МИНИСТЕРСТВО ОБРАЗОВАНИЯ ОРЕНБУРГСКОЙ ОБЛАСТИ **ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ**

«**ОРЕНБУРГСКИЙ КОЛЛЕДЖ ЭКОНОМИКИ И ИНФОРМАТИКИ**»

**(ГАПОУ СПО ОКЭИ)**

**ОТЧЁТ**

*ОКЭИ 09.02.07.70 23. 11*

МДК 02.02 Инструментальные средства разработки программного обеспечения

Разработал: *Панов Е.М.*

Руководитель: *Вареников Л.А.*

**Лабораторная работа №6**

Тема: шифрование.

Ход работы

Задание № 1. Квадрат Полибия для русского алфавита

Квадрат Полибия - это метод шифрования, в котором каждая буква заменяется парой чисел, представляющих её координаты в квадратной сетке. Обычно для латинского алфавита используется сетка 5x5, где строки и столбцы пронумерованы от 1 до 5. Каждая буква шифруется как пара чисел, соответствующих ее позиции по строке и столбцу в квадрате.Поскольку в русском алфавите больше 25 букв, необходимо адаптировать традиционный квадрат Полибия 5x5. Вот один из способов это сделать:

Расширение квадрата: Создайте квадрат 6x6, чтобы вместить все 33 буквы русского алфавита, а также любые дополнительные символы или пробелы, которые вы можете захотеть включить.

Нумерация строк и столбцов: Пронумеруйте строки и столбцы от 1 до 6.

Заполнение квадрата: Заполните квадрат буквами русского алфавита по порядку, объединяя буквы, такие как е/ё и и/й, в одну ячейку, если это необходимо.

Таблица 1 - Квадрат Полибия для русского алфавита

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | А | Б | В | Г | Д | Е, Ё |
| 2 | Ж | З | И, Й | К | Л | М |
| 3 | Н | О | П | Р | С | Т |
| 4 | У | Ф | Х | Ц | Ч | Ш |
| 5 | Щ | Ъ | Ы | Ь | Э | Ю |
| 6 | Я |  |  |  |  |  |

Задание № 2. Шифрование трёх строк с использованием русского квадрата Полибия

Используя таблицу 1:

Строка 1: «ПРИВЕТ МИР»

П -> 33

Р -> 34

И -> 23

В -> 13

Е -> 16

Т -> 36

(пробел) -> в нашей таблице пробела нет, игнорируем его

М -> 26

И -> 23

Р -> 34

Зашифрованная строка 1: 333423131636262334

Строка 2: «КАК ДЕЛА?»

К -> 24

А -> 11

К -> 24

(пробел) -> игнорируем

Д -> 15

Е -> 16

Л -> 25

А -> 11

? -> Предположим, что знаки препинания не шифруются, а просто переносятся в зашифрованный текст.

Зашифрованная строка 2: 24112415162511?

Строка 3: «Я ЛЮБЛЮ ТЕБЯ»

Я -> 61

(пробел) -> игнорируем

Л -> 25

Ю -> 56

Б -> 12

Л -> 25

Ю -> 56

(пробел) -> игнорируем

Т -> 36

Е -> 16

Б -> 12

Я -> 61

Зашифрованная строка 3: 61255612255636161261

Таблица 2 - Результаты шифрования

|  |  |  |  |
| --- | --- | --- | --- |
| Тестовая строка | Ожидаемый результат | Фактический результат | Результат тестирования |
| ПРИВЕТ МИР | 333423131636262334 | 333423131636262334 | Пройдено |
| КАК ДЕЛА? | 24112415162511? | 24112415162511? | Пройдено |
| Я ЛЮБЛЮ ТЕБЯ | 61255612255636161261 | 61255612255636161261 | Пройдено |

Задание № 3. Шифр Виженера

Шифр Виженера - это метод полиалфавитной подстановки для шифрования алфавитного текста, использующий серию различных шифров Цезаря, основанных на буквах ключевого слова. Это простая форма полиалфавитной подстановки.

Как он работает:

Ключевое слово: Выберите ключевое слово. Ключ повторяется, чтобы соответствовать длине открытого текста.

Таблица Виженера: Используется таблица Виженера, представляющая собой матрицу алфавитов, где каждая строка сдвинута на одну позицию (как в шифре Цезаря). Обычно это квадрат 26x26 для латинского алфавита (можно адаптировать для русского).

Шифрование: Для каждой буквы открытого текста, найдите строку, соответствующую букве ключа, и столбец, соответствующий букве открытого текста. Буква на пересечении строки и столбца - это зашифрованная буква. Или, что то же самое, сдвиньте каждую букву открытого текста на количество позиций, соответствующее букве ключа.

Открытый текст: ПРИМЕР ШИФРА

Ключ: КЛЮЧ

Шифруем, сдвигая буквы открытого текста на количество позиций, соответствующее букве ключа в алфавите (А=0, Б=1, В=2, ...):

П (позиция 16) + К (позиция 11) = Ф (позиция 27 % 33 = 27) 33 - количество букв в русском алфавите

Р (позиция 18) + Л (позиция 12) = Г (позиция 30 % 33 = 30)

И (позиция 9) + Ю (позиция 31) = А (позиция 40 % 33 = 7)

М (позиция 13) + Ч (позиция 25) = У (позиция 38 % 33 = 5)

Е (позиция 5) + К (позиция 11) = О (позиция 16)

Р (позиция 18) + Л (позиция 12) = Г (позиция 30 % 33 = 30)

Ш (позиция 26) + Ю (позиция 31) = Ц (позиция 57 % 33 = 24)

И (позиция 9) + К (позиция 11) = Л (позиция 20 % 33 = 20)

Ф (позиция 21) + Л (позиция 12) = Х (позиция 33 % 33 = 0)

Р (позиция 18) + Ю (позиция 31) = Ъ (позиция 49 % 33 = 16)

А (позиция 0) + Ч (позиция 25) = Я (позиция 25)

Зашифрованный текст: ФГАУОГ ЦЛХЪЯ