Элементы криптографии. Однократное гаммирование

Назарьева Алена НФИбд-03-18

2021, 4 december

inst{1}RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

1)

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Функция шифрования (рис. -fig. 1)

In [75]:
```
import re
```

In [76]:
```
alphabeth = ['А','Б','В','Г','Д','Е','Ё','Ж','З','И','Й','К','Л','М','Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ','Ы',
```

In [77]:
```
def encrypt(text, gamma):
    textLen = len(text)
    gammaLen = len(gamma)

    keyText = []
    for i in range(textLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(textLen % gammaLen):
        keyText.append(gamma[i])

    code = []
    for i in range(textLen):
        code.append(alphabeth[(alphabeth.index(text[i]) + alphabeth.index(keyText[i])) % 71])

    return(print(*code,sep=''))
```

In [99]:
```
encrypt('С Новым Годом, друзья!', 'ААъАЙАААААААААААААААА')
```

```
С Голым Годом, друзья!
```

Figure 1: Функция шифрования

Функция расшифрования (рис. -fig. 2)

```
[93]: def decrypt(code, gamma):
          codeLen = len(code)
          gammaLen = len(gamma)

          keyText = []
          for i in range(codeLen // gammaLen):
              for symb in gamma:
                  keyText.append(symb)
          for i in range(codeLen % gammaLen):
              keyText.append(gamma[i])

          text = []
          for i in range(codeLen):
              text.append(alphabeth[(alphabeth.index(code[i]) - alphabeth.index(keyText[i]) + 71) % 71])

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

100]: decrypt('С Голым Годом, друзья!', 'ААъАЙАААААААААААААААА')

      С Новым Годом, друзья!
```

Figure 2: Функция расшифрования

4)

ункция, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис. -fig. 3)

```
]: def crypt(code, text):
       codeLen = len(code)
       textLen = len(text)

       gamma = []
       for i in range(codeLen):
           text.append(alphabeth[(alphabeth.index(code[i]) - alphabeth.index(text[i]) + 71) % 71])

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

]: decrypt('С Голым Годом, друзья!!', 'С Белым Годом, друзья!')

   ААВЙАААААААААААААААААо
```

Figure 3: функция 3

Выводы

Выводы

В результате выполнения работы я освоила на практике применение режима однократного гаммирования.