

Лабораторная работа № 3

Дисциплина: Информационная безопасность

Новосельцев Данила Сергеевич

Содержание

1	Цель работы	4
2	Код программы	5
3	Вывод	8

Список иллюстраций

2.1	Вывод программы для текста на русском	7
-----	---	---

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)

```

```

Введите первый открытый текст: Шла саша по шоссе и сосала сушку.
Введите второй открытый текст: Мама мыла раму, рама мыла маму.
Ключ: й957ны5кгыт6121кымюкйагызюбччнн
Ключ в 16 бит: 439 39 35 37 43d 44b 35 43a 433 44b 44b 442 431 31 32 31 43a 44b 43c 44e 43a 43a 439 430 433 44b 437 44e 431 447 447 43d 438
Первый зашифрованный текст: "hS"|{
ГтуЪUеΨ"ж"3{x{3"г"~Ж
Первый зашифрованный текст в 16 бит: 11 402 405 17 7c 7b 47d а 413 74 75 462 79 40f 473 470 f 46b 4 46e 7b 4 78 0 8 7b 417 f 72 f 7d 7e 416
"за
Второй зашифрованный текст в 16 бит: 25 409 409 407 41d 77 47e 1 3 46b b 72 d 472 1e 11 7a 7b 0 7e 41a 6 72 b 3 46b b 7e d 4 469
Первый расшифрованный текст: Шла саша по шоссе и сосала сушку.
Второй расшифрованный текст: Мама мыла раму, рама мыла маму.
Результат XOR двух зашифрованных текстов: 4"~"Аш"~"АП~At}жжUA~Аш"~
"~"Анq~"Д

```

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.