Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

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.

Программа шифровки

Приложение может:

1. Определять вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Определение шифротекста

```
def ciphertext(text, key):
    encoded_bytes = text.encode('utf-8', 'replace')
    x = binascii.hexlify(encoded_bytes)
    y = str(x, 'utf-8')
    binary = lambda x: " ".join(reversed(
        [i + j for i, j in zip(*[["{0:04b}".format(int(c, 16)) for c in reversed("0" + x)][n::2] for n in [1, 0]])]))
    x1 = binary(y)

    key1 = bytearray.fromhex(key)
    x_key = binascii.hexlify(key1)
    y_key = str(x_key, 'utf-8')
    x1_key = binary(y_key)
```

Рис. 1: Представление данных в двоичном виде

Определение шифротекста

```
text2 = ""
for i in range(len(x1)):
    if x1[i] == ' ':
        text2 += ' '
    elif x1[i] == x1_key[i]:
        text2 += '0'
    elif x1[i] != x1_key[i]:
        text2 += '1'

text2_ = text2.split()
crypt = ' '
for n in text2_:
    crypt += hex(int(n, 2))[2:] + ' '
return crypt
```

Рис. 2: Реализация сложения по модулю

Определение ключа

```
def getkey(cipher, text):
    encoded_bytes = bytearray.fromhex(cipher)
    x = binascii.hexlify(encoded_bytes)
    y = str(x, 'utf-8')
    binary = lambda x: " ".join(reversed(
        [i + j for i, j in zip(*[["{0:04b}".format(int(c, 16)) for c in reversed("0" + x)][n::2] for n in [1, 0]])]))
    x1 = binary(y)

    text1 = text.encode('utf-8', 'replace')
    x_text = binascii.hexlify(text1)
    y_text = str(x_text, 'utf-8')
    x1_text = binary(y_text)
```

Рис. 3: Представление данных в двоичном виде

Определение ключа

```
key = ""
for i in range(len(x1)):
    if x1[i] == ' ':
        key += ' '
    elif x1[i] == x1_text[i]:
        key += '0'
    elif x1[i] != x1_text[i]:
        key += '1'

key_ = key.split()
pos_key = ' '
for n in key_:
    pos_key += hex(int(n, 2))[2:] + ' '
return pos_key
```

Рис. 4: Получение ключа

Сообщение «С Новым Годом, друзья!»

```
a = 'Штирлиц - Вы Герой!!!'
key = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 05"
text = "С Новым Годом, друзья"

cipher = ciphertext(a, key)
print("Шифротекст:", cipher)
print("Ключ:", getkey(cipher, text))
```

```
XORcipher
C:\Users\lilyp_032u5e1\PycharmProjects\IS_lab1\venv\Scripts\python.exe C:/Users/lilyp_032u5e1/PycharmProjects/Encryption/XORcipher
Шифротекст:  d5 a4 c6 fd de f6 e6 52 44 ab d9 96 f3 d1 df 2a 8b 21 50 84 97 dd 9c 5f de dd e7 67 45 90 d9 90 f2 ee de e9 24
Ключ:  5 5 e6 2d 43 26 58 82 f6 7a 52 46 4f f1 f b9 5b 9f 80 30 47 63 4c e3 f2 fd 37 d3 94 10 8 13 22 59 f 65 f5
```

Рис. 5: Ключ

Проверка

```
59  a = 'Штирлиц - Вы Герой!!!'
60  key = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 05"
61  text = "С Новым Годом, друзья"
62
63  cipher = ciphertext(a, key)
64  print("Шифротекст:", cipher)
65  print("Ключ:", getkey(cipher, a))
66
```

```
XORcipher
C:\Users\lilyp_032u5e1\PycharmProjects\IS_lab1\venv\Scripts\python.exe C:/Users/lilyp_032u5e1/PycharmProjects/Encryption/XORcipher
Шифротекст:  d5 a4 c6 fd de f6 e6 52 44 ab d9 96 f3 d1 df 2a 8b 21 50 84 97 dd 9c 5f de dd e7 67 45 90 d9 90 f2 ee de e9 24
Ключ:  5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 b b2 70 54 5 c 17 7f e 4e 37 d2 94 10 9 2e 22 57 ff c8 5
```

Рис. 6: Получение изначального ключа

Вывод

Освоили на практике применение режима однократного гаммирования.