Министерство образования и науки Украины
Севастопольский национальный технический университет

Методические указания

по выполнению расчетно-практического задания

«Основы криптографии»

по дисциплине «Радиоэлектронные системы
защиты объектов и информации»

для студентов специальности 7.090701 «Радиотехника»
дневной формы обучения

Севастополь
2006

УДК 681.322.067

Методические указания для выполнения расчетно-практической работы по дисциплине «Радиоэлектронные системы защиты объектов и информации» для студентов специальности 7.090701 «Радиотехника» дневной формы обучения / Сост. И.В. Лащенко, В.М. Иськив. – Севастополь: Изд-во СевНТУ, 2006. – 12с.

Целью методических указаний является оказание помощи студентам в выполнении расчетно-практического задания по дисциплине «Радиоэлектронные системы защиты объектов и информации» по теме «Основы криптографии».

Методические указания рассмотрены и утверждены на заседании кафедры (протокол № …. от ……. 2006 г.)

Допущено учебно-методическим центром СевНТУ в качестве методических указаний.

Рецензент: к.т.н., доц. кафедры радиотехники СевНТУ Зиборов С.Р.

СОДЕРЖАНИЕ

Цель работы – ознакомиться с основными классическими и современными методами криптографии, изучить применение симметричных и несимметричных методов шифрования.

1. Краткие теоретические сведения

Криптография (от греч. *«тайнопись»*) – наука о методах преобразования информации в целях ее защиты от незаконных пользователей.

Шифр – алгоритм преобразования информации, ***ключ*** – сменяемый элемент шифра.

Можно выделить симметричные и несимметричные методы криптографии.

При использовании ***симметричных методов*** шифрование исходного сообщения и дешифрация криптограммы происходит по определенным алгоритмам с использованием одного и того же ключа. К симметричным методам относят такие классы шифров, как перестановка, подстановка, блочные комбинированные шифры, шифры, основанные на аналитических преобразованиях, гаммирование.

В ***несимметричных системах*** имеются два ключа: открытый ключ, доступный многим, и закрытый – секретный. Шифрование исходных сообщений и дешифрация криптограмм проводится с использованием различных ключей.

Криптографическая защита информации находит широкое применение для хранения и передачи конфиденциальных сообщений, данных, подтверждения подлинности электронных документов.

1.1. Перестановочные шифры

Знаки исходного сообщения переставляются по определенному алгоритму.

Алгоритм перестановок может определяться аналитическим путем, либо могут использоваться специальные механические приспособления (скиталы, решетки и др.)

1.2. Подстановочные шифры

Знаки исходного алфавита замещаются любыми знаками: буквами, цифрами, символами. Подстановка может быть однозначной и многозначной.

Простая (моноалфавитная) замена. Каждому символу исходного алфавита соответствует определенная пара.

Возможны различные варианты замены. Простейший буквенный пример - первое известное применение тайнописи на Руси - парная замена согласных букв (см. рис.1.1), гласные остаются незашифрованными.

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Рисунок 1.1

При замене букв цифрами можно записать алфавит в несколько строк и пронумеровать строки и столбцы, а затем каждую букву заменять парой цифр - строка, столбец (см.рис.1.2). При использовании такой замены можно передавать не записанное зашифрованное сообщение, а озвученное - например, перестукиванием.

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

Рисунок 1.2 - Русский аналог «Квадрата Полибия»

1.2.2. Для скрытия статистических характеристик исходного сообщения применяют более сложные подстановки. Шифры с использованием **ключа** обладают большей конфиденциальностью.

Полиалфавитная замена – исходному алфавиту соответствует несколько групп знаков, при этом одним и тем же знаком могут зашифровываться различные символы исходного сообщения. Выбор знака из алфавитов замены осуществляется по определенным правилам, например, при использовании ключа - сочетанием символа исходного сообщения и соответствующего символа ключа.

Гомофоническая замена – каждому символу открытого текста соответствует несколько неповторяющихся символов.

1.3. Гамма шифры

Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности случайных чисел, которая называется ***гаммой***. Может выполняться не сложение, а другие математические, логические операции. Используются конечные либо бесконечные гаммы.

1.4. Другие типы симметричных шифров

Метод аналитических преобразований, которые проводят над преобразованными в математическую форму символами исходного сообщения и ключа, например, умножение матрицы (ключа) на вектор (исходное сообщение).

Комбинированные методы – последовательное шифрование блоков исходного текста с помощью двух и более методов (подстановка, замена и гаммирование). Использование произведения простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеяние и переме-

шивание, позволяет обеспечить высокую стойкость, достаточную для применения такого метода в национальном стандарте закрытия данных.

1.5. Криптографические системы с открытым ключом

Такие системы относятся к ассиметричным криптосистемам.

Алгоритм преобразования информации построен таким образом, что расшифровывание сообщения, закрытого общедоступным ключом возможно только с использованием секретного личного ключа адресата.

2. ТИПОВЫЕ ЗАДАЧИ ДЛЯ РЕШЕНИЯ НА ПРАКТИЧЕСКОМ ЗАНЯТИИ И ИНДИВИДУАЛЬНЫЕ РАСЧЕТНЫЕ ЗАДАНИЯ

Рекомендуется в течение лабораторного занятия изучить все предложенные методы шифрования и расшифровать криптограммы, а индивидуальные задания выполнять как самостоятельную работу.

Вариант (а) - для студентов с четной последней цифрой номера зачетной книжки,

(б) - для студентов с нечетной последней цифрой номера зачетной книжки.

2.1.Тип шифра - перестановка

а) **Маршрутная транспозиция**

Сообщение записывается в прямоугольник, столбцы которого затем переставляются заданным образом. Количество столбцов и порядок перестановок определяется ключом - алфавитным порядком следования букв в некотором слове.

Выбираем в качестве ключа слово "шифр". Это слово содержит 4 буквы, значит, в таблице должно быть 4 столбца. Алфавитный порядок следования букв – 4132. Расшифруйте : ПКИРРТГОЯАИФ.

Задание : зашифруйте свою фамилию, имя, отчество (как одно слово).

б) **Решетка Кардано**

Используют специальные карточки с отверстиями (см. Приложение А). При переворачивании их в определенной последовательности, закрываются все клетки поля, кроме тех, в которых просматривается очередной отрывок сообщения. Такого же результата можно добиться, пронумеровав клетки поля в заданном порядке.

Расшифруйте : СШПОИВТЕКФРАЕАНР.

Задание : зашифруйте свою фамилию, имя, отчество (как одно слово).

2.2. Тип шифра -подстановка

2.2.1. **Простая замена**

Расшифровав простейшие буквенную (а) и цифровую (б) криптограммы,

определить названия соответствующих шифров.
а) Расшифруйте : КАМАЩАМЛТАЯЧМАРОКА (используйте рис.1.1).

Задание : зашифруйте свою фамилию, имя.

б) Расшифруйте : 43 64 41 21 32 33 11 65 11 13 12 44 25 11 (используйте рис.1.2).

Задание : зашифруйте свою фамилию, имя.

2.2.2.
а) **Шифр Виженера (полиалфавитная замена)**

Над буквами сообщения записывают повторяющееся слово или словосочетание - ключ. По буквам верхней строки определяют столбец в таблице Виженера (Приложение Б), по букве нижней строки - строку этой таблицы. В криптограмму записывают букву, стоящую на пересечении выбранных столбца и строки.

Выбираем ключ «ВИЖЕНЕР». Расшифруйте : ГЫКААКТПРТЕАКЫЭХК.

Задание : зашифруйте свою фамилию, имя, отчество.

б) **Шифрование по книге (гомофоническая замена)**

Ключом может служить известный текст - достаточно объемное стихотворение, заданная страница в книге. Каждой букве текста ключа соответствует пара цифр (строка, столбец). Часто встречающимся буквам соответствует много пар, из которых выбирается любая.

Выбираем ключ - отрывок стихотворения, приведенный в приложении В. Расшифруйте: 4,1 3,4 1,16 9,9 3,8 6,4 2,1 1,8 7,8 2,8 3,18 4,5 4,9.

Задание : зашифруйте свою фамилию, имя, отчество.

2.3. Тип шифра - гаммирование

Открытый текст предварительно преобразуют в двоичный код. С помощью датчика псевдослучайных чисел формируют гамму, числа которой последовательно складываются по модулю 2 с числами исходного текста.

Пример:

В соответствии с приложением Г преобразуем текст «УРА» в двоичный код: 10011 10000 00001.

Выберем гамму (произвольно): 1 3 5 , также преобразуем в двоичный код: 00001 00011 00101

Выполним поэлементное логическое сложение.

Криптограмма: 10010 10011 00100.

Расшифруйте: 00101 00010 01001 01101 00010

Задание : зашифруйте свою фамилию, выбрав в качестве гаммы последовательность цифр, определяющих дату Вашего рождения - 8 цифр: ДДММГГГГ. (Например: «29071980» для 29 июля 1980 года).

2.4. Шифрование с открытым ключом

Сформируем открытый и закрытый ключи:

- Выберем два простые числа **p** и **q**, так чтобы их произведение **n= p ˣq** было больше, чем число знаков алфавита исходного сообщения. (Реально используются очень большие числа порядка 10^{150} … 10^{200}).
- Выберем число **d** - взаимно простое с результатом умножения **(p-1)(q-1)**.
- Определим такое число **e**, для которого является истинным соотношение

e ˣ d mod(p-1)(q-1) = 1.

Открытым ключом являются числа **e** и **n**, а закрытым – числа **d** и **n**.

Чтобы зашифровать данные по известному открытому ключу { **e** ; **n** }, необходимо

- разбить исходный текст на блоки, каждый из которых представить в виде чисел

$$M (i) = 0, 1, 2 \ldots n-1;$$

- вычислить*

$$C (i) = M (i)^{e} \bmod (n) .$$

Чтобы расшифровать эти данные, необходимо, используя закрытый ключ выполнить преобразование:

$$M (i) = C (i)^{d} \bmod (n) .$$

Пример.

- Выбираем простые числа **p=3** и **q=11**, тогда **n= 33.**
- **(p-1)(q-1) = 20 =2ˣ2ˣ5.**
- Выбираем **d = 3.**
- Определим число **e** из условия **e ˣ 3 mod(20) = 1**.

e = 7.

Исходному тексту «ЕДА» соответствует «651», если буквы алфавита заменить целыми числами,

$$M (i) = 6, 5, 1 .$$

Вычислим $C (i) = M (i)^{7} \bmod (33)$.

$$C (0) = 6^{7} \bmod (33)=30;$$
$$C (1) = 5^{7} \bmod (33)=14;$$
$$C (2) = 1^{7} \bmod (33)=1.$$

Криптограмма «301401».

Расшифруйте: 29301401.

Задание: зашифруйте свое имя.

Примечание*:

За результат операции (A mod B) принимается остаток от целочисленного деления A на B (вычет).

СОДЕРЖАНИЕ ОТЧЕТА

1. Цель работы.
2. Классификация шифров.
3. Результаты решения типовых задач и индивидуальных расчетных заданий.
4. Выводы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите основные методы шифрования.
2. Поясните разницу между симметричным и несимметричным шифрованием.
3. Поясните принцип, положенный в основу шифров "перестановка", недостатки и методы модификации.
4. Поясните принцип, положенный в основу шифров "перестановка", недостатки и методы модификации.
5. Поясните суть метода гаммирования.
6. Поясните принцип применения шифров с открытым ключом.

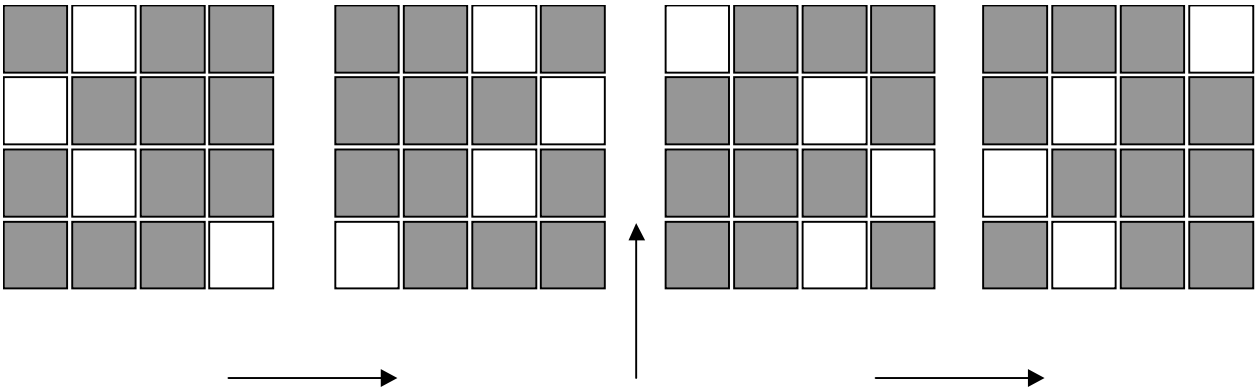
БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нечаев В.И. Элементы криптографии : (Основы теории защиты информации): [Учеб. пособие для ун-тов и пед. вузов]/ В.И. Нечаев; Ред. В.А. Садовничий. - М.: Высш. шк., 1999. - 108,[4] с.
2. Хорошко В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А. Чекатков; Ред. Ю. С. Ковтанюк. - К.: ЮНИОР, 2003. - 505 с.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях/ М.А. Иванов. - М.: Кудиц - образ, 2001.- 363с.
4. Баричев С. Г. Основы современной криптографии: Учеб. курс/ С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2002. - 176 с.

ПРИЛОЖЕНИЕ А
(справочное)

ПРИМЕР РЕШЕТКИ КАРДАНО

Решетка Кардано - это прямоугольная карточка с отверстиями, чаще квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При последовательном ее переворачивании каждая клетка лежащего под ней листа окажется открытой по одному разу.



ПРИЛОЖЕНИЕ Б
(справочное)

ТАБЛИЦА ВИЖЕНЕРА

В первой строке записан весь используемый алфавит, в каждой последующей осуществляется циклический сдвиг на одну букву.

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

ПРИЛОЖЕНИЕ В

Отрывок из поэмы Н. А. Некрасова «Кому на Руси жить хорошо»

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
1	**В**	**к**	**а**	**к**	**о**	**м**	**г**	**о**	**д**	**у**	**р**	**а**	**с**	**с**	**ч**	**и**	**т**	**ы**	**в**	**а**	**й**	1
2	**В**	**к**	**а**	**к**	**о**	**й**	**з**	**е**	**м**	**л**	**е**	**у**	**г**	**а**	**д**	**ы**	**в**	**а**	**й**			2
3	**Н**	**а**	**с**	**т**	**о**	**л**	**б**	**о**	**в**	**о**	**й**	**д**	**о**	**р**	**о**	**ж**	**е**	**н**	**ь**	**к**	**е**	3
4	**С**	**о**	**ш**	**л**	**и**	**с**	**ь**	**с**	**е**	**м**	**ь**	**м**	**у**	**ж**	**и**	**к**	**о**	**в**				4
5	**С**	**е**	**м**	**ь**	**в**	**р**	**е**	**м**	**е**	**н**	**н**	**о**	**о**	**б**	**я**	**з**	**а**	**н**	**н**	**ы**	**х**	5
6	**П**	**о**	**д**	**т**	**я**	**н**	**у**	**т**	**о**	**й**	**г**	**у**	**б**	**е**	**р**	**н**	**и**	**и**				6
7	**У**	**е**	**з**	**д**	**а**	**Т**	**е**	**р**	**п**	**и**	**г**	**о**	**р**	**е**	**в**	**а**						7
8	**П**	**у**	**с**	**т**	**о**	**п**	**о**	**р**	**о**	**ж**	**н**	**е**	**й**	**в**	**о**	**л**	**о**	**с**	**т**	**и**		8
9	**И**	**з**	**с**	**м**	**е**	**ж**	**н**	**ы**	**х**	**д**	**е**	**р**	**е**	**в**	**е**	**н**	**ь**					9
10	**З**	**а**	**п**	**л**	**а**	**т**	**о**	**в**	**а**	**Д**	**ы**	**р**	**я**	**в**	**и**	**н**	**а**					10
11	**Р**	**а**	**з**	**у**	**т**	**о**	**в**	**а**	**З**	**н**	**о**	**б**	**и**	**ш**	**и**	**н**	**а**					11
12	**Г**	**о**	**р**	**е**	**л**	**о**	**в**	**а**	**Н**	**е**	**е**	**л**	**о**	**в**	**а**							12
13	**Н**	**е**	**у**	**р**	**о**	**ж**	**а**	**й**	**к**	**а**	**т**	**о**	**ж**									13
14	**С**	**о**	**ш**	**л**	**и**	**с**	**я**	**и**	**з**	**а**	**с**	**п**	**о**	**р**	**и**	**л**	**и**					14
15	**К**	**о**	**м**	**у**	**ж**	**и**	**в**	**е**	**т**	**с**	**я**	**в**	**е**	**с**	**е**	**л**	**о**					15
16	**В**	**о**	**л**	**ь**	**г**	**о**	**т**	**н**	**о**	**н**	**а**	**Р**	**у**	**с**	**и**							16
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	

ПРИЛОЖЕНИЕ Г

Русский алфавит в двоичном представлении

А – 1 – 00001	Б – 2 – 00010	В – 3 – 00011
Г – 4 – 00100	Д – 5 – 00101	Е – 6 – 00110
Ж – 7 – 00111	З – 8 – 01000	И – 9 – 01001
К – 10 – 01010	Л – 11– 01011	М – 12 – 01100
Н – 13 – 01101	О – 14 – 01110	П – 15 – 01111
Р – 16 – 10000	С – 17 – 10001	Т – 18 – 10010
У – 19 – 10011	Ф – 20 – 10100	Х – 21 – 10101
Ц – 22 – 10110	Ч – 23 –10111	Ш – 24 – 11000
Щ – 25 –11001	ь – 26 – 11010	ы – 27 – 11011
ъ – 28 – 11100	Э – 29 – 11101	Ю – 30 – 11110
	Я – 31 – 11111