Отчёт по лабораторной работе №8

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

# 2 Выполнение лабораторной работы

Постановка задания: 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 P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Создаем функцию, генерирующую ключ из ascii-символов и цифр, и функцию, кодирующую исходный текст по ключу. На вход функция принимает текст и ключ. Переводит ключ в 16-ричную ИС, далее использует XOR, переводит из 16-ричной ИС. Возвращает шифротекст.

import random  
import string  
  
  
def generate\_key(length: int):  
 return random.sample(string.ascii\_letters + string.digits, length)  
  
  
def encrypt(text: str, key: list = None):  
 if not key:  
 key = generate\_key(length=len(text))  
  
 text\_16 = [ord(char) for char in text]   
 key = [ord(el) for el in key]  
  
 print(f"Ключ шифрования:", ' '.join(str(s) for s in key))  
 print(f"Исходный текст:", text)  
  
 encrypted\_text = []  
 for i in range(len(text)):  
 encrypted\_text.append(text\_16[i] ^ key[i])  
  
 ciphertext = ''.join([chr(i) for i in encrypted\_text])  
 print(f'Шифротекст: {ciphertext}\n\n')  
  
 return ciphertext

Задаем два текста. Генерируем ключ. Зашифровываем оба текста по одному ключу. Зашифровываем первый шифротекст по второму шифротексту. Используем один из текстов в качестве ключа дешифровки.

p1 = 'НаВашисходящийот1204'  
p2 = 'ВСеверныйфилиалБанка'  
key = generate\_key(20)  
  
c1 = encrypt(p1, key=key)  
c2 = encrypt(p2, key=key)  
  
c1\_c2 = encrypt(c1, key=c2)  
  
encrypt(c1\_c2, p1)  
encrypt(c1\_c2, p2)

Компилируем программу (рис. 1).

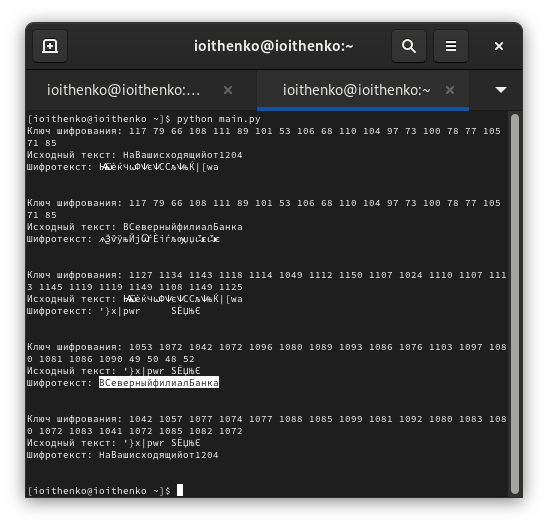


Рис. 1: Вывод программы

# 3 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа? Нужно применить XOR для двух шифротекстов, а к полученному результату применить XOR с ключом, равным известному открытому тексту. Тогда результатом будет второй открытый текст
2. Что будет при повторном использовании ключа при шифровании текста? Шифрование будет небезопасным, т.к. с помощью шифротекстов и одного открытого текста можно дешифровать другой текст
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? Каждый текст шифруется однократным гаммированием отдельно с использованием этого ключа
4. Перечислите недостатки шифрования одним ключом двух открытых текстов Главный недостаток - можно дешифровать открытый текст без знания ключа.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов. Т.к. ключей используется меньше, то тратится меньше памяти на хранение и передачу ключей.

# 4 Выводы

В ходе выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.