Лабораторная работа № 3

Дисциплина: Информационная безопасность

Новосельцев Данила Сергеевич

Содержание

# 1 Цель работы

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

# 2 Код программы

import random  
import string  
  
class TextEncoding:  
  
 @staticmethod  
 def determine\_alphabet(text):  
 if text[0] in string.ascii\_lowercase:  
 return string.ascii\_lowercase + string.digits  
 else:  
 return "абвгдеёжзийклмнопрстуфхцчшщъыьэюя" + string.digits  
  
 @staticmethod  
 def generate\_key(size, alphabet):  
 return "".join(random.choice(alphabet) for \_ in range(size))  
  
 @staticmethod  
 def to\_hex(coding):  
 return " ".join(hex(ord(character))[2:] for character in coding)  
  
 @staticmethod  
 def encode\_string(text, key):  
 return "".join(chr(ord(char) ^ ord(key\_char)) for char, key\_char in zip(text, key))  
  
 @staticmethod  
 def xor\_texts(ciphertext1, ciphertext2):  
 return "".join(chr(ord(char1) ^ ord(char2)) for char1, char2 in zip(ciphertext1, ciphertext2))  
  
  
plaintext1 = input("Введите первый открытый текст: ")  
plaintext2 = input("Введите второй открытый текст: ")  
alphabet = TextEncoding.determine\_alphabet(plaintext1)  
key = TextEncoding.generate\_key(len(plaintext1), alphabet)  
  
print(f"Ключ: {key}", f"Ключ в 16 бит: {TextEncoding.to\_hex(key)}", sep='\n')  
  
ciphertext1 = TextEncoding.encode\_string(plaintext1, key)  
ciphertext2 = TextEncoding.encode\_string(plaintext2, key)  
print(f"Первый зашифрованный текст: {ciphertext1}", f"Первый зашифрованный текст в 16 бит: {TextEncoding.to\_hex(ciphertext1)}",  
 sep='\n')  
print(f"Второй зашифрованный текст: {ciphertext2}", f"Второй зашифрованный текст в 16 бит: {TextEncoding.to\_hex(ciphertext2)}",  
 sep='\n')  
  
decrypted\_text1 = TextEncoding.encode\_string(ciphertext1, key)  
decrypted\_text2 = TextEncoding.encode\_string(ciphertext2, key)  
print("Первый расшифрованный текст:", decrypted\_text1)  
print("Второй расшифрованный текст:", decrypted\_text2)  
  
xor\_result = TextEncoding.xor\_texts(ciphertext1, ciphertext2)  
print("Результат XOR двух зашифрованных текстов:", xor\_result)

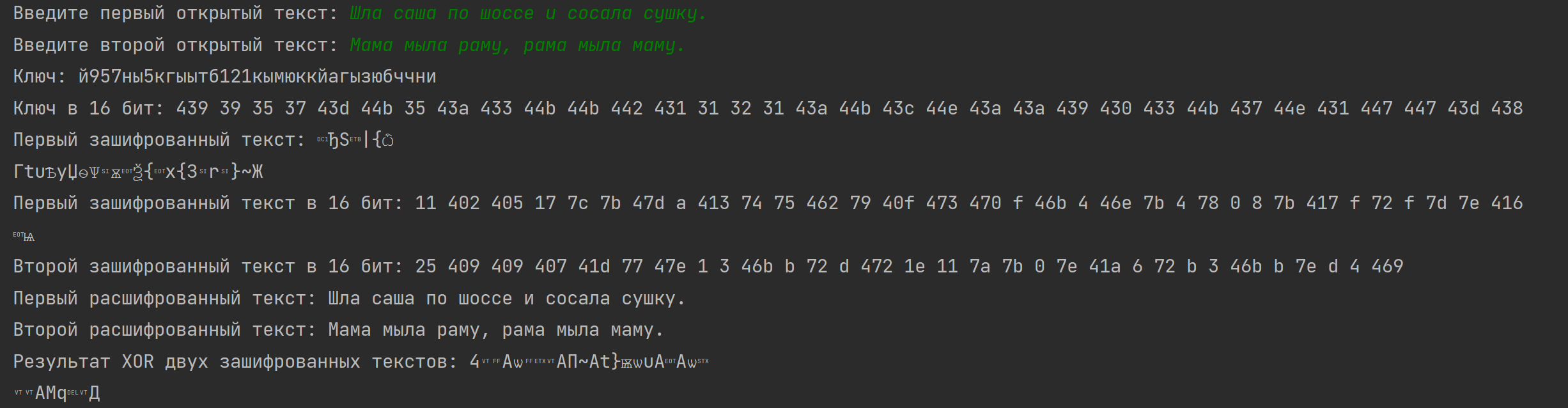


Рис. 1: Вывод программы для текста на русском

# 3 Вывод

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