Отчёт по лабораторной работе №8

дисциплина: Информационная безопасность

Морозова Ульяна

Содержание

Список иллюстраций

1 Цель работы

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

2 Выполнение лабораторной работы

Для выполнения лабораторной работы я написала программу на языке программирования Python.

1. Для начала импортируем необходимые для работы библиотеки (рис. 2.1).

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

Рис. 2.1: Импорт

2. Создадим функцию для генерации ключа (рис. 2.2).

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

Рис. 2.2: Генерация ключа

3. Затем напишем функцию для (де)шифрования (рис. 2.3).

```
[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
```

Рис. 2.3: (Де)шифрование

4. Проверка работы всех функций. Зашифруем две фразы и расшифруем их с использованием одного ключа (рис. 2.4).

```
[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)
```

Рис. 2.4: Шифрование двух фраз

5. Выведем результат работы программы, а также попробуем расшифровать одну из фраз, зная вторую (рис. 2.5)

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

Рис. 2.5: Результат

3 Выводы

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