Лабораторная работа No 6.

Тагиев Байрам Алтай оглы

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Выполнение лабораторной работы

1. Напишем функцию для генерации случайной последовательности, которая будет являться нашим ключем.

import random  
  
def generate\_key\_hex(word):  
 key = ""  
 for \_ in range(len(word)):  
 key += random.choice("0123456789abcdef")  
 return key

1. Также сделаем функцию шифрования. В основе используется XOR (бинарное ИЛИ НЕТ).

def encrypt(plaintext, key):  
 ciphertext = ""  
 for i in range(len(plaintext)):  
 char = plaintext[i]  
 key\_char = key[i % len(key)]  
 encrypted\_char = chr(ord(char) ^ ord(key\_char))  
 ciphertext += encrypted\_char  
 return ciphertext

1. Аналогичный принцип стоит за дешифрованием (XOR).

def decrypt(ciphertext, key):  
 decrypted\_text = ""  
 for i in range(len(ciphertext)):  
 char = ciphertext[i]  
 key\_char = key[i % len(key)]  
 decrypted\_char = chr(ord(char) ^ ord(key\_char))  
 decrypted\_text += decrypted\_char  
 return decrypted\_text

1. А также функция нахождения возможного ключа.

def find\_possible\_key(ciphertext, fragment):  
 possible\_keys = []  
 for i in range(len(ciphertext) - len(fragment) + 1):  
 possible\_key = ""  
 for j in range(len(fragment)):  
 char = ciphertext[i + j]  
 fragment\_char = fragment[j]  
 key\_char = chr(ord(char) ^ ord(fragment\_char))  
 possible\_key += key\_char  
 possible\_keys.append(possible\_key)  
 return possible\_keys

1. После запуска программы мы получим следующее.

Ключ: dc924107ba191baa4710c3  
Зашифрованный текст: хCФЌІѺЌѱџЅЇЍNAѕѴѴІѼЬ  
Дешифрованный текст: С Новым Годом, друзья!  
Возможные ключи: ['dc92410', 'ѢЄ\x118HGЫ',

# 3 Выводы

По мере выполнения лабораторной работы были выполнены все цели.