

Шифр гаммирования

Гаглов Олег Мелорович

11 октября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма гаммирования

Выполнение лабораторной работы

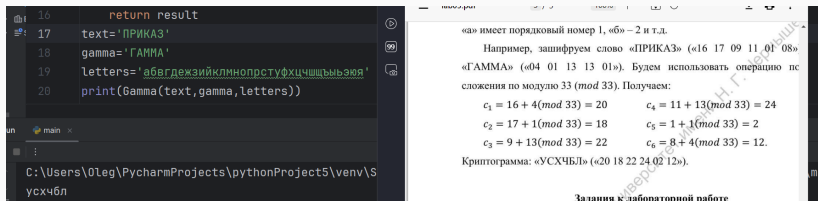
Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения XORится с блоком криптографической гаммы, длина которого должна соответствовать длине блоков открытого сообщения. При этом, если размер блока исходного текста меньше, чем размер блока гаммы, блок гаммы обрезается до размера блока исходного текста (выполняется процедура усечения гаммы).

```
3 def Gamma(text:str,gamma:str,alph: str)->str:
4     result=""
5     text=text.lower()
6     gamma=gamma.lower()
7     dic1={char:index+1 for index,char in enumerate(alph)}#словарь букв
8     dic2={value:key for key,value in dic1.items()} #словарь цифр по буквам
9     l=0
10    for i in text:
11        if l==len(gamma):
12            l=0
13            tmp_sum=(dic1[i]+dic1[gamma[l]]%(len(alph)))
14            result+=dic2[tmp_sum]
15            l+=1
16    return result
```

Рис. 1: Работа алгоритма

Контрольный пример



The image shows a Python IDE on the left and a document on the right. The IDE contains the following code:

```
16     return result
17 text='ПРИКАЗ'
18 gamma='ГАММА'
19 letters='абвгдежзийклмнопрстуфхцчшщъыьэя'
20 print(Gamma(text,gamma,letters))
```

The document on the right explains the algorithm. It states that 'а' has a sequential number 1, 'б' has 2, and so on. It then shows an example of encrypting the word 'ПРИКАЗ' (16 17 09 11 01 08) with the key 'ГАММА' (04 01 13 13 01). The operation used is addition modulo 33 (mod 33). The calculations are as follows:

$$\begin{aligned} c_1 &= 16 + 4(\text{mod } 33) = 20 & c_4 &= 11 + 13(\text{mod } 33) = 24 \\ c_2 &= 17 + 1(\text{mod } 33) = 18 & c_5 &= 1 + 1(\text{mod } 33) = 2 \\ c_3 &= 9 + 13(\text{mod } 33) = 22 & c_6 &= 8 + 4(\text{mod } 33) = 12. \end{aligned}$$

The resulting ciphertext is: «УСХЧБЛ» («20 18 22 24 02 12»).

Задания к лабораторной работе

Рис. 2: Работа алгоритма

Выводы

Изучили алгоритмы шифрования с помощью перестановок