Лабораторная работа №8

Основы информационной безопасности

Ищенко Ирина

Российский университет дружбы народов, Москва, Россия

Докладчик

- Ищенко Ирина Олеговна
- НПИбд-02-22

Цель работы

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

Выполнение лабораторной работы

```
def encrypt(text: str, key: list = None):
    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
```

Реализация

```
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)
```

Выполнение

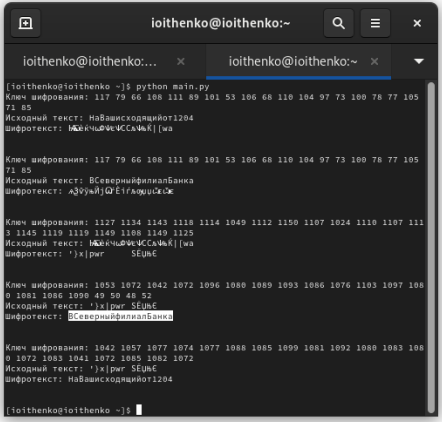

Рис. 1: Вывод программы

Выводы

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