ЛАБОРАТОРНАЯ РАБОТА 1

ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДА

ШИФРУЮЩИХ ТАБЛИЦ И МЕТОДА МАГИЧЕСКОГО КВАДРАТА

**Цель работы**: формирование умений шифрования с исполь-

зованием методов шифрующих таблиц и магического квадрата.

Вариант 4

**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 пробе-

лов разделяются символом «|».

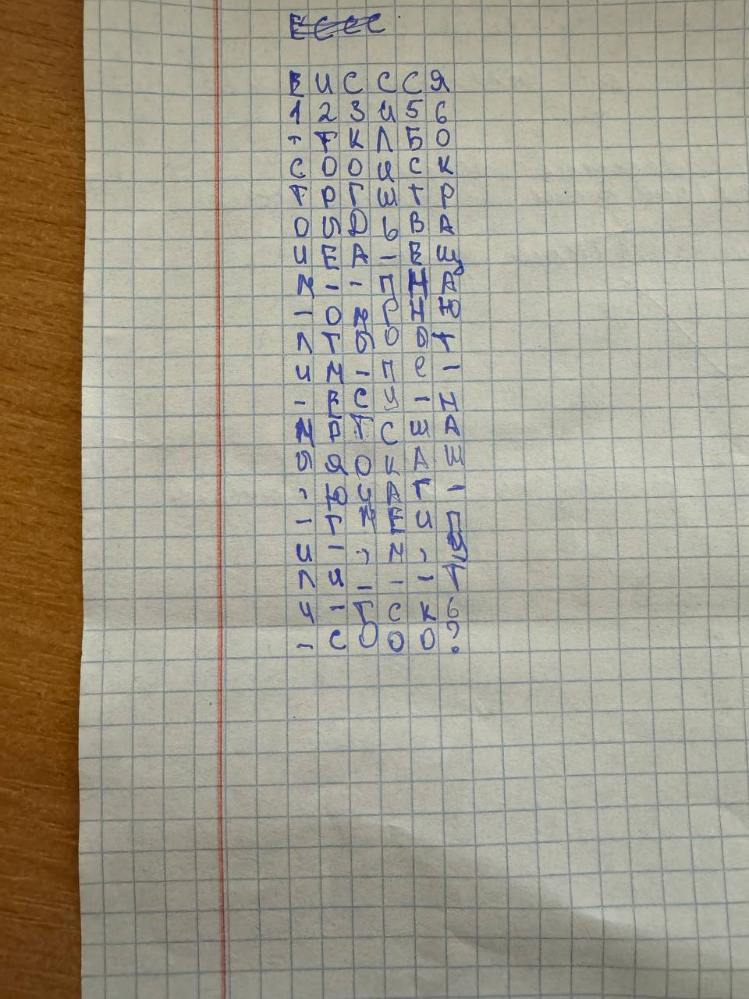
4. Зашифруйте сообщение «КОГДА МЫ СТОИМ, ТО СТОИМ

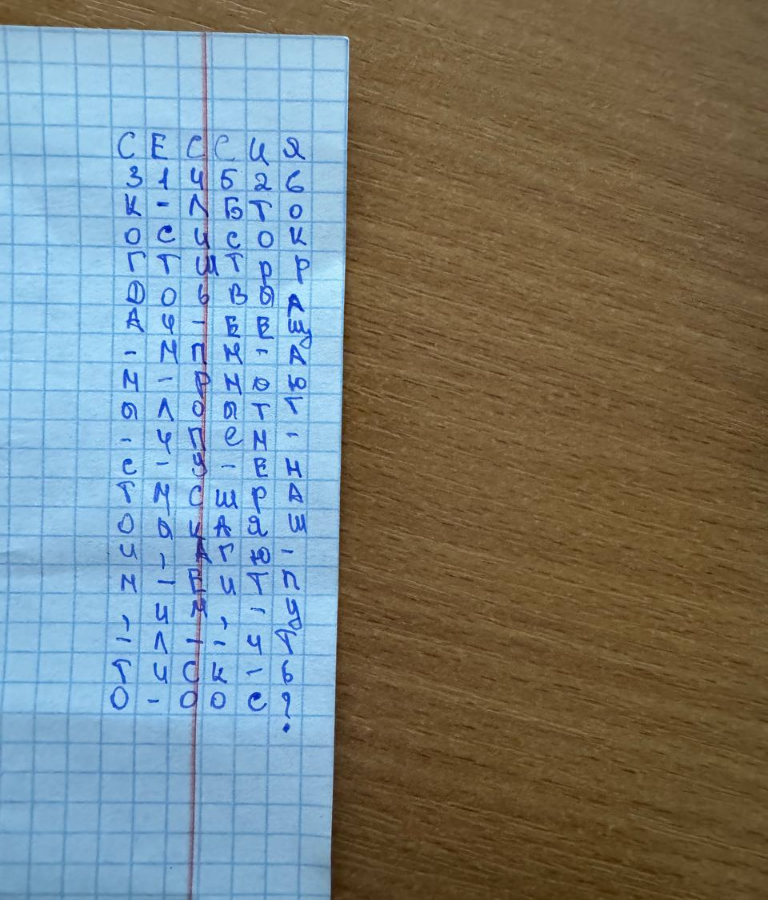
ЛИ МЫ, ИЛИ ЛИШЬ ПРОПУСКАЕМ СОБСТВЕННЫЕ ШАГИ, КОТОРЫЕ

ОТМЕРЯЮТ И СОКРАЩАЮТ НАШ ПУТЬ?» методом одиночной пе-

рестановки по ключу (ключевое слово «СЕССИЯ», размер табли-

цы 18 × 6).





Зашифрованная пословица: -ТКЛБОСООИСКТРГШТРОЫДЬВАИЕА-ЕЩМ—ПНА-ОМРНЮЛТЫОЫТИМ-ПЕ-ЕСУ-НМРТСШАЫЯОКАШ,ЮИАГ—ГМЕИПИ-,М,УЛИ---ТИ-ТСКЬ-СООО?

**Задание 2**

Выполните шифрование/расшифрование согласно варианту,

используя метод магического квадрата.

4. Зашифруйте сообщение «ВРЕМЕНА МЕНЯЮТСЯ», исполь-

зуя магический квадрат 4 × 4.

14 11 5 4

1 8 10 15

12 13 3 6

7 2 16 9

|  |  |  |  |
| --- | --- | --- | --- |
| Т | Н | Е | М |
| В | \_ | Е | С |
| Я | Ю | Е | Н |
| А | Р | Я | М |

Шифртекст: ТНЕМВ\_ЕСЯЮЕНАРЯМ

**Контрольные вопросы**

1. Укажите возможные ключи шифрования методом перестановок.

* Номера позиций символов в открытом тексте, которые указывают порядок перестановки;
* Определённый алгоритм или правило, обозначающее, как именно переставляются символы (например, по определённым предыдущим или случайным числам);
* Секретный ключ, который может быть представлен в виде числа, последовательности чисел или текстовой строки.

1. Перечислите разновидности метода шифрующих таблиц.

* Прямые таблицы подстановки (где каждый символ заменяется другим символом);
* Обратные таблицы подстановки (где символы заменяются с использованием обратного ключа);
* Блочные шифры, использующие таблицы для шифрования фиксированных блоков текста;
* Многоуровневые таблицы, где шифрование выполняется на нескольких уровнях с разными правилами.

1. Как выполняется шифрование методом двойной перестановки? Что при этом является ключом?

* Сначала открытый текст разбивается на строки или блоки.
* Затем выполняется первая перестановка, основанная на первичном ключе, которая изменяет порядок символов в строках или блоках.
* После этого результат первой перестановки повторно переставляется с использованием второго ключа. Ключом при этом служат два (или более) числа, указывающие порядок перестановки символов в каждой из операций.

1. Что такое магический квадрат?

Магический квадрат — это квадратная матрица чисел, в которой сумма чисел в каждой строке, каждом столбце и обеих диагоналях одинаковая. Каждое число в магическом квадрате уникально и находится в определённом диапазоне.

1. Как выполняется шифрование методом магического квадрата?

* Текст разбивается на блоки, соответствующие размерам магического квадрата.
* Каждый символ заменяется на число, соответствующее его позиции в магическом квадрате (или инверсно — из магического квадрата берётся символ по номеру).
* Процесс продолжается, пока весь текст не будет обработан, и результаты собираются для получения зашифрованного текста. Таким образом, порядок символов будет зависеть от конфигурации магического квадрата и использованного ключа.