Лабораторная работа No 7.

Тагиев Б. А.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить на практике применение режима однократного гаммирования.

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
```

2. 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
```

3. 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
```

4. 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
```

5. После запуска программы мы получим следующее.

```
Ключ: dc924107ba191baa4710c3
Зашифрованный текст: xCФЌI?ЌψџSЇЙNAsVVI?Ь
Дешифрованный текст: С Новым Годом, друзья!
Возможные ключи: ['dc92410', 'ЂЄ\x118HGЫ',
```

Выводы

По мере выполнения лабораторной работы были выполнены все цели.