Лабораторная работа №7

Морозова У.К.

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Цели и задачи

- Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

Импорт библиотек

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

Создание функции для генерации ключа

[2]:
```
def generate_key_hex(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits) #генерация цифры для каждого символа в тексте
    return key
```

Функция для (де)шифрования

[3]:
```python
#для шифрования и дешифрования
def en_de_crypt(text, key):
    new_text = ''
    for i in range(len(text)): #проход по каждому символу в тексте
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text
```

Функция нахождения всех возможных ключей

[4]:
```python
def find_possible_key(text, fragment):
    possible_keys = []
    for i in range(len(text) - len(fragment) + 1):
        possible_key = ""
        for j in range(len(fragment)):
            possible_key += chr(ord(text[i + j]) ^ ord(fragment[j]))
        possible_keys.append(possible_key)
    return possible_keys
```

Проверка работы программы

```python
t = 'С Новым Годом, друзья!'
key = generate_key_hex(t)
en_t = en_de_crypt(t, key)
de_t = en_de_crypt(en_t, key)
keys_t_f = find_possible_key(en_t, 'С Новым')
fragment = "С Новым"
print('Открытый текст: ', t, "\nКлюч: ", key, '\nШифротекст: ', en_t, '\nИсходный текст: ', de_t, '\n')

print('Возможные ключи: ', keys_t_f)
print('Расшифрованный фрагмент: ', en_de_crypt(en_t, keys_t_f[0]))
```

```
Открытый текст:  С Новым Годом, друзья!
Ключ:  BYKCDCcmFLiruH3EPtHPgA
Шифротекст:  ѣyiѽѶJџMsѲйьщd?ѱАзѿMШ`
Исходный текст:  С Новым Годом, друзья!

Возможные ключи:  ['BYKCDCc', 'jѶ`H:\x14ѱ', 'wӥk6mIi', '\\i\x15aѿ\x1eN', 'WШBөg9a', ')ѿѐk@\x16p', '~mHLo\x07u', 'Ѭvoc~\x02j', 'tђ@r{ЯЯ', 'SѽQwijM', '|ѬТњ
C:,', 'ѭѩЭС[\x0b', 'hDЎO"|C', 'x3l.\x054 ', 'вё\r\tMW\x14', 'Pa*A.cќ']
Расшифрованный фрагмент:  С Новым?ЌйOЈћ?QШћVлџы"
```

Выводы

Выводы

Мы освоили на практике применение режима однократного гаммирования