Отчёт по лабораторной работе №3

Шифр гаммирования

Логинов Сергей НФИмд 01-22

Содержание

[Цель работы 1](#_Toc116487478)

[Теоретические сведения 1](#_Toc116487479)

[Шифр гаммирования 1](#_Toc116487480)

[Выполнение работы 2](#_Toc116487481)

[Шифрование 2](#_Toc116487482)

[Результат выполнения 3](#_Toc116487483)

[Дешифровка 3](#_Toc116487484)

[Результат выполнения 3](#_Toc116487485)

[Выводы 3](#_Toc116487486)

[Список литературы 3](#_Toc116487487)

# 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:

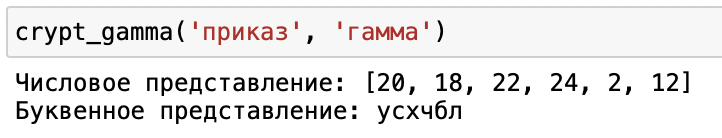
1. Генерация сегмента гаммы H(1) и наложение его на соответствующий участок шифруемых данных.
2. Подсчет контрольной суммы участка, соответствующего сегменту гаммы H(1).
3. Генерация с учетом контрольной суммы уже зашифрованного участка данных следующего сегмента гамм H(2).
4. Подсчет контрольной суммы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

# Выполнение работы

## Шифрование

# задаем алфавит  
alph = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'  
# создаем словари формата число-буква и буква-число  
dict = {}  
for i in range(1, 33):  
 dict[i] = alph[i - 1]  
dict1 = {v: k for k, v in dict.items()}  
# меняем местами для удобства  
dict, dict1 = dict1, dict  
  
# функция шифрования  
def crypt\_gamma(word, key):  
 a = []  
 for i in range(len(word)):  
 try:  
 a.append(dict[word[i]] + dict[key[i]])  
 except:  
 a.append(dict[word[i]] + dict[key[i % len(key)]])  
 print('Числовое представление:', a)  
 crypto = ''  
 for i in a:  
 crypto += dict1[i]  
 print('Буквенное представление:', crypto)  
  
crypt\_gamma('приказ', 'гамма')

### Результат выполнения

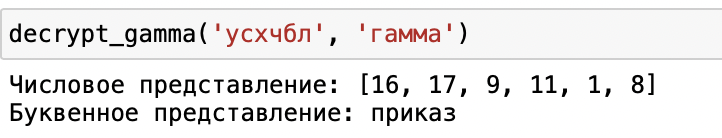


Шифровка гаммированием

## Дешифровка

# функция дешифровки  
def decrypt\_gamma(crypto, key):  
 a = []  
 for i in range(len(word)):  
 try:  
 a.append(dict[word[i]] - dict[key[i]])  
 except:  
 a.append(dict[word[i]] - dict[key[i % len(key)]])  
 print('Числовое представление:', a)  
 crypto = ''  
 for i in a:  
 crypto += dict1[i]  
 print('Буквенное представление:', crypto)  
  
decrypt\_gamma('усхчбл', 'гамма')

### Результат выполнения



Дешифровка

# Выводы

Изучили алгоритмы шифрования на основе гаммирования

# Список литературы

1. [Шифрование методом гаммирования](http://altaev-aa.narod.ru/security/XOR.html)
2. [Режим гаммирования в блочном алгоритме шифрования](https://kabinfo.ucoz.ru/index/shifr_reshetka_kardano/0-374)