

Отчёт по лабораторной работе №1

**Дисциплина: Математические основы защиты информации и
информационной безопасности**

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 4 |
| 2 | Задание | 5 |
| 3 | Теоретическое введение | 6 |
| 4 | Выполнение лабораторной работы | 9 |
| 5 | Выводы | 10 |
| | Список литературы | 11 |

Список иллюстраций

| | | |
|-----|----------------------------|---|
| 4.1 | Код шифра Цезаря | 9 |
| 4.2 | Код шифра Атбаш | 9 |

1 Цель работы

Изучить шифры простой замены.

2 Задание

1. Реализовать шифр Цезаря с произвольным ключом k .
2. Реализовать шифр Атбаш.

3 Теоретическое введение

1. Шифр Цезаря.

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (*алфавитная перестановка*). Для запоминания нового порядка букв перемешивание алфавита осуществляется с помощью пароля. В качестве пароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: в первой записывается стандартный алфавит открытого текста, во второй - начиная с некоторой позиции размещается пароль (пробелы опускаются), а далее идут в алфавитном порядке оставшиеся буквы, не вошедшие в пароль. В случае несовпадения начала пароля с началом строки процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим положение начальной буквы пароля. Таблица шифрования на ключе 4 *пароль* будет иметь вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ы ь э ю я

ы э ю я **п а р о л ь** б в г д е ж з и й к м н с т у ф х ц ч ш щ ь

В процессе шифрования каждая буква открытого текста заменяется на стоящую под ней букву.

В 1 в. н.э. Ю. Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (А) на четвертую (D), вторую (В) - на пятую (Е), наконец, последнюю - на третью:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHOL YLGL YLFL (“Veni, vidi, vici” - лат. “Пришел, увидел, победил”).

Император Август (1 в. н. э.) в своей переписке заменял первую букву на вторую, вторую - на третью и т. д., наконец, последнюю - на первую:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Любимое изречение императора Августа выглядело так:

GFTUJOB MFOUF (“Festina lente” - лат. “Торопись медленно”).

Из примеров видно, что изменяя величину сдвига, можно получить несколько разных криптограмм для одного исходного текста.

Математически процедуру шифрования можно описать следующим образом:

$$T_m = \{T^j\}, j = 0, 1, \dots, m - 1$$

$$T^j(a) = (a + j) \bmod m$$

где $(a + j) \bmod m$ - операция нахождения остатка от целочисленного деления $a + j$ на m ; T_m - циклическая подгруппа. Пронумеруем буквы латинского алфавита от 0 до 25: $a = 0, b = 1, c = 3, \dots, z = 25$. В латинском алфавите 26 букв и поэтому примем $m = 26$. Тогда операцию шифрования запишем в виде: буква с номером i заменяется на букву с номером $(i + 3) \bmod 26$. Возможно и обобщение

шифра Цезаря на случай произвольного ключа k : символ с номером i заменится на символ с номером $(i + k) \bmod 26$.

Таким образом, открытый текст a_0, a_1, \dots, a_{N-1} преобразуется в криптограмму $T^j(a_0), T^j(a_1), \dots, T^j(a_{N-1})$. При использовании для шифрования подстановки T_j символ a открытого текста заменяется символом $a + j$ шифрованного текста. Цезарь обычно для шифрования использовал подстановку T^3 .

Взлом такого шифра осуществляется путем анализа частотных характеристик языка открытых текстов. Например, в русском тексте длиной 10000 символов буква О встречается в среднем 1047 раз, Е - 836, А - 808, Н - 723 и т.д. Поэтому, если в достаточно длинной криптограмме какой-то символ встречается чаще остальных, то есть все основания полагать, что это буква О.

1. Шифр Атбаш.

Данный шифр является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, таблица шифрования будет иметь следующий вид:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | _ |
| _ | я | ю | э | ы | ь | щ | ш | ч | ц | х | ф | у | т | с | р | п | н | м | л | к | й | и | з | ж | е | д | г | в | б | а | | |

Более подробно см. в [1–6].

4 Выполнение лабораторной работы

1. Реализуем шифр Цезаря с произвольным ключом k (рис. 4.1).

Шифр Цезаря

```
Ввод [15]: alpha = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
            k = int(input()) # шаг шифровки
            message = input().split()
            res = list()
            for word in message:
                res_word = ''
                for c in word:
                    res_word += alpha[(alpha.index(c) + k) % len(alpha)]
                res.append(res_word)
            print(*res)

3
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ЛРЧСУПГЩЛСРРГВ ДЭКСТГФРСФХЯ
```

Рис. 4.1: Код шифра Цезаря

1. Реализуем шифр Атбаш (рис. 4.2).

Шифр Атбаш

```
Ввод [18]: alpha = 'абвгдеёжзийклмнопрстуфхцчщъыьэюя '
            message = input()
            res = ''
            for c in message:
                res += alpha[len(alpha) - alpha.index(c) - 1]
            print(res)

информационная безопасность
чтлспу йчстт баяышр отсонд
```

Рис. 4.2: Код шифра Атбаш

5 Выводы

Изучила шифры простой замены на примере шифра Цезаря и шифра Атбаш.

Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016.
URL: <https://www.gnu.org/software/bash/manual/>.
2. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.
6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.