Цель работы

Изучение алгоритма шифрования гаммированием

Теоретические сведения

Шифр гаммирования

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные.
Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

Метод гаммирования с обратной связью заключается в том, что для получения сегмента гаммы используется контрольная сумма определенного участка шифруемых данных. Например, если рассматривать гамму шифра как объединение непересекающихся множеств H(j), то процесс шифрования можно пердставить следующими шагами:

1. Генерация сегмента гаммы H(1) и наложение его на соответствующий участок шифруемых данных.
2. Подсчет контрольной суммы участка, соответствующего сегменту гаммы H(1).
3. Генерация с учетом контрольной суммы уже зашифрованного участка данных следующего сегмента гамм H(2).
4. Подсчет контрольной суммы участка данных, соответствующего сегменту данных H(2) и т.д.

Выполнение работы

Реализация шифратора и дешифратора Python

```
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)
```

Контрольный пример

```
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:  жбчцНСРяиТЙЖЯ7ЗЪЗ
Расшифрованный текст СНовымГодомДрузья
```

Выводы

Изучили алгоритмы шифрования на основе гаммирования

Список литературы

- Лабораторная работа №7