ГУАП

КАФЕДРА № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

канд. техн. наук, доцент		В. А. Рындюк
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ

Лабораторная работа по криптографии №1

по курсу: Защита информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ гр. № 4131з		М. Д. Быстров
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2026

Задание

ЗАДАНИЕ 1. Осуществить шифровку текста (с проверкой) шифром циклических подстановок (иначе шифром Цезаря), с прогоном текста 4, 5 и 6 интервалов. В состав алфавита не включать буквы «Й» и «Ё». Ниже приведены варианты текста требующие его шифрации.

Вариант 3.

ВСТРЕЧАЕМСЯ В ПАРКЕ ПАРОЛЬ И ОТЗЫВ ТЕ ЖЕ

Выполнение задания

Для выполнения шифровки необходимо составить таблицу с зашифрованным алфавитом для каждого прогона текста, затем заменить каждую букву из текста на соответствующую ей букву из второй строки таблицы с алфавитом. Для проверки шифра необходимо провести обратную операцию и для каждой буквы зашифрованного текста подставить букву из первой строки таблицы с алфавитом, после чего сравнить получившийся текст.

1. Прогон текста – 4 символа:

Алфавит:

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

Шифрование и проверка:

В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Исходный
Ж	Х	Ц	Ф	К	Ы	Д	К	Р	Х	Г	Ж	У	Д	Ф	О	К	У	Д	Ф	Т	П	А	Н	Т	Ц	М	Я	Ж	Ц	К	Л	К	Шифрованный
В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Дешифрованный

2. Прогон текста – 5 символов:

Алфавит:

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
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

Шифрование и проверка:

В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Исходный
З	Ц	Ч	Х	Л	Ь	Е	Л	С	Ц	Д	З	Ф	Е	Х	П	Л	Ф	Е	Х	У	Р	Б	О	У	Ч	Н	А	З	Ч	Л	М	Л	Шифрованный
В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Дешифрованный

3. Прогон текста – 6 символов:

Алфавит:

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
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

Шифрование и проверка:

В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Исходный
И	Ч	Ш	Ц	М	Э	Ж	М	Т	Ч	Е	И	Х	Ж	Ц	Р	М	Х	Ж	Ц	Ф	С	В	П	Ф	Ш	О	Б	И	Ш	М	Н	М	Шифрованный
В	С	Т	Р	Е	Ч	А	Е	М	С	Я	В	П	А	Р	К	Е	П	А	Р	О	Л	Ь	И	О	Т	З	Ы	В	Т	Е	Ж	Е	Дешифрованный

ЗАДАНИЕ 2. Осуществить шифровку текста (с проверкой), используя шифр спартанцев, с прогоном текста 4, 5 и 6 интервалов. Ниже приведены варианты текста требующие его шифрации.

Вариант 3.

СИММЕТРИЧНЫЕ СИСТЕМЫ ДЕЛЯТСЯ НА БЛОЧНЫЕ И ПОТОЧНЫЕ

Выполнение задания

Для каждого из прогонов по алгоритму необходимо составить матрицу с N+1 строк, где N-прогон текста, в которой исходный текст будет записан по столбцам. Затем прочитать текст из матрицы построчно, получив зашифрованное сообщение.

Для восстановления надо зашифрованное сообщение уместить в такую же матрицу, количество символов в строке которой можно вычислить, используя длину текста и известную величину прогона текста. Далее прочитать текст из матрицы по столбцам, в результате чего получится исходное сообщение.

В данном случае длина текста (без пробелов) – 44 символа

1. Прогон текста – 4 интервала

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

Составленная матрица:

С Т Ы Т Е Я О И Ч

И Р Е Е Л Н Ч П Н

М И С М Я А Н О Ы

М Ч И Ы Т Б Ы Т Е

Е Н С Д С Л Е О

Закодированное сообщение:

СТЫТЕЯОИЧИРЕЕЛНЧПНМИСМЯАНОЫМЧИЫТБЫТЕЕНСДСЛЕО

Кол-во символов в строке = 44 / (4+1) = 8, остаток 4 – что дает длину строки 9 символов у четырех строк и 8 символов у пятой строки.

Составленная матрица:

С Т Ы Т Е Я О И Ч

И Р Е Е Л Н Ч П Н

М И С М Я А Н О Ы

М Ч И Ы Т Б Ы Т Е

Е Н С Д С Л Е О

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

2. Прогон текста – 5 интервала

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

Составленная матрица:

С Р С Ы С О П Ы

И И И Д Я Ч О Е

М Ч С Е Н Н Т

М Н Т Л А Ы О

Е Ы Е Я Б Е Ч

Т Е М Т Л И Н

Закодированное сообщение:

СРСЫСОПЫИИИДЯЧОЕМЧСЕННТМНТЛАЫОЕЫЕЯБЕЧТЕМТЛИН

Кол-во символов в строке = 44 / (5+1) = 7, остаток 2 – что дает длину строки 8 символов у строк 1, 2 и 7 символов у остальных строк.

Составленная матрица:

С Р С Ы С О П Ы

И И И Д Я Ч О Е

М Ч С Е Н Н Т

М Н Т Л А Ы О

Е Ы Е Я Б Е Ч

Т Е М Т Л И Н

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

3. Прогон текста – 6 интервалов

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

Составленная матрица:

С И С Л Б И Ы

И Ч Т Я Л П Е

М Н Е Т О О

М Ы М С Ч Т

Е Е Ы Я Н О

Т С Д Н Ы Ч

Р И Е А Е Н

Закодированное сообщение:

СИСЛБИЫИЧТЯЛПЕМНЕТООМЫМСЧТЕЕЫЯНОТСДНЫЧРИЕАЕН

Кол-во символов в строке = 44 / (6+1) = 6, остаток 2 – что дает длину строки 7 символов у строк 1, 2 и 6 символов у остальных строк.

Составленная матрица:

С И С Л Б И Ы

И Ч Т Я Л П Е

М Н Е Т О О

М Ы М С Ч Т

Е Е Ы Я Н О

Т С Д Н Ы Ч

Р И Е А Е Н

Исходное сообщение:

СИММЕТРИЧНЫЕСИСТЕМЫДЕЛЯТСЯНАБЛОЧНЫЕИПОТОЧНЫЕ

ЗАДАНИЕ 3. Осуществить шифровку текста (с проверкой), используя шифр перестановки по ключевому слову. Ниже приведены варианты ключевых слов и сам текст шифрации.

Вариант 3.

Ключевые слова: КРИСТАЛЛ (6 символов в столбце), ЕВРОПА (5 символов в столбце).

Текст: СИММЕТРИЧНЫЕ СИСТЕМЫ ДЕЛЯТСЯ НА БЛОЧНЫЕ И ПОТОЧНЫЕ

Выполнение задания.

Для шифрования необходимо записать в таблицу с заданным количеством строк исходный текст поколоночно, каждой из колонок сопоставить букву ключевого слова, затем упорядочить колонки соответственно алфавитному порядку сопоставленных букв. Из получившейся таблицы построчно взять текст, который и будет представлять из себя шифр.

Для расшифровки необходимо проделать обратную операцию: записать в таблицу зашифрованное сообщение построчно, рассчитав длину строки, зная длину зашифрованного текста и количество строк таблицы. Затем сопоставить столбцы таблицы с буквами отсортированного в алфавитном порядке ключевого слова и привести слово и сопоставленные столбцы к первоначальному порядку, после чего можно прочитать исходное сообщение, двигаясь по колонкам таблицы.

1. Ключевое слово: КРИСТАЛЛ, 6 символов в столбце.

Таблица до перестановки:

К Р И С Т А Л Л К

3 7 2 8 9 1 5 6 4

С Р - М Я А Н П Ы

И И С Ы Т - Ы О Е

М Ч И - С Б Е Т -

М Н С Д Я Л - О -

Е Ы Т Е - О И Ч -

Т Е Е Л Н Ч - Н -

Таблица после перестановки:

А И К К Л Л Р С Т

1 2 3 4 5 6 7 8 9

А - С Ы Н П Р М Я

- С И Е Ы О И Ы Т

Б И М - Е Т Ч - С

Л С М - - О Н Д Я

О Т Е - И Ч Ы Е -

Ч Е Т - - Н Е Л Н

Зашифрованное сообщение:

А-СЫНПРМЯ-СИЕЫОИЫТБИМ-ЕТЧ-СЛСМ--ОНДЯОТЕ-ИЧЫЕ-ЧЕТ—НЕЛН

Для обратной операции необходимо рассчитать длину строки: 54/6 = 9. Дальнейшие действия очевидны на примере вышеприведенных таблиц.

2. Ключевое слово: ЕВРОПА, 5 символов в столбце.

Таблица до перестановки:

Е В Р О П А Е В Р О

4 2 9 6 8 1 5 3 10 7

С Т Ы С - Т А Ч И О

И Р Е Т Д С - Н - Ч

М И - Е Е Я Б Ы П Н

М Ч С М Л - Л Е О Ы

Е Н И Ы Я Н О - Т Е

Таблица после перестановки:

А В В Е Е О О П Р Р

1 2 3 4 5 6 7 8 9 10

Т Т Ч С А С О - Ы И

С Р Н И - Т Ч Д Е -

Я И Ы М Б Е Н Е - П

- Ч Е М Л М Ы Л С О

Н Н - Е О Ы Е Я И Т

Зашифрованное сообщение:

ТТЧСАСО-ЫИСРНИ-ТЧДЕ-ЯИЫМБЕНЕ-П-ЧЕМЛМЫЛСОНН-ЕОЫЕЯИТ

Для обратной операции необходимо рассчитать длину строки: 50/5 = 10. Дальнейшие действия очевидны на примере вышеприведенных таблиц.

ЗАДАНИЕ 4. Шифровка текста на русском языке произведена с использованием шифра Цезаря. Осуществить дешифрацию текста, приведенного ниже, если известно, что кратность прогона текста лежит в интервале от 2 до 6. В состав алфавита не включать буквы «Й» и «Ё». Ниже приведены варианты шифротекста

Вариант 3.
ТУМЫИО ЦЕМЗИО ТСДИЗМО

Выполнение задания.

Прогон текста найден перебором, он равен 3.

Алфавит:

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
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

Шифрование и проверка:

Т	У	М	Ы	И	О	Ц	Е	М	З	И	О	Т	С	Д	И	З	М	О	Шифрованный
П	Р	И	Ш	Е	Л	У	В	И	Д	Е	Л	П	О	Б	Е	Д	И	Л	Дешифрованный

ЗАДАНИЕ 5. Шифровка текста на русском языке произведена с использованием шифра спартанцев. Осуществить дешифрацию текста, приведенного ниже, если известно,

что кратность прогона текста лежит в интервале от 2 до 7. Ниже приведены варианты шифротекста

Вариант 3.

Н_ЦТ_АОИОСЧПИГЕАЕ_ОМЛРП_ЬОАЯВ

Выполнение задания.

Прогон текста найден перебором, он равен 5.

Составленная матрица с количеством строк 5+1=6:

```
Н _ Ц Т _
А О И О С
Ч П И Г Е
А Е _ О М
Л Р П _ Ь
О А Я В
```

Расшифрованное сообщение: НАЧАЛО_ОПЕРАЦИИ_ПЯТОГО_В_СЕМЬ

ЗАДАНИЕ 6. Шифровка текста на русском языке произведена с использованием шифра перестановки по ключевому слову. Осуществить дешифрацию текста, приведенного ниже, если известны возможные варианты ключевых слов, а также возможные варианты числа символов в строке.

Вариант 3.

Возможные варианты ключевых слов: АЛМАЗ.
Количество строк: 4, 5 или 6.

Шифротекст: ЯБЖБОВЫЕИВАТТЛЬСЬ.ЛЕЛМ.ЮЩЮО.БЕ

Выполнение задания.

Перебором было найдено подходящее количество строк, оно равно 6.

Таблица с зашифрованным сообщением:

```
А А З Л М
1 2 3 4 5
Я Б Ж Б О
В Ы Е И В
А Т Т Л Ь
С Ь . Л Е
Л М . Ю Щ
```

Ю О . Б Е

Таблица с расшифрованным сообщением:

А Л М А З

1 4 5 2 3

Я Б О Б Ж

В И В Ы Е

А Л Ь Т Т

С Л Е Ь .

Л Ю Щ М .

Ю Б Е О .

Расшифрованное сообщение: ЯВАСЛЮБИЛЛЮБОВЬЕЩЕБЫТЬМОЖЕТ...

Вывод

В ходе выполнения первой лабораторной работы были получены навыки применения на практике шифра Цезаря, шифра спартанцев и шифра с перестановкой ключевым словом.

Произведено шифрование текста различными шифрами в соответствии с вариантом.

Произведен подбор параметров шифров для расшифровки исходного сообщения.