

**Автономная некоммерческая организация  
профессионального образования  
«ПЕРМСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»  
(АНО ПО «ПГТК»)**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
МЕЖДИСЦИПЛИНАРНОГО КУРСА  
МДК 02.05 «Безопасность информационных систем»**

для студентов специальности

**09.02.03 Программирование в компьютерных системах**

(код и наименование специальности)

Квалификация выпускника

**Техник-программист**

(базовая подготовка)

Форма обучения

**Очная**

**Пермь, 2020 г**

Методические рекомендации по изучению междисциплинарного курса МДК 02.05 «Безопасность информационных систем» предназначены для студентов и преподавателей АНО ПО «ПГТК». Методические указания определяют ориентиры и способствуют более обстоятельному усвоению программного материала, организации самостоятельного процесса изучения учебного предмета обучающимися по специальности Программирование в компьютерных системах.

Данные методические рекомендации помогут организовать самостоятельную деятельность студентов на основе деятельного и компетентного подходов к обучению, что соответствует ФГОС СПО по специальности 09.02.03 Программирование в компьютерных системах.

Автор-составитель: Тимохова Н.А., ст. преподаватель

Утверждено на заседании кафедры математических и естественно-научных дисциплин, протокол № 6 от «6» февраля 2020 г.

Рекомендованы к утверждению педагогическим советом АНО ПО «ПГТК» (протокол от «21» февраля 2020 г. № 3).

## Содержание

|                               |    |
|-------------------------------|----|
| Введение .....                | 4  |
| Практическая работа № 1 ..... | 5  |
| Практическая работа №2 .....  | 8  |
| Практическая работа №3 .....  | 15 |
| Практическая работа № 4 ..... | 23 |
| Практическая работа № 5 ..... | 26 |

## **Введение**

Целью данного практикума является реализация государственных требований к минимуму содержания и уровню подготовки выпускников по МДК 02.05 «Безопасность информационных систем».

Данный практикум может быть использован преподавателями для проведения практических занятий по темам «Идентификация и аутентификация субъектов» и «Криптографические средства защиты информации».

Каждая практическая работа по курсу содержит название, цели работы, теоретические сведения, задания для самостоятельной работы. В каждой работе подробно описан ход выполнения работы.

Практические работы выполняются студентами индивидуально.

Практическая работа выполняется согласно заданию. Результат работы представляется студентом преподавателю.

По ходу выполнения работы при возникновении вопросов студент может получить консультацию у преподавателя или самостоятельно воспользоваться лекционным материалом.

Результат выполнения практической работы оценивается по пятибалльной шкале.

## **Формируемые компетенции практических работ**

Общие компетенции (ОК):

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональные компетенции (ПК):

ПК 2.1 Разрабатывать объекты базы данных.

ПК 2.2 Реализовывать базу данных в конкретной системе управления базами данных (далее - СУБД).

ПК 2.3 Решать вопросы администрирования базы данных.

ПК 2.4 Реализовывать методы и технологии защиты информации в базах данных.

### **Практическая работа № 1**

**Тема:** Количественная оценка стойкости парольной защиты»

Порядок выполнения работы

1. Записать в тетради тему и цель работы.
2. Ознакомиться с краткими теоретическими сведениями.
3. Выполнить задания
4. Ответить на контрольные вопросы.

#### **Теоретические сведения**

Подсистемы идентификации и аутентификации пользователя играют очень важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской

аутентификации. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

#### К паролю

1. Минимальная длина пароля должна быть не менее 6 символов.
2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).
3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

#### К подсистеме парольной аутентификации.

1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.
2. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (как правило, не более 3).
3. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

### **Количественная оценка стойкости парольной защиты**

Пусть  $A$  – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то  $A=26$ ).

$L$  – длина пароля.

$S = A^L$  – число всевозможных паролей длины  $L$ , которые можно составить из символов алфавита  $A$ .

$V$  – скорость перебора паролей злоумышленником.

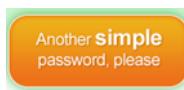
$T$  – максимальный срок действия пароля.

Тогда, вероятность  $P$  подбора пароля злоумышленником в течении срока его действия  $V$  определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

### Задание к работе

1. Откройте программу генерации паролей, которая находится на сайте <http://www.dinopass.com/>



2. При помощи кнопки сгенерируйте 15 паролей различной длины и запишите их в тетрадь
3. Для каждого пароля рассчитать оценку стойкости парольной защиты по приведенной формуле с использованием таблицы (см. приложение 1), согласно своего варианта.

### Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Как определить вероятность подбора пароля злоумышленником в течении срока его действия?
3. Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

### Приложение 1.

| Вариант | V                | T        |
|---------|------------------|----------|
| 1       | 15 паролей/мин   | 2 недели |
| 2       | 3 паролей/мин    | 10 дней  |
| 3       | 10 паролей/мин   | 5 дней   |
| 4       | 11 паролей/мин   | 6 дней   |
| 5       | 100 паролей/день | 12 дней  |
| 6       | 10 паролей/день  | 1 месяц  |
| 7       | 20 паролей/мин   | 3 недели |
| 8       | 15 паролей/мин   | 20 дней  |
| 9       | 3 паролей/мин    | 15 дней  |
| 10      | 10 паролей/мин   | 1 неделя |
| 11      | 11 паролей/мин   | 2 недели |
| 12      | 100 паролей/день | 10 дней  |
| 13      | 10 паролей/день  | 5 дней   |
| 14      | 20 паролей/мин   | 6 дней   |
| 15      | 15 паролей/мин   | 12 дней  |
| 16      | 3 паролей/мин    | 1 месяц  |
| 17      | 10 паролей/мин   | 3 недели |
| 18      | 11 паролей/мин   | 20 дней  |
| 19      | 100 паролей/день | 15 дней  |
| 20      | 10 паролей/день  | 1 неделя |
| 21      | 20 паролей/мин   | 2 недели |
| 22      | 15 паролей/мин   | 10 дней  |
| 23      | 3 паролей/мин    | 5 дней   |

## Практическая работа №2

**Тема:** «Шифрование информации»

**Цель работы:** изучение простейших методов криптографической защиты информации и закрепление навыков работы в программной среде Microsoft Excel.

### План работы:

1. Изучение теоретического материала.
2. Зашифровывание своих фамилии и имени, используя метод Цезаря и среду Microsoft Excel.
3. Расшифровывание фразы с карточки, используя метод Цезаря и среду Microsoft Excel.
4. Зашифровать, расшифрованную в п.4 фразу методом перестановки с ключом. В качестве ключа взять свою фамилию.
5. Ответить устно на вопросы.
6. Предъявить работу преподавателю.

### Теоретические сведения:

**Система шифрования Цезаря** – частный случай шифра простой замены. Метод основан на замене каждого символа сообщения (открытого текста) на другой символ того же алфавита, путем смещения от исходного на  $k$  позиций (получаем закрытый текст). Величина  $k$  называется ключом шифра (ключ – это информация, необходимая для беспрепятственного дешифрования информации). Ключ в методе Цезаря – целое число. Если поставить в соответствие каждому символу используемого алфавита число, то процесс шифрования будет проходить по формуле:

$$y_i = (x_i + k) \bmod n,$$

где  $x_i$  – номер  $i$ -того символа в открытом тексте,  $y_i$  – номер  $i$ -того символа в закрытом тексте,  $k$  – ключ,  $n$  – число символов в алфавите. Операция  $\bmod$  – это

взятие остатка от деления одного числа на другое (например:  $5 \bmod 2 = 1$ ,  $10 \bmod 5 = 0$ ,  $20 \bmod 7 = 6$ ).

Дешифрование (расшифровывание) будет проходить по формуле

$$x_i = (y_i + (n - k)) \bmod n.$$

### Пример.

Зашифруем методом Цезаря с ключом  $k=7$  слово «шифр».

Будем использовать русский алфавит без буквы ё, где букве А соответствует число 0, а следовательно букве Я – 31. Т.е.  $n=32$ .

Поставим в исходном слове в соответствие каждой букве число:

$$\text{ш} \rightarrow 24 = x_1$$

$$\text{и} \rightarrow 8 = x_2$$

$$\text{ф} \rightarrow 20 = x_3$$

$$\text{р} \rightarrow 16 = x_4$$

$$\text{Тогда } y_1 = (x_1 + k) \bmod 32 = (24 + 7) \bmod 32 = 31 \bmod 32 = 31 \rightarrow \text{я}$$

$$y_2 = (x_2 + k) \bmod 32 = (8 + 7) \bmod 32 = 15 \bmod 32 = 15 \rightarrow \text{п}$$

$$y_3 = (x_3 + k) \bmod 32 = (20 + 7) \bmod 32 = 27 \bmod 32 = 27 \rightarrow \text{ы}$$

$$y_4 = (x_4 + k) \bmod 32 = (16 + 7) \bmod 32 = 23 \bmod 32 = 23 \rightarrow \text{ч}$$

Таким образом, получили слово «япыч»

### Дешифрование.

Для дешифрования необходимо каждому символу слова «япыч» поставить в соответствие число:

$$\text{я} \rightarrow 31 = y_1$$

$$\text{п} \rightarrow 15 = y_2$$

$$\text{ы} \rightarrow 27 = y_3$$

$$\text{ч} \rightarrow 23 = y_4$$

$$\text{Тогда } x_1 = (y_1 + (32 - k)) \bmod 32 = (31 + (32 - 7)) \bmod 32 = 56 \bmod 32 = 24 \rightarrow \text{ш}$$

$$x_2 = (y_2 + (32 - k)) \bmod 32 = (15 + 25) \bmod 32 = 40 \bmod 32 = 8 \rightarrow \text{и}$$

$$x_3 = (y_3 + (32 - k)) \bmod 32 = (27 + 25) \bmod 32 = 52 \bmod 32 = 20 \rightarrow \text{ф}$$

$$x_4 = (y_4 + (32 - k)) \bmod 32 = (23 + 25) \bmod 32 = 48 \bmod 32 = 16 \rightarrow \text{р}$$

Получили слово «шифр», следовательно шифрование было выполнено правильно.

**Шифр перестановки с ключом** – является одним из многочисленных видов шифров перестановки (символы исходного сообщения переставляются по определенным законам).

Для перестановки с ключом выбирается ключ – любое слово. Символы ключа нумеруются в порядке следования их в алфавите. Строится таблица, в которой количество столбцов равно количеству букв в ключе. Исходный текст вместе с пробелами и знаками препинания записывается в эту таблицу. Если последняя строка заполнена не полностью, до до конца строки записываются любые символы («пустышки»). Затем текст переписывается по столбцам, учитывая их нумерацию согласно ключу.

### Пример.

Выберем в качестве ключа слово «информация». Пронумеруем ключ (первая, из имеющихся в ключе, в алфавите буква А, следовательно ей присваивается номер 1; следующая по алфавиту буква И, следовательно первая буква И будет иметь номер 2, а вторая – 3; далее идет буква М, ей присваиваем номер 4 и т.д.):

|   |   |   |   |   |   |   |   |   |    |
|---|---|---|---|---|---|---|---|---|----|
| и | н | ф | о | р | м | а | ц | и | я  |
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |

Зашифруем пословицу: От умного научишься, от глупого разучишься.

Запишем ее в таблицу под ключом. Оставшиеся ячейки до конца строки заполняют «пустышками».

|   |   |   |   |   |   |   |   |   |    |
|---|---|---|---|---|---|---|---|---|----|
| и | н | ф | о | р | м | а | ц | и | я  |
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |
| о | т |   | у | м | н | о | г | о |    |
| н | а | у | ч | и | ш | ь | с | я | ,  |
|   | о | т |   | г | л | у | п | о | г  |
| о |   | р | а | з | у | ч | и | ш | ь  |
| с | я | а | б | в | г | д | е | ж | з  |

Переписываем столбцы, учитывая их номер:

Оьучдон осояошжншлугтао яуч абмигзв утрагспие ,гъз

Для дешифрования зашифрованный текст записывается в таблицу по столбцам, учитывая их номер.

### Задание к работе.

1. Ознакомьтесь с теоретической частью практической работы.
2. Загрузите программу Microsoft Excel.
3. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).

|    | А | В  | С | Д |
|----|---|----|---|---|
| 1  | а | 0  | а |   |
| 2  | б | 1  | б |   |
| 3  | в | 2  | в |   |
| 4  | г | 3  | г |   |
| 5  | д | 4  | д |   |
| 6  | е | 5  | е |   |
| 7  | ж | 6  | ж |   |
| 8  | з | 7  | з |   |
| 9  | и | 8  | и |   |
| 10 | й | 9  | й |   |
| 11 | к | 10 | к |   |
| 12 | л | 11 | л |   |
| 13 | м | 12 | м |   |
| 14 | н | 13 | н |   |
| 15 | о | 14 | о |   |
| 16 | п | 15 | п |   |
| 17 | р | 16 | р |   |
| 18 | с | 17 | с |   |
| 19 | т | 18 | т |   |
| 20 | у | 19 | у |   |
| 21 | ф | 20 | ф |   |
| 22 | х | 21 | х |   |
| 23 | ц | 22 | ц |   |
| 24 | ч | 23 | ч |   |
| 25 | ш | 24 | ш |   |
| 26 | щ | 25 | щ |   |
| 27 | ь | 26 | ь |   |
| 28 | ы | 27 | ы |   |
| 29 | ь | 28 | ь |   |
| 30 | э | 29 | э |   |
| 31 | ю | 30 | ю |   |
| 32 | я | 31 | я |   |

4. Переименуйте лист1 в Алфавит.
5. На втором листе электронной книги запишите название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключа можно взять любым и обязательно его значение

записать в отдельную ячейку (B5). В столбец S, начиная с 8 строки, впишите фамилию и имя, каждую букву в отдельной ячейке.

|    | A | B | C | D  | E | F | G |
|----|---|---|---|----|---|---|---|
| 1  |   |   |   |    |   |   |   |
| 2  |   |   |   |    |   |   |   |
| 3  |   |   |   |    |   |   |   |
| 4  |   |   |   |    |   |   |   |
| 5  |   |   |   |    |   |   |   |
| 6  |   |   |   |    |   |   |   |
| 7  | S | X | Y | S1 |   |   |   |
| 8  | и |   |   |    |   |   |   |
| 9  | в |   |   |    |   |   |   |
| 10 | а |   |   |    |   |   |   |
| 11 | н |   |   |    |   |   |   |
| 12 | о |   |   |    |   |   |   |
| 13 | в |   |   |    |   |   |   |
| 14 | а |   |   |    |   |   |   |
| 15 | н |   |   |    |   |   |   |
| 16 | д |   |   |    |   |   |   |
| 17 | р |   |   |    |   |   |   |
| 18 | е |   |   |    |   |   |   |
| 19 | й |   |   |    |   |   |   |
| 20 |   |   |   |    |   |   |   |

6. В столбце X должны быть числовые значения символов из столбца S. Эти значения хранятся на листе Алфавит. Чтобы получить их, можно воспользоваться функцией **ВПР** (категория – ссылки и массивы). Встаем в ячейку B8 и вызываем функцию ВПР. Заполняем ее окно следующим образом:

**Аргументы функции**

**ВПР**

Искомое\_значение: A8 = "и"

Таблица: Алфавит!\$A\$1:\$B\$32 = {"а";0;"б";1;"в";2;"г";3;"д";4;"е";...}

Номер\_столбца: 2 = 2

Интервальный\_просмотр: ЛОЖЬ = ЛОЖЬ

= 8

Ищет значение в крайнем левом столбце таблицы и возвращает значение ячейки, находящейся в указанном столбце той же строки. По умолчанию таблица должна быть отсортирована по возрастанию.

**Интервальный\_просмотр** логическое значение, определяющее, точно (ЛОЖЬ) или приблизительно (ИСТИНА или отсутствие значения) должен производиться поиск в первом столбце (отсортированном по возрастанию).

Значение: 8

[Справка по этой функции](#)

OK Отмена

7. Растянуть формулу вниз до конца таблицы.
8. В ячейку C8 (столбец Y) записывается формула для шифрования. Исходная формула метода Цезаря имеет вид:  $y_i = (x_i + k) \mod n$ . Операции mod в Excel соответствует функция **ОСТАТ(число; делитель)**. В нашем случае **число** – это  $(x_i + k)$ , а **делитель** – 32. Т.е. функция **ОСТАТ** будет иметь вид **=ОСТАТ((B8+\$B\$5);32)**.
9. Эту формулу необходимо растянуть вниз до конца таблицы.
10. В ячейку D8 (столбец S1) опять записываем функцию **ВПР**, которая по числу Y найдет букву. Эта функция будет выглядеть следующим образом:

**Аргументы функции**

**ВПР**

Искомое\_значение: С8 = 13

Таблица: Алфавит!\$B\$1:\$C\$32 = {0;"а";1;"б";2;"в";3;"г";4;"д";5;"е"...}

Номер\_столбца: 2 = 2

Интервальный\_просмотр: ЛОЖЬ = ЛОЖЬ

= "н"

Ищет значение в крайнем левом столбце таблицы и возвращает значение ячейки, находящейся в указанном столбце той же строки. По умолчанию таблица должна быть отсортирована по возрастанию.

**Интервальный\_просмотр** логическое значение, определяющее, точно (ЛОЖЬ) или приближенно (ИСТИНА или отсутствие значения) должен производиться поиск в первом столбце (отсортированном по возрастанию).

Значение: н

[Справка по этой функции](#)

OK Отмена

11. Окончательно таблица должна выглядеть следующим образом:

|    | A        | B        | C        | D         | E | F | G                      |
|----|----------|----------|----------|-----------|---|---|------------------------|
| 1  |          |          |          |           |   |   | <b>Шифр Цезаря</b>     |
| 2  |          |          |          |           |   |   |                        |
| 3  |          |          |          |           |   |   | <b>1. Зашифрование</b> |
| 4  |          |          |          |           |   |   |                        |
| 5  |          |          | k= 5     |           |   |   |                        |
| 6  |          |          |          |           |   |   |                        |
| 7  | <b>S</b> | <b>X</b> | <b>Y</b> | <b>S1</b> |   |   |                        |
| 8  | и        | 8        | 13       | н         |   |   |                        |
| 9  | в        | 2        | 7        | з         |   |   |                        |
| 10 | а        | 0        | 5        | е         |   |   |                        |
| 11 | н        | 13       | 18       | т         |   |   |                        |
| 12 | о        | 14       | 19       | у         |   |   |                        |
| 13 | в        | 2        | 7        | з         |   |   |                        |
| 14 | а        | 0        | 5        | е         |   |   |                        |
| 15 | н        | 13       | 18       | т         |   |   |                        |
| 16 | д        | 4        | 9        | й         |   |   |                        |
| 17 | р        | 16       | 21       | х         |   |   |                        |
| 18 | е        | 5        | 10       | к         |   |   |                        |
| 19 | й        | 9        | 14       | о         |   |   |                        |
| 20 |          |          |          |           |   |   |                        |

Запишите полученный закрытый текст (столбец S1) в тетрадь.

12. Рядом приготовьте место для дешифрования информации. Получите у преподавателя карточку с закрытым текстом и впишите его в столбец S1 новой таблицы.

|    | A        | B        | C        | D         | E | F | G | H | I | J | K |
|----|----------|----------|----------|-----------|---|---|---|---|---|---|---|
| 1  |          |          |          |           |   |   |   |   |   |   |   |
| 2  |          |          |          |           |   |   |   |   |   |   |   |
| 3  |          |          |          |           |   |   |   |   |   |   |   |
| 4  |          |          |          |           |   |   |   |   |   |   |   |
| 5  |          |          | k= 5     |           |   |   |   |   |   |   |   |
| 6  |          |          |          |           |   |   |   |   |   |   |   |
| 7  | <b>S</b> | <b>X</b> | <b>Y</b> | <b>S1</b> |   |   |   |   |   |   |   |
| 8  | и        | 8        | 13       | н         |   |   |   |   |   |   |   |
| 9  | в        | 2        | 7        | з         |   |   |   |   |   |   |   |
| 10 | а        | 0        | 5        | е         |   |   |   |   |   |   |   |
| 11 | н        | 13       | 18       | т         |   |   |   |   |   |   |   |
| 12 | о        | 14       | 19       | у         |   |   |   |   |   |   |   |
| 13 | в        | 2        | 7        | з         |   |   |   |   |   |   |   |
| 14 | а        | 0        | 5        | е         |   |   |   |   |   |   |   |
| 15 | н        | 13       | 18       | т         |   |   |   |   |   |   |   |
| 16 | д        | 4        | 9        | й         |   |   |   |   |   |   |   |
| 17 | р        | 16       | 21       | х         |   |   |   |   |   |   |   |
| 18 | е        | 5        | 10       | к         |   |   |   |   |   |   |   |
| 19 | й        | 9        | 14       | о         |   |   |   |   |   |   |   |
| 20 |          |          |          |           |   |   |   |   |   |   |   |
| 21 |          |          |          |           |   |   |   |   |   |   |   |
| 22 |          |          |          |           |   |   |   |   |   |   |   |
| 23 |          |          |          |           |   |   |   |   |   |   |   |
| 24 |          |          |          |           |   |   |   |   |   |   |   |
| 25 |          |          |          |           |   |   |   |   |   |   |   |
| 26 |          |          |          |           |   |   |   |   |   |   |   |
| 27 |          |          |          |           |   |   |   |   |   |   |   |
| 28 |          |          |          |           |   |   |   |   |   |   |   |
| 29 |          |          |          |           |   |   |   |   |   |   |   |
| 30 |          |          |          |           |   |   |   |   |   |   |   |
| 31 |          |          |          |           |   |   |   |   |   |   |   |
| 32 |          |          |          |           |   |   |   |   |   |   |   |
| 33 |          |          |          |           |   |   |   |   |   |   |   |
| 34 |          |          |          |           |   |   |   |   |   |   |   |
| 35 |          |          |          |           |   |   |   |   |   |   |   |

13. Проведите дешифрования текста по аналогии с зашифровыванием. Для расшифровывания (столбца X) используйте формулу

$$x_i = (y_i + (32 - k)) \mod 32.$$

| Шифры.xls |                        |          |          |           |   |                         |          |          |          |   |
|-----------|------------------------|----------|----------|-----------|---|-------------------------|----------|----------|----------|---|
| A         | B                      | C        | D        | E         | F | G                       | H        | I        | J        | K |
| 1         | <b>Шифр Цезаря</b>     |          |          |           |   |                         |          |          |          |   |
| 2         |                        |          |          |           |   |                         |          |          |          |   |
| 3         | <b>1. Зашифрование</b> |          |          |           |   | <b>2. Расшифрование</b> |          |          |          |   |
| 4         |                        |          |          |           |   |                         |          |          |          |   |
| 5         | k= 5                   |          |          |           |   | k= 7                    |          |          |          |   |
| 6         |                        |          |          |           |   |                         |          |          |          |   |
| 7         | <b>S</b>               | <b>X</b> | <b>Y</b> | <b>S1</b> |   | <b>S1</b>               | <b>Y</b> | <b>X</b> | <b>S</b> |   |
| 8         | и                      | 8        | 13       | н         |   | х                       | 21       | 14       | о        |   |
| 9         | в                      | 2        | 7        | з         |   | л                       | 11       | 4        | д        |   |
| 10        | а                      | 0        | 5        | е         |   | ф                       | 20       | 13       | н        |   |
| 11        | н                      | 13       | 18       | т         |   | п                       | 15       | 8        | и        |   |
| 12        | о                      | 14       | 19       | у         |   | у                       | 19       | 12       | м        |   |
| 13        | в                      | 2        | 7        | з         |   | с                       | 17       | 10       | к        |   |
| 14        | а                      | 0        | 5        | е         |   | х                       | 21       | 14       | о        |   |
| 15        | н                      | 13       | 18       | т         |   | ф                       | 20       | 13       | н        |   |
| 16        | д                      | 4        | 9        | й         |   | м                       | 12       | 5        | е        |   |
| 17        | р                      | 16       | 21       | х         |   | у                       | 19       | 12       | м        |   |
| 18        | е                      | 5        | 10       | к         |   | й                       | 9        | 2        | в        |   |
| 19        | й                      | 9        | 14       | о         |   | ш                       | 24       | 17       | с        |   |
| 20        |                        |          |          |           |   | м                       | 12       | 5        | е        |   |
| 21        |                        |          |          |           |   | ц                       | 22       | 15       | п        |   |
| 22        |                        |          |          |           |   | х                       | 21       | 14       | о        |   |
| 23        |                        |          |          |           |   | т                       | 18       | 11       | л        |   |
| 24        |                        |          |          |           |   | м                       | 12       | 5        | е        |   |
| 25        |                        |          |          |           |   | ф                       | 20       | 13       | н        |   |
| 26        |                        |          |          |           |   | м                       | 12       | 5        | е        |   |
| 27        |                        |          |          |           |   | х                       | 21       | 14       | о        |   |
| 28        |                        |          |          |           |   | и                       | 8        | 1        | б        |   |
| 29        |                        |          |          |           |   | б                       | 1        | 26       | ъ        |   |
| 30        |                        |          |          |           |   | м                       | 12       | 5        | е        |   |
| 31        |                        |          |          |           |   | л                       | 11       | 4        | д        |   |
| 32        |                        |          |          |           |   | м                       | 12       | 5        | е        |   |
| 33        |                        |          |          |           |   | я                       | 31       | 24       | ш        |   |
| 34        |                        |          |          |           |   | г                       | 3        | 28       | ь        |   |

14. Запишите полученную фразу в тетрадь.

15. Зашифруйте в тетради расшифрованную фразу методом перестановки с ключом. В качестве ключа используйте свою фамилию.

16. Предъявите работу преподавателю.

### Контрольные вопросы.

1. Какой текст называется открытым?
2. Какой текст называется закрытым?
3. Что такое ключ?
4. Как осуществляется процесс шифрования в методе Цезаря?
5. Что такое «шифрование методом перестановки»?
6. Как работает функция ОСТАТ?
7. Что делает функция ВПР?

### Варианты заданий

|   |   |
|---|---|
| <p><b>№1</b></p> <p>Используя ключ 8 проведите дешифрование информации, зашифрованной методом Цезаря: фицтрщцкти - еьц эрыщщд р щхцщцкти</p>  | <p><b>№2</b></p> <p>Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: ршф ыфэлш туфйф нужшв, шфтщ ужкф тжсф чхжшв</p> |
| <p><b>№3</b></p> <p>Используя ключ 4 проведите дешифрование информации, зашифрованной методом Цезаря: уфйичуфйимца жтжфйрг - ийпт ифчлийн</p> | <p><b>№4</b></p> <p>Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: ифнвтлшче ужцфк - фнлцф хлцлсвлш</p>            |

|   |   |
|---|---|
| <p>№5</p> <p>Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: хлфпу схфму йшм цхтм фм хибмляг</p>        | <p>№6</p> <p>Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: мно ъфчлй щонус, ьйх чцс лоъ схозы</p>         |
| <p>№7</p> <p>Используя ключ 10 проведите дешифрование информации, зашифрованной методом Цезаря: цкх йсеф, ок мыпц ьхщц мхкоппь</p>        | <p>№8</p> <p>Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: юму ихтгям фзъсп, щму ъуфмм чъсп</p>           |
| <p>№9</p> <p>Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: хйфч нсшфчх схоые, цйнч нофч щйрьхоые</p>  | <p>№10</p> <p>Используя ключ 4 проведите дешифрование информации, зашифрованной методом Цезаря: ррифтхца - сдмрйсаьдг цгкйпдг стьд ж учцм</p> |
| <p>№11</p> <p>Используя ключ 10 проведите дешифрование информации, зашифрованной методом Цезаря: щъшнэхжчеп очт мшъшмыьмэ ыъшочт</p>      | <p>№12</p> <p>Используя ключ 5 проведите дешифрование информации, зашифрованной методом Цезаря: уч ирем чурпш серу, кцрн шс цркф</p>          |
| <p>№13</p> <p>Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: рфтц цжзфшж и шейфчшв, шфтц ул илкфтж</p> | <p>№14</p> <p>Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: ьхчхямм йхщцщзфпм - тьюямм фзштмлшщйх</p>     |
| <p>№15</p> <p>Используя ключ 8 проведите дешифрование информации, зашифрованной методом Цезаря: чцфиэинад тцщцс - йымнъ шуимцт чцтцс</p>  | <p>№16</p> <p>Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: уыч хцчмч цйасцйоы, ычы хйфч учцайоы</p>      |

## Практическая работа №3

**Тема:** Изучение методов шифрования. Шифры замены и шифры перестановки.

**Цель работы:** Научится применять шифры замены и шифры перестановки для шифрования данных.

### Порядок выполнения работы.

1. Записать в тетради тему и цель работы.
2. Ознакомиться с теоретическими сведениями.
3. Выполнить задания
4. Оформить отчет

### Теоретические сведения.

#### Шифры замены

**1. Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.

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

Рис.1. Таблица шифрозамен для полибианского квадрата

Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то

шифrogramма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца.

**2. Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».

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

Рис.2. Таблица шифрозамен для шифра Трисемуса

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ЖЗЦЖУФЙ».

**Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов.

**3. Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для  $26 \times 26 = 676$  возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни

еЯ». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»

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

Рис.3. Ключевая таблица для шифра Playfair

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;
- биграмма «ши» находятся в одном столбце – заменяется на «юе»;
- биграмма «фр» находятся в одной строке – заменяется на «хс»;
- биграмма «ов» формирует прямоугольник – заменяется на «йж»;
- биграмма «ан» находятся в одной строке – заменяется на «ба»;
- биграмма «но» формирует прямоугольник – заменяется на «ам»;
- биграмма «ес» формирует прямоугольник – заменяется на «гт»;
- биграмма «оя» формирует прямоугольник – заменяется на «ка»;
- биграмма «об» формирует прямоугольник – заменяется на «па»;
- биграмма «ще» формирует прямоугольник – заменяется на «шё»;
- биграмма «ни» формирует прямоугольник – заменяется на «ан»;
- биграмма «ея» формирует прямоугольник – заменяется на «ги».

Шифrogramма – «жб юе хс йж ба ам гт ка па шё ан ги».

Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении.

### Полиалфавитные шифры.

**4. Таблица Трисемуса.** Одним из шифров, придуманных немецким аббатом Трисемусом, стал многоалфавитный шифр, основанный на так называемой «таблице Трисемуса» - таблице со стороной равной **n**, где **n** – количество символов в алфавите. В первой строке матрицы записываются

буквы в порядке их очередности в алфавите, во второй – та же последовательность букв, но с циклическим сдвигом на одну позицию влево, в третьей – с циклическим сдвигом на две позиции влево и т.д.

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

Рис.4. Таблица Трисемуса

Здесь первая строка является одновременно и строкой букв открытого текста. Первая буква текста шифруется по первой строке, вторая буква по второй и так далее после использования последней строки вновь возвращаются к первой. Так сообщение «АБРАМОВ» приобретет вид «АВТГРУИ».

**5. Система шифрования Виженера.** В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

Перед шифрованием выбирается ключ из символов алфавита. Сама процедура шифрования заключается в следующем. По *i*-ому символу открытого сообщения в первой строке определяется столбец, а по *i*-ому символу ключа в крайнем левом столбце – строка. На пересечении строки и столбца будет находиться *i*-ый символ, помещаемый в шифрограмму. Если длина ключа меньше сообщения, то он используется повторно. Например, исходное сообщение «АБРАМОВ», ключ – «ДЯДИНА», шифрограмма – «ДАФИЩОЖ».

Справедливости ради, следует отметить, что авторство данного шифра принадлежит итальянцу Джованни Батиста Беллазо, который описал его в 1553 г. История «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания». Беллазо предложил называть секретное слово или фразу **паролем** (ит. password; фр. parole - слово).

## Шифры перестановки

**6. Шифр блочной одинарной перестановки.** При использовании этого шифра задается таблица перестановки блока символов, которая последовательно применяется до тех пор, пока исходное сообщение не закончится. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными символами.

|   |   |   |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |

Рис.5. Таблица перестановок

Для примера выберем размер блока, равный 3, и примем таблицу перестановок, показанную на рис.5. Дополним исходное сообщение «АБРАМОВ» буквами Ъ и Э, чтобы его длина была кратна 3. В результате шифрования получим «РАБОАМЭВЬ».

Количество ключей для данного шифра при фиксированном размере блока равно  $m!$ , где  $m$  – размер блока.

**7. Шифр табличной маршрутной перестановки.** Наибольшее распространение получили шифры маршрутной перестановки, основанные на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) - по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

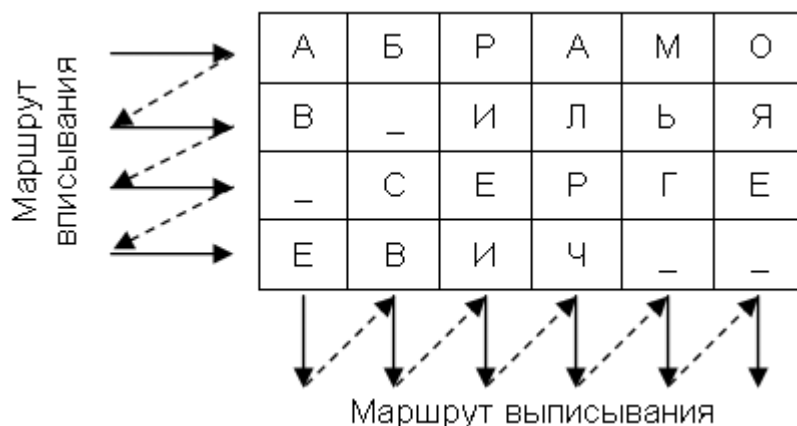


Рис. 6.. Пример использования шифра маршрутной перестановки

Например, исходное сообщения «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» вписывается в прямоугольную таблицу размерами 4х6, маршрут вписывания – слева-направо сверху-вниз, маршрут выписывания – сверху-вниз слева-направо. Шифрограмма в этом случае выглядит «АВ\_ЕБ\_СВРИЕИАЛР ЧМЬГ\_ОЯЕ\_».

**8. Шифры с использованием треугольников и трапеций.** Помочь выполнить перестановки могут как треугольники, так и трапеции. Открытый текст вписывается в эти фигуры в соответствии с количеством слов и формой выбранной фигуры, которая может быть растянута или сжата, чтобы в ней

поместилось сообщение. Для первой фигуры, треугольника, открытый текст записывается построчно от вершины до основания.

|   |    |   |   |   |   |   |    |   |   |   |
|---|----|---|---|---|---|---|----|---|---|---|
|   |    |   |   |   | А |   |    |   |   |   |
|   |    |   |   | Б |   | Р |    |   |   |   |
|   |    | А |   |   | М |   | О  |   |   |   |
|   | В  |   |   | – |   | И |    | Л |   |   |
|   | Ь  |   | Я |   | – |   | С  |   | Е |   |
| Р |    | Г |   | Е |   | Е |    | В |   | И |
| Д | Я  | Д | И | Н | А | Д | Я  | Д | И | Н |
| 2 | 10 | 3 | 6 | 8 | 1 | 4 | 11 | 5 | 7 | 9 |

Рис.7. Пример использования шифра перестановки при вписывании в треугольник

Ниже записывается ключевое слово. Поскольку основание широкое, ключевое слово повторяется. Буквы строки с ключевым словом нумеруются последовательно согласно их алфавитному порядку. Зашифрованное сообщение выписывается по столбцам согласно выполненной нумерации. Таким образом, для открытого текста «АБРАМОВ ИЛЬЯ СЕРГЕЕВИ» и ключевого слова «ДЯДИНА» шифрограмма будет выглядеть «АМ\_РВГРИЕЛВАЯЕБ\_ЕИЬРС».

**9. Магические квадраты.** Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами начиная с 1, которые в сумме по каждому столбцу, каждой строке и каждой диагонали дают одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты. Магических квадратов 4x4 насчитывается уже 880, а число магических квадратов размером 5x5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был невыносим.

Рассмотри квадрат размером 4x4. В него вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным диагоналям равняется одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

Рис.8. Магический квадрат 4x4

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «АБРАМОВДЯДИНА...». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка или любая буква.

|      |      |      |      |
|------|------|------|------|
| 16 . | 3 Р  | 2 Б  | 13 А |
| 5 М  | 10 Д | 11 И | 8 Д  |
| 9 Я  | 6 О  | 7 В  | 12 Н |
| 4 А  | 15 . | 14 . | 1 А  |

Рис.9. Пример шифрования с помощью магического квадрата

После этого зашифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – «.РБАМДИДЯОВНА..А».

**10. Шифр двойной перестановки.** В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на рис.10. Результат шифрования – «ОАБЯ+ АИВ РДМНАД».



Рис.10. Пример использования шифра двойной перестановки

Ключом к шифру являются размеры таблицы, маршруты вписывания и выписывания, а также порядки перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно  $n! \cdot m!$ ,  $n$  и  $m$  – количество столбцов и строк в таблице.

### Задания к работе

1. Необходимо зашифровать свою фамилию с помощью следующих шифров:

- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair
- таблицы Трисемуса.
- шифра Виженера.
- блочной одинарной перестановки;

3. Необходимо зашифровать фамилию и имя с помощью следующих шифров:

- табличной маршрутной перестановки;
- шифры с использованием треугольника.
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

При оформлении отчета необходимо привести исходное сообщение (фамилию или фамилию и имя), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, зашифрованное сообщение.

## Практическая работа № 4

**Тема: Изучение методов шифрования. Аддитивные шифры.**

**Цель работы: Изучить аддитивные методы шифрования на примере аддитивных шифров.**

**Порядок выполнения работы.**

1. Записать в тетради тему и цель работы
2. Ознакомиться с теоретическими сведениями.
3. Выполнить задания

### **Теоретические сведения.**

В аддитивных шифрах используется сложение по модулю (**mod**) исходного сообщения с гаммой, представленных в числовом виде. Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например,  $5+10 \bmod 4 = 15 \bmod 4 = 3$ ).

В литературе шифры этого класса часто называют **потокowymi**. Стойкость закрытия этими шифрами определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду.

**Длиною периода гаммы** называется минимальное количество символов, после которого последовательность цифр в гамме начинает повторяться. **Случайность распределения символов по периоду** означает отсутствие закономерностей между появлением различных символов в пределах периода.

По длине периода различаются гаммы с **конечным** и **бесконечным периодом**. Если длина периода гаммы превышает длину шифруемого текста, гамма является истинно случайной и не используется для шифрования других сообщений, то такое преобразование является абсолютно стойким (совершенный шифр). Такой шифр нельзя вскрыть на основе статистической обработки шифрограммы.

## Сложение по модулю N.

В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы

$$C_i = (P_i + K_i) \bmod N, \quad (1)$$

$$P_i = (C_i + N - K_i) \bmod N, \quad (2)$$

где  $P_i$ ,  $C_i$  -  $i$ -ый символ открытого и зашифрованного сообщения;

$N$  - количество символов в алфавите;

$K_i$  -  $i$ -ый символ гаммы (ключа). Если длина гаммы меньше, чем длина сообщения, то она используется повторно.

Данные формулы позволяют выполнить зашифрование / расшифрование по Вижнеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ы  | Ь  | Ъ  | Э  | Ю  | Я  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

**Рис.1. Таблица кодирования символов**

Например, для шифрования используется русский алфавит ( $N = 33$ ), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква **А** будет представлена как 0, **Б** – 1, ..., **Я** – 32. Результат шифрования показан в следующей таблице.

**Таблица 1. Пример аддитивного шифрования по модулю N**

|        |                            |   |    |    |   |    |    |    |
|--------|----------------------------|---|----|----|---|----|----|----|
| Символ | открытого сообщения, $P_i$ | А | Б  | Р  | А | М  | О  | В  |
|        |                            | 0 | 1  | 17 | 0 | 13 | 15 | 2  |
|        | гаммы, $K_i$               | Ж | У  | Р  | И | Х  | И  | Н  |
|        |                            | 7 | 20 | 17 | 9 | 22 | 9  | 14 |
|        | шифrogramмы, $C_i$         | Ж | Ф  | Б  | И | В  | Ч  | П  |
|        |                            | 7 | 21 | 1  | 9 | 2  | 24 | 16 |

## Сложение по модулю 2.

Является частным случаем предыдущего шифра и используется при шифровании в автоматизированных системах. Символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2 ( $\oplus$ , для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C_i = P_i \oplus K_i, \quad (3)$$

$$P_i = C_i \oplus K_i. \quad (4)$$

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

**Таблица 2. Коды символов Windows 1251 и их двоичное представление**

| Буква | Дес-код | Bin-код   | Буква | Дес-код | Bin-код   | Буква | Дес-код | Bin-код   |
|-------|---------|-----------|-------|---------|-----------|-------|---------|-----------|
| А     | 192     | 1100 0000 | Л     | 203     | 1100 1011 | Ц     | 214     | 1101 0110 |
| Б     | 193     | 1100 0001 | М     | 204     | 1100 1100 | Ч     | 215     | 1101 0111 |
| В     | 194     | 1100 0010 | Н     | 205     | 1100 1101 | Ш     | 216     | 1101 1000 |
| Г     | 195     | 1100 0011 | О     | 206     | 1100 1110 | Щ     | 217     | 1101 1001 |
| Д     | 196     | 1100 0100 | П     | 207     | 1100 1111 | Ъ     | 218     | 1101 1010 |
| Е     | 197     | 1100 0101 | Р     | 208     | 1101 0000 | Ы     | 219     | 1101 1011 |
| Ж     | 198     | 1100 0110 | С     | 209     | 1101 0001 | Ь     | 220     | 1101 1100 |
| З     | 199     | 1100 0111 | Т     | 210     | 1101 0010 | Э     | 221     | 1101 1101 |
| И     | 200     | 1100 1000 | У     | 211     | 1101 0011 | Ю     | 222     | 1101 1110 |
| Й     | 201     | 1100 1001 | Ф     | 212     | 1101 0100 | Я     | 223     | 1101 1111 |
| К     | 202     | 1100 1010 | Х     | 213     | 1101 0101 |       |         |           |

Примечание. Дес-код – десятичный код символа, Bin-код – двоичный код символа.

Пример шифрования сообщения «ВОВА» с помощью гаммы «ЮЛЯ» показан в следующей таблице.

**Таблица 3. Пример аддитивного шифрования по модулю 2**

|                    |         |           |           |           |           |
|--------------------|---------|-----------|-----------|-----------|-----------|
| Открытое сообщение | Буква   | В         | О         | В         | А         |
|                    | Дес-код | 194       | 206       | 194       | 192       |
|                    | Bin-код | 1100 0010 | 1100 1110 | 1100 0010 | 1100 0000 |
| Гамма              | Буква   | Ю         | Л         | Я         | Ю         |
|                    | Дес-код | 222       | 203       | 223       | 222       |
|                    | Bin-код | 1101 1110 | 1100 1011 | 1101 1111 | 1101 1110 |
| Шифрограмма        | Дес-код | 28        | 5         | 29        | 30        |
|                    | Bin-код | 0001 1100 | 0000 0101 | 0001 1101 | 0001 1110 |

Таблица истинности:

- для бинарного сложения по модулю 2 (применяется в двоичных полусумматорах):

| $a$ | $b$ | $a \oplus b$ |
|-----|-----|--------------|
| 0   | 0   | 0            |
| 0   | 1   | 1            |
| 1   | 0   | 1            |
| 1   | 1   | 0            |

### Задания к работе

1. Зашифровать свою фамилию с помощью шифров гаммирования по модулю N
2. Зашифровать свою фамилию с помощью шифров гаммирования и модулю 2.
3. При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования.

## Практическая работа № 5

**Тема:** Шифрование с открытым ключом

**Цель работы:** Научиться шифровать данные с помощью метода шифрования с открытым ключом.

### Порядок выполнения работы.

1. Записать в тетради тему и цель работы
2. Ознакомиться с теоретическими сведениями
3. Выполнить задания
4. Оформить отчет

### Задания к работе

Необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке  
ранца;
- алгоритма шифрования Эль-Гамала.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

**Таблица1. Коды символов Windows 1251 и их двоичное представление**

| Буква | Дес-код | Bin-код   | Буква | Дес-код | Bin-код   | Буква | Дес-код | Bin-код   |
|-------|---------|-----------|-------|---------|-----------|-------|---------|-----------|
| А     | 192     | 1100 0000 | Л     | 203     | 1100 1011 | Ц     | 214     | 1101 0110 |
| Б     | 193     | 1100 0001 | М     | 204     | 1100 1100 | Ч     | 215     | 1101 0111 |
| В     | 194     | 1100 0010 | Н     | 205     | 1100 1101 | Ш     | 216     | 1101 1000 |
| Г     | 195     | 1100 0011 | О     | 206     | 1100 1110 | Щ     | 217     | 1101 1001 |
| Д     | 196     | 1100 0100 | П     | 207     | 1100 1111 | Ъ     | 218     | 1101 1010 |
| Е     | 197     | 1100 0101 | Р     | 208     | 1101 0000 | Ы     | 219     | 1101 1011 |
| Ж     | 198     | 1100 0110 | С     | 209     | 1101 0001 | Ь     | 220     | 1101 1100 |
| З     | 199     | 1100 0111 | Т     | 210     | 1101 0010 | Э     | 221     | 1101 1101 |
| И     | 200     | 1100 1000 | У     | 211     | 1101 0011 | Ю     | 222     | 1101 1110 |
| Й     | 201     | 1100 1001 | Ф     | 212     | 1101 0100 | Я     | 223     | 1101 1111 |
| К     | 202     | 1100 1010 | Х     | 213     | 1101 0101 |       |         |           |

### Теоретические сведения

Главная проблема использования одноключевых (симметричных) криптосистем заключается в распределении ключей. Для того, чтобы был возможен обмен информацией между двумя сторонами, ключ должен быть сгенерирован одной из них, а затем в конфиденциальном порядке передан другой. Особую остроту данная проблема приобрела в наши дни, когда криптография стала общедоступной, вследствие чего количество пользователей больших криптосистем может исчисляться сотнями и тысячами.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Находясь под влиянием работы Ральфа Меркле (Ralph Merkle) о распространении открытого ключа, они предложили метод получения секретных ключей для симметричного шифрования, используя открытый канал. В 2002 году Хеллман предложил называть данный алгоритм «Диффи - Хеллмана - Меркле», признавая вклад Меркле в изобретение криптографии с открытым ключом.

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов - Рон Ривест (Ronald Linn Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman) из Массачусетского Технологического Института (MIT)).

Справедливости ради следует отметить, что в декабре 1997 года была обнародована информация, согласно которой британский математик Клиффорд Кокс (Clifford Cocks), работавший в центре правительственной связи (GCHQ) Великобритании, описал систему, аналогичную RSA, в 1973 году, а несколькими месяцами позже в 1974 году Малькольм Вильямсон изобрел математический алгоритм, аналогичный алгоритму Диффи – Хеллмана - Меркле.

**Суть шифрования с открытым ключом** заключается в том, что для шифрования данных используется один ключ, а для расшифрования другой (поэтому такие системы часто называют **ассиметричными**).

**Основная предпосылка**, которая привела к появлению шифрования с открытым ключом, заключалось в том, что отправитель сообщения (тот, кто зашифровывает сообщение), не обязательно должен быть способен его расшифровывать. Т.е. даже имея исходное сообщение, ключ, с помощью которого оно шифровалось, и зная алгоритм шифрования, он не может расшифровать закрытое сообщение без знания ключа расшифрования.

Первый ключ, которым шифруется исходное сообщение, называется **открытым** и может быть опубликован для использования всеми пользователями системы. Расшифрование с помощью этого ключа невозможно. Второй ключ, с помощью которого дешифруется сообщение, называется **секретным** (закрытым) и должен быть известен только законному получателю закрытого сообщения.

Алгоритмы шифрования с открытым ключом используют так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством: при заданном значении аргумента  $x$  относительно просто вычислить значение функции ( $x$ ), однако, если известно значение функции  $y = f(x)$ , то нет простого пути для вычисления значения аргумента  $x$ . Например, функция **SIN**. Зная  $x$ , легко найти значение **SIN(x)** (например,  $x = \pi$ , тогда  $\text{SIN}(\pi) = 0$ ). Однако, если  $\text{SIN}(x) = 0$ , однозначно определить  $x$  нельзя, т.к. в этом случае  $x$  может быть любым числом, определяемым по формуле  $i * \pi$ , где  $i$  – целое число.

Однако не всякая необратимая функция годится для использования в реальных криптосистемах. В их числе и функция **SIN**. Следует также отметить, что в самом определении необратимости функции присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к криптосистемам с открытым ключом предъявляются два важных и очевидных **требования**.

1. Преобразование исходного текста должно быть условно необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне.

Все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих **типов односторонних преобразований**.

1. Разложение больших чисел на простые множители (алгоритм RSA).
2. Вычисление дискретного логарифма или дискретное возведение в степень (алгоритм Диффи-Хелмана-Меркле, схема Эль-Гамала).
3. Задача об укладке рюкзака (ранца) (авторы Хелман и Меркл).
4. Вычисление корней алгебраических уравнений.
5. Использование конечных автоматов (автор Тао Ренжи).
6. Использование кодовых конструкций.
7. Использование свойств эллиптических кривых.

## Алгоритм RSA.

Стойкость RSA основывается на большой вычислительной сложности известных алгоритмов разложения произведения простых чисел на сомножители. Например, легко найти произведение двух простых чисел 7 и 13 даже в уме – 91. Попробуйте в уме найти два простых числа, произведение которых равно 323 (числа 17 и 19). Конечно, для современной вычислительной техники найти два простых числа, произведение которых равно 323, не проблема. Поэтому для надежного шифрования алгоритмом RSA, как правило, выбираются простые числа, количество двоичных разрядов которых равно нескольким сотням.

Описание RSA было опубликовано в августе 1977 года в журнале «Scientific American». Авторы RSA поддерживали идею её активного распространения. В свою очередь, Агентство национальной безопасности (США), опасаясь использования этого алгоритма в негосударственных структурах, на протяжении нескольких лет безуспешно требовало прекращения распространения системы. Ситуация порой доходила до абсурда. Например, когда программист Адам Бек (Adam Back) описал на языке Perl алгоритм RSA, состоящий из пяти строк, правительство США запретило распространение этой программы за пределами страны. Люди, недовольные подобным ограничением, в знак протеста напечатали текст этой программы на своих футболках.

Первым этапом любого асимметричного алгоритма является создание получателем шифрограмм пары ключей: открытого и секретного. Для алгоритма RSA этап создания ключей состоит из следующих операций.

**Таблица 2. Процедура создания ключей**

| № п/п | Описание операции  | Пример                               |
|-------|--|--------------------------------------|
| 1     | Выбираются два простых числа <b>p</b> и <b>q</b> .   | $p=7, q=13$                          |
| 2     | Вычисляется произведение $n = p * q$ .   | $n=91$                               |
| 3     | Вычисляется <b>функция Эйлера <math>\phi(n)</math></b> .   | $\phi(n)=(7-1)(13-1)=91-7-13+1 = 72$ |
| 4     | Выбирается произвольное число <b>e</b> ( $0 < e < n$ ), взаимно простое с результатом функции Эйлера ( $e \perp \phi(n)$ ). Число <b>e</b> называется открытой экспонентой.  | $e=5$                                |
| 5     | Вычисляется секретный ключ <b>d</b> из соотношения $(d * e) \bmod \phi(n) = 1$ . Число <b>d</b> называется закрытой экспонентой. Обычно пользуются выражением $de = 1 + k\phi(n)$ , где $k$ - некоторое целое число. | $(d * 5) \bmod 72 = 1, d = 29$       |
| 6     | Публикуются открытые ключи <b>e</b> и <b>n</b> в специальном хранилище, где исключается возможность его подмены ( <b>общедоступном сертифицированном справочнике</b> ).  |                                      |

Примечания. **Простое число** – натуральное число, большее единицы и не имеющее других делителей, кроме самого себя и единицы. **Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1 (например,  $p=3, q=5, n=15, j(n)=8$  – взаимно простые с 15 – 1, 2, 4, 7, 8, 11, 13, 14).

Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C = T^e \bmod n, \quad (1)$$

$$T = C^d \bmod n. \quad (2)$$

где  $T$ ,  $C$  - числовые эквиваленты символов открытого и шифрованного сообщения.

Пример шифрования по алгоритму RSA приведен в следующей таблице. Коды букв соответствуют их положению в русском алфавите (начиная с 1).

**Таблица 3. Пример шифрования по алгоритму RSA**

| Открытое сообщение,<br>$T$                | Символ | А | Б  | Р  | А | М  | О  | В  |
|---|--------|---|----|----|---|----|----|----|
|   | Код    | 1 | 2  | 18 | 1 | 14 | 16 | 3  |
| Шифрограмма, $C = T^5 \bmod 91$           |        | 1 | 32 | 44 | 1 | 14 | 74 | 61 |
| Открытое сообщение, $T = C^{29} \bmod 91$ |        | 1 | 2  | 18 | 1 | 14 | 16 | 3  |

Следует отметить, что  $p$  и  $q$  выбираются таким образом, чтобы  $n$  было больше кода любого символа открытого сообщения. В автоматизированных системах исходное сообщение переводится в двоичное представление, после чего шифрование выполняется над блоками бит, равной длины. При этом длина блока должна быть меньше, чем длина двоичного представления  $n$ .

В заключении следует отметить стойкость данного алгоритма. В 2003 г. Ади Шамир и Эран Тромер разработали схему устройства TWIRL, которое при стоимости \$ 10 000 может дешифровать 512-битный ключ за 10 минут, а при стоимости \$ 10 000 000 – 1024-битный ключ меньше, чем за год. В настоящее время Лаборатория RSA рекомендует использовать ключи размером 2048 битов.

### Алгоритм на основе задачи об укладке ранца.

В 1978 г. Меркль и Хеллман предложили использовать задача об укладке ранца (рюкзака) для асимметричного шифрования. Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений  $M_1, M_2, \dots, M_n$  и суммарное значение  $S$ ; требуется вычислить значения  $b_i$  такие что

$$S = b_1 M_1 + b_2 M_2 + \dots + b_n M_n, \quad (3)$$

где  $n$  – количество предметов;

$b_i$  - бинарный множитель. Значение  $b_i = 1$  означает, что предмет  $i$  кладут в рюкзак,  $b_i = 0$  - не кладут.

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, используя предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям  $b$ , а текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

**Таблица 4. Пример шифрования на основе задачи об укладке ранца**

|                |                      |                      |                      |
|----------------|----------------------|----------------------|----------------------|
| Открытый текст | 1 1 1 0 0 1 0 0      | 0 1 0 1 1 0 0 1      | 0 0 0 0 0 0 0 0      |
| Рюкзак (ключ)  | 1 5 6 11 14 20 32 43 | 1 5 6 11 14 20 32 43 | 1 5 6 11 14 20 32 43 |
| Шифрограмма    | 32 (1+5+6+20)        | 73 (5+11+14+43)      | 0                    |

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа **трудный** для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить **легкий** для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. **Сверхвозрастающей** называется **последовательность**, в которой каждый последующий член больше суммы всех предыдущих. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число **n** по модулю **m**. Значение модуля **m** должно быть больше суммы всех чисел последовательности, например, 420 (2+3+6+13+27+52+105+210=418). Множитель **n** должен быть взаимно простым числом с модулем **m**, например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

**Таблица 5. Пример получения открытого ключа**

|  |    |    |     |     |     |     |     |     |
|--|----|----|-----|-----|-----|-----|-----|-----|
| Закрытый ключ, $k$                                       | 2  | 3  | 6   | 13  | 27  | 52  | 105 | 210 |
| Открытый ключ,<br>$(k * n) \bmod m = (k * 31) \bmod 420$ | 62 | 93 | 186 | 403 | 417 | 352 | 315 | 210 |

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль — на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение «АБРАМОВ», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

**Таблица 6. Пример шифрования**

| Открытое сообщение |           | Сумма весов       | Шифрограмма<br>(рюкзак), $c_i$ |
|--------------------|-----------|-------------------|--------------------------------|
| Символ             | Bin-код   |                   |                                |
| А                  | 1100 0000 | 62+93             | 155                            |
| Б                  | 1100 0001 | 62+93+210         | 365                            |
| Р                  | 1101 0000 | 62+93+403         | 558                            |
| А                  | 1100 0000 | 62+93             | 155                            |
| М                  | 1100 1100 | 62+93+417+352     | 924                            |
| О                  | 1100 1110 | 62+93+417+352+315 | 1239                           |
| В                  | 1100 0010 | 62+93+315         | 470                            |

Для расшифрования сообщения получатель должен сначала определить обратное число  $n^{-1}$ , такое что  $(n * n^{-1}) \bmod m = 1$ . В математике **обратное число**  $n^{-1}$  (обратное значение, обратная величина) - число, на которое надо умножить данное число  $n$ , чтобы получить единицу ( $n * n^{-1} = 1$ ). Пара чисел, произведение которых равно единице, называются **взаимно обратными**. Например: 5 и 1/5, -6/7 и -7/6. **Обратными числами по модулю  $m$**  называются такие числа  $n$  и  $n^{-1}$ , для которых справедливо выражение  $(n * n^{-1}) \bmod m = 1$ . Для вычисления обратных чисел по модулю обычно используется расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы умножается на  $n^{-1}$  по модулю  $m$  и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {2, 3, 6, 13, 27, 52, 105, 210},  $m = 420$ ,  $n = 31$ . Значение  $n^{-1}$  равно 271 ( $31 * 271 \bmod 420 = 1$ ).

**Таблица 7. Пример расшифрования**

| Шифрограмма<br>(рюкзак), $c_i$ | $(c_i \cdot n^{-1}) \bmod m =$<br>$(c_i \cdot 271) \bmod 420$ | Сумма весов   | Открытое сообщение |        |
|--------------------------------|---|---------------|--------------------|--------|
|                                |   |               | Bin-код            | Символ |
| 155                            | 5   | 2+3           | 1100 0000          | А      |
| 365                            | 215   | 2+3+210       | 1100 0001          | Б      |
| 558                            | 18  | 2+3+13        | 1101 0000          | Р      |
| 155                            | 5   | 2+3           | 1100 0000          | А      |
| 924                            | 84  | 2+3+27+52     | 1100 1100          | М      |
| 1239                           | 189   | 2+3+27+52+105 | 1100 1110          | О      |
| 470                            | 110   | 2+3+105       | 1100 0010          | В      |

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности). В заключении следует отметить, что задача вскрытия данного способа шифрования успешно решена Шамиром и Циппелом в 1982 г.

### Алгоритм шифрования Эль-Гамала.

Схема была предложена Тахером Эль-Гамалем в 1984 году. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и обеспечения аутентификации. Стойкость данного алгоритма базируется на сложности решения задачи дискретного логарифмирования.

Суть задачи заключается в следующем. Имеется уравнение

$$g^x \bmod p = y. \quad (13)$$

Требуется по известным  $g$ ,  $y$  и  $p$  найти целое неотрицательное число  $x$  (дискретный логарифм).

Порядок создания ключей приводится в следующей таблице.

**Таблица 7. Процедура создания ключей**

| №<br>п/п | Описание операции  | Пример                                |
|----------|--|---------------------------------------|
| 1        | Выбирается простое число $p$ .   | $p=37$                                |
| 2        | Выбирается число $g$ , являющееся первообразным корнем по модулю $p$ и меньшее $p$ .                                       | $g=2$                                 |
| 3        | Выбираются произвольное число $x$ , меньшее $p$ .  | $x=5$                                 |
| 4        | Вычисляется $y = g^x \bmod p$  | $y = 2^5 \bmod 37 = 32 \bmod 37 = 32$ |
| 5        | Открытый ключ - $y$ , $g$ и $p$ . Причем $g$ и $p$ можно сделать общими для группы пользователей.<br>Закрытый ключ - $x$ . |                                       |

Для шифрования каждого отдельного блока исходного сообщения должно выбираться случайное число  $k$  ( $1 < k < p - 1$ ). После чего шифрограмма генерируется по следующим формулам

$$a = g^k \bmod p, \quad (14)$$

$$b = (y^k T) \bmod p, \quad (15)$$

где  $T$  – исходное сообщение;

( $a$ ,  $b$ ) – зашифрованное сообщение.

Дешифрование сообщения выполняется по следующей формуле

$$T = (b (a^x)^{-1}) \bmod p \quad (16)$$

или

$$T = (b a^{p-1-x}) \bmod p, \quad (17)$$

где  $(a^x)^{-1}$  – обратное значение числа  $a^x$  по модулю  $p$ .

Пример шифрования и дешифрования по алгоритму Эль-Гамала при  $k = 7$  приведен в таблице, хотя для шифрования каждого блока (в нашем случае буквы) исходного сообщения надо использовать свое случайное число  $k$ .

Первая часть шифрованного сообщения –  $a = 5^7 \bmod 23 = 17$ .

$a^x = 17^3 = 4913$ ,  $(a^x)^{-1} = 5$  ( $4913 * 5 \bmod 23 = 1$ ) или  $a^{p-1-x} = 17^{23-1-3} = 239072435685151324847153$ .

**Таблица 8. Пример шифрования по алгоритму Эль-Гамала (при  $k = \text{const}$ )**

|  |        |    |   |    |    |    |    |    |
|--|--------|----|---|----|----|----|----|----|
| Открытое сообщение,<br>Т                               | Символ | А  | Б | Р  | А  | М  | О  | В  |
|  | Код    | 1  | 2 | 18 | 1  | 14 | 16 | 3  |
| Вторая часть шифрограммы,<br>$b = (32^7 * T) \bmod 37$ |        | 19 | 1 | 9  | 19 | 7  | 8  | 20 |
| Открытое сообщение,<br>$T = (b * 2) \bmod 37$          |        | 1  | 2 | 18 | 1  | 14 | 16 | 3  |

Ввиду того, что число  $k$  является произвольным, то такую схему еще называют схемой **вероятностного шифрования**. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамала, т.к. у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования. Недостатком схемы шифрования Эль-Гамала является удвоение длины зашифрованного текста по сравнению с начальным текстом. Для схемы вероятностного шифрования само сообщение  $T$  и ключ не определяют шифртекст однозначно. В схеме Эль-Гамала необходимо использовать различные значения случайной величины  $k$  для шифровки различных сообщений  $T$  и  $T'$ . Если использовать одинаковые  $k$ , то для соответствующих шифртекстов  $(a, b)$  и  $(a', b')$  выполняется соотношение  $b (b')^{-1} = T (T')^{-1} \pmod{p}$ . Из этого выражения можно легко вычислить  $T$ , если известно  $T'$ .

### ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| №<br>п.п. | Содержание изменения | Дата, номер<br>протокола<br>заседания<br>педагогического<br>совета |
|-----------|----------------------|--|
| 1         | 2                    | 3  |
| 1         |                      |  |
| 2         |                      |  |
| 3         |                      |  |
| 4         |                      |  |
| 5         |                      |  |
| 6         |                      |  |
| 7         |                      |  |
| 8         |                      |  |
| 9         |                      |  |
| 10        |                      |  |
| 11        |                      |  |
| 12        |                      |  |
| 13        |                      |  |
| 14        |                      |  |