h шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию h = hash(M) принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению h хэш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП без знания секретного ключа.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Каждая подпись содержит следующую информацию:

– дату подписи;
– срок окончания действия ключа данной подписи;
– информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
– идентификатор подписавшего (имя открытого ключа);
– собственно цифровую подпись.

Существуют различные виды цифровой подписи, основанные на криптосистемах с открытым ключом. Одни опираются на сложность разложения больших чисел на простые множители, другие – на сложность дискретного логарифмирования в одной из конечных групп.

С 1 июля 2002 г. в России введен стандарт электронной цифровой подписи ГОСТ Р.34.10-2001, опирающийся на сложность решения задачи «дискретного логарифмирования» в группе точек на эллиптической кривой. Эллиптические кривые изучаются в алгебраической геометрии и широко применяются в различных разделах математики, в том числе в теории чисел.

Рассмотрим (как более простую) реализацию цифровой подписи на основе криптосистемы RSA. Пользователь A, подписывающий сообщение M, генерирует пару ключей k_A, K_A, где k_A – секретный ключ пользователя A; K_A – открытый ключ пользователя A. Затем A сообщает пользователям сети значения K_A и n, где n – параметр, необходимый для генерации ключей и проверки ЭЦП.

Далее пользователь A создает (вычисляет) ЭЦП по формуле:

$$sign = M^{k_A} \bmod n, \tag{9.1}$$

где $sign$ – цифровая подпись сообщения M.

ЭЦП приписывается к сообщению и передается вместе с ним (рис. 22).

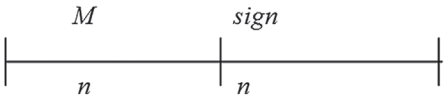

Рис. 22. Сообщение с ЭЦП

Любой другой пользователь сети, приняв сообщение M, при необходимости проверки цифровой подписи производит вычисление согласно:

$$\left(sign\right)^{K_A} \bmod n = h'. \tag{9.2}$$

Далее он сравнивает результат h' с полученным значением hash(M), которое вычисляет независимо. При h' = hash(M) ЭЦП пользователя A считается подлинной. Схема формирования и проверки ЭЦП по алгоритму RSA приведена на рис. 23.

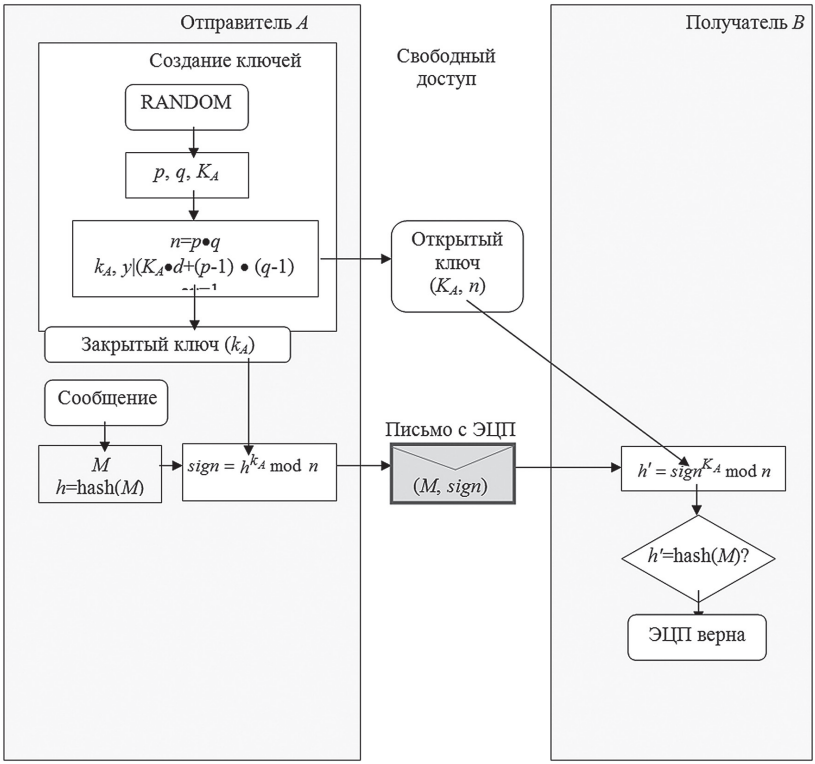

Рис. 23. Схема формирования и проверки ЭЦП RSA

Первая схема ЭЦП – RSA – была разработана еще в конце 1970-х гг. Однако проблема подтверждения авторства стала актуальной настолько, что потребовалось установление стандарта только в 1990-х гг. во время взрывного роста глобальной сети Интернет и массового распространения электронной торговли и оказания услуг. Именно поэтому стандарты ЭЦП в России и США были приняты практически одновременно в 1994 г. Из предложенных криптологами схем ЭЦП наиболее удачными оказались RSA и схема Эль-Гамаля. Первая была запатентована в США и ряде других стран. Вторая имеет множество модификаций и осталась по большей части свободной от патентов. Обладает она и целым рядом практических преимуществ: размер блоков, которыми оперируют алгоритмы, и соответственно размер ЭЦП в ней оказались значительно меньше, чем в RSA, при той же стойкости. Именно поэтому современные стандарты ЭЦП России и США базируются на схеме Эль-Гамаля. Согласно подписанному Президентом РФ 10 января 2002 г. Федеральному Закону «Об электронной цифровой подписи» ЭЦП должна обеспечить юридическую значимость, как самих электронных документов, так и действий пользователей над ними (визирование, подписание, утверждение и т.п.).

Рассмотрим пример формирования и проверки ЭЦП. Пусть заданы следующие исходные данные:

$p = 13$; $q = 23$; $n = 299$; $\varphi(n) = 264$; $K_A = 5$; $k_A = 53$.

Результаты вычислений представлены в табл. 8.

Таблица 8

Результаты вычислений формирования и проверки ЭЦП

h_i	h^{K_A}	*sign*	Письмо + ЭЦП	$sign^{K_A}$	h'	$h = h'$?	Результат
110	1,56E+108	288	110,288	1981355655168	110	Да	ЭЦП верна
111	2,52E+108	102	111,102	11040808032	111	Да	ЭЦП верна
112	4,06E+108	281	112,281	1751989905401	112	Да	ЭЦП верна
113	6,50E+108	224	113,224	563949338624	113	Да	ЭЦП верна
114	1,04E+109	160	114,160	104857600000	114	Да	ЭЦП верна

9.2. Порядок выполнения работы

В лабораторной работе выполняются процедуры подписывания сообщений (вернее их хэш-функций) h_i ($i = 1, ..., 5$), предположительно вычисленных от некоторых гипотетических документов M_i с уравнением проверки:

$$\left(sign\right)^{K_A} \bmod n = h.$$

Последовательность выполняемых действий включает следующие шаги.

1. Сформировать два простых числа p и q длиной 2 десятичных знака.
2. Вычислить модуль $n = p \cdot q$.
3. Вычислить функцию Эйлера от модуля n: $\varphi(n) = (p-1)(q-1)$.
4. Выбрать случайный открытый ключ K_A длиной 2-3 десятичных знака ($K_A < n$).
5. Вычислить подбором закрытый ключ k_A из уравнения с двумя неизвестными k_A и y (k_A и y – целые, $k_A > 0$):

$$K_A \cdot k_A + \varphi(n) \cdot y = 1.$$

6. Для каждого значения хэш-функций от предполагаемых сообщений выполнить следующее:
   6.1. Вычислить подпись по формуле $sign = h^{K_A} \bmod n$.
   6.2. Вычислить значение $h' = sign^{K_A} \bmod n$.
   6.3. Сравнить значения h и h'.
7. Результаты оформить в виде табл. 8.

9.3. Содержание отчёта

Отчет по лабораторной работе содержит следующие элементы:

- Исходные данные.
- Результаты вычислений формирования и проверки ЭЦП в виде табл. 8.
- Ответ на контрольный вопрос.
- Выводы о полученных результатах.

9.4. Контрольные вопросы

1. Почему сравнительно короткий открытый ключ является безопасным, тогда как секретный ключ всегда должен быть большим?
2. Какому требованию должны удовлетворять простые делители модуля в системе RSA?
3. При изменении открытого ключа можно ли сохранить старое значение модуля n?
4. Какие особенности системы RSA необходимо учитывать при ее практическом использовании?
5. На каких особенностях математических преобразований опирается метод ЭЦП RSA?
6. Какое число является простым?
7. Почему подписывается не само сообщение, а его хэш-образ?
8. Почему схема ЭЦП называется асимметричной?
9. Определите назначение ЭЦП.
10. Определите назначение открытого и секретного ключей в системе ЭЦП.

9.5. Литература

1. *Молдовян Н.А.* Теоретический минимум и алгоритмы цифровой подписи. – СПб.: Петербург-БХВ, 2010. – 304 с.
2. *Татарникова Т.М.* Криптографические методы защиты информации. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации. Учеб. пособие. – СПб.: изд. РГГМУ, 2010. – 104 с.

ASCII – таблица символов

Символы с кодами 128–255 (Кодовая таблица 866 – MS-DOS)

Код	Символ	Код	Символ	Код	Символ	Код	Символ
128	А	160	а	192	└	224	р
129	Б	161	б	193	┴	225	с
130	В	162	в	194	┬	226	т
131	Г	163	г	195	├	227	у
132	Д	164	д	196	─	228	ф
133	Е	165	е	197	┼	229	х
134	Ж	166	ж	198	╞	230	ц
135	З	167	з	199	╟	231	ч
136	И	168	и	200	╚	232	ш
137	Й	169	й	201	╔	233	щ
138	К	170	к	202	╩	234	ъ
139	Л	171	л	203	╦	235	ы
140	М	172	м	204	╠	236	ь
141	Н	173	н	205	═	237	э
142	О	174	о	206	╬	238	ю
143	П	175	п	207	╧	239	я
144	Р	176	▒	208	╨	240	Ё
145	С	177	▒	209	╤	241	ё
146	Т	178	▓	210	╥	242	Є
147	У	179	│	211	╙	243	є
148	Ф	180	┤	212	╘	244	Ї
149	Х	181	╡	213	╒	245	ї
150	Ц	182	╢	214	╓	246	Ў
151	Ч	183	╖	215	╫	247	ў
152	Ш	184	╕	216	╪	248	°
153	Щ	185	╣	217	┘	249	∙
154	Ъ	186	║	218	┌	250	·
155	Ы	187	╗	219	▉	251	√
156	Ь	188	╝	220	▄	252	№
157	Э	189	╜	221	▌	253	¤
158	Ю	190	╛	222	▐	254	■
159	Я	191	┐	223	▀	255	

СОДЕРЖАНИЕ

УЧЕБНОЕ ИЗДАНИЕ

Татарникова Татьяна Михайловна

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум

Редактор: *О.С. Крайнова*
Компьютерная верстка: *Ю.И. Климов*

ЛР № 020309 от 30.12.96.

Подписано в печать 21.10.13. Формат 60×90 1/16. Гарнитура Newton.
Печать цифровая. Усл. печ. л. 4,0. Тираж 200 экз. Зак. № 216.
РГГМУ, 195196, Санкт-Петербург, Малоохтинский пр., 98.
Отпечатано в ЦОП РГГМУ