ОТЧЕТ

ЛАБОРАТОРНАЯ РАБОТА 2

Кражевский Алексей, 15 группа

7 вариант

Результат выполнения программы:

Шифр Хилла:

```
Hill encryption:  ГАВЗЩ?ЯМТЯАДЫЯЫЕЖОЧИП
Hill decription:  ЗАШИФРОВАННЫЙ ТЕКСТ
```

Входные данные: ключ = ‘АЛЬПИНИЗМ’, текст = ‘ЗАШИФРОВАННЫЙ ТЕКСТ’

Шифр сдвига:

```
First encryption result:
    mjqqtbtwqi
```

```
Decryption results:
    helloworld
```

Входные данные: текст ‘helloworld’, ключ = 5

1) Шифр сдвига

В шифрах сдвига для шифрования и дешифровки используются операции по модулю. В шифре сдвига используется **ключ K**, представляющий собой **целое число от 0 до 32**.

Порядок шифрования:

Для каждой буквы в сообщении **M**:

1. Преобразуйте букву в число, соответствующее порядку этой буквы в алфавите, начиная с 0, и обозначьте это число за **X**.
(А=0, Б=1, В=2, ...,Ю=31, Я=32)

2. Вычислите:**Y**=**(X+K)** mod**26**

3. Преобразуйте число **Y** в букву, стоящую на соответствующем месте алфавита, начиная с 0.

(А=0, Б=1, В=2, ...,Ю=31, Я=32)

Порядок дешифровки:

Для каждой буквы **C** в зашифрованном тексте проделайте следующее:

1. Преобразуйте букву в число, соответствующее его порядковому номеру в алфавите, начиная с 0, и назовите это числом Y.
(A=0, B=1, C=2, ..., Y=24, Z=25)

2. Вычислите: **X**=**(Y-K)** mod**26**

3. Преобразуйте число **X** в букву, стоящую на соответствующем месте алфавита, начиная с 0.
(A=0, B=1, C=2, ..., Y=24, Z=25)

2) Шифр Хилла

Шифр Хилла — полиграммный шифр подстановки, основанный на линейной алгебре и модульной арифметике. Изобретён американским математиком Лестером Хиллом в 1929 году. Это был первый шифр, который позволил на практике (хотя и с трудом) одновременно оперировать более чем с тремя символами.

Полная статья с описанием алгоритма: https://habr.com/ru/post/332714/