

Информационная безопасность. Отчет по лабораторной работе № 1

Шифры простой заменой

Мухамеджанов Исматулло Иззатуллоевич

Содержание

1	Цель работы	5
2	Указание к работе	6
3	Выводы	9
4	Список литературы	10

List of Figures

2.1	Программа (1)	8
2.2	Программа (2)	8

List of Tables

1 Цель работы

Освоить на практике применение шифрование простой заменой [1].

2 Указание к работе

Исходные данные. Шифр Цезаря Шифр Атбаш # Выполнение лабораторной работы 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 ъ ы ь э ю я м э ю я в 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 ъ В процессе шифрования каждая буква открытого текста заменяется на

стоящую под ней букву.

В 1 В. Н.З. Ю. Л езарь Во Время Воґньї С ФалґиїиМН, переписыІВііztGh СО ГВОИМН друзьяМН В РіиМе, заМенхл В сообіиенНН перВ бухВу латННСКОFO НН ЁтВНТЁт (А) Нит четВертуіо (D), ВТОj3 (B) — НЁт Іля (E), НакоНеил, послерНіоіо — На ТреТбю: А В С 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 А В С QoНесеНие Ю. Л езаря СеНату об одержанНоґ М победе Наq фІОНТНІІСКНМ царем Выґлядело так: YHQL YLGL YLFL (“Veni, vidi, vici” — лат, фришел, уВНцел, победНл”). ИМпераТОр Вруст (1 В. Н. 3.) В сВоей перепНске ЗаМенял перВ 6 В Нит ВТОj3, ВТОj3ую — На ТреТбю Н Т, q., НакоНеу, посленНюіо — та перВуто: А В С D E F G H I J K L M N O P Q R S T U V W X Y Z В С D E F G H I I K L M N O P Q R S T U V W X Y Z А JіiOòНМое НзречеНне НМпераТОра Августіи ВhIF’ляпело ТаК: GFTUJOB MFOUF (“Festina lente” — лат. “ТоропНсь Менленно”). Нз прНмеров ВН,QHO, НТО изМенхс ВелНчННу сдВНФЕІ, МОКНО НОJІ НТh Несколво разНбІХ KQ НТОРQЁИММ QJIB O,QHOФ’O HGXOqHOго теКсТа. МатеМатичесКН проиеоуру шНфj3ОВЁіННН МОНтНО Описатс следуюІи НМ Образом: $Tg \rightarrow T', j \rightarrow 0, 1, \dots, m-1, T' \{a\} (a - F j) \bmod m, \text{rue } \{a - j\} \bmod m$ — операциR НаХождеНня OGTaТка о+ иеночНснеННого qенеНия $a + / \text{НЁт Tit}$; Тр — ІJHKnНчесКая подгруппа. ПроНумеруем бухВЕ•І JІЁтТННСКОЕ’O all іаВНТā OT 0 до 25: $n = 0, f = 1, c = 3, \dots, z = 25$. В нІлТННГКОМ аfлфІлВНте 26 fіJВ Н НОэтоМу приМеМ m 26. Тогда операуНіо ІІН j3OBdННzt 3ЕfnНшеМ В ВНде: бухВЁт С НоМером i ЗаМеНсеТся На бухøу с НоМером $(i - 1 - 3) \bmod 26$. ВО8МОННО Н ОбообщеНне шифра езаря На GJІучаі пj3OH3BOJІhHOFO Kflюча k : CHMBOJІ С НоМером i ЗаМенНТСzt НЁт CHMBOJі С НоМером $(i + k) \bmod 26$. ТакиМ обj3азОМ, ОТКj3hITбій ТеКсТ аО, at. — . •N - і преобразуеТся В крНпТОФрамМу Г’ (із0). Т (’), ..., Т’ (aN _). ІпрН иCHOJІh8OBzìННН ,fī,Jlzt ІІН j3OBііННzt НОØ,СТЁтНОВКН Т’ GHMBOJІ n ОТКQbІТОго теКсТа заМеняеТся CHMBOJІОМ О +

шифрованного текста. Цезарь обычно для тифрования использовал подстановку Т’. 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. 2. 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 р я ю э ы ь щ ш ч ц х ф у т с р п о н м л к и и з ж е д г в б а При программной реализации шифра Атбаш на языке Pascal целесообразно использовать таблицу ASCII и функции работы с ней (ord и char). Далее показана функция перевода символа открытого текста в шифр путем зеркального отражения по таблице ASCII.

Function Atbash(openchar:char):char; Begin Atbash := 255 — ord(openchar); End.

```

import string

alphabet = list(string.ascii_uppercase)

print(alphabet)
def cesar_cipher(k, text):
    ciphered_text = ""
    for letter in text:
        location = alphabet.index(letter)
        location += k
        ciphered_text += alphabet[location % 26]
    return ciphered_text

cesar_cipher(3, "YZZ")

```

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']
CC'

Figure 2.1: Программа (1)

Программа (2)

Figure 2.2: Программа (2)

3 Выводы

Освоено на практике применение шифрования на основах шифрования Цезаря и Атбаш.

4 Список литературы

1. Методические материалы курса
2. Википедия