

Лабораторная работа №7

Основы информационной безопасности

Ищенко Ирина

Российский университет дружбы народов, Москва, Россия

- Ищенко Ирина Олеговна
- НПИбд-02-22

Освоить на практике применение режима однократного гаммирования.

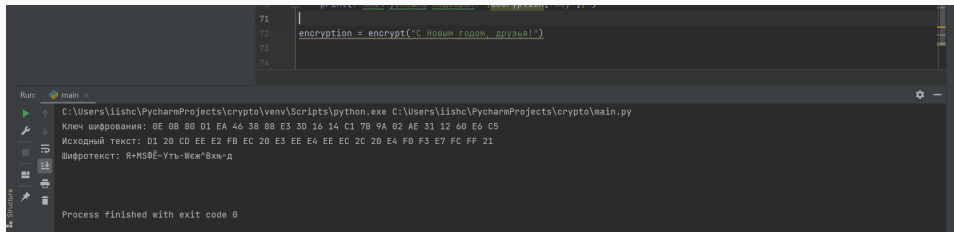
Выполнение лабораторной работы

```
def encrypt(text: str, key: list = None):
    text_16 = [char.encode(encoding='cp1251').hex().upper() for char in text]
    if not key:
        key = generate_key(length=len(text))

    print(f"Ключ шифрования:", ' '.join(str(s) for s in key))
    print(f"Исходный текст:", ' '.join(text_16))
    encrypted_text = []
    for i in range(len(text)):
        xor_char = int(text_16[i], 16) ^ int(key[i], 16)
        encrypted_text.append(int2hex(xor_char))
```

```
encrypted_text = validate(encrypted_text)
ciphertext = bytes.fromhex(''.join(encrypted_text)).decode('cp1251')
print(f'Шифротекст: {ciphertext}\n\n')

return {
    'key': key,
    'ciphertext': ciphertext
}
```



```
71 |  
72 | encryption = encrypt("С Новым годом, друзья!")  
73 |  
74 |
```

Run: main x

C:\Users\iishc\PycharmProjects\crypto\venv\Scripts\python.exe C:\Users\iishc\PycharmProjects\crypto\main.py

Ключ шифрования: 0E 0B 80 D1 EA 46 38 88 E3 3D 16 14 C1 7B 9A 02 AE 31 12 60 E6 C5

Исходный текст: D1 20 CD EE E2 FB EC 20 E3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21

Шифротекст: Я+MS0E-Уть-Исж^Вхь-д

Process finished with exit code 0

Рис. 1: Функция encrypt()

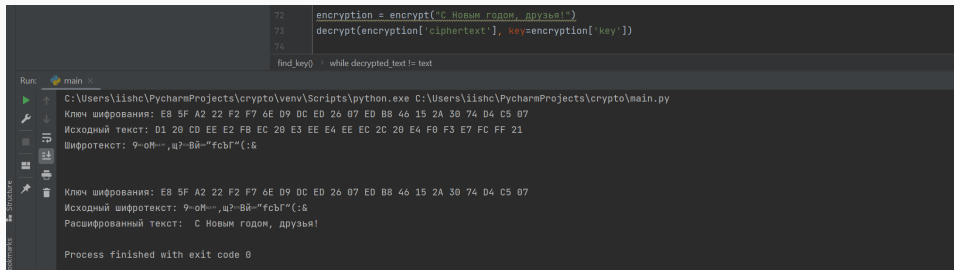
```
def decrypt(ciphertext: str, key: list = None):  
    ciphertext_16 = [char.encode('cp1251').hex().upper() for char in ciphertext]  
    if not key:  
        key = generate_key(length=len(ciphertext))  
  
    print(f"Ключ шифрования:", ' '.join(str(s) for s in key))  
    print(f"Исходный шифротекст:", ciphertext)
```



```
decrypted_text = []
for i in range(len(ciphertext)):
    xor_char = int(ciphertext_16[i], 16) ^ int(key[i], 16)
    decrypted_text.append(int2hex(xor_char))

decrypted_text = validate(decrypted_text)
decrypted_text = bytes.fromhex(''.join(decrypted_text)).decode('cp1251')
print('Расшифрованный текст: ', decrypted_text)
return {
    'key': key,
    'text': decrypted_text
}
```

Дешифрование с известным ключом



```
72 encryption = encrypt("С Новым годом, друзья!")
73 decrypt(encryption['ciphertext'], key=encryption['key'])
74
```

find_key() > while decrypted_text != text

Run: main

C:\Users\iishc\PycharmProjects\crypto\venv\Scripts\python.exe C:\Users\iishc\PycharmProjects\crypto\main.py

Ключ шифрования: E8 5F A2 22 F2 F7 6E 09 DC ED 26 07 ED B8 46 15 2A 30 74 D4 C5 07

Исходный текст: D1 20 CD EE E2 FB EC 20 E3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21

Шифротекст: 9-oM--щ?-Вй-"fсбГ"(:&

Ключ шифрования: E8 5F A2 22 F2 F7 6E 09 DC ED 26 07 ED B8 46 15 2A 30 74 D4 C5 07

Исходный шифротекст: 9-oM--щ?-Вй-"fсбГ"(:&

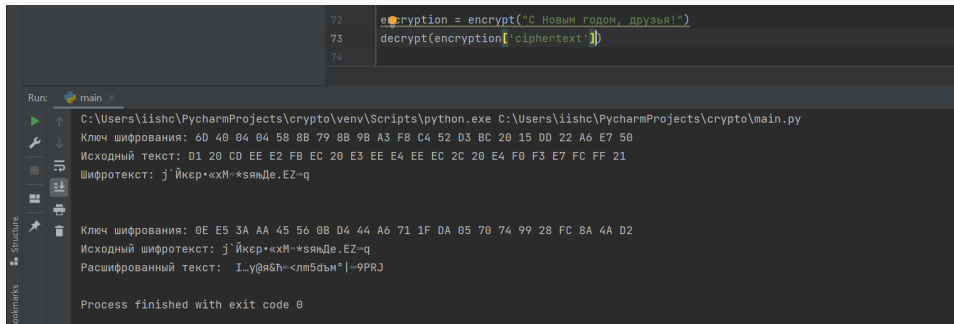
Расшифрованный текст: С Новым годом, друзья!

Process finished with exit code 0

Рис. 2: decrypt() с тем же ключом

```
def find_key(text):  
    decrypted_text = ''  
    encryption = encrypt(text)  
    while decrypted_text != text:  
        decryption = decrypt(encryption['ciphertext'])  
        decrypted_text = decryption['text']  
        print(f'Полученный текст: {decrypted_text}')  
    print(f"Ключ успешно подобран! {decryption['key']}")
```

Дешифрование с подбором



The screenshot shows a Python IDE with a code editor and a run console. The code in the editor defines an encryption function and uses it to encrypt a message. The console output shows the execution of the script, displaying the encryption key, the original text in hexadecimal, the ciphertext, and the decrypted text.

```
72 encryption = encrypt("С Новым годом, друзья!")
73 decrypt(encryption['ciphertext'])
74
```

Run: main ×

C:\Users\iishc\PycharmProjects\crypto\venv\Scripts\python.exe C:\Users\iishc\PycharmProjects\crypto\main.py

Ключ шифрования: 6D 40 04 04 58 8B 79 8B 9B A3 F8 C4 52 D3 BC 20 15 DD 22 A6 E7 50

Исходный текст: D1 20 CD EE E2 FB EC 20 E3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21

Шифротекст: j`Йкер•«хМ~*сяьДе.EZ~q

Ключ шифрования: 0E E5 3A AA 45 56 0B D4 44 A6 71 1F DA 05 70 74 99 28 FC 8A 4A D2

Исходный шифротекст: j`Йкер•«хМ~*сяьДе.EZ~q

Расшифрованный текст: I...y@я&h~<лm5dъм°|~9PRJ

Process finished with exit code 0

Рис. 3: decrypt() со случайным ключом

В ходе выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования.