Шифрование (кодирование) различных исходных текстов одним ключом

Сасин Ярослав НФИбд-03-18

2021, 18 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

1)

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 P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

2)

Функция, которая определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе (рис. -fig. 1)

```
В [1]:
1 import re

В [2]:
1 ['Ж','Э','И','Й','К','Л','М','Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ','Ы','Ь','Э','Ю','Я','!','?','.',',',' ']

В [6]:
def encrypt(text1, text2, gamma):
    textlen1 = len(text1)
    textlen2 = len(text2)
    gammalen = len(gamma)

    key_text = []
    for i in range (textlen1 // gammalen):
        for symb in gamma:
            key_text.append(symb)

    for i in range (textlen1 % gammalen):
        key_text.append(gamma[i])

    code1 = []
    code2 = []
    for i in range(textlen1):
        code1.append(alph[(alph.index(text1[i]) + alph.index(key_text[i])) % 71])
    for i in range(textlen1):
        code2.append(alph[(alph.index(text2[i]) + alph.index(key_text[i])) % 71])

    return(print(*code1,sep='')),(print(*code2,sep=''))

В [7]:
encrypt ('С Новым Годом, друзья!','С Левым Годом, друзья!', 'ааъайааaЁЫаааааааааааа')

С голым дедом, друзья!
С белым дедом, друзья!
```

Figure 1: первая функция

3)

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

```
В [8]:
def decrypt(text, code1,code2):
    codelen1 = len(code1)
    codelen2 = len(code2)
    textlen = len(text)

    text2 = []
    for i in range(codelen1):
        text2.append(alph[alph.index(code1[i]) - (alph.index(code2[i]) - alph.index(text[i]))% 71])

    return(print(*text2,sep = ''))

В [11]:
decrypt('С Левым Годом, друзья!', 'С голым дедом, друзья!', 'С белым дедом, друзья!')

С Новым Годом, друзья!
```

Figure 2: вторая функция

Выводы

Выводы

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