Лабораторная работа №8

Основы информационной безопасности

Мишина А. А.

23 мая 2024

Докладчик

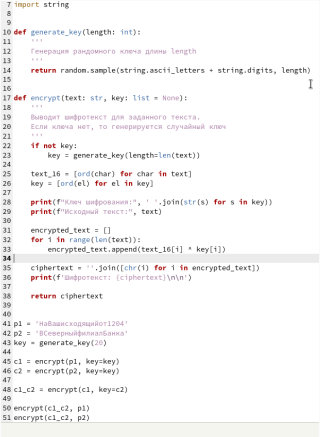
- Мишина Анастасия Алексеевна
- НПИбд-02-22

Выполнение лабораторной работы

Цель работы

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

Файл main2.py



```python
import string


def generate_key(length: int):
    '''
    Генерация рандомного ключа длины length
    '''
    return random.sample(string.ascii_letters + string.digits, length)


def encrypt(text: str, key: list = None):
    '''
    Выводит шифротекст для заданного текста.
    Если ключа нет, то генерируется случайный ключ
    '''
    if not key:
        key = generate_key(length=len(text))

    text_16 = [ord(char) for char in text]
    key = [ord(el) for el in key]

    print(f"Ключ шифрования:", ''.join(str(s) for s in key))
    print(f"Исходный текст:", text)

    encrypted_text = []
    for i in range(len(text)):
        encrypted_text.append(text_16[i] ^ key[i])

    ciphertext = ''.join([chr(i) for i in encrypted_text])
    print(f'Шифротекст: {ciphertext}\n\n')

    return ciphertext


p1 = 'НаВашисходящийот1204'
p2 = 'ВСеверныйфилиалБанка'
key = generate_key(20)

c1 = encrypt(p1, key=key)
c2 = encrypt(p2, key=key)

c1_c2 = encrypt(c1, key=c2)

encrypt(c1_c2, p1)
encrypt(c1_c2, p2)
```

Рис. 1: Исходный код программы

Запуск main2.py

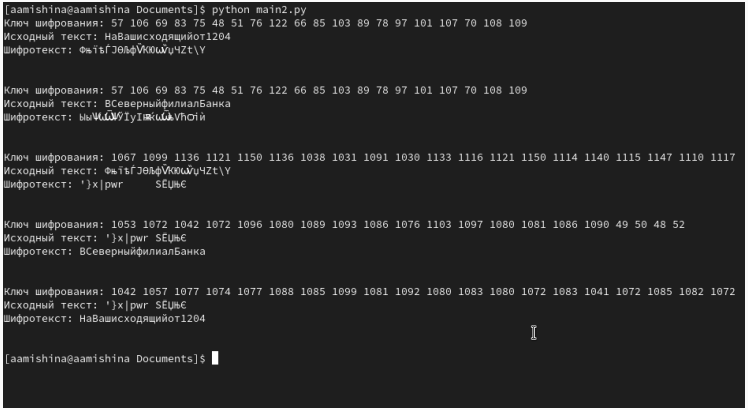


Рис. 2: Работа программы

Вывод

- В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.