Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Лилия М. Пономарёва НПИбд-02-19[1]

2022, 19 March, Moscow, Russian Federation

[1]RUDN University, Moscow, Russian Federation

Цель работы

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

Задание

Два текста кодируются одним ключом (однократное гаммирование).
P1 = НаВашисходящийот1204
P2 = ВСеверныйфилиалБанка

Требуется не зная ключа и не стремясь его определить, прочитать оба текста.

Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.

Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

Функция генерации ключа для текстов

```python
import string
import random


def key_gen(text):
    key = ' '.join(random.choice(string.hexdigits)+random.choice(string.hexdigits) for _ in range(len(text)))
    return key


P1 = 'НаВашисходящийот1204'
P2 = 'ВСеверныйфилиалБанка'
key = key_gen(P1)
print("Ключ:", key)
```

Рис. 1: Генерация ключа

Функция шифровки двух текстов с известным ключом

```python
def crypt(text1, text2):
    key1 = [ord(i) for i in key]
    text1 = [ord(i) for i in text1]
    text2 = [ord(i) for i in text2]
    crypt1 = ''.join(chr(a ^ b) for a, b in zip(text1, key1))
    crypt2 = ''.join(chr(a ^ b) for a, b in zip(text2, key1))
    return crypt1, crypt2


code1, code2 = crypt(P1, P2)
print("Шифротекст 1:", code1)
print("Шифротекст 2:", code2)
```

Рис. 2: Шифровка текстов при известном ключе

Функция дешифровки сообщений без знания ключа.

```
def decrypt(code1, code2):
    code1 = [ord(i) for i in code1]
    code2 = [ord(i) for i in code2]
    key_ = ''.join(chr(a ^ b) for a, b in zip(code1, code2))
    text1 = ''.join(chr(a ^ b) for a, b in zip(code1, key_))
    text2 = ''.join(chr(a ^ b) for a, b in zip(code1, key_))
    return text1, text2


txt1, txt2 = crypt(code1, code2)
print("Дешифровка 1 текста:", txt1)
print("Дешифровка 2 текста:", txt2)
```

Рис. 3: Дешифровка сообщений без ключа

Итог

```
C:\Users\lilyp_032u5e1\PycharmProjects\IS_lab1\venv\Scripts\python.
Ключ: 5d C6 Fe 5E c7 00 E4 cb 24 06 2c Cf 0b 7A eb 46 f3 c0 15 26
Шифротекст 1: ШєвѳѿИЇРОЁЊѪћЎОѳ▯▯u
Шифротекст 2: ЧхЕѱЃѡѻЮЙѱѽЛћЇЛСѢНѽЄ
Дешифровка 1 текста: НаВашисходящийот1204
Дешифровка 2 текста: ВСеверныйфилиалБанка

Process finished with exit code 0
```

Рис. 4: Вывод

Вывод

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