Отчёт по лабораторной работе №3

Шифрование гаммированием

Гаглоев Олег Мелорович

Содержание

Список иллюстраций

1 Цель работы

Изучение алгоритма Шифрования гаммированием

2 Теоретические сведения

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные. Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

3 Выполнение работы

3.1 Реализация шифра Гамма

```
def Gamma(text:str,gamma:str,alph: str)->str:
    result=""
    text=text.lower()
    gamma=gamma.lower()
    dic1={char:index+1 for index,char in enumerate(alph)}#словарь букв
    dic2={value:key for key,value in  dic1.items()} #словарь цифр по буквам
    l=0
    for i in text:
        if l==len(gamma):
            l=0
        tmp_sum=(dic1[i]+dic1[gamma[l]])%(len(alph))
        result+=dic2[tmp_sum]
        l+=1
    return result
text='ПРИКАЗ'
gamma='ГАММА'
letters='абвгдежзийклмнопрстуфхцчшщъыьэюя'
print(Gamma(text,gamma,letters))
```

3.2 Контрольный пример

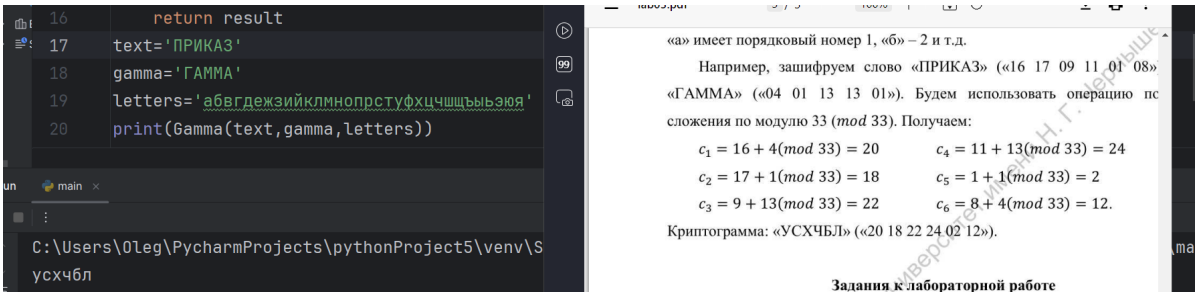

Рис. 3.1: Работа алгоритма маршрутной перестановки

4 Выводы

Изучили алгоритмы шифрования гаммированием

Список литературы