**Лабораторная работа № 1**

**Тема:** " Шифрование с использованием метода шифрующих таблиц и метода магического квадрата"

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

**Вариант №13**

**Ход работы**

**Задание №1**

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

**Расшифруйте шифротекст «ААНТДОМНЫЕАСЫСХЛЖТХ\_|\_ЬЕА\_ВОС\_** **ЁСЫБТПТТЖСВРСРИТАИЯАТОХ\_|\_ШЬЯ\_СШ», полученный методом одиночной перестановки по ключу(ключевое слово “РАБОТА”, размер таблицы 10\*6)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Р** | **А** | **Б** | **О** | **Т** | **А** |
| **5** | **1** | **3** | **4** | **6** | **2** |
| Д | А | Н | Т | О | А |
| А | М | Ы | Е | С | Н |
| Ж | Ы | Х | Л | Т | С |
| Е | Х | \_ | Ь | А | \_ |
| \_ | \_ | О | С | Ё | В |
| П | С | Б | Т | Т | Ы |
| Р | Т | С | В | С | Ж |
| И | Р | Т | А | Я | И |
| \_ | А | О | Х | \_ | Т |
| С | Ш | Я | \_ | Ш | Ь |

Полученная фраза: “Даже при самых страшных обстоятельствах остаётся шанс выжить”

**Задание №2**

**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 |

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

Зашифровка сообщения: “ТМЮВРЯАСЕННЯ\_ЕЕМ”

**Контрольные вопросы**

1. **Возможные ключи шифрования методом перестановки:**

* Размер таблицы;
* Слово или фраза, задающие перестановку;
* Последовательность, сформированная из натурального ряда числа 1, 2, …, n случайной перестановкой.

1. **Разновидности метода шифрующих таблиц:**

* простая перестановка, для которой ключом служит размер таблицы;
* Двойная перестановка, где ключи определяются для столбцов и для строк;
* Магические квадраты - 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;

1. **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).
2. **Магический квадрат –** 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 тоже число.
3. Шифруемый текст вписывается в магические квадраты в соответствии с нумерацией их клеток. Для получения шифротекста содержимое получившейся таблицы считывается построчно. Пример магического квадрата и его заполнения сообщением «ПРИЛЕТАЮ ВОСЬМОГО» показан ниже