

Шифрование (кодирование) различных исходных текстов одним ключом

Назарьева Алена НФИбд-03-18

2021, 13 december

inst{1}RUDN University, Moscow, Russian Federation

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, прочесть оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

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

```
def decrypt2(code1, code2, text1):
    code1Len = len(code1)
    code2Len = len(code2)
    text1Len = len(text1)

    text2 = []
    for i in range(code1Len):
        text2.append(alphabeth[(alphabeth.index(code1[i]) - (alphabeth.index(code2[i]) - alphabeth.index(text1[i])) % 71))])
    return(print(*text2,sep=''))

decrypt2('С Голым Годом, друзья!', 'С Белым Годом, друзья!', 'С Левым Годом, друзья!')
```

С Новым Годом, друзья!

Figure 2: вторая функция

Выводы

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