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

Критский Сергей Димитриевич

Цель работы

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

Ход выполнения работы

Написание программы

In [1]:

```
a = ord("a")
alphabeth = [chr(i) for i in range(a, a + 32)]
a = ord("0")
for i in range(a, a+10):
    alphabeth.append(chr(i))

a = ord("А")
for i in range(1040, 1072):
    alphabeth.append(chr(i))
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
key = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54"


def vzlom(P1, P2):
    code = []
    for i in range(20):
        code.append(alphabeth[(alphabeth.index(P1[i]) + alphabeth.index(P2[i]))
    print(code)
    print(code[16], " и ", code[19])
    p3 = "".join(code)
    print(p3)

vzlom(P1, P2)
```

Рис. 1: Инициализация переменных, получение гаммы

Написание программы

```
for i in text:
    listofdigitsoftext.append(dicts[i])
print("Числа текста", listofdigitsoftext)

for i in gamma:
    listofdigitsofgamma.append(dicts[i])
print("числа гаммы", listofdigitsofgamma)
listofdigitsresult = list()
ch = 0
for i in text:
    try:
        a = dicts[i] + listofdigitsofgamma[ch]
    except:
        ch = 0
        a = dicts[i] + listofdigitsofgamma[ch]
    if a > 75:
        a = a%75
        print(a)
    ch += 1
    listofdigitsresult.append(a)
print("Числа зашифрованного текста", listofdigitsresult)
textencrypted = ""
for i in listofdigitsresult:
    textencrypted += dict2[i]
```

Написание программы

```
    for i in listofdigits:
        try:
            a = i - listofdigitsofgamma[ch]
        except:
            ch=0
            a = i - listofdigitsofgamma[ch]
        if a < 1:
            a = 75 + a
        listofdigits1.append(a)
        ch += 1
    textdecrypted = ""
    for i in listofdigits1:
        textdecrypted += dict2[i]
    print("Расшифрованный текст", textdecrypted)

shifr(P1)
```


Рис. 3: Дешифровка

Результат

```
['щ', 'С', 'З', 'в', 'э', 'ш', 'ю', 'Ж', 'ч', 'ш', '7', '4', 'р', 'й', 'щ',
'У', '1', 'Е', 'А', '4']
1  и  4
щСЗвэшюЖчш74рйщУ1ЕА4
```

Рис. 4: Получение гаммы

Результат

```
Введите гаммущСЗвэшюЖчш74рйщУ1ЕА4
Числа текста [47, 1, 35, 1, 26, 10, 19, 23, 16, 5, 32, 27, 10, 11, 16, 20, 66,
67, 75, 69]
числа гаммы [27, 51, 41, 3, 31, 26, 32, 40, 25, 26, 72, 69, 18, 11, 27, 53, 66,
38, 33, 69]
1
29
21
57
30
33
63
Числа зашифрованного текста [74, 52, 1, 4, 57, 36, 51, 63, 41, 31, 29, 21, 28,
22, 43, 73, 57, 30, 33, 63]
Зашифрованный текст:  9ТагЧГСЭЗэыуъфЙ8ЧьАЭ
Расшифрованный текст НаВашисходящийот1204
```

Рис. 5: Дешифровка данных

Вывод

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