Отчет по лабораторной работе №8

Основы информационной безопасности

Федоров Андрей

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Федоров Андрей Андреевич
- студент
- НБИ 2 курс
- Российский университет дружбы народов

Цели и задачи

- Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Содержание исследования

- Я выполнял лабораторную работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7.

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом, Расшифровываю оба текста сначала с помощью одного ключа, затем предполагаю, что мне неизвестен ключ, но известен один из текстов и уже расшифровываю второй, зная шифротексты и первый текст, расшифровываю оба текста сначала с помощью одного ключа, затем предполагаю, что мне неизвестен ключ, но известен один из текстов и уже расшифровываю второй, зная шифротексты и первый текст (рис. (fig:001?)).

Содержание исследования

```python
import random
import string

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

#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

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)

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) #C1^C2
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:  fDAoMYovvkmdiVwZWpQppf
Шифротекст:  чdкёшBrVкѕљъszWЗ3гAmnG
Исходный текст:  С Новым Годом, друзья!
Открытый текст:  У Слона домов, огого!!
Ключ:  fDAoMYovvkmdiVwZWpQppf
Шифротекст:  xdШeяКuVтsёњhzWЄЖюЬюQG
Исходный текст:  У Слона домов, огого!!
Расшифровать второй текст, зная первый:  У Слона домов, огого!!
Расшифровать первый текст, зная второй:  С Новым Годом, друзья!
```

Результаты

В ходе лабораторной работы были освоины на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.