Отчёт по лабораторной работе №7

Шифр гаммирования

Турсунов Баходурхон Азимджонович

Содержание

List of Figures

1 Цель работы

Изучение алгоритма шифрования гаммированием

2 Теоретические сведения

2.1 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.

3 Выполнение работы

3.1 Реализация шифратора и дешифратора Python

```
def main():
        dict = {"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
            }

        dict2 = {v : k for k, v in dict.items()}
        gamma = input("Введите текст гаммы ")
        text = input("Введите текст для шифровки").lower()

        listoddigitsoftext = list()
        listoddigitsofgamma = list()

        for i in text:
            listoddigitsoftext.append(dict[i])
        print("Числа текста", listoddigitsoftext)

        for i in gamma:
            listoddigitsofgamma.append(dict[i])
        print("Числа гаммы", listoddigitsofgamma)

        listoddigitresult = list()

        ch = 0
        for i in text:
            try:
                a = dict[i] + listoddigitsofgamma[ch]
            except:
                ch = 0
                a = dict[i] + listoddigitsofgamma[ch]
            if a>33:
                a = a%33
            ch+=1
            listoddigitresult.append(a)

            print("Числа шифротекста", listoddigitresult)
```

Figure 3.1: code

```
print("Числа шифротекста", listoddigitresult)

textencrypted=""
for i in listoddigitresult:
    textencrypted+=dict2[i]

print("шифротекст ", textencrypted)

listofdigits = list()

for i in textencrypted:
    listofdigits.append(dict[i])
ch = 0
listofdigits1 = list()

for i in listofdigits:
    a = i - listoddigitsofgamma[ch]
    if a < 1:
        a = 33 + a
    listofdigits1.append(a)
    ch+=1

textdecrypted = ""

for i in listofdigits1:
    textdecrypted+=dict2[i]

print("рассшифровка", textdecrypted)
```

Figure 3.2: code

3.2 Контрольный пример

```
Ввод [5]: main()

Введите текст гаммы альмалинукс
Введите текст для шифровкиальмалинукс
Числа текста [1, 13, 30, 14, 1, 13, 10, 15, 21, 12, 19]
Числа гаммы [1, 13, 30, 14, 1, 13, 10, 15, 21, 12, 19]
Числа шифротекста [2]
шифротекст  б
рассшифровка а
Числа шифротекста [2, 26]
шифротекст  бш
рассшифровка ал
Числа шифротекста [2, 26, 27]
шифротекст  бшщ
рассшифровка аль
Числа шифротекста [2, 26, 27, 28]
шифротекст  бшщь
рассшифровка альм
Числа шифротекста [2, 26, 27, 28, 2]
шифротекст  бшщьб
рассшифровка альма
Числа шифротекста [2, 26, 27, 28, 2, 26]
шифротекст  бшщьбш
рассшифровка альмал
Числа шифротекста [2, 26, 27, 28, 2, 26, 20]
шифротекст  бшщьбшт
рассшифровка альмали
Числа шифротекста [2, 26, 27, 28, 2, 26, 20, 30]
шифротекст  бшщьбшть
рассшифровка альмалин
Числа шифротекста [2, 26, 27, 28, 2, 26, 20, 30, 9]
шифротекст  бшщьбштьз
рассшифровка альмалину
Числа шифротекста [2, 26, 27, 28, 2, 26, 20, 30, 9, 24]
шифротекст  бшщьбштьзц
рассшифровка альмалинук
Числа шифротекста [2, 26, 27, 28, 2, 26, 20, 30, 9, 24, 5]
шифротекст  бшщьбштьзцд
рассшифровка альмалинукс
```

Figure 3.3: Работа алгоритма гаммирования

4 Выводы

Изучили алгоритмы шифрования на основе гаммирования

Список литературы

1. Шифрование методом гаммирования
2. Режим гаммирования в блочном алгоритме шифрования