**Лабораторная работа № 1**

**Тема:** шифрование и использованием метода шфирующих таблиц и метода магического квадрата.

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

Задание 1.

Выполните шифрование/расшифрование, испольуя метод шифрующих таблиц согласно варианту. При шифровании/расшифровании все пробелы учитываются. Пробелы в шифртексте обозначаются символом «\_», несколько подряд идущих пробелов разделяются символов «|».

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

Шифрование:

1) заполним таблицу

Таблица 1 – Заполнение таблицы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | 3 | 2 | 1 |
| 2 | В | Р | Е | М |
| 3 | Е | Н | А | \_ |
| 4 | М | Е | Н | Я |
| 1 | Ю | Т | С | Я |

2) переставим столбцы

Таблица 2 – Переставленные столбцы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 2 | М | Е | Р | В |
| 3 | \_ | А | Н | Е |
| 4 | Я | Н | Е | М |
| 1 | Я | С | Т | Ю |

3) переставим строки

Таблица 3 – Переставленные строки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 1 | Я | С | Т | Ю |
| 2 | М | Е | Р | В |
| 3 | \_ | А | Н | Е |
| 4 | Я | Н | Е | М |

Зашифрованное сообщение: ЯСТЮМЕРВ\_АНЕЯНЕМ

Дешифрование: по ключам 4321 2341

1) заполним таблицу

Таблица 4 – Заполнение таблицы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 1 | Я | С | Т | Ю |
| 2 | М | Е | Р | В |
| 3 | \_ | А | Н | Е |
| 4 | Я | Н | Е | М |

2) переставим столбцы

Таблица 5 – Переставленные столбцы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | 3 | 2 | 1 |
| 1 | Ю | Т | С | Я |
| 2 | В | Р | Е | М |
| 3 | Е | Н | А | \_ |
| 4 | М | Е | Н | Я |

3) переставим строки

Таблица 6 – Переставленные строки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | 3 | 2 | 1 |
| 2 | В | Р | Е | М |
| 3 | Е | Н | А | \_ |
| 4 | М | Е | Н | Я |
| 1 | Ю | Т | С | Я |

Дешифрованное сообщение: «ВРЕМЕНА МЕНЯЮТСЯ»

Задание 2.

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

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

Таблица 7 – Магический квадрат (ключ)

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

Заполним таблицу в соответствии с сообщением

Таблица 8 – Заполнение таблицы

|  |  |  |  |
| --- | --- | --- | --- |
| Д | О | Ы | Ю |
| А | Л | Т | Я |
| Г | Е | \_ | В |
| Е | Т | С | О |

Полученное зашифрованное сообщение: «ДОЫЮАЛТЯГЕ\_ВЕТСО»

Контрольные вопросы:

1. Укажите возможные ключи шифрования методом перестановок.

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

2. Перечислите разновидности метода шифрующих таблиц.

* простая перестановка
* двойная перестановка
* магическими квадратами

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

Ключи определяется 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.

4. Что такое магический квадрат?

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.

5. Как выполняется шифрование методом магического квадрата?

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