Информационная безопасность. Лабораторная работа #7.

Элементы криптографии. Однократное гаммирование

Хохлачева Яна

Содержание

# Цель работы

* Освоить на практике применение режима однократного гаммирования.

# Программа шифровки и дешифровки

## Функция шифрования

import numpy as np  
import operator as op  
import sys  
  
sms = "С Новым Годом, друзья!"  
  
def encryption(text):  
 print("Открытый текст: ",text)  
 new\_text = []  
 for i in text:  
 new\_text.append(i.encode("cp1251").hex())  
 print("\nОткрытый текст в 16-ой системе: ", new\_text)  
   
 r = np.random.randint(0, 255, len(text))  
 key = [hex(i)[2:] for i in r]  
 new\_key = []  
 for i in key:  
 new\_key.append(i.encode("cp1251").hex().upper())  
 print("\nКлюч в 16-ой системе: ", key)  
   
 xor\_text = []  
 for i in range(len(new\_text)):  
 xor\_text.append("{:02x}".format(int(key[i], 16) ^ int(new\_text[i], 16)))  
 print("\nШифротекст в 16-ой системе: ", xor\_text)  
   
 en\_text = bytearray.fromhex("".join(xor\_text)).decode("cp1251")  
 print("\nШифротекст: ", en\_text)  
 return key,xor\_text, en\_text  
   
k, t, et = encryption(sms)

## Результат выполнения функции шифрования

Открытый текст в 16-ой системе: ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20',  
 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']  
  
Ключ в 16-ой системе: ['58', 'a5', '6f', '1e', 'e0', '2c', 'db', '44', '74', '6b',  
 '88', 'e', '52', 'db', '86', 'b0', '85', '33', 'd1', '44', '7d', '9d']  
  
Шифротекст в 16-ой системе: ['89', '85', 'a2', 'f0', '02', 'd7', '37', '64', 'b7',  
 '85', '6c', 'e0', 'be', 'f7', 'a6', '54', '75', 'c0', '36', 'b8', '82', 'bc']  
  
Шифротекст: ‰…ўрSTXЧ7d·…lаѕч¦TuА6ё‚ј

## Функция декодирования

def find\_key(text, en\_text):  
 print("Открытый текст: ",text)  
 print("\nШифротекст: ", en\_text)  
   
 new\_text = []  
 for i in text:  
 new\_text.append(i.encode("cp1251").hex())  
 print("\nОткрытый текст в 16-ой системе:", new\_text)  
   
 tmp\_text = []  
 for i in en\_text:  
 tmp\_text.append(i.encode("cp1251").hex())  
 print("\nШифротекст текст в 16-ой системе", tmp\_text)  
   
 xor\_text = [hex(int(k,16)^int(t,16))[2:] for (k,t) in zip(new\_text, tmp\_text)]  
 print("\nНайденный ключ в 16-ой системе: ", xor\_text)  
 return xor\_text  
   
key = find\_key(sms, et)

## Результат функции декодирования

Открытый текст: С Новым Годом, друзья!  
  
Шифротекст: ‰…ўрSTXЧ7d·…lаѕч¦TuА6ё‚ј  
  
Открытый текст в 16-ой системе: ['d1', '20', 'cd', 'ee', 'e2',  
 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4',  
 'f0', 'f3', 'e7', 'fc', 'ff', '21']  
  
Шифротекст текст в 16-ой системе ['89', '85', 'a2', 'f0', '02',  
 'd7', '37', '64', 'b7', '85', '6c', 'e0', 'be', 'f7', 'a6', '54',  
 '75', 'c0', '36', 'b8', '82', 'bc']  
  
Найденный ключ в 16-ой системе: ['58', 'a5', '6f', '1e', 'e0', '2c',  
 'db', '44', '74', '6b', '88', 'e', '52', 'db', '86', 'b0', '85', '33',  
 'd1', '44', '7d', '9d']

## Результат проверки

if k == key:  
 print("Ключ найден")  
else:  
 print("Н")

Ключ найден

# Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование – выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

1. Перечислите недостатки однократного гаммирования.

Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

1. Перечислите преимущества однократного гаммирования.

* Такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
* шифрование и расшифрование может быть выполнено одной и той же программой.
* Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

1. Почему длина открытого текста должна совпадать с длиной ключа?

Если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то появится неоднозначность декодирования.

1. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение

1. Как по открытому тексту и ключу получить шифротекст?

т.е. мы поэлементно получаем символы зашифрованного сообщения, применяя операцию исключающего или к соответствующим элементам ключа и открытого текста.

1. Как по открытому тексту и шифротексту получить ключ?

Подобная задача решается путем применения операции исключающего или к последовательностям символов зашифрованного и открытого сообщений:

1. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

Необходимые и достаточные условия абсолютной стойкости шифра:

* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа.

# Вывод

* Освоила на практике применение режима однократного гаммирования.