

Информационная безопасность

лабораторная работа №8

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

Ким Илья Владиславович НФИбд-01-21

Содержание

Цель работы	3
Выполнение лабораторной работы	4
Листинг	7
Выводы	10

Цель работы

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

Выполнение лабораторной работы

1. Подключил библиотеки и ввел сообщения (рис. [-@fig:001])

```
import numpy as np
import pandas as pd
```

```
a="НаВашисходящийот1204"
b="ВСеверныйфилиалБанка"
```

2. Перевод сообщений в шестнадцатеричную систему счисления (рис. [-@fig:002])(рис. [-@fig:003])

```
def cr(a,b):
    print ("Текст №1: ", a)
    print ("Текст №2: ", b)
    print("\n№1 Кодировка текста")
    print("_____ \n")
    text=[]
    for i in a:
        text.append(i.encode("cp1251").hex().upper())
    print ("Закодированный текст №1 (P1): ", *text)
    text1=[]
    for i in b:
        text1.append(i.encode("cp1251").hex().upper())
    print ("Закодированный текст №2 (P2): ", *text1)
```

Текст №1: НаВашисходящийот1204
Текст №2: ВСеверныйфилиалБанка

№1 Кодировка текста

Закодированный текст №1 (P1): CD E0 C2 E0 F8 E8 F1 F5 EE E4 FF F9 E8 E9 EE F2 31 32 30 34
Закодированный текст №2 (P2): C2 D1 E5 E2 E5 F0 ED FB E9 F4 E8 EB E8 E0 EB C1 E0 ED EA E0

3. Создание ключа (рис. [-@fig:004])(рис. [-@fig:005])

```
print("\n№2 Создание ключа")
print("_____ \n")
k=np.random.randint(0,255,20)
key=[hex(i).upper()[2:] for i in k]
print("Ключ: ", *key)
```

№2 Создание ключа

Ключ: 17 36 C3 B8 9F B2 84 D2 79 7A F6 22 9D CF 2D 36 3B 2F 40 19

4. Кодировка текстов ключем (рис. [-@fig:006])(рис. [-@fig:007])

```
print("\n№3 Кодировка текста ключем")
print("_____ \n")
newa=[]
for i in range(len(text)):
    newa.append("{:02x}".format(int(key[i],16)^int(text[i],16)).upper())
print("Закодированный ключем текст №1 (C1):",*newa )
newb=[]
for i in range(len(text1)):
    newb.append("{:02x}".format(int(key[i],16)^int(text1[i],16)).upper())
print("Закодированный ключем текст №2 (C2):",*newb )
```

№3 Кодировка текста ключем

Закодированный ключем текст №1 (C1): DA D6 01 58 67 5A 75 27 97 9E 09 DB 75 26 C3 C4 0A 1D 70 2D
Закодированный ключем текст №2 (C2): D5 E7 26 5A 7A 42 69 29 90 8E 1E C9 75 2F C6 F7 DB C2 AA F9

5. Расшифровка текстов по C1, C2, P1, P2 (рис. [-@fig:008])(рис. [-@fig:009])

```
print("\n№4 Расшифровка текста №1 по (C1), (C2) и (P2)")
print("_____ \n")
p1=[]
for i in range(len(text)):
    p1.append("{:02x}".format(int(newa[i],16)^int(newb[i],16)^int(text1[i],16)).upper())

p1=bytearray.fromhex("".join(p1)).decode("cp1251")
print("Расшифрованный текст №1 по (C1), (C2) и (P2): ", p1)

print("\n№5 Расшифровка текста №2 по (C1), (C2) и (P1)")
print("_____ \n")
p2=[]
for i in range(len(text1)):
    p2.append("{:02x}".format(int(newa[i],16)^int(newb[i],16)^int(text[i],16)).upper())

p2=bytearray.fromhex("".join(p2)).decode("cp1251")
print("Расшифрованный текст №2 по (C1), (C2) и (P1): ", p2)
```

№4 Расшифровка текста №1 по (C1), (C2) и (P2)

Расшифрованный текст №1 по (C1), (C2) и (P2): НаВашисходящийот1204

№5 Расшифровка текста №2 по (C1), (C2) и (P1)

Расшифрованный текст №2 по (C1), (C2) и (P1): ВСеверныйфилиалБанка

6. Расшифровка текстов по известному ключу (рис. [-@fig:010])(рис. [-@fig:011])

```
print("\n№6 Расшифровка текста №1 по известному ключу")
print("_____ \n")
truetext=[]
for i in range(len(text)):
    truetext.append("{:02x}".format(int(key[i],16)^int(newa[i],16)).upper())
truetext=bytearray.fromhex("".join(truetext)).decode("cp1251")
print("Расшифрованный по известному ключу текст №1: ", truetext)

print("\n№7 Расшифровка текста №2 по известному ключу")
print("_____ \n")
truetext1=[]
for i in range(len(text)):
    truetext1.append("{:02x}".format(int(key[i],16)^int(newb[i],16)).upper())
truetext1=bytearray.fromhex("".join(truetext1)).decode("cp1251")
print("Расшифрованный по известному ключу текст №2: ", truetext1)
return
```

№6 Расшифровка текста №1 по известному ключу

Расшифрованный по известному ключу текст №1: НаВашисходящийот1204

№7 Расшифровка текста №2 по известному ключу

Расшифрованный по известному ключу текст №2: ВСеверныйфилиалБанка

Листинг

```
import numpy as np
import pandas as pd
a="НаВашиисходящийот1204"
b="ВСеверныйфилиалБанка"
def cr(a,b): print ("Текст №1:", a)

print ("Текст №2: ", b)

print("\n№1 Кодировка текста")
print("_____ \n")
text=[]
for i in a:
    text.append(i.encode("cp1251").hex().upper())
print ("Закодированный текст №1 (P1): ", *text)
text1=[]
for i in b:
    text1.append(i.encode("cp1251").hex().upper())
print ("Закодированный текст №2 (P2): ", *text1)

print("\n№2 Создание ключа")
print("_____ \n")
k=np.random.randint(0,255,20)
key=[hex(i).upper()[2:] for i in k]
```

```

print("Ключ:                ", *key)

print("\n№3 Кодировка текста ключем")
print("_____ \n")
newa=[]
for i in range(len(text)):
    newa.append("{:02x}".format(int(key[i],16)^int(text[i],16)).upper())
print("Закодированный ключем текст №1 (C1):",*newa )
newb=[]
for i in range(len(text1)):
    newb.append("{:02x}".format(int(key[i],16)^int(text1[i],16)).upper())
print("Закодированный ключем текст №2 (C2):",*newb )

print("\n№4 Расшифровка текста №1 по (C1), (C2) и (P2)")
print("_____ \n")
p1=[]
for i in range(len(text)):
    p1.append("{:02x}".format(int(newa[i],16)^int(newb[i],16)^int(text1[i],16)).upper())

p1=bytearray.fromhex("".join(p1)).decode("cp1251")
print("Расшифрованный текст №1 по (C1), (C2) и (P2): ", p1)

print("\n№5 Расшифровка текста №2 по (C1), (C2) и (P1)")
print("_____ \n")
p2=[]
for i in range(len(text1)):
    p2.append("{:02x}".format(int(newa[i],16)^int(newb[i],16)^int(text[i],16)).upper())

p2=bytearray.fromhex("".join(p2)).decode("cp1251")

```



```

print("Расшифрованный текст №2 по (C1), (C2) и (P1): ", p2)

print("\n№6 Расшифровка текста №1 по известному ключу")
print("_____ \n")
truetext=[]
for i in range(len(text)):
    truetext.append("{:02x}".format(int(key[i],16)^int(newa[i],16)).upper())
truetext=bytearray.fromhex("".join(truetext)).decode("cp1251")
print("Расшифрованный по известному ключу текст №1: ", truetext)

print("\n№7 Расшифровка текста №2 по известному ключу")
print("_____ \n")
truetext1=[]
for i in range(len(text)):
    truetext1.append("{:02x}".format(int(key[i],16)^int(newb[i],16)).upper())
truetext1=bytearray.fromhex("".join(truetext1)).decode("cp1251")
print("Расшифрованный по известному ключу текст №2: ", truetext1)
return

```

Выводы

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