Лабораторная работа №8

Элементы криптографии. Шифрование(кодирование) различных исходных текстов одним ключом

Кармацкий Н. С. Группа НФИбд-01-21

29 Сентября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Задание

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.

Выполнение лабораторной работы

Мы выполняли лабораторную работу на языке программирования Python, используя функции из 7 лабораторной работы листинг программы и результаты выполнения приведены в отчете

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом (рис. [-@fig:001]).

report > lab8.py > ...

```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)

```

Рис. 1: Функции

Расшифровываем оба текста сначала с помощью одного ключа, затем мы предполагаем, что нам не известен ключ, но известен один из текстов и уже расшифровываем неизвестный, зная шифротексты и первый текст (рис. [-@fig:002])

```
print("--------")
print(f"Открыт текст: {t1} \nКлюч: {key} \nШифротекст: {en_t1} \n Исходный текст: {de_t1} ")
print("--------")
print(f"Открыт текст: {t2} \nКлюч: {key} \nШифротекст: {en_t2} \n Исходный текст: {de_t2} ")
print("--------")

r = en_de_crypt(en_t2, en_t1)
print(f"Расшифровать второй текст, зная первый: {en_de_crypt(t1, r)}")
print(f"Расшифровать первый текст, зная второй: {en_de_crypt(t2, r)}")
```

Рис. 2: Вывод

Запускаем программу и получем положительные результаты выполнеия алгоритма (рис. [-@fig:003]).

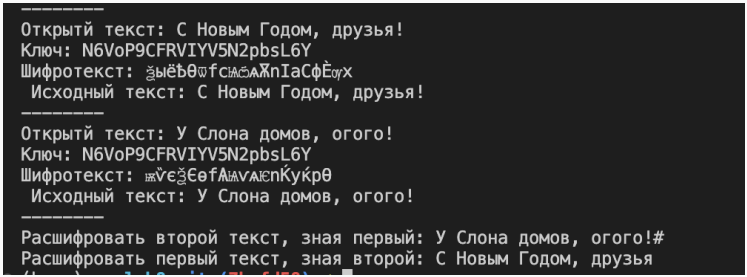

Рис. 3: Результат работы программы

Выводы

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