Лабораторная работа № 3

Дисциплина: Информационная безопасность

Новосельцев Данила Сергеевич

Содержание

Список иллюстраций

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(t

    @staticmethod
    def xor_texts(ciphertext1, ciphertext2):
        return "".join(chr(ord(char1) ^ ord(char2)) for char1, char2 in zip(ciphe


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
      sep='\n')
print(f"Второй зашифрованный текст: {ciphertext2}", f"Второй зашифрованный текст
      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)
```

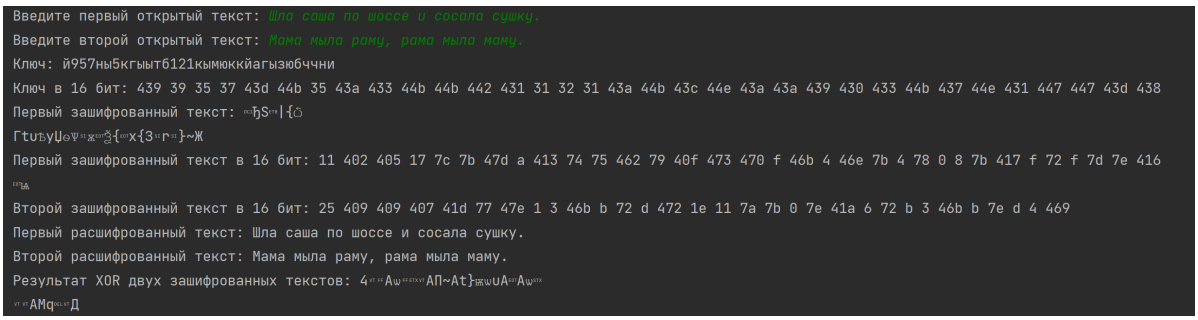

Рис. 2.1: Вывод программы для текста на русском

3 Вывод

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