ГУАП

КАФЕДРА № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

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

ЛАБОРАТОРНАЯ РАБОТА

КРИПТОГРАФИЯ

Вариант 7

по курсу: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 4128		В. А. Воробьев
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2025

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.

Текст: РАСШИФРОВКА ПРОЦЕСС ОБРАТНОГО ПРИМЕНЕНИЯ ШИФРА

Создадим таблицы прогонов для 4, 5 и 6 интервалов.

Таблица 1 – 4 интервала

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

Таблица 2 – 5 интервалов

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

Таблица 3 – 6 интервалов

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

Далее на основе созданных таблиц зашифруем текст: Получившийся зашифрованный текст шифром Цезаря:

По 4 интервалам: ФДХЪНШФТЖОДУФТЬКХХТЕФДЦСТЗТУФНРКСКСНГЪНШФФ

По 5 интервалам: ХЕЦЭОЩХУЗПЕФХУЫЛЦЦУЖХЕЧТУИУФХОСЛТЛТОДЭОЩХЕХ

По 6 интервалам: ЦЖЧЮПЬЦФИРЖХЦФЪМЧЧФЗЦЖШУФКФХЦПТМУМУП ЕЮПЬЦЖЦ

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.

Текст: КРИПТОГРАФИЯ НАУКА БЕЗОПСНОЙ СВЯЗИ

В исходном тексте 32 символов. Для шифровки составим матрицы состоящие из строк в количестве числа интервалов +1.

Таблица 7 – 4 интервала

К	О	И	К	О	О	З
Р	Г	Я	А	П	Й	И
И	Р	Н	Б	А	С	-
П	А	А	Е	С	В	-
Т	Ф	У	З	Н	Я	-

Таблица 8 – 5 интервала

К	Г	Н	Е	Н	З
Р	Р	А	З	О	И
И	А	У	О	Й	-
П	Ф	К	П	С	-
Т	И	А	А	В	-
О	Я	Б	С	Я	-

Таблица 9 – 6 интервала

К	Р	У	П	В
Р	А	К	А	Я
И	Ф	А	С	З
П	И	Б	Н	И
Т	Я	Е	О	-
О	Н	З	Й	-
Г	А	О	С	-

Получившийся зашифрованный текст шифром древней Спарты:

По 4 интервалам: КОИКООЗРГЯАПЙИИРНБАСПААЕСВТФУЗНЯ

По 5 интервалам: КГНЕНЗРРАЗОИИАУОЙПФКПСТИААВОЯБСЯ

По 6 интервалам: КРУПВРАКАЯИФАСЗПИБНИТЯЕООНЗЙГАОС

Дешифровка производится путём составления аналогичных таблиц, но уже в обратном порядке на основе зашифрованного текста.

Таблица 10 – Дешифровка через 4 интервала

К	О	И	К	О	О	З	-
Р	Г	Я	А	П	Й	И	-
И	Р	Н	Б	А	С	-	-
П	А	А	Е	С	В	-	-
Т	Ф	У	З	Н	Я	-	-

Таблица 11 – Дешифровка через 5 интервалов

К	Г	Н	Е	Н	З
Р	Р	А	З	О	И
И	А	У	О	Й	-
П	Ф	К	П	С	-
Т	И	А	А	В	-
О	Я	Б	С	Я	-

Таблица 12 – Дешифровка через 6 интервалов

К	Р	У	П	В
Р	А	К	А	Я
И	Ф	А	С	З
П	И	Б	Н	И
Т	Я	Е	О	-
О	Н	З	Й	-
Г	А	О	С	-

В итоге во всех случаях дешифровки получился исходный текст: КРИПТОГРАФИЯНАУКАБЕЗОПАСНОЙСВЯЗИ

ЗАДАНИЕ 3. Осуществить шифровку текста (с проверкой), используя шифр перестановки по ключевому слову.

Ключевые слова: ВЕКТОР (3 символа в столбце), УГОЛ (6 символов в столбце).

Текст: КРИПТОГРАФИЯ НАУКА БЕЗОПСНОЙ СВЯЗИ

Построим таблицы на основе ключевых слов, после чего запишем в них исходный текст по вертикали, а затем поменяем столбцы в соответствии с алфавитным порядком букв в ключевом слове.

Таблица 13

В	Е	К	Т	О	Р	В	Е	К	Т	О	Р
1	3	5	11	7	9	2	4	6	12	8	10
К	П	Г	Ф	-	У	-	З	А	О	С	З
Р	Т	Р	И	Н	К	Б	О	С	Й	В	И
И	О	А	Я	А	А	Е	П	Н	-	Я	-

В	В	Е	Е	К	К	О	О	Р	Р	Т	Т	
1	2	3	4	5	6	7	8	9	10		11	12
К	-	П	З	Г	А	-	С	У	З	Ф	О	
Р	Б	Т	О	Р	С	Н	В	К	И	И	Й	
И	Е	О	П	А	Н	А	Я	А	-	Я	-	

Таблица 14

У	Г	О	Л	У	Г
5	1	4	3	6	2
К	Г	Я	А	П	-
Р	Р	-	-	А	С
И	А	Н	Б	С	В
П	Ф	А	Е	Н	Я
Т	И	У	З	О	З
О	Я	К	О	Й	И

Г	Г	Л	О	У	У
1	2	3	4	5	6
Г	-	А	Я	К	П
Р	С	-	-	Р	А
А	В	Б	Н	И	С
Ф	Я	Е	А	П	Н
И	З	З	У	Т	О
Я	И	О	К	О	Й

Получившийся зашифрованный текст шифром одиночной перестановки по ключевому слову:

С ключевым словом ВЕКТОР (3 символа в столбце):

К-ПЗГА-СУЗФОРБТОРСНВКИИЙИЕОПАНАЯА-Я-

С ключевым словом УГОЛ (6 символов в столбце)::

Г-АЯКПРС—РААВБНИСФЯЕАПНИЗЗУТОЯИОКОЙ

Для дешифровки все происходит в обратном виде.

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».

Текст: УФНЪКП ЧЖНИКП УТЕКИНП

Начнём строить таблицы со смещением от 2 до 6 и будем дешифровать текст, пока не найдём нужное смещение.

Таблица 17 – 2 интервала

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

СТЛЬЗН - неверно.

Таблица 18 – 3 интервала

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

РСКЩЖМ - неверно.

Таблица 19 – 4 интервала

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

Дешифрованный текст: ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ

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.

Текст: НПП_АЕЯСЧРТЕААОМЛЦГЬОИО_И_О_В

Количество символов 29.

Таблица 23 – Дешифровка через 2 интервала

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

Таблица 24 – Дешифровка через 3 интервала

Н	П	П	-	А	У	Я	С
Ч	Р	Т	А	А	О	М	-
Л	Ц	Г	Ь	О	И	О	-
-	И	-	О	-	В	-	-

Таблица 25 – Дешифровка через 4 интервала

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

Таблица 26 – Дешифровка через 7 интервалов

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

НАЧАЛО ОПЕРАЦИИ ПЯТОГО В СЕМЬ - текст дешифрован.

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.

Текст: КЛ-А-ФРЮБНРРИЧЕААОПАЗЛСВТ--ИШКО-КЗИА

Возможные варианты ключевых слов: УЛИТКА или ВОСТОК.

Количество символов в столбце: 5 или 6.

Таблица 28 - ВОСТОК (6 строк)

В	К	О	О	С	Т
К	Л	-	А	-	Ф
Р	Ю	Б	Н	Р	Р
И	Ч	Е	А	А	О
П	А	З	Л	С	В
Т	-	-	И	Ш	К
О	-	К	З	И	А

Таблица 29

В	О	С	Т	О	К
К	А	-	Ф	-	Л
Р	Н	Р	Р	Б	Ю
И	А	А	О	Е	Ч
П	Л	С	В	З	А
Т	И	Ш	К	-	-
О	З	И	А	К	-

Дешифрованный текст: КРИПТОАНАЛИЗ РАСШИФРОВКА БЕЗ КЛЮЧА.