Лабораторная работа № 7

Новосельцев Данила Сергеевич

2023, Москва

Цель работы

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

Код программы

```
import random
import string

class TextEncoding:
```

Код программы

```
@staticmethod
def determine_alphabet(text):
    if text[0] in string.ascii_lowercase:
        return string.ascii_lowercase + string.digits
    else:
        return "абвгдеёжзийклмнопрстуфхцчшщъыьэюя" + string.digits
```

Код программы

```
@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)
```

Код программы

```
@staticmethod
def encode_string(text, key):
    return "".join(chr(ord(char) ^ ord(key_char)) for char, key_char in z
```

Код программы

```
@staticmethod
def find_possible_keys(text, fragment):
    key_length = len(fragment)
    possible_keys = []

    for index in range(len(text) - key_length + 1):
        key = [chr(ord(char) ^ ord(key_char)) for char, key_char in zip(t
        presumed_plaintext = TextEncoding.encode_string(text, key)

        if fragment in presumed_plaintext:
            possible_keys.append(''.join(key))

    return possible_keys
```

Код программы

```
plaintext = input("Введите открытый текст: ")
alphabet = TextEncoding.determine_alphabet(plaintext)
key = TextEncoding.generate_key(len(plaintext), alphabet)

print(f"Ключ: {key}", f"Ключ в 16 бит: {TextEncoding.to_hex(key)}", sep='\n')
```

Код программы

```
ciphertext = TextEncoding.encode_string(plaintext, key)
print(f"Зашифрованный текст: {ciphertext}", f"Зашифрованный текст в 16 бит: {
      sep='\n')
```

```
decrypted_text = TextEncoding.encode_string(ciphertext, key)
print("Расшифрованный текст:", decrypted_text)
```

Код программы

```
known_fragment = input("Введите фрагмент открытого текста: ")
possible_keys = TextEncoding.find_possible_keys(ciphertext, known_fragment)
print("Возможные ключи для шифротекста:", possible_keys)
```

Вывод программы

```
Введите открытый текст: С Новым Годом, друзья!
Ключ: 7ъэ0ю7амшсрувяз7з4чпсф
Ключ в 16 бит: 37 44a 44d 30 44e 37 430 43c 448 441 440 443 432 44f 437 37 437 34 447 43f 441 444
Зашифрованный текст: ЖРЎ|M[t}Ѣ3ЃwpsЄ
Зашифрованный текст в 16 бит: 416 46a 50 40e 7c 47c c 41c 5b 7f 74 7d e 463 417 403 77 477 70 73 e
Расшифрованный текст: С Новым Годом, друзья!
Введите фрагмент открытого текста: Новым
Возможные ключи для шифротекста: ['\x0bTЪEp']
```

Рис. 1: Вывод программы для текста на русском

Вывод

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