Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Я подобрала ключ, чтобы получить сообщение «С Новым Годом, друзья!» (рис.1). Разработала приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1.Определить 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.

```
def shifr(P1):
    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(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)
```

```
1 shifr("СНовымГодомДрузья")
```

```
Введите гамму(Только символы из dict): яьзурДмодГывНС
Числа текста [51, 47, 16, 3, 29, 14, 36, 16, 5, 16, 14, 37, 18, 21, 9, 30, 32]
числа гаммы [32, 30, 9, 21, 18, 37, 14, 16, 5, 36, 29, 3, 47, 51]
8
2
Числа зашифрованного текста [8, 2, 25, 24, 47, 51, 50, 32, 10, 52, 43, 40, 65, 72, 41, 60, 41]
Зашифрованный текст:  жбчцНСРяиТЙЖЯ73Ъ3
Расшифрованный текст СНовымГодомДрузья
```

рис.1

Контрольные вопросы

1.Поясните смысл однократного гаммирования.

Гаммирование – выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

2.Перечислите недостатки однократного гаммирования.

Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

3.Перечислите преимущества однократного гаммирования.

Такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение. Шифрование и расшифрование может быть выполнено одной и той же программой. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

4.Почему длина открытого текста должна совпадать с длиной ключа?

Если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то появится неоднозначность декодирования.

5.Какая операция используется в режиме однократного гаммирования, назовите её особенности?

Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение

6.Как по открытому тексту и ключу получить шифротекст?

В таком случае задача сводится к правилу: $Ci = Pi \oplus Ki$, т.е. мы поэлементно получаем символы зашифрованного сообщения, применяя операцию исключающего или к соответствующим элементам ключа и открытого текста.

7.Как по открытому тексту и шифротексту получить ключ? Подобная задача решается путем применения операции исключающего или к последовательностям символов зашифрованного и открытого сообщений: $Ki = Pi \oplus Ci$.

8.В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра:

1)полная случайность ключа;

2)равенство длин ключа и открытого текста;

3)однократное использование ключа.

Выводы

В ходе выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования.

Список литературы

1.Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №7.