Отчёт по лабораторной работе №1

Шифр простой замены

Адьяту Ибрайма Коллаволе Топе НФИмд 01-22

Содержание

List of Figures

1 Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

2 Теоретические сведения

2.1 Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

```
y = (x + k) mod n
x = (y - k + n) mod n
```

где *x — символ открытого текста,* y — символ шифрованного текста *n — мощность алфавита* k — ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

2.2 Шифр Атбаш

Атбаш — простой шифр подстановки, изначально придуманный для иврита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите.

3 Выполнение работы

3.1 Реализация шифра Цезаря на языке Python

Блок шифрования

```
def cesar():
    lettre = 'ABCDEFGHIJKLMNOPQRSTUVXYZABCDEFGHIJKLMNOPQRSTUVXYZ'
    step = 5
    teste = input("cesar chiffrovanie :)")
    resultat = ''
    for i in teste:
        ind= lettre.find(i)
        newind = ind + step
        if i in lettre:
            resultat += lettre[newind]
        else:
            resultat += i
        print(resultat)
```

Блок дешифровки

```
# процесс дешифровки уже должен быть ясен
# вместо добавления шага, надо, наоборот же, вычитать,
# чтоб из зашифр сообщения получить открытый текст
# по сути код такой же, лишь маленькое отличие: вместо + -
```

```
def cesar_deshifr():
    lettre = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    teste1 = 5
    teste = input(" cesar- dechiffrovanie")
    resultat = ''

    for i in teste:
        ind = lettre.find(i)
        newind = ind - teste1
        if i in lettre:
            resultat += lettre[newind]
        else:
            resultat += i
    print(resultat)
```

3.2 Реализация шифра Атбаш на языке Python

Блок шифрования

```
def cesbash():
    # задаем алфавит из английских букв больших(пОЧЕМУ БОЛЬШИХ?  Мы просто указал
    # алфавит увеличить
    lettre = [chr(x) for x in range(65, 91)]
    # алфавит-наоборот
    lettre_vu = [x for x in lettre]
    lettre_vu.reverse()

    teste = input("cesbash - chiffrovanie")
    resultat = ""
    # тут для перебираются буквы из исходного текста
```

```
    for i in teste:
        # перебираются индексы и значения из letters
        for j,l in enumerate(lettre):
            if i == l: # если буквы i и l равны, то
                resultat += lettre_vu[j] # ставим в результат букву из реверсиров
    print(resultat)
```

Блок дешифровки

```
# функция дешифровки практически такая же
# тут просто местами мы поменяли списки чтоб наоборот дешифровать сообщения
def cesbash_dchivro():
    lettre = [chr(x) for x in range(65, 91)]
    lettre_vue = [x for x in lettre]
    lettre_vue.reverse()

    teste = input("cesbash - dechirovka")
    resultat = ""
    for i in teste:
        for j, l in enumerate(lettre_vue):
            if i == l:
                resultat += lettre[j]
    print(resultat)
```

Блок Запускаем

```
# функция мейн: тут запускаем поочередно каждую функцию
def main():
    cesar()
    cesar_deshifr()
```

```
cesbash()
cesbash_dchivro()
```

3.3 Контрольный пример

```
Entrée [6]: if __name__ == "__main__":
                main()
```

```
cesar chiffrovanie :)WORLD
W
WT
WTX
WTXQ
WTXQI
 cesar- dechiffrovanieWTX
ROS
cesbash - chiffrovanieWORLD
DLIOW
cesbash - dechirovkaDLIOW
WORLD
```

Figure 3.1: Работа алгоритмов

4 Выводы

Изучили алгоритмы шифрования Цезаря и Атбаш.

Список литературы

1. Шифр Цезаря
2. Шифр Атбаш