# Шифрование (кодирование) различных исходных текстов одним ключом

Назарьева Алена НФИбд-03-18 2021, 13 december

 $inst\{1\} RUDN\ University, Moscow, Russian\ Federation$ 

Цель работы

### Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## \_\_\_\_

Выполнение лабораторной

работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты Р1 и Р2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов С1 и С2 обоих текстов Р1 и Р2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Функция, которая определяет вид шифротекстов С1 и С2 обоих текстов Р1 и Р2 при известном ключе (рис. -fig. 1)

```
In [1]: import re
In [6]: def decrypt(text1, text2, gamma):
          text1Len = len(text1)
          text2Len = len(text2)
         gammaLen = len(gamma)
         kevText • [1
          for 1 in range(text1Len // gammaLen):
             for symb in gamma:
               keyText.append(symb)
          for i in range(text1Len % gammaLen):
             keyText.append(gamma[i])
          code1 . []
         code2 . []
          for i in range(text1Len):
             code1.append(alphabeth[(alphabeth.index(text1[i]) + alphabeth.index(keyText[i])) % 71])
          for 1 in range(text2Len):
             code2.append(alphabeth[(alphabeth.index(text2[i]) + alphabeth.index(keyText[i])) % 71])
         return(print(*code1,sep=''),print(*code2,sep=''))
In [7]: decrypt('C Hossm Годом, друзья!', 'C Левым Годом, друзья!', 'AAsAAAAAAAAAAAAAAAAAAAAAA
      С Голым Годом, друзья!
      С Белым Годом, друзья!
```

Figure 1: первая функция

Функция, которая позволяет злоумышленнику прочитать оба текста, не зная ключа и не стремясь его определить (рис. -fig. 2)

```
def discrpt2(cods), cods), text);
codellen = len(code)
codellen = len(code)
textline = len(co
```

Figure 2: вторая функция

### Выводы

### Выводы

В результате выполнения работы я освоила на практике применение шифрования (кодирования) различных исходных текстов одним ключом.