Отчет по лабораторной работе №8

Евдокимова Юлия НПИбд-01-18[1]

Информационная Безопасность–2022, 19 февраля, 2022, Москва, Россия

[1]Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

Задание к лабораторной работе

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста.

Процесс выполнения лабораторной работы

Процесс выполнения

В ходе выполнения данной лабораторной работы была написана следующая программа.

```
def gamm(t_text, t_key):
    res = ''
    for i, j in zip(t_text, t_key):
        if i == '-':
            temp='-'
        else:
            temp = chr(ord(i) ^ ord(j))
        res += temp
    return res
```

```
P1 = 'С Новым годом, друзья!'
P2 = 'лабораторная работа н7'
Key = 'qwertyuiopasdfghjklzxc'

C1 = gamm(P1, Key)
C2 = gamm(P2, Key)
print(C1, C2, '\n')

t_P1 = '- -овы- го-о-, -руз-я!'
t_C = gamm(C1, C2)
t_P2 = gamm(t_P1, t_C)
print(t_P1)
print(t_P2)
```

Первая функция - функция гаммирования. Далее определяем первый и второй шифротексты из текстов и ключа.

Рассмотрим пример со злоумышленником. Он знает некоторую часть первого текста. Он гаммирует шифротекст 1 и 2 и получает ключ к гаммированию между P1 и P2. После этого злоумышленник гаммирует P1 полученным ключом, получает часть P2. У него появляется возможность методом подстановки выяснить оставшуюся часть текста. Когда оставшаяся часть второго текста будет известна, можно гаммировать её и получить полный первый текст.

Выводы по проделанной работе

Вывод

На основе проделанной работы освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.