Отчёт по лабораторной работе №7

Шифр гаммирования

Миша Нкого Хосе Адольфо Мба НФИбд-02-19

Содержание

# 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 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

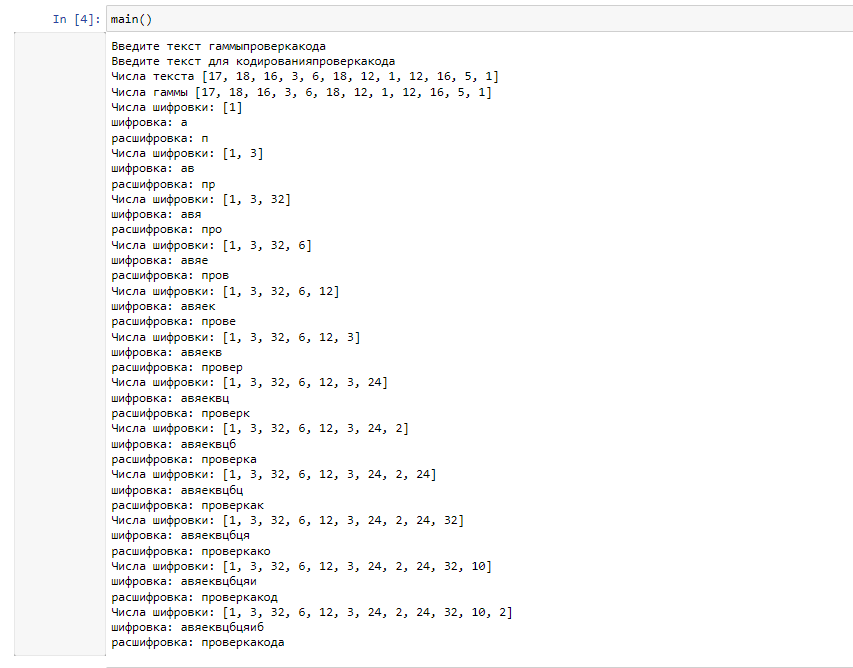


Figure 1: Работа алгоритма гаммирования

# 4 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)