РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: *Математические основы защиты информации и информационной безопасности*

Студент: Лапшенкова Любовь Олеговна, 1032217633
Группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

List of Figures

List of Tables

1 Цель работы

Целью данной лабораторной работы является ознакомление с двумя методами шифрования: шифром Цезаря и шифром Атбаш. Также необходимо реализовать оба шифра на одном из известных языков программирования.

2 Задание

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

3 Теоретическое введение

3.1 Шифр Цезаря

3.1.1 Введение

С быстрым развитием обмена цифровыми данными в электронном виде, информационная безопасность приобретает все большее значение при хранении и передаче данных. Поэтому для обмена данными необходимо обеспечить их шифрование. Шифрование - это процесс кодирования сообщения таким образом, чтобы его мог прочитать только предполагаемый получатель [1]. Необходимо принять во внимание одну из простейших систем шифрования - шифр Цезаря. Предполагается, что знаменитый римский император и полководец, живший в 1 веке до нашей эры, использовал этот шифр в своей переписке [2]. Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – ключом[3].

3.1.2 Математическая модель

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра [4].Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

$y = x + k(modn),$

$x = y - k(modn),$

где x - символ открытого текста, y - символ шифрованного текста, n - мощность алфавита, k - ключ[5].

Пример:

Шифрование с использованием ключа $k = 3$. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З» [4]. Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», и так далее:

```
{
  Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ


  Шифрованный алфавит: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
}
```

3.1.3 Слабые места

У шифра Цезаря есть некоторые слабые места, которые позволяют нам использовать атаку методом грубой силы [6]. 1. Алгоритм шифрования и дешифрования известен. 2. Всего 25 ключей. 3. Язык открытого текста известен и легко узнаваем.

3.2 Шифр Атбаш

3.2.1 Введение

Атбаш - способ шифрования текста, в котором элементы исходного текста заменяются зашифрованным текстом в соответствии с некоторым правилом [7].

3.2.2 Математическая модель

Алгоритм этого шифра прост: первая буква алфавита заменяется на последнюю, вторая на предпоследнюю в алфавите и т.д [8]. Иначе говоря, правило шифро-

вания состоит в замене k буквы алфавита буквой с номером $n - k + 1$, где $n -$ число букв в алфавите[9].

Пример:

```
{
  Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ


  Шифрованный алфавит: ЯЮЭЬЫЪЩШЧЦХФУТСРПОНМЛКЙИЗЖЁЕДГВБА
}
```

3.2.3 Слабые места

Основное слабое место - для успешной дешифрации необходимо знать только алфавит сообщения[8].

4 Выполнение лабораторной работы

Реализация шифров производилась на языке Python 3. Через Anaconda-Navigator, Jupyter Notebook. Процесс реализации кода доступен по ссылке.

5 Реализация шифра Цезаря

Реализация шифра Цезаря выглядит следующим образом(рис. 5.1).

```
def tsezar_code():
    alphabet_kir="абвгдежзийклмнопрстуфхцчшщъыьэюя"#задаем алфавит
    alphabet_latin="abcdefghijklmnopqrstuvwxyz"#задаем алфавит
    k=input('Введите k:',)#просим пользователя ввести k
    k=int(k)#делаем k интовым
    phrase=input('Введите фразу для зашифровки:',)#просим пользователя ввести фразу для зашифровки
    new_phrase=""#задали пустую строку для шифра
    for i in phrase:#прогоняем фразу посимвольно
        if (i==" ") or (i==".") or (i==",") or (i=="!") or (i=="?") or (i==":") or (i==";") or (i=="-"):#проверка условия на наличие определеннных символов
            new_phrase=new_phrase+i#прибавление символа без изменения к шифру
            continue #переход к следующему прогону цикла
        if ((phrase[0] in alphabet_latin) or (phrase[1] in alphabet_latin) or (phrase[2] in alphabet_latin)):#проверка на алфавит
            index=alphabet_latin.find(i)#определяем индекс для буквы из фразы в алфавите
            index=int(index)#делаем интовым
            jindex=(index+k)%(len(alphabet_latin))#расчет нового индекса для шифровки
            new_phrase=new_phrase+alphabet_latin[jindex]#создание шифра
        else:#проверка на алфавит
            index=alphabet_kir.find(i)#определяем индекс для буквы из фразы в алфавите
            index=int(index)#делаем интовым
            jindex=(index+k)%(len(alphabet_kir))#расчет нового индекса для шифровки
            new_phrase=new_phrase+alphabet_kir[jindex]#создание шифра
    print('Зашифрованная фраза:',new_phrase)#вывод шифра
tsezar_code()#запуск функции
```

Figure 5.1: Программа Шифр Цезаря

При запуске функции, получили следующий вывод (рис. 5.2).

```
Введите k:3
Введите фразу для зашифровки:veni,vidi,vici!
Зашифрованная фраза: yhql,ylgl,ylfl!
```

Figure 5.2: Результат выполнения программы Шифр Цезаря

6 Реализация шифра Атбаш

Реализация шифра Атбаш выглядит следующим образом(рис. 6.1).

6.1 Шифр Атбаш

```
def atbash_code():
    alphabet_kir_2="абвгдежзийклмнопрстуфхцчшщъыьэюя "#задаем алфавит с пробелом
    alphabet_latin_2="abcdefghijklmnopqrstuvwxyz "#задаем алфавит с пробелом
    rev_alphabet_kir_2=alphabet_kir_2[::-1]#все элементы списка в обратном порядке
    rev_alphabet_latin_2=alphabet_latin_2[::-1]#все элементы списка в обратном порядке
    phrase=input('Введите фразу для зашифровки:',)#просим пользователя ввести фразу для зашифровки
    new_phrase=""#задали пустую строку для шифра
    for i in phrase:#прогоняем фразу посимвольно
        if ((phrase[0] in alphabet_latin_2) or (phrase[1] in alphabet_latin_2) or (phrase[2] in alphabet_latin_2)):#проверка на алфавит
            index=alphabet_latin_2.find(i)#определяем индекс для буквы из фразы в алфавите
            new_phrase=new_phrase+rev_alphabet_latin_2[index]#создание шифра с помощью реверснутого алфавита
        else:
            index=alphabet_kir_2.find(i)#определяем индекс для буквы из фразы в алфавите
            new_phrase=new_phrase+rev_alphabet_kir_2[index]#создание шифра с помощью реверснутого алфавита
    print('Зашифрованная фраза:',new_phrase)#вывод шифра
atbash_code()
```

Figure 6.1: Программа Шифр Атбаш

При запуске функции, получили следующий вывод (рис. 6.2).

```
Введите фразу для зашифровки:abcd
Зашифрованная фраза:  zyx
```

Figure 6.2: Результат выполнения программы Шифр Атбаш

7 Выводы

В процессе выполнения данной лабораторной работы нам удалось ознакомиться с двумя методами шифрования: шифром Цезаря и шифром Атбаш, а также реализовать оба шифра на одном из известных языков программирования (в моем случае на языке Python 3). Код программ был написан в соответствии с теоретическими сведениями, предоставленными в задании к лабораторной работе, а также найденными самостоятельно.

Список литературы

1. Habr. Шифр Цезаря или как просто зашифровать текст [Электронный ресурс]. Habr, 2020, URL:https://habr.com/ru/post/534058/ (дата обращения 09.11.2021)
2. ИНТУИТ. Лекция 2: Основные понятия криптографии [Электронный ресурс]. ИНТУИТ, 2021, URL:https://intuit.ru/studies/courses/691/547/lecture/12371?page=3 (дата обращения 09.11.2021)
3. Инфоурок. Система шифрования Цезарь. Аффинная система трансплантации Цезаря [Электронный ресурс]. Инфоурок, 2021, URL:https://infourok.ru/sistema-shifrovaniya-cezar-affinnaya-sistema-transplantacii-cezarya-4640938.html (дата обращения 10.11.2021)
4. Google. Криптография. Шифр Цезаря [Электронный ресурс]. Google, 2021, URL:https://www.sites.google.com/site/kriptografics/sifr-cezara (дата обращения 10.11.2021)
5. Mind Control. Шифр Цезаря [Электронный ресурс]. Mind Control, 2021, URL:https://mind-control.fandom.com/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6% (дата обращения 10.11.2021)
6. MySeldon. Шифр Цезаря или как просто зашифровать текст [Электронный ресурс]. MySeldon, 2020, URL:https://news.myseldon.com/ru/news/index/242705590 (дата обращения 11.11.2021)
7. Wiki93. Атбаш [Электронный ресурс]. Wiki93, 2020, URL:http://www.wiki93.ru/index.php?ti (дата обращения 11.11.2021)
8. Hi-edu. Криптография[Электронный ресурс]. Hi-edu, 2021, URL:http://www.hi-

edu.ru/e-books/xbook1019/01/info.pdf (дата обращения 11.11.2021)

9. Academic dictionary. Атбаш [Электронный ресурс]. Academic dictionary, 2020, URL:https://dic.academic.ru/dic.nsf/ruwiki/247899 (дата обращения 12.11.2021)