Цель работы

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

Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). 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. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Реализация приложения:

```
a = ord("а")
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))
print(alphabeth)
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
#длина ключа 20
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]))
 % len(alphabeth)])
    #получили известные символы в шаблоне
    print(code)
    print(code[16], " и ", code[19])
    p3 = "".join(code)
    print(p3)

vzlom(P1, P2)
def shifr(P1):
    #создаем алфавит
    dicts = {"а": 1, "б": 2, "в": 3, "г": 4, "д": 5, "е": 6, "ё": 7, "ж": 8,
"з": 9, "и": 10, "й": 11, "к": 12, "л": 13,
             "м": 14, "н": 15, "о": 16, "п": 17,
             "р": 18, "с": 19, "т": 20, "у": 21, "ф": 22, "х": 23, "ц": 24, "ч":
25, "ш": 26, "щ": 27, "ъ": 28,
```

```
            "ы": 29, "ь": 30, "э": 31, "ю": 32, "я": 32, "А":33 , "Б": 34, "В":
35 , "Г":36 , "Д":37 , "Е":38 , "Ё":39 , "Ж":40 , "З":41 ,
               "И":42,"Й":43 , "К":44 , "Л":45 , "М":46 , "Н":47 , "О":48 ,
"П":49 , "Р":50 , "С":51 , "Т":52 , "У":53 , "Ф":54 , "Х":55 , "Ц":56 , "Ч":57 ,
    "Ш":58,"Щ":59 , "Ъ":60 , "Ы":61 , "Ь":62 , "Э":63 , "Ю":64 , "Я":65 , "1":66
, "2":67 , "3":68 , "4":69 , "5":70 , "6":71 , "7": 72, "8":73 , "9":74 , "0":75
    }
    dict2 = {v: k for k, v in dicts.items()}
    text = P1
    gamma = input("Введите гамму(на русском языке! Да и пробелы тоже нельзя!
Короче, только символы из dict")
    listofdigitsoftext = list()
    listofdigitsofgamma = list()
    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]
    print("Зашифрованный текст: ", textencrypted)
    listofdigits = list()
    for i in textencrypted:
        listofdigits.append(dicts[i])
    ch = 0
    listofdigits1 = list()
    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)
```

Проверка работы приложения (рис.1-2):

```
18
19 def vzlom(P1, P2):
20     code = []
21     for i in range(20):
22         code.append(alphabeth[(alphabeth.index(P1[i]) + alphabeth.index(P2[i]))  % len(alphabeth)])
23     #получили известные символы в шаблоне
24     print(code)
25     print(code[16], " и ", code[19])
26     p3 = "".join(code)
27     print(p3)
28
29 vzlom(P1, P2)
['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.1

```
Введите гамму(на русском языке! Да и пробелы тоже нельзя! Короче, только символы из dictщСЗвэшюЖчш74рйщУ1ЕА4
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:  9ТагЧГСЭЭэыуъфЙ8ЧьАЭ
Расшифрованный текст НаВашисходящийот1204
```

рис.2

Контрольные вопросы

1.Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

С помощью формулы C1⊕C2⊕P1=P1⊕P2⊕P1=P2, где C1 и C2 – шифротексты.

2.Что будет при повторном использовании ключа при шифровании текста?

При таких условиях мы получим исходное сообщение.

3.Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

С помощью формул C1=P1⊕K, C2=P2⊕K, где где Ci – шифротексты, Pi – открытые тексты, K – единый ключ шифрования.

4.Перечислите недостатки шифрования одним ключом двух открытых текстов.

1)Имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа.

2)Зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения P2, которые находятся на позициях известного шаблона сообщения P1.

3)Зная ключ, злоумышленник смоет расшифровать все сообщения, которые были закодированы при его помощи.

5.Перечислите преимущества шифрования одним ключом двух открытых текстов.

1)Данный способ помогает упростить процесс шифрования и дешифровки.

2)При отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных.

Выводы

В ходе выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

1.Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №8.