

Отчёт по лабораторной работе №7

Шифр гаммирования

Кан Ир-сен Сергеевич НПИ-бд-01-19

Содержание

1	Цель работы	4
2	Теоретические сведения	5
2.1	Шифр гаммирования	5
3	Выполнение работы	7
3.1	Реализация шифратора и дешифратора Python	7
3.2	Контрольный пример	9
4	Выводы	10
	Список литературы	11

List of Figures

3.1	Работа алгоритма гаммирования	9
-----	---	---

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 представить 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 = {"a" :1, "б" :2 , "в" :3 , "г" :4 , "д" :5 , "е" :6 , "ё" :7 , "ж": 8, "з":
           "м": 14, "н": 15, "о": 16, "п": 17, "р": 18, "с": 19, "т": 20, "у": 2
           "ш": 26, "щ": 27, "ъ": 28, "ы": 29, "ь": 30, "э": 31, "ю": 32, "я": 3

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

    digits_text = list()
    digits_gamma = list()

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

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

```

digits_result = list()

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

print("Числа шифровки:", digits_result)

text_encr=""
for i in digits_result:
    text_encr+=dict2[i]

print("шифровка:",text_encr)

digits_decr = list()

for i in text_encr:
    digits_decr.append(dict[i])
ch = 0
digits_decr1 = list()

```



```

for i in digits_decr:
    a = i - digits_gamma[ch]
    if a < 1:
        a = 33+a
    digits_decr1.append(a)
    ch=ch+1

text_decr = ""
for i in digits_decr1:
    text_decr+=dict2[i]

print("расшифровка:", text_decr)

```

3.2 Контрольный пример

```

In [2]: main()
Введите текст гаммыпроверка
Введите текст для кодированияпроверка
Числа текста [17, 18, 16, 3, 6, 18, 12, 1]
Числа гаммы [17, 18, 16, 3, 6, 18, 12, 1]
Числа шифра [1]
Шифр а
Раскодированный текст п
Числа шифра [1, 3]
Шифр ав
Раскодированный текст пр
Числа шифра [1, 3, 32]
Шифр авя
Раскодированный текст про
Числа шифра [1, 3, 32, 6]
Шифр авяе
Раскодированный текст пров
Числа шифра [1, 3, 32, 6, 12]
Шифр авяек
Раскодированный текст прове
Числа шифра [1, 3, 32, 6, 12, 3]
Шифр авяекв
Раскодированный текст провер
Числа шифра [1, 3, 32, 6, 12, 3, 24]
Шифр авяеквц
Раскодированный текст проверк
Числа шифра [1, 3, 32, 6, 12, 3, 24, 2]
Шифр авяеквцб
Раскодированный текст проверка

```

Figure 3.1: Работа алгоритма гаммирования

4 Выводы

Изучили алгоритмы шифрования на основе гаммирования

Список литературы

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