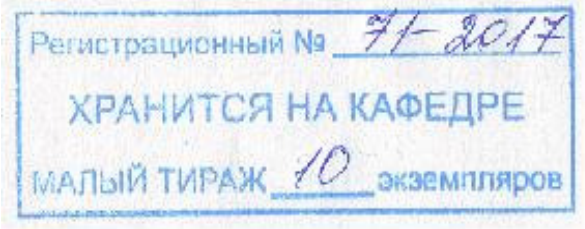
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ имени академика С.П.Королева»
(Самарский университет)

АЛГОРИТМЫ И МЕТОДЫ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ



САМАРА 2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ имени академика С.П.Королева»
(Самарский университет)

АЛГОРИТМЫ И МЕТОДЫ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ

Рекомендовано редакционно-издательской комиссией Института информатики, математики и электроники Самарского университета в качестве методических указаний к лабораторному практикуму по курсам «Защита информации», «Методы и средства защиты информации» и иным курсам аналогичной тематики.

САМАРА 2017

УДК 003.26.09+004.056.55

Составители **О.А.Заякин, К.Е.Климентьев**

Рецензент к.т.н., доц. А.В. Баландин

Классические методы криптографии: метод. указания / сост. О.А.Заякин, К.Е.Климентьев.

Предназначены для студентов, изучающих курсы «Методы и средства защиты информации», «Защита информации» и прочие курсы аналогичной тематики.
Содержат необходимый теоретический и справочный материал для выполнения лабораторных работ. Также могут быть использованы в курсовом и дипломном проектировании.
Подготовлены на кафедре информационных систем и технологий.

УДК 003.26.09+004.056.55

© Самарский университет, 2017

Оглавление

Введение 3
1. Методы шифрования 3
1.1. Шифры на основе сложения букв 4
1.1.1 Шифр Цезаря 5
1.1.2. Шифр Вижинера 5
1.2. Шифр простой замены 6
1.3. Решетка Кардано 7
1.4. Квадрат Полибия 7
1.5. Шифр Вернама 8
1.6. Прочие «классические шифры» 9
2. Контроль целостности данных 10
2.1. Бит четности 10
2.2. Продольно-поперечный контроль четности 11
2.3. Коды Хэмминга 12
2.4. Циклический избыточный код 12
Литература 13
Приложение А. Варианты индивидуальных заданий 14
Приложение Б. Справочные данные 16

Введение

Одним из важных разделов современной системы методов и средств защиты компьютерной информации является *криптография* - наука о шифровании данных. Также предметом изучения криптографии служат методы обеспечения и проверки подлинности сообщений.

Целью лабораторной работы является практическое изучение простейших методов шифрования и проверки подлинности.

Индивидуальные задания см. в Приложении А. Необходимый справочный материал приведен в Приложении Б.

1. Методы шифрования

Шифрование - обратимое преобразование данных в форму, не пригодную для непосредственного восприятия и использования (см. рис. 1.1). Обратная к шифрованию операция называется

расшифровыванием. Попытка расшифрования без знания ключа называется *дешифрованием*.

Ключ шифра – секретный параметр алгоритма шифрования, без знания которого ни шифрование, ни расшифрование не должны быть возможны.

Принцип Кирхгофа (*Керкхоффа*, *Керкхоффена*) гласит: алгоритм шифрования может быть общедоступным, секретным должен быть только ключ.

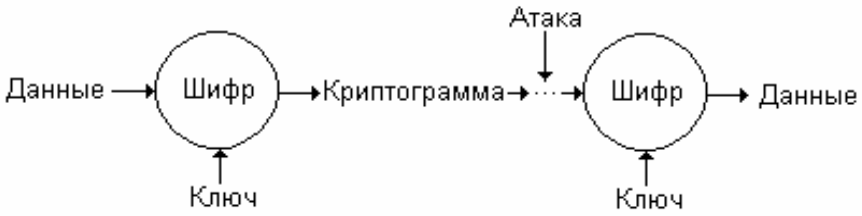


Рис. 1.1. Схема использования шифров

Различные методы шифрования известны с древности. В старинных шифрах ключом могло служить какое-нибудь слово, фраза, таблица подстановок, палка определенного диаметра, карточка с прорезями и т.п. В современных шифрах ключ – целое число, причем настолько большое, что его невозможно подобрать в разумные сроки (например, 100 двоичных или 30 десятичных цифр).

1.1. Шифры на основе сложения букв

Шифры, использующие «линейные» операции над буквами («сложение» и «умножение»), относят к группе «*аффинных*» *шифров*. Их частную разновидность, использующую только «сложение», изучил и описал в XV в. Иоганн Тритемиус (Трисемиус, Трисемий).

Каждой букве алфавита сопоставляется ее номер по порядку - например, буква «А» имеет номер 0, буква «Б» номер 1 и так далее до буквы «Я», которая имеет номер 32. Полную нумерацию букв для русского и латинского алфавитов см. в Приложении Б.

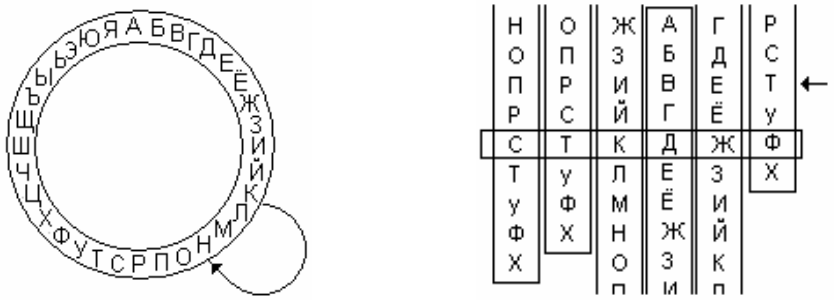
Арифметические операции над буквами («сложение», «умножение» и т.п.) заключаются в действиях над их номерами. Например, «Б» + «В» = «Г». Кроме того, алфавит считается «зацикленным» (см. рис. 1.2, а), так что после буквы «Я» с номером 32 опять идет «А» с номером 0, поэтому, например, «Ю» + «Г» = «Б».

1.1.1 Шифр Цезаря

Метод Гая Юлия Цезаря (относящийся к группе Тритемиуса) основывается на «сложении» всех букв шифруемого сообщения с одной и той же буквой. Фактически, это означает сдвиг всех букв в шифруемом сообщении на одно и то же количество позиций в алфавите. Сам Цезарь использовал в качестве ключа сдвиг на 3. Для латинского алфавита это буква «D» или для русского буква «Г».

Пример шифрования. Пусть слово «КРИПТОГРАФИЯ» зашифровано с ключом 3, тогда буква «К» переходит в «Н» (см. рис. 1.2,а); буква «Р» в «У», и так далее до буквы «Я», которая переходит в «В». Окончательно получаем слово «НУЛТХСЁУГЧЛВ».

Сообщения, закодированные шифром Цезаря, подвергаются дешифровке при помощи простого перебора вариантов ключа.



а) Принцип шифрования б) «Метод полосок»

Рис. 1.2. Шифрование методом Цезаря

Наиболее прост перебор вариантов «методом полосок»: вырезаются несколько (по числу букв в зашифрованном сообщении) бумажных полосок, на них выписываются буквы алфавита, полоски прикладываются друг к другу так, чтобы образовалось зашифрованное слово, тогда на одной из горизонталей автоматически образуется это же слово в расшифрованном виде (см. рис. 1.2,б).

1.1.2. Шифр Вижинера

Шифр Вижинера (относящийся к группе Тритемиуса) является усложненным вариантом шифра Цезаря. На этот раз все буквы в сообщении сдвигаются на разное число позиций, зависящее от ключевого слова или фразы. Если ключ слишком короток, то он «размножается».

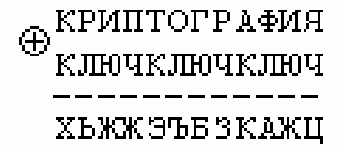


Рис. 1.3. Шифр Вижинера

Пример шифрования. Пусть слово «КРИПТОГРАФИЯ» зашифровано ключом «КЛЮЧ». Определим номера букв ключа в алфавите: буква «К» имеет номер 11, «Л» - 12, «Ю» - 31, «Ч» - 24. Тогда первая буква в шифруемом слове будет сдвинута на 11 позиций (получится «Х») и так далее, а результатом шифрования будет слово «ХЬЖЖЭЪБЗКАЖЦ».

Если шифрование методом Вижинера выполняется именно в описанном виде, то существуют методы, позволяющие определить ключ и дешифровать сообщение.

1.2. Шифр простой замены

Самым известным из «исторических» шифров является «шифр простой замены», который каждую букву одного алфавита заменяет на определенный знак, принадлежащий некоему другому алфавиту. Ключом шифрования служит таблица соответствия, определяющая правила подстановки (пример см. на рис. 1.4).

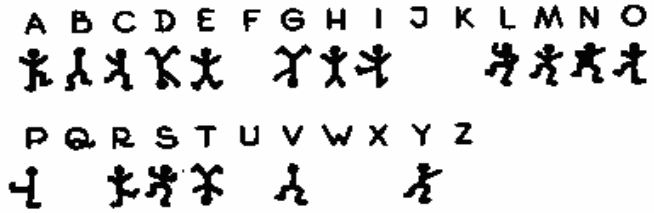


Рис. 1.4. Шифр «Пляшущие человечки»

Дешифрование текстовых данных, преобразованных таким методом, основано на свойстве избыточности естественных языков: частоты встречаемости букв и их сочетаний различны, и эти пропорции постоянны для любых, достаточно больших текстовых выборок. Например, в русском языке частота встречаемости буквы «О» примерно 0.094, «Е» - 0.071, «А» - 0.069, «И» - 0.064... «Н» - 0.057, «Т» - 0.054, «С» - 0.046... «ТО» - 0.12, «СТ» - 0.11... «НН» - 0.04, «СС» - 0.01 и т.д. Это обстоятельство позволяет дешифровать достаточно длинные тексты автоматически, без участия человека.

Пример шифрования. Пусть слово «КРИПТОГРАФИЯ» зашифровано с ключом

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456

тогда результатом шифрования будет слово «LRJQTPDRAVJ6».

Для затруднения дешифровании в таблицы соответствия принудительно вносят неоднозначность, то есть возможность представления одного и того же сочетания разными способами. Так, в одном из русских дипломатических шифров XVIII века буква «Б» кодировалась однозначно - как «588», буква «А» могла кодироваться или как «584», или как «792», а сочетание «БА» могло кодироваться либо как «588584», либо как «588792», либо как отдельное число «517».

1.3. Решетка Кардано

Решетка Кардано (или *поворотная решетка*) - остроумная и красивая реализация перестановочного шифра, которую можно увидеть, например, в титрах фильма «Шерлок Холмс и доктор Ватсон». В прямоугольной карточке вырезаются отверстия одинакового размера, карточка накладывается на лист бумаги и в прорези поочередно вписываются буквы шифруемого сообщения. После заполнения первой группы отверстий карточка поворачивается или переворачивается, и заполнение карточки буквами продолжается, так повторяется несколько раз.

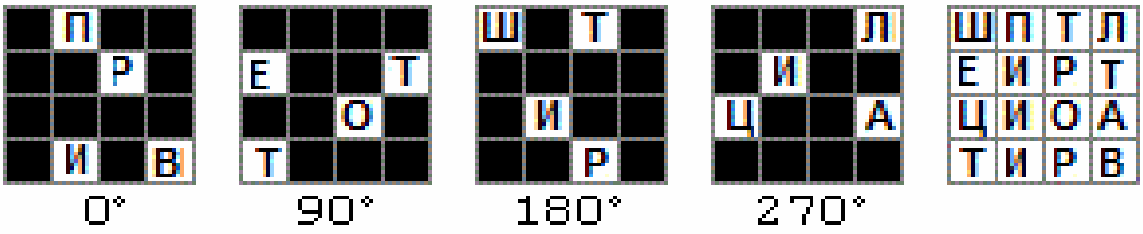


Рис. 1.5. Пример применения квадратной решетки Кардано

При исходном размещении отверстий на карточке важно, чтобы при поворотах и переворотах отверстия не совмещались бы друг с другом. Оставшиеся пустыми клетки заполняются случайными буквами. Расшифрование сообщения выполняется при помощи наложения этой же карточки, служащей ключом.

Дешифрование подобных шифров выполняется перебором вариантов на ЭВМ.

1.4. Квадрат Полибия

Так называется метод придумывания и легкого запоминания «перемешанных» алфавитов, лежащих в основе многих шифров.

Шаг 1. Алфавит «сокращается» так, чтобы все его буквы можно было разместить в прямоугольной таблице. Например, в латинском алфавите полагается «I»=«J», а оставшиеся 25 букв можно разместить в квадрате 5x5. В русском алфавите можно положить, что «И»=«Й», «Е»=«Ё» и «Ь»=«Ъ», а оставшиеся 30 букв можно разместить в таблицах 5x6 или 6x5.

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

Рис. 1.6. Квадрат Полибия

Шаг 2. Выбирается и запоминается «ключ» - слово, которое: 1) содержит разные буквы и 2) его можно целиком разместить в первой строке таблицы. Например: «ШЛЯПА».

Шаг 3. Ключ размещается в первой строке, а оставшиеся буквы выписываются в таблице в прежнем порядке. «Перемешанный» алфавит готов!

«Квадрат Полибия» можно использовать в шифре «простой замены». Например, в соответствии с рис. 1.6 получается ключ.

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
ШЛЯПАБВГДЕЖЗИКМНОРСТУФХЦЧЩЬЫЭЮ

Так же «квадрат Полибия» можно использовать в шифре «простой замены», заменяя каждую букву ее «соседкой» (например, взятой «сверху-справа»). При этом строки и столбцы так же считаются «зацикленными», например «сверху-справа» от буквы «А» лежит буква «Щ» (см. рис. 1.6).

«Квадрат Полибия» с пронумерованными строками и столбцами (см. рис. 1.6) можно использовать для замены каждой буквы ее «координатами». Например, буква «К» имеет координаты 34 (см. рис. 1.6), буква «Р» координаты 43 и т.д., а слово «КРИПТОГРАФИЯ» будет зашифровано как «34 43 33 14 45 42 23 43 15 52 33 13».

1.5. Шифр Вернама

Этот метод шифрования был разработан в начале XX в. Дж. Вернамом, инженером американской компании A&T Labs, специализирующейся на производстве телеграфного оборудования. Он основан на двоичном представлении знаков передаваемого сообщения. Ключ шифрования представлял собой закольцованную

вращающуюся «ленту», на которой в случайном порядке размещались точки и тире (фактически, нули и единицы). Устройство шифрования воспринимало поток нулей и единиц шифруемого сообщения, одновременно считывало со своей ленты биты ключа и генерировало выходной поток по правилу логической функции «исключающее ИЛИ» (см. табл. 1.1).

Таблица 1.1 – Правило «сложения» битов

Бит данных	Бит ключа	Бит результата
0	0	0
0	1	1
1	0	1
1	1	0

На приемном конце располагалось устройство расшифрования, использующее тот же ключ и ту же логическую операцию (см. рис. 1.6).

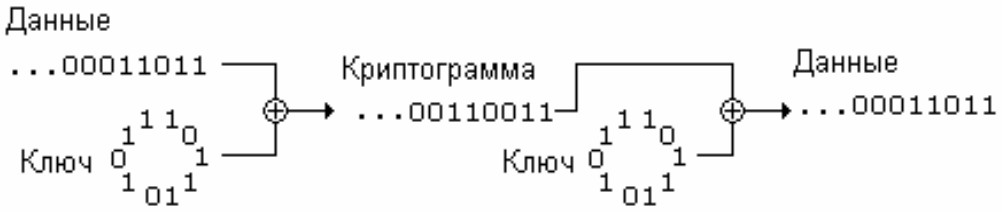


Рис. 1.6. Шифр Вернама

Пример шифрования. Пусть слово «МИР» шифруется с ключом 10. Представим буквы слова (в кодировке DOS-866, см. Приложение Б) и ключ в двоичной форме и сложим их по модулю 2:

```
М=8Ch          И=88h          Р=90h
10001100       10001000       10010000
10101010       10101010       10101010
-----------------------------------
00100110       00100010       00111010
26h            22h            3Ah
```

1.6. Прочие «классические шифры»

Начиная с глубокой древности и вплоть до середины XX в. было придумано и использовано множество «классических» шифров. С ними можно ознакомиться по литературным источникам [1-9].

В настоящее время все они легко «вскрываются» с использованием средств вычислительной техники, однако некоторые идеи, лежащие в их основе, используются и в современных шифрах.

1.7. Абсолютно стойкие шифры

При определенных условиях шифры «Вижинера» и «Вернама» являются абсолютно стойкими ко «взлому». Не зная ключа, их невозможно дешифровать даже теоретически. Вот эти условия:

1) длина ключа равна длине шифруемого сообщения, «размножение» ключа запрещено;

2) все знаки ключа строго случайны, то есть, не составляют какое-либо слово, фразу и не вычисляются один из другого по какому-нибудь алгоритму;

3) ключ применяется однократно, а после использования уничтожается.

Такие шифры называются «*одноразовыми шифроблокнотами*» или «*одноразовыми кодовыми книгами*».

2. Контроль целостности данных

При управлении целостностью данных приходится решать задачи двух типов:

- обнаружение искажения данных;
- если данные искажены, то восстановление их в исходном виде.

Общий подход заключается в том, что для блока защищаемых данных дважды рассчитывается некоторая контрольная величина (отдельный бит или число): первый раз до выполнения какой-либо «опасной» операции (например, до передачи по каналу связи), и второй раз - после. Оба значения сравниваются, и если они не совпадают, то делается вывод о произошедших искажениях.

2.1. Бит четности

Контрольный «*бит четности*» (или «*бит паритета*») широко используется в технике связи. Защищаемые данные рассматриваются как цепочка битов определенной длины, а контрольный бит четности рассчитывается как результат сложения всех битов блока по модулю 2.

Например, пусть исходные данные: 11100100, тогда результат: $1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$.

Если добавить рассчитанный бит к исходной цепочке и вновь просуммировать по модулю 2, то должен получиться 0. Если этого не происходит, то делается вывод об искажении либо цепочки битов, либо контрольного бита.

2.2. Продольно-поперечный контроль четности

Продольно-поперечный контроль четности позволяет не только обнаруживать одиночные ошибки, но и избавляться от них. Защищаемые данные рассматриваются как группа битов, расположенных прямоугольником. Для каждой строки и каждого столбца рассчитывается бит четности, вся совокупность которых рассматривается как контрольное число. Например, пусть исходные данные: 1001110011100101, тогда их можно расположить в прямоугольной таблице 4x4 и рассчитать биты четности:

```
1001 | 0
1100 | 0
1110 | 1
0101 | 0
------
1110
```

Контрольное число: 11100010.

Пусть в процессе передачи данных искажение произошло в 11-м по счету бите: 1001110011**0**00101, тогда контрольное число изменится:

```
1001 | 0
1100 | 0
11*0* | *0*
0101 | 0
------
11*0*1
```

Новое контрольное число: 11**0**100**0**0.

Итак, если контрольные числа, рассчитанные до передачи данных и после нее не совпадают, то делается вывод об искажении цепочки битов. Кроме того, по номерам битов, изменивших свои значения в контрольном числе, можно определить, какой бит данных был искажен, - и восстановить его правильное значение.

Контрольное число, которое позволяет не только обнаружить ошибку, но и исправить ее, называется *синдромом*.

2.3. Коды Хэмминга

Коды Хэмминга позволяют не только обнаруживать одиночные ошибки, но и избавляться от них. Основное преимущество перед другими методами – оптимальность, то есть, коды Хэмминга используют самые короткие контрольные коды.

Для блока данных из N битов контрольный *синдром* имеет длину $M=Log_2(N)+1$ битов. Биты данных нумеруются, начиная с 1. Синдром представляет собой результат сложения «по модулю 2» номеров тех битов в блоке данных, значение которых равно 1. На приемном конце контрольный код рассчитывается вновь. Если исходный и новый не совпадают, то результат их сложения «по модулю 2» дает номер искаженного бита.

Пример. Пусть передается блок данных: 11100100. Номера «единичных» битов: 3, 6, 7, 8.

Синдром: 3⊕6⊕7⊕8=0011⊕0110⊕0111⊕1000=1010.

Искаженный блок данных: 1110**1**100.

Синдром для искаженного блока данных:

3⊕4⊕6⊕7⊕8=0011⊕0100⊕0110⊕0111⊕1000=1110.

Сложение контрольных кодов: 1010⊕1110=0100 - номер искаженного бита.

Существуют и другие разновидности кодов Хэмминга. Например, одна из них предполагает размещение битов синдрома между битами защищаемых данных.

2.4. Циклический избыточный код

Циклический избыточный код (CRC - cyclic redundancy code) очень широко используется в вычислительной технике. Он основан на представлении блока данных в виде непрерывного полинома с битовыми коэффициентами. В качестве контрольного кода используется остаток от деления этого полинома на более короткий «*порождающий*» *полином*, обычно длиной N=4, 8, 12, 16 или 32 бита. Техника деления: 1) в конец блока данных добавляется N-1 нулевых битов; 2) вместо арифметического деления используется операция «сложение по модулю 2»; 3) фрагмент исходного полинома длиной N битов, с которым производится сложение «порождающего» полинома,

каждый раз сдвигается влево до тех пор, пока его (фрагмента) старший бит не окажется равен 1.

Пример. Исходные данные: 1010. «Порождающий» полином: 1011. Дополнительные биты: 000.

```
1010000 | 1011
1011
0001000
   1011
   0011 ← CRC
```

На практике используются стандартные порождающие полиномы. Например, методу расчета «CRC-32» соответствует полином $1EDB88320_{16}$. Кроме того, стандартные алгоритмы расчета CRC нередко содержат «лишние» операции (например, инвертирование всех битов результата), что не влияет на способность обнаруживать искажения, но упрощает аппаратную реализацию алгоритма.

Литература

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.
2. Аршинов М.А., Садовский Л.Е. Коды и математика (рассказы о кодировании).- М.: Наука, 1983. – 144 с.
3. Гомес Ж. Математики, шпионы и хакеры. Кодирование и криптография. – М.: ДеАгостини, 2014. – 144 с.
4. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. Популярно о современной криптографии. – М.: ТЕИС, 1994. – 69 с.
5. Жданов О.Н., Куденкова И.А. Криптоанализ классических шифров. – Красноярск: Изд-во. Сибирского госуд. аэрокосм. ун-та, 2008. – 107 с.
6. Канн Д. Взломщики кодов. – Центрполиграф, 2000. – 480 с.
7. Перельман Я.И. Живая математика. – М.: Наука, 1967. – 160 с.
8. Сингх С. Книга шифров. Тайная история шифров и расшифровки. – АСТ, Астрель, 2007. – 446 с.
9. Соболева Т.А. История шифровального дела в России. – М.: ОЛМА-ПРЕСС, 2002. – 512 с.

Приложение А. Варианты индивидуальных заданий

Задание А.1. Дешифровать слово, зашифрованное шифром Цезаря

№	Слово	№	Слово
1	ЧХПДЖЛГКП	5	БТУСПВМЁНБ
2	УИУМСАИФОД	6	ХГУХЛРНГ
3	ЧУФНТЕСЁШХ	7	КЧФКРН
4	ЕХООКВТВГКМ	8	ДВЁЖОЖМХО

Задание А.2. Дешифровать слово, зашифрованное шифром Вернама (длина ключа 2 бита). Все числа 16-ричные.

№	Слово	№	Слово
1	47 4B 4D 44 4F 50 43 5B	**5**	62 75 74 7A 75 6D 77 75 7F
2	B8 B4 BE A7 BA A5 BA B1	**6**	08 1E 0B 1A 0D 0F 1E 0C
3	61 75 65 7B 79 7B	**7**	6B 64 61 64 78 79 6E 79
4	10 14 0C 1E 13 1E 0B	**8**	7B 7F 75 6D 77 74 63

Задание А.3. Дешифровать фразу, зашифрованную методом простой замены.

Вариант 1.

```
T7M7G6 FKSV7LLQ M7G72C4XAPSR QT IQMY4IA 2Q FAIHNI4 4 QWGATLQ.
```

Вариант 2.

```
HJ 4 7SVHL TNS TW4H6LI 64 1 PT7 6T 12LFJTDK, 1J74 C6JTFT
XFSNS DPSHZ4ESNS PSFJ.
```

Вариант 3.

```
Z W ON4TL1ZWV2X TZVZO2 17E7V2Q B7 MO2 A76SZO, 7JOSQ 6N 1Q2KZ
EN Z 4BN6NQ: «M7Q7E2D, 232MN, 4NM737E7B T7 M7X 67Q7T7X»!
```

Вариант 4.

```
KZBD KQZCMRS BX PKS2VKB WCQSBEQZMK, R IC TNKVBEVRB FKEC KWC
WB ZKS2YK Q6OBSC QK1NCWRZ2 BFK, WK B3B R TNR6OWK5RZ2.
```

Вариант 5.

```
R4T7UHQ4 KAUHQ 347T7IM 2XU1U2K XMKJQSQ 41U, Q U7 2MS4WV41U
VK2M UX YAUTGYMSTB AMXOV4, J42 41U RQIU7XU4.
```

Вариант 6.

```
H YTMTN TD YTNT5R1 NDL ILPMH QTL-QRQHL 2L1R.
```

Вариант 7.

```
SP R4UMBI ISOYDS S LMESRB, E13SRB, PM5NEB, M Q UBZIMJ S
KBTDSF1TIPSU TO45BPNN EBONDSW NRBB, S ASREN3B.
```

Вариант 8.

```
Q2CW VX2Z FY14X 1VC2ZLR Y6C FYFHYLIXD FHMKFM4MDZ TX6B W 1VYX7
PLWX, C VYD QDY IE 6MWCW 6X VJY2MD V TYM F4C6R.
```

Задание Б.1. Рассчитать бит четности для указанного набора данных. Все числа 16-ричные.

№	Данные	№	Данные
1	12345678	5	DEADBABE
2	1234ABCD	6	1020F00D
3	ABCDEF12	7	5A5AFF44
4	D0CF11E0	8	10203040

Задание Б.2. Рассчитать CRC для указанных данных и порождающего полинома 1011. Все числа двоичные.

№	Данные	№	Данные
1	11001	5	10011
2	11000	6	11111
3	10111	7	11110
4	10101	8	11100

Задание В.1. Восстановить слово, защищенное продольно-поперечным контролем четности. Кодировка неизвестна. Все числа 16-ричные. В каждой строке одна буква. Порядок нумерации битов синдрома:

```
******** B
******** A
******** 9
******** 8
76543210
```

№	Данные	Синдром	№	Данные	Синдром
1	90 93 88 80	093	**5**	8F 92 87 8E	158
2	8D 8C 83 80	003	**6**	99 87 8A 80	167
3	CD CE C1 C0	00C	**7**	8A 8F 86 80	02B
4	F1 FA FB ED	198	**8**	8F 9D 92 80	02B

Задание В.2. Восстановить слово, защищенное кодом Хэмминга. Для каждой буквы свой 4-битовый синдром. Все числа 16-ричные. Кодировка неизвестна.

№	Данные	Синдромы	№	Данные	Синдромы
1	91 8E 90	D D F	**5**	85 93 81	8 E 9
2	CC CE D3	9 A B	**6**	85 8E 8A	9 D E
3	8F 93 8E	C E C	**7**	99 85 9F	9 A 9
4	93 95 8C	E F D	**8**	8E 8A 8C	D E D

Приложение Б. Справочные данные

Частоты встречаемости русских букв

0	1	2	3	4	5	6	7	8	9	10
А	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**
0.069	0.013	0.038	0.014	0.024	0.071	0.071	0.007	0.016	0.064	0.010
11	12	13	14	15	16	17	18	19	20	21
К	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**
0.029	0.039	0.027	0.057	0.094	0.026	0.042	0.046	0.054	0.023	0.003
22	23	24	25	26	27	28	29	30	31	32
Х	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
0.008	0.005	0.012	0.006	0.004	0.001	0.015	0.013	0.002	0.005	0.017

Частоты встречаемости латинских букв

0	1	2	3	4	5	6	7	8	9	10	11	12
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0.084	0.015	0.031	0.040	0.125	0.023	0.019	0.055	0.073	0.002	0.007	0.041	0.002
13	14	15	16	17	18	19	20	21	22	24	24	25
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0.071	0.076	0.020	0.001	0.061	0.065	0.039	0.027	0.010	0.019	0.002	0.017	0.001

Кодировка ASCII

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
40		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z					

Кодировка Win-1251

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
A0									Ё							
								...								
C0	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
D0	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Кодировка KOI-8

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
B0			Ё													
								...								
E0	Ю	А	Б	Ц	Д	Е	Ф	Г	Х	И	Й	К	Л	М	Н	О
F0	П	Я	Р	С	Т	У	Ж	В	Ь	Ы	З	Ш	Э	Щ	Ч	Ъ

Кодировка DOS-866

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
80	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
90	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
								...								
F0	Ё															

Представления чисел в разных системах счисления

10	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
2	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111
8	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Учебное издание

АЛГОРИТМЫ И МЕТОДЫ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ

Методические указания

Составители О.А.Заякин, К.Е.Климентьев

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ имени академика С.П.Королева»
(Самарский университет)
443086, САМАРА, МОСКОВСКОЕ ШОССЕ, 34

443086, Самара, Московское шоссе, 34.