Лабораторная работа №8

Морозова У.К.

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Цели и задачи

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

Выполнение лабораторной работы

Импорт библиотек

[1]:
```
import random
import string
```

Создание функции для генерации ключа

[3]:
```
def generate_key_hex(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
```

Функция для (де)шифрования

[4]:
```
def en_de_crypt(text, key):
    new_text = ''
    for i in range(len(text)):
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text
```

Шифрование и дешифрование

[6]:
```
t1 = 'С Новым годом, друзья!'
key = generate_key_hex(t1)
en_t1 = en_de_crypt(t1, key)
de_t1 = en_de_crypt(en_t1, key)

t2 = 'У Слона домов, огого!!'
en_t2 = en_de_crypt(t2, key)
de_t2 = en_de_crypt(en_t2, key)
```

Проверка работы программы

[7]:
```
print('Открытый текст: ', t1, "\nКлюч: ", key, '\nШифротекст: ', en_t1, '\nИсходный текст: ', de_t1,)
print('Открытый текст: ', t2, "\nКлюч: ", key, '\nШифротекст: ', en_t2, '\nИсходный текст: ', de_t2,)
r = en_de_crypt(en_t2, en_t1)
print('Расшифровать второй текст, зная первый: ', en_de_crypt(t1, r))
print('Расшифровать первый текст, зная второй: ', en_de_crypt(t2, r))
```

```
Открытый текст:  С Новым годом, друзья!
Ключ:  0B5p1jWhwrdZtxTyhgk9g4
Шифротекст:  БЬШюЃСжНфьёЊшТтэШФќvШ
Исходный текст:  С Новым годом, друзья!
Открытый текст:  У Слона домов, огого!!
Ключ:  0B5p1jWhwrdZtxTyhgk9g4
Шифротекст:  ГЬДыЦїаНуьjЌцТтчЋьjЇF
Исходный текст:  У Слона домов, огого!!
Расшифровать второй текст, зная первый:  У Слона домов, огого!!
Расшифровать первый текст, зная второй:  С Новым годом, друзья!
```

Выводы

Выводы

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