Лабораторная работа №8

Основы информационной безопасности

Чистов Д. М.

31 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Цель работы

Цель работы

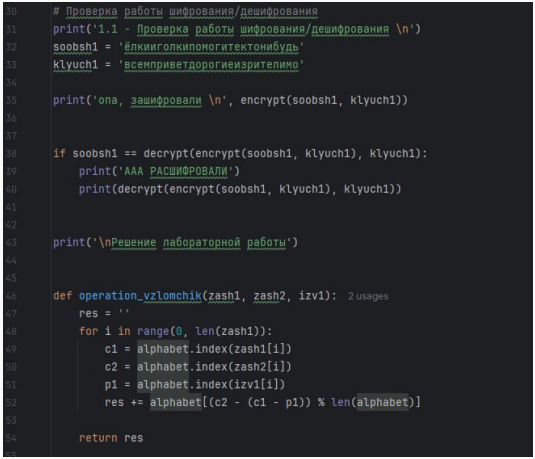
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Требуется написать программу, которая сможет получить расшифрованное сообщение 2, зная только оба зашифрованных сообщения и расшифрованное сообщение 1, без наглядного поиска ключа.

```python
alphabet = [
    "а", "б", "в", "г", "д", "е", "ё", "ж", "з", "и", "й", "к", "л", "м", "н", "о",
    "п", "р", "с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ъ", "ы", "ь", "э", "ю", "я",
    "А", "Б", "В", "Г", "Д", "Е", "Ё", "Ж", "З", "И", "Й", "К", "Л", "М", "Н", "О",
    "П", "Р", "С", "Т", "У", "Ф", "Х", "Ц", "Ч", "Ш", "Щ", "Ъ", "Ы", "Ь", "Э", "Ю", "Я",
    "0", "1", "2", "3", "4", "5", "6", "7", "8", "9"
]

# Шифрование
def encrypt(text, key):  5 usages
    res = ''
    for i in range(0, len(text)):
        i1 = alphabet.index(text[i])
        i2 = alphabet.index(key[i])
        res += alphabet[(i1 + i2) % len(alphabet)]
    return res


# Дешифрование
def decrypt(text, key):  2 usages
    res = ''
    for i in range(0, len(text)):
        i1 = alphabet.index(text[i])
        i2 = alphabet.index(key[i])
        res += alphabet[(i1 - i2) % len(alphabet)]
    return res
```

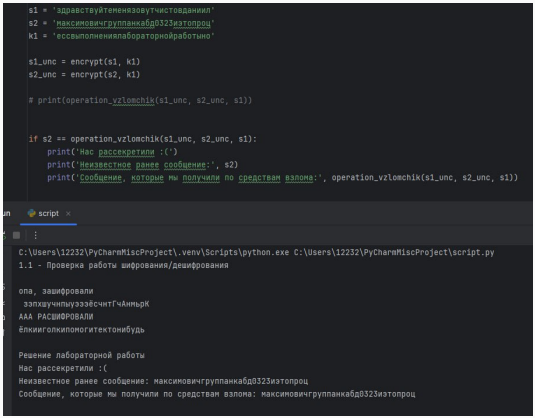
Рис. 1: Функции шифрования и дешифрования

На втором фото: функция получения расшифрованного сообщения 2, зная сообщение 1 и оба зашифрованных сообщений.



```
# Проверка работы шифрования/дешифрования
print('1.1 - Проверка работы шифрования/дешифрования \n')
soobsh1 = 'ёлкииголкипомогитектонибудь'
klyuch1 = 'всемприветдорогиеизрителимо'

print('она, зашифровали \n', encrypt(soobsh1, klyuch1))


if soobsh1 == decrypt(encrypt(soobsh1, klyuch1), klyuch1):
    print('ААА РАСШИФРОВАЛИ')
    print(decrypt(encrypt(soobsh1, klyuch1), klyuch1))


print('\nРешение лабораторной работы')


def operation_vzlomchik(zash1, zash2, izv1):  2 usages
    res = ''
    for i in range(0, len(zash1)):
        c1 = alphabet.index(zash1[i])
        c2 = alphabet.index(zash2[i])
        p1 = alphabet.index(izv1[i])
        res += alphabet[(c2 - (c1 - p1)) % len(alphabet)]

    return res
```

На третьем фото: результат работы всей программы



```
s1 = 'здравствуйтеменязовутчистованаим!'
s2 = 'максимовичгруппанкабд0323итопроц'
k1 = 'всвыполнениялабораторнойработыно'

s1_unc = encrypt(s1, k1)
s2_unc = encrypt(s2, k1)

# print(operation_vzlomchik(s1_unc, s2_unc, s1))


if s2 == operation_vzlomchik(s1_unc, s2_unc, s1):
    print('Нас рассекретили :(')
    print('Неизвестное ранее сообщение:', s2)
    print('Сообщение, которые мы получили по средствам взлома:', operation_vzlomchik(s1_unc, s2_unc, s1))
```

```
script
C:\Users\12232\PyCharmMiscProject\.venv\Scripts\python.exe C:\Users\12232\PyCharmMiscProject\script.py
1.1 - Проверка работы шифрования/дешифрования

опа, зашифровали
 зэпхвучнпыуээзёсчнтГчАнньрК
ААА РАСШИФРОВАЛИ
ёлкиголкипомогитектонибудь

Решение лабораторной работы
Нас рассекретили :(
Неизвестное ранее сообщение: максимовичгруппанкабд0323итопроц
Сообщение, которые мы получили по средствам взлома: максимовичгруппанкабд0323итопроц
```

Рис. 3: Результат взлома

Выводы

Выводы

В результате выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Список литературы

Список литературы

Лабораторная работа №8