ЛАБОРАТОРНАЯ РАБОТА 1
ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДА ШИФРУЮЩИХ ТАБЛИЦ И МЕТОДА МАГИЧЕСКОГО КВАДРАТА

Цель работы: формирование умений шифрования с использованием методов шифрующих таблиц и магического квадрата.

Теоретические сведения

Шифрование методом шифрующих таблиц

При шифровании методом шифрующих таблиц (перестановкой) символы шифруемого текста переставляются по определенным правилам в пределах блока этого текста.

В качестве ключа в шифрующих таблицах могут использоваться:

- размер таблицы;
- слово или фраза, задающие перестановку;
- последовательность, сформированная из натурального ряда чисел 1, 2, ..., *n* случайной перестановкой.

Одним из самых примитивных табличных шифров перестановки является *простая перестановка*, для которой ключом служит размер таблицы.

Рассмотрим шифрование сообщения «ПРИЛЕТАЮ СЕДЬМОГО В ПОЛДЕНЬ». В качестве ключа примем размер таблицы 4 × 6 (4 строки, 6 столбцов).

Запишем сообщение в таблицу по столбцам (табл. 1.1). Пробелы при этом могут игнорироваться, как в рассматриваемом случае.

Таблица 1.1

П	Е	С	М	В	Д
Р	Т	Е	О	П	Е
И	А	Д	Г	О	Н
Л	Ю	Ь	О	Л	Ь

Для формирования шифртекста содержимое таблицы считываем по строкам. Таким образом, результатом шифрования рассматриваемого сообщения будет текст: «ПЕСМВДРТЕОПЕИАДГОН ЛЮЬОЛЬ».

При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый *одиночной перестановкой по ключу*. Этот метод отличается от предыдущего тем, что столбцы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим слово «КОРОВА» в качестве ключа шифрования сообщения из предыдущего примера.

Построим таблицу с количеством столбцов, равным количеству букв в ключевом слове. Ключ шифрования побуквенно запишем в первую строку таблицы. Затем во второй строке таблицы для каждой буквы отобразим ее номер в слове согласно следованию букв в алфавите. Если буквы повторяются, они нумеруются слева направо. Далее заполняем таблицу шифруемым сообщением по столбцам, аналогично предыдущему рассматриваемому методу (табл. 1.2).

Таблица 1.2

К	**О**	**Р**	**О**	**В**	**А**
3	**4**	**6**	**5**	**2**	**1**
П	Е	С	М	В	Д
Р	Т	Е	О	П	Е
И	А	Д	Г	О	Н
Л	Ю	Ь	О	Л	Ь

Следующим шагом шифрования является перестановка столбцов в соответствии с упорядоченными номерами букв ключа. Результат перестановки представлен в табл. 1.3.

Таблица 1.3

А	**В**	**К**	**О**	**О**	**Р**
1	**2**	**3**	**4**	**5**	**6**
Д	В	П	Е	М	С
Е	П	Р	Т	О	Е
Н	О	И	А	Г	Д
Ь	Л	Л	Ю	О	Ь

При считывании содержимого табл. 1.3 по строкам получим следующий шифртекст: «ДВПЕМСЕПРТОЕНОИАГДЬЛЛЮОЬ».

Возможны различные варианты реализации метода шифрующих таблиц. В рамках одного из вариантов в качестве ключа

может использоваться последовательность, сформированная из натурального ряда чисел 1, 2, ..., *n* случайной перестановкой. При этом шифруемый текст может записываться не по столбцам таблицы, как в предыдущих примерах, а по строкам, и после перестановки считываться соответственно по столбцам.

Для обеспечения дополнительной криптоустойчивости можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется *двойной перестановкой*. В случае двойной перестановки ключи определяются отдельно для столбцов и строк. В таблицу заданных размеров построчно записывается текст сообщения, затем в соответствии с ключами поочередно переставляются сначала столбцы, затем строки. При расшифровании порядок перестановок должен быть обратным.

Рассмотрим пример выполнения шифрования методом двойной перестановки.

Шифрование будет выполняться с использованием таблицы 4 × 4. Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере – последовательности 4132 и 3142).

Исходным текстом будет сообщение «ПРИЛЕТАЮ СЕДЬМОГО».

Сначала запишем сообщение в таблицы и расставим ключи перестановки (табл. 1.4).

Таблица 1.4

	4	**1**	**3**	**2**
3	П	Р	И	Л
1	Е	Т	А	Ю
4	С	Е	Д	Ь
2	М	О	Г	О

Следующим шагом является перестановка столбцов (табл. 1.5).

Таблица 1.5

	1	**2**	**3**	**4**
3	Р	Л	И	П
1	Т	Ю	А	Е
4	Е	Ь	Д	С
2	О	О	Г	М

В соответствии с ключом переставляются строки (табл. 1.6).

Таблица 1.6

	1	**2**	**3**	**4**
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	Е	Ь	Д	С

Шифртекст можно получить, считывая построчно содержимое таблицы: «ТЮАЕООГМРЛИПЕЬДС».

Двойная перестановка не отличается высокой стойкостью и сравнительно просто «взламывается».

Шифрование методом магического квадрата

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывается в магические квадраты в соответствии с нумерацией их клеток. Для получения шифртекста содержимое получившейся таблицы считывается построчно.

Пример магического квадрата и его заполнения сообщением «ПРИЛЕТАЮ ВОСЬМОГО» показан на рис. 1.1.

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

О	**И**	**Р**	**М**
Е	**О**	**С**	**Ю**
В	**Т**	**А**	**Ь**
Л	**Г**	**О**	**П**

Рис. 1.1

В результате получаем следующий шифртекст: «ОИРМЕОСЮВТАЬЛГОП».

Содержание заданий

Задание 1

Выполните шифрование/расшифрование, используя метод шифрующих таблиц согласно варианту. При шифровании/рас-

шифровании все пробелы учитываются. Пробелы в шифртексте обозначаются символом «_», несколько подряд идущих пробелов разделяются символом «|».

1. Зашифруйте сообщение «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя метод простой перестановки. Размер шифрующей таблицы 6 × 10.

2. Напишите программу расшифровки шифра «БМ_Д_АДЫН ЭНУТРТЫТОМЬУЬМО,Н_Г_|_|_И–ОУ–ОАЧ_Е», полученного с использованием метода простой перестановки. Размер таблицы 6 × 7.

3. Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ» методом одиночной перестановки по ключу (ключевое слово «МЫСЛЕННО», размер таблицы 8 × 8).

4. Зашифруйте сообщение «КОГДА МЫ СТОИМ, ТО СТОИМ ЛИ МЫ, ИЛИ ЛИШЬ ПРОПУСКАЕМ СОБСТВЕННЫЕ ШАГИ, КОТОРЫЕ ОТМЕРЯЮТ И СОКРАЩАЮТ НАШ ПУТЬ?» методом одиночной перестановки по ключу (ключевое слово «СЕССИЯ», размер таблицы 18 × 6).

5. Зашифруйте сообщение «ЕСЛИ ДУМАЕШЬ ДОЛГО И ДОБРОСОВЕСТНО, ТО В КОНЦЕ КОНЦОВ ВСЕГДА ПОЙМЕШЬ. ПРОСТО МАЛО КТО ХОРОШО ДУМАЕТ.» методом одиночной перестановки по ключу (ключевое слово «НЕПРЕРЫВНО», размер таблицы 10 × 10).

6. Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ» методом одиночной перестановки по ключу (ключевое слово «ВЕСНА», размер таблицы 8 × 5).

7. Зашифруйте сообщение «ИЛЛЮЗИИ, ЧЕМ БОЛЬШЕ О НИХ ДУМАЕШЬ, ИМЕЮТ СВОЙСТВО МНОЖИТЬСЯ, ПРИОБРЕТАТЬ БОЛЕЕ ВЫРАЖЕННУЮ ФОРМУ.» методом одиночной перестановки по ключу (ключевое слово «МЫСЛЕННО», размер таблицы 12 × 8).

8. Зашифруйте сообщение «МУЗЫКА ОБЛАДАЕТ МАГИЧЕСКОЙ СИЛОЙ – ВДРУГ СОБИРАЕТ РАССЕЯННЫЕ МЫСЛИ И ДАЕТ ПОКОЙ ВСТРЕВОЖЕННОЙ ДУШЕ.» методом одиночной перестановки по ключу (ключевое слово «ВЕДОМОСТЬ», размер таблицы 11 × 9).

9. Зашифруйте сообщение «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ» методом одиночной перестановки по ключу (ключевое слово «МЫСЛЕННО», размер таблицы 5 × 8).

10. Расшифруйте шифртекст «ЬЕСОУЬ,ГТСХК_ОАТООУ_НАД _ВДОЁЯПЫОВТЩР,СИСИО_ТШЯЙЖНОЬ_|_ИЕЙ_ТДТ_Н-ОЕЬОО_ЛН_», полученный методом одиночной перестановки по ключу (ключевое слово «РАБОТА», размер таблицы 12 × 6).

11. Расшифруйте шифртекст «АМЧЕМЮЕЕ_НТНМЛЕ,Ь_ЮВ_ШМДАТЕЕИЮЕ_Н_ТМСЬЗС_ОШНЯ», полученный методом одиночной перестановки по ключу (ключевое слово «ОСЕНЬ», размер таблицы 9 × 5).

12. Расшифруйте шифртекст «_ОВЯНВТИ_ЕМОНВ_ЕРО_КШЫВ ДАИЕЕЕСВ_НЛААЕ_АЮЕГК,ТТОТ_СС_ОКЯ», полученный методом одиночной перестановки по ключу (ключевое слово «ЛИНИЯ», размер таблицы 11 × 5).

13. Расшифруйте шифртекст «ААНТДОМНЫЕАСЫСХЛЖТХ_|_ЬЕА_ВОС_ЁСЫБТПТТЖСВРСРИТАИЯАТОХ_|_ШЬЯ_СШ», полученный методом одиночной перестановки по ключу (ключевое слово «РАБОТА», размер таблицы 10 × 6).

14. Расшифруйте шифртекст «ОЕОЕНЫТНБТЕЛОНЛ_|_ОРОЕТС_ОГМАУБЙОЫКЩЫ_|_,ОЕ_НД_ЙСБЕАВ_ТЕ_Р_ПВСБАКРУЦ», полученный методом одиночной перестановки по ключу (ключевое слово «СОНАТА», размер таблицы 11 × 6).

15. Зашифруйте сообщение «НИКТО НИЧЕГО НЕ МОЖЕТ СКАЗАТЬ ПРО ВАС. ЧТО БЫ ЛЮДИ НИ ГОВОРИЛИ, ОНИ ГОВОРЯТ ПРО САМИХ СЕБЯ» методом одиночной перестановки по ключу (размер таблицы 10 × 9, ключевая последовательность чисел – 713254986, сообщение записывается по строкам, считывается по столбцам).

16. Расшифруйте шифртекст «ЛДАЛК_|_|_НЫАЧЕЛГДПУЫНЕ_ГЛ_|_ДС_О_ОЧННЛСЮДАОТ,И_БДУ_ЕИ_ДВЗЩООСЬЫСЖ,УОИБГК_СИИ_ИАГВВИ_|_АБВОЬБТЖОЕИЕО», полученный методом одиночной перестановки по ключу (размер таблицы 12 × 8, ключевая последовательность чисел – 24173865, сообщение записывалось по строкам, считывалось по столбцам).

17. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ» методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 4321, 2341).

18. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ» методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 1324, 4321).

19. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ» методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 3421, 1432).

20. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ» методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 1243, 4213).

21. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ» методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 1342, 1324).

22. Расшифруйте шифртекст «ЕЛЫВ_ЮАТОГОТЯСЕД», полученный методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 4321, 1243).

23. Расшифруйте шифртекст «_ТРИ_Д_ВЗПОЕАЧАС», полученный методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 2341, 3214).

24. Расшифруйте шифртекст «_НОНАВОГЯПЬТЕМ_Р», полученный методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 2143, 2143).

25. Расшифруйте шифртекст «ТООГ_СШЕЕЮТАПЛРИ», полученный методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 1342, 4321).

Задание 2

Выполните шифрование/расшифрование согласно варианту, используя метод магического квадрата.

1. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

2. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

3. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

4. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

5. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

6. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

7. Расшифруйте шифртекст «АЕРУТНСВЧ», полученный при использовании метода магического квадрата 3 × 3.

2	7	6
9	5	1
4	3	8

8. Расшифруйте шифртекст «КЫПЕТКЛСА», полученный при использовании метода магического квадрата 3 × 3.

4	9	2
3	5	7
8	1	6

9. Расшифруйте шифртекст «ЮЯВОЫТ_СОЛЕТДАГЕ», полученный при использовании метода магического квадрата 4 × 4.

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

10. Расшифруйте шифртекст «ВОЫЮАЛМЬГО_ВЕТСО», полученный при использовании метода магического квадрата 4 × 4.

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

11. Расшифруйте шифртекст «ЗС_ТДРЕАИ_ЧОАП_В», полученный при использовании метода магического квадрата 4 × 4.

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

12. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

13. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», используя магический квадрат 4 × 4.

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

14. Зашифруйте сообщение «ВЕДОМОСТЬ», используя магический квадрат 3 × 3.

2	7	6
9	5	1
4	3	8

15. Зашифруйте сообщение «ВЕДОМОСТЬ», используя магический квадрат 3 × 3.

4	9	2
3	5	7
8	1	6

16. Зашифруйте сообщение «ВЕДОМОСТЬ», используя магический квадрат 3 × 3.

8	3	4
1	5	9
6	7	2

17. Зашифруйте сообщение «ВЫЛЕТАЮ ДЕСЯТОГО», используя магический квадрат 4 × 4.

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

18. Зашифруйте сообщение «ВЕДОМОСТЬ», используя магический квадрат 3 × 3.

6	1	8
7	5	3
2	9	4

19. Расшифруйте шифртекст «С_ЗЕПЮВТШЕИЖАРЬ_», полученный при использовании метода магического квадрата 4 × 4.

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

20. Расшифруйте шифртекст «АИРВЛ_ЗАЮЫВАПРТП», полученный при использовании метода магического квадрата 4 × 4.

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

21. Расшифруйте шифртекст «ОМНЬТ_ЕГЯНРАВ_ОП», полученный при использовании метода магического квадрата 4 × 4.

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

22. Расшифруйте шифртекст «ПАСЗ_В_Д_АВДЧОЕА», полученный при использовании метода магического квадрата 4 × 4.

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

23. Расшифруйте шифртекст «АЕЧЖД_ССИЬ_ОВВМ_», полученный при использовании метода магического квадрата 4 × 4.

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

24. Расшифруйте шифртекст «НЕКПРОАСР», полученный при использовании метода магического квадрата 3 × 3.

8	3	4
1	5	9
6	7	2

25. Расшифруйте шифртекст «ЕВИНЖРЫЕА», полученный при использовании метода магического квадрата 3 × 3.

6	1	8
7	5	3
2	9	4

Контрольные вопросы

1. Укажите возможные ключи шифрования методом перестановок.
2. Перечислите разновидности метода шифрующих таблиц.
3. Как выполняется шифрование методом двойной перестановки? Что при этом является ключом?
4. Что такое магический квадрат?
5. Как выполняется шифрование методом магического квадрата?

Отчетность по лабораторной работе

Выполните в рабочей тетради задания согласно своему варианту с подробным описанием хода решения.

ЛАБОРАТОРНАЯ РАБОТА 2
Шифрование с использованием систем Цезаря и системы Трисемуса

Цель работы: формирование умений шифрования с использованием систем Цезаря и системы Трисемуса.

Теоретические сведения

При шифровании *заменой* (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки).

Ключом шифрования является целое число 1 … N, где N – количество букв алфавита шифруемого слова, уменьшенное на 1. Ключ будет обозначаться символом K. При шифровании исходного текста каждая буква заменяется на другую букву того же алфавита. Заменяющая буква определяется путем смещения от исходной буквы алфавита на K букв. При достижении конца алфавита выполняется циклический переход к его началу.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы Цезаря. Ключ шифрования K примем равным 3.

Сначала сформируем таблицу подстановок, содержащую соответствующие пары букв исходного текста и шифртекста (табл. 2.1).

Таблица 2.1

↓	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с

↓	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в

При шифровании каждая буква исходного текста (из верхней строки таблицы) заменяется на соответствующую букву из нижней строки.

Таким образом, в результате шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» будет получен шифртекст «ТУЛОЗХГБКГЕХУГ».

Аффинная система подстановок Цезаря

При шифровании с использованием аффинной системы подстановок Цезаря буква с порядковым номером t в соответствующем алфавите заменяется на букву, порядковый номер которой в этом же алфавите рассчитывается по формуле $(at + b) \bmod m$, где a, b – числовые ключи, а m – количество букв в алфавите.

При выборе ключа a необходимо учитывать следующее требование: a и m должны быть взаимно простыми числами, то есть наибольший общий делитель a и m должен быть равен 1.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием аффинной системы подстановок Цезаря. Ключи шифрования примем следующими: $a = 4$, $b = 2$. Так как количество букв в алфавите $m = 33$, то требование к выбору ключа a соблюдается.

В первую очередь построим таблицу соответствия порядковых номеров букв исходного текста и шифртекста в соответствии с формулой (табл. 2.2). Нумерация букв начинается с 0.

Таблица 2.2

t	$4t + 2$	t	$4t + 2$	t	$4t + 2$	t	$4t + 2$
0	2	9	5	18	8	27	11
1	6	10	9	19	12	28	15
2	10	11	13	20	16	29	19
3	14	12	17	21	20	30	23
4	18	13	21	22	24	31	27
5	22	14	25	23	28	32	31
6	26	15	29	24	32		
7	30	16	0	25	3		
8	1	17	4	26	7		

Затем на основании табл. 2.2 построим таблицу соответствия конкретной букве исходного текста буквы шифртекста для заданных ключей шифрования (табл. 2.3).

Таблица 2.3

→		→		→		→	
а	в	и	е	с	з	ъ	к
б	ё	й	и	т	л	ы	о
в	й	к	м	у	п	ь	т
г	н	л	р	ф	у	э	ц
д	с	м	ф	х	ч	ю	ъ
е	х	н	ш	ц	ы	я	ю
ё	щ	о	ь	ч	я		
ж	э	п	а	ш	г		
з	б	р	д	щ	ж		

Соответствующим образом заменив буквы исходного текста «ПРИЛЕТАЮ ЗАВТРА», получим шифртекст «АДЕРХЛВЪБВЙЛДВ».

Система шифрования Цезаря с ключевым словом

Особенность системы шифрования Цезаря с ключевым словом – использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки. Для этой системы ключ должен быть составным и содержать некоторое число (например, k) и ключевое слово. Для числа k должно соблюдаться требование

$0 \le k < m - 1$,

где m – количество букв в алфавите.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы шифрования Цезаря с ключевым словом. Примем $k = 5$, в качестве ключевого слова будем использовать слово «РАБОТА».

Первым этапом шифрования является запись ключевого слова в таблицу подстановок, начиная с буквы исходного алфавита с номером k. Если ключевое слово имеет повторяющиеся буквы, в таблицу подстановок повторно они не записываются (табл. 2.4).

Таблица 2.4

№	→		№	→		№	→		№	→	
0	а		9	и	т	18	с		27	ъ	
1	б		10	й		19	т		28	ы	
2	в		11	к		20	у		29	ь	
3	г		12	л		21	ф		30	э	
4	д		13	м		22	х		31	ю	
5	е	р	14	н		23	ц		32	я	
6	ё	а	15	о		24	ч				
7	ж	б	16	п		25	ш				
8	з	о	17	р		26	щ				

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке (табл. 2.5).

Таблица 2.5

№	→		№	→		№	→		№	→	
0	а	ы	9	и	т	18	с	й	27	ъ	х
1	б	ь	10	й	в	19	т	к	28	ы	ц
2	в	э	11	к	г	20	у	л	29	ь	ч
3	г	ю	12	л	д	21	ф	м	30	э	ш
4	д	я	13	м	е	22	х	н	31	ю	щ
5	е	р	14	н	ё	23	ц	п	32	я	ъ
6	ё	а	15	о	ж	24	ч	с			
7	ж	б	16	п	з	25	ш	у			
8	з	о	17	р	и	26	щ	ф			

Таким образом, в результате шифрования исходного сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием данной системы шифрования получим шифртекст: «ЗИТДРКЫЩ ОЫЭКИЫ».

Система шифрования Трисемуса

Составной ключ шифрования в данной системе включает ключевое слово и размер таблицы подстановок.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы шифрования Трисемуса. В качестве ключевого слова будем использовать слово «РАБОТА», размер таблицы подстановки – 4 × 8.

Примечание – Так как при размере таблицы 4 × 8 в нее может быть записано только 32 буквы, из исходного алфавита будет исключена буква «ё».

В таблицу сначала по строкам вписывается ключевое слово, причем повторно встречающиеся в нем буквы не записываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку (табл. 2.6).

Таблица 2.6

р	а	б	о	т	в	г	д
е	ж	з	и	й	к	л	м
н	п	с	у	ф	х	ц	ч
ш	щ	ъ	ы	ь	э	ю	я

При шифровании в этой таблице находим очередную букву открытого текста и записываем в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Таким образом, при шифровании с помощью этой таблицы исходного сообщения «ПРИЛЕТАЮ ЗАВТРА» будет получен шифртекст «ЩЕУЦНЙЖГ СЖКЙЕЖ».

Содержание заданий

Задание 1

Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа соответствующим номеру варианта (например, для варианта 10 – ключ $K = 10$).

Задание 2

Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами, согласно своему варианту (табл. 2.7).

Таблица 2.7

Вариант	Ключ	Вариант	Ключ	Вариант	Ключ
1	$a = 5, b = 1$	10	$a = 7, b = 2$	19	$a = 5, b = 4$
2	$a = 2, b = 5$	11	$a = 8, b = 2$	20	$a = 7, b = 4$
3	$a = 4, b = 7$	12	$a = 2, b = 3$	21	$a = 8, b = 3$
4	$a = 2, b = 10$	13	$a = 4, b = 2$	22	$a = 4, b = 6$
5	$a = 7, b = 1$	14	$a = 5, b = 3$	23	$a = 5, b = 6$
6	$a = 8, b = 1$	15	$a = 7, b = 3$	24	$a = 7, b = 5$
7	$a = 2, b = 4$	16	$a = 8, b = 4$	25	$a = 8, b = 6$
8	$a = 4, b = 10$	17	$a = 2, b = 2$		
9	$a = 5, b = 2$	18	$a = 4, b = 5$		

Задание 3

Выполните шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту.

1. $k = 1$, ключевое слово «РАДОСТЬ».
2. $k = 2$, ключевое слово «УСПЕХ».
3. $k = 3$, ключевое слово «УДАЧА».
4. $k = 4$, ключевое слово «ЛЕТО».

5. k = 5, ключевое слово «ВЕСНА».
6. k = 6, ключевое слово «ЗИМА».
7. k = 7, ключевое слово «ОСЕНЬ».
8. k = 8, ключевое слово «АЛГОРИТМ».
9. k = 9, ключевое слово «ПРОГРАММИРОВАНИЕ».
10. k = 10, ключевое слово «КРИПТОГРАФИЯ».
11. k = 11, ключевое слово «КРИПТОАНАЛИЗ».
12. k = 12, ключевое слово «ШИФРТЕКСТ».
13. k = 13, ключевое слово «ОРЕХИ».
14. k = 14, ключевое слово «ТЕЛЕФОН».
15. k = 15, ключевое слово «КОМПЬЮТЕР».
16. k = 16, ключевое слово «ЧАСЫ».
17. k = 17, ключевое слово «МУЗЫКА».
18. k = 18, ключевое слово «РУЧКА».
19. k = 19, ключевое слово «ИНФОРМАЦИЯ».
20. k = 20, ключевое слово «РАБОТА».
21. k = 21, ключевое слово «СОЛНЦЕ».
22. k = 22, ключевое слово «ПЕРЕМЕНЫ».
23. k = 23, ключевое слово «ЖИЗНЬ».
24. k = 24, ключевое слово «ЛАБОРАТОРНАЯ».
25. k = 25, ключевое слово «СПРАВОЧНИК».

Задание 4

Выполните шифрование сообщения «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя систему Трисемуса с ключевым словом из задания 3. Размер таблицы подстановок 4 × 8.

Контрольные вопросы

1. В чем особенность шифров простой замены?
2. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?
3. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?
4. Для каких шифров простой замены используется составной ключ?
5. Каким образом заполняется таблица подстановок для шифрования с использованием системы Трисемуса?

Отчетность по лабораторной работе

Выполните в рабочей тетради задания согласно своему варианту с подробным описанием хода решения.

ЛАБОРАТОРНАЯ РАБОТА 3
Реализация алгоритма шифрования Плейфейра

Цель работы: формирование умений шифрования с использованием алгоритма шифрования Плейфейра.

Теоретические сведения

В основе алгоритма Плейфейра – использование шифрующей таблицы, формируемой аналогично таблице подстановок Трисемуса. Составной ключ шифрования также включает ключевое слово и размер шифрующей таблицы.

Для демонстрации процедуры шифрования используется таблица подстановок Трисемуса 4 × 8 для ключевого слова «РАБОТА» (табл. 2.6).

Процедура шифрования включает следующие шаги:

1. Открытый текст исходного сообщения разбивается на пары букв (*биграммы*). Шифруемый текст должен иметь четное количество букв, и в нем не должно быть биграмм, содержащих две одинаковые буквы.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

а) если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и Й в табл. 2.6), тогда находят буквы в углах прямоугольника, определяемого данной парой букв. В нашем примере это буквы АЙТЖ. Пара букв АЙ отображается в пару ТЖ. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста;

б) если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются

буквы, которые лежат под ними. Например, биграмма ОУ дает биграмму шифртекста ИЫ. Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца;

в) если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. Например, биграмма НС дает биграмму шифртекста ПУ. Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке. Например, биграмма КМ дает биграмму шифртекста ЛЕ.

Таким образом, в результате шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием алгоритма Плейфейра для рассматриваемых ключей получим шифртекст «НАЙМЙРГЩ ЖБГВАБ».

Содержание задания

Зашифруйте сообщение, используя алгоритм Плейфейра согласно своему варианту (табл. 3.1). Размер шифрующей таблицы 4 × 8.

Таблица 3.1

Вариант	Сообщение	Ключевое слово
1	За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами	РАДОСТЬ
2	Смысл жизни подобен карабканию по канату, который мы же сами подкинули в воздух	УСПЕХ
3	Первые каналы связи были очень простыми, их организовывали с помощью надежных курьеров	ЛЕТО
4	Проблемы конфиденциальности и целостности тесно связаны между собой	УДАЧА
5	Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом	ЛАБОРАТОРНАЯ
6	В симметричной криптосистеме секретный ключ передается по защищенному каналу	СПРАВОЧНИК

Продолжение табл. 3.1

Вариант	Сообщение	Ключевое слово
7	Знания бывают двоякого рода: либо мы что-нибудь знаем, либо мы знаем, где най-ти сведения об этом	ПРАЗДНИК
8	Оптимист – это человек, который еще не читал утренних газет	КАНИКУЛЫ
9	Криптосистема является криптостойкой, если предпринятые криптоаналитические атаки не достигают поставленных целей	КОМПЬЮТЕР
10	Стойкость шифра должна определяться только секретностью ключей	РУЧКА
11	Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника	КИНОТЕАТР
12	Криптосистема, реализующая семейство криптографических преобразований, обычно является открытой системой	ФИАЛКА
13	Если мечтаешь о радуге, будь готов к дождю	ИНФОРМАЦИЯ
14	Самый непобедимый человек – это тот, кому не страшно быть глупым	РАБОТА
15	Системы шифрования дисковых данных могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков	ВЕСНА
16	Другим классификационным признаком систем шифрования является способ их функционирования	СОЛНЦЕ
17	Тот, кто смотрит на дело с обеих сторон, обычно не видит ни одной из них	ЖИЗНЬ
18	Системы второго типа являются утилитами шифрования, которые необходимо специально вызывать	ПЕРЕМЕНЫ
19	В случае канального шифрования защищается информация, передаваемая по каналу связи, включая служебную	ПИСЬМО
20	Лотерея – наиболее точный способ учета количества оптимистов	МАРКЕР
21	Защищается только содержание сообщений, служебная информация остается открытой	КАРАНДАШ

Окончание табл. 3.1

Вариант	Сообщение	Ключевое слово
22	При обмене данными по сетям возникает проблема установления подлинности авторов	ЦВЕТОК
23	Получатель проверяет цифровую подпись, используя при этом открытый ключ	ВЕТЕР
24	В системах прозрачного шифрования преобразования осуществляются незаметно для пользователя	ПАПКА
25	Счастливые обстоятельства создают друзей, печальные – их испытывают	ЗАНЯТИЕ

Контрольные вопросы

1. Как формируется шифрующая таблица для реализации алгоритма Плейфейра?
2. Какие ограничения накладываются на шифруемый текст?
3. Что такое биграмма?
4. В чем заключается процедура шифрования с помощью алгоритма Плейфейра?

Отчетность по лабораторной работе

Выполните в рабочей тетради задания согласно своему варианту с подробным описанием хода решения.

ЛАБОРАТОРНАЯ РАБОТА 4
Шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона

Цель работы: формирование умений шифрования с использованием системы Вижинера и шифра «двойной квадрат» Уитстона.

Теоретические сведения

Шифры *сложной замены* называют многоалфавитными, так как для шифрования каждого символа исходного сообщения

применяют свой шифр простой замены. К таким шифрам относятся система Вижинера и «двойной квадрат» Уитстона.

Система Вижинера

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены описывается таблицей шифрования, называемой таблицей Вижинера (Приложение А).

Таблица Вижинера имеет два входа:

- верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;
- крайний левый столбец ключа.

Последовательность ключей получают из порядковых номеров в алфавите букв ключевого слова (начиная с 0).

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ДЕСЯТОГО». Ключевое слово – «РАБОТА».

Ход шифрования и его результат отображены в табл. 4.1.

Таблица 4.1

Сообщение	п	р	и	л	е	т	а	ю		д	е	с	я	т	о	г	о
Ключ. слово	р	а	б	о	т	а	р	а		б	о	т	а	р	а	б	о
Ключи	16	0	1	14	18	0	16	0		1	14	18	0	16	0	1	14
Шифртекст	я	р	й	щ	ч	т	р	ю		е	у	г	я	в	о	д	ь

Шифр «двойной квадрат» Уитстона

Шифр «двойной квадрат» использует две таблицы со случайно расположенными в них буквами русского алфавита, размещенными по одной горизонтали; шифрование идет биграммами, как в шифре Плейфейра. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется от-

дельно. Первую букву биграммы находят в левой таблице, а вторую букву в правой. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Пример шифрующих таблиц для данного метода приведен на рис. 4.1.

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

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

Рис. 4.1

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, то есть получаем биграмму шифртекста ОВ.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Вторая буква биграммы шифртекста берется из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ.

Таким образом, в результате шифрования сообщения «ПРИЛЕТАЮ ШЕСТОГО» будет получен шифртекст «ПЕОВЩНФМЕШРФ ЖБДЦ».

Содержание заданий

Задание 1

Используя систему Вижинера, зашифруйте сообщения. Текст сообщения и ключевое слово должны соответствовать варианту задания лабораторной работы 3.

Задание 2

Используя шифр «двойной квадрат» Уитстона и шифрующие таблицы, представленные на рис. 4.1, выполните шифрование сообщения из задания лабораторной работы 3.

Контрольные вопросы

1. Чем шифры сложной замены отличаются от шифров простой замены?
2. Что используется в качестве ключа в системе Вижинера?
3. Как осуществляется шифрование текста с использованием системы Вижинера?
4. Какие требования предъявляются к шифруемому тексту при использовании шифра «двойной квадрат» Уитстона?
5. Как осуществляется шифрование текста с использованием шифра «двойной квадрат» Уитстона?

Отчетность по лабораторной работе

Выполните в рабочей тетради задания согласно своему варианту с подробным описанием хода решения.

ЛАБОРАТОРНАЯ РАБОТА 5
РЕАЛИЗАЦИЯ ЭЛЕМЕНТОВ КРИПТОСИСТЕМЫ RSA

Цель работы: формирование умений шифрования с использованием метода асимметрического шифрования RSA.

Теоретические сведения

RSA относится к так называемым *асимметричным алгоритмам*, у которых ключ шифрования не совпадает с ключом рас-