Лабораторная Работа №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Основы информационной безопасности

Барсегян В.Л.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Докладчик

- Барсегян Вардан Левонович
- НПИбд-01-22
- Российский университет дружбы народов
- [1132222005@pfur.ru]
- https://github.com/VARdamn/oib

Вводная часть

Цели и задачи

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

Выполнение лабораторной работы

Создаю функцию encrypt(), которая будет шифровать заданный текст с помощью однократного гаммирования. На вход функция получает открытый текст, также можно задать определенный ключ шифрования. Если ключа нет, то он генерируется рандомно. Сначала исходный текст и ключ шифрования преобразуются в 16-ную СС, затем, применяется операция XOR для каждого элемента ключа и текста. Полученный шифротекст декодируется из 16-ной СС и получается набор из символов.

Функция encrypt()

```
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)
```

Генерация ключа, если он не задан, происходит в функции generate_key() из ascii-символов и цифр

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

Работа программмы:

- сначала создается случайный ключ и с этим ключом шифруются тексты p1 и p1 (переменные c1 и c2)
- далее, шифротекст c1 шифруется по ключу c2
- полученный шифротекст c1_c2 шифруется по ключу открытого текста. в результате, получаем второй открытый текст, ранее неизвестный

```
0
1   p1 = 'НаВашисходящийот1204'
2   p2 = 'ВСеверныйфилиалБанка'
3   key = generate_key(20)
4
5   c1 = encrypt(p1, key=key)
6   c2 = encrypt(p2, key=key)
```

Полный вывод работы программы

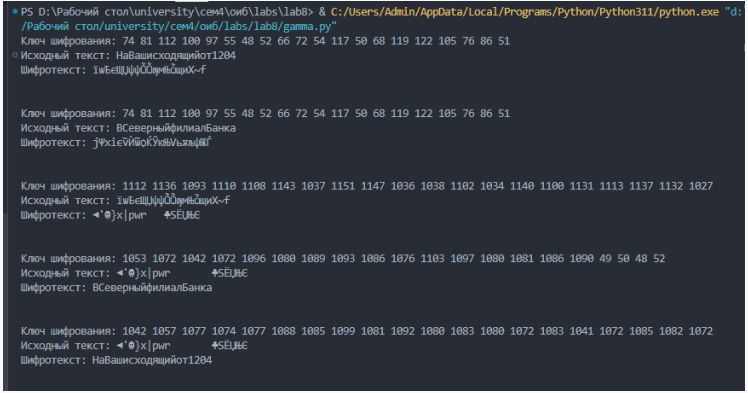

Figure 2: Работа программы

Вывод

Я применил режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом