Отчёт по лабораторной работе №8

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

1 Цель работы **5**

2 Выполнение лабораторной работы **6**

3 Вывод **9**

Список литературы **10**

Список иллюстраций

2.1 Генерация ключа 6
2.2 Шифрование 6
2.3 Подбор ключа 6
2.4 Результаты 7
2.5 Код расшифровки 7
2.6 Результаты расшифровки 7
2.7 Листинг программы 8

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

1) Функция для генерации ключа. (рис. 2.1)

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

Рис. 2.1: Генерация ключа

2) Функция для (де)шифрования. (рис. 2.2)

```
def 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
```

Рис. 2.2: Шифрование

3) Код для вывода результатов и результаты. рис. 2.3) - (рис. 2.4)

```
t1 = 'С Новым Годом, друзья!'
key = generate_key(t1)
encrypt1 = crypt(t1, key)
decrypt1 = crypt(encrypt1, key)

t2 = 'Я люблю инфор, безопа!'
encrypt2 = crypt(t2, key)
decrypt2 = crypt(encrypt2, key)

print('Открытый текст:', t1, "\nКлюч:", key, "\nШифротекст:", encrypt1, "\nИсходный текст
print('\n')
print('Открытый текст:', t2, "\nКлюч:", key, "\nШифротекст:", encrypt2, "\nИсходный текст
print('\n')
```

Рис. 2.3: Подбор ключа

```
Открытый текст: С Новым Годом, друзья!
Ключ: fR6qkp7o1M1yBg3AKjjj9A
Шифротекст: чгЫяЊлЋОТѲSчѿK‼vЋЩЍЦѶ`
Исходный текст: С Новым Годом, друзья!


Открытый текст: Я люблю инфор, безопа!
Ключ: fR6qkp7o1M1yBg3AKjjj9A
Шифротекст: щгЍпњыЏОЉѰvчЂK‼Ѱѿйєsљ`
Исходный текст: Я люблю инфор, безопа!
```

Рис. 2.4: Результаты

4) Код для расшифровки фразы с помощью второй фразы и результаты. (рис. 2.5) - (рис. 2.6)

```
recrypt = crypt(encrypt2, encrypt1)

print('Расшифровка второго текста при помощи первого: ', crypt(t1, recrypt))
print('Расшифровка первого текста при помощи второго: ', crypt(t2, recrypt))
```

Рис. 2.5: Код расшифровки

```
Расшифровка второго текста при помощи первого:  Я люблю инфор, безопа!
Расшифровка первого текста при помощи второго:  С Новым Годом, друзья!
```

Рис. 2.6: Результаты расшифровки

5) Листинг программы. (рис. 2.7)

```python
import random
import string

def generate_key(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key

def 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

t1 = 'С Новым Годом, друзья!'
key = generate_key(t1)
encrypt1 = crypt(t1, key)
decrypt1 = crypt(encrypt1, key)

t2 = 'Я люблю инфор, безопа!'
encrypt2 = crypt(t2, key)
decrypt2 = crypt(encrypt2, key)

print('Открытый текст:', t1, "\nКлюч:", key, "\nШифротекст:", encrypt1, "\nИсходный текст:", decrypt1)
print('\n')
print('Открытый текст:', t2, "\nКлюч:", key, "\nШифротекст:", encrypt2, "\nИсходный текст:", decrypt2)
print('\n')

recrypt = crypt(encrypt2, encrypt1)

print('Расшифровка второго текста при помощи первого: ', crypt(t1, recrypt))
print('Расшифровка первого текста при помощи второго: ', crypt(t2, recrypt))
```

Рис. 2.7: Листинг программы

3 Вывод

В результате выполнения работы мы научились на практике применять режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

1) https://esystem.rudn.ru/pluginfile.php/2357159/mod_resource/content/2/008-lab_crypto-key.pdf