Лабораторная работа №8

Титаренко Анастасия Дмитриевна

Содержание

Цель работы	1
ь. Выполнение лабораторной работы	
Вывод	
Список литературы	

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты Р1 и Р2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов С1 и С2 обоих текстов Р1 и Р2 при известном ключе. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

1. Используя язык Python написала программу. В качестве примера ввела 2 текста: 'ЖелтоеСолнце', 'ГолубыеОблака'

```
import random as rnd
import string as str
# Создание ключа
def create_key(size=6, chars=str.ascii_letters + str.digits):
    return ''.join(rnd.choice(chars) for _ in range(size))
# Перевод ключа в шестнадцатиричную форму
def hexadical_form(s):
    return ''.join("{:02x}".format(ord(c)) for c in s)
# Гаммирование
def gamming(fst_text, sec_text):
   fst_text_ascii = [ord(i) for i in fst_text]
    sec_text_ascii = [ord(i) for i in sec_text]
    return ''.join(chr(s^k) for s,k in zip(fst_text_ascii,sec_text_ascii))
# Выполним шифрование
Р1, Р2 = 'ЖелтоеСолнце', 'ГолубыеОблака'
print('Исходные тексты:')
print(P1)
print(P2)
key = create_key(len(P1))
print('\nKлюч для кодирования текстов:', create_key(len(P1)))
print('Шестнадцатиричный ключ для кодирования текстов:', hexadical_form(key))
print('\nШифротекст для открытого текста 1 и ключа:', gamming(P1, key))
print('Шифротекст для открытого текста 2 и ключа:', gamming(P2, key))
print('\nПолучим тексты путём гаммирования двух шифровок и исходного текста:')
print(gamming(gamming(P1, key) + gamming(P2, key), P1))
print(gamming(gamming(P1, key) + gamming(P2, key), P2))
```

Листинг программы

2. Результат выполнения программы

```
Исходные тексты:

ЖелтоеСолнце

ГолубыеОблака

Ключ для кодирования текстов: ZpHliAYgpY19

Шестнадцатиричный ключ для кодирования текстов: 6b6c3067744a46696c686532

Шифротекст для открытого текста 1 и ключа: ѽъЋХъѿѧїїѕУЇ

Шифротекст для открытого текста 2 и ключа: ŊђЋФхЁөѷѝѓѕЈ

Получим тексты путём гаммирования двух шифровок и исходного текста:

kl0gtJFilhe2

ng0f{4RIfn⊡=H
```

Вывод программы

Вывод

Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

1. Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом