

Отчет по лабораторной работе №7

Valery A. Dinkiev¹

11 December 2021 Moscow, Russia

¹RUDN University, Moscow, Russian Federation

Цель выполнения работы

Освоить на практике применение режима однократного гаммирования.

Результаты выполненной работы

- Написал программу на языке программирования Python для выполнения данной лабораторной работы.

```
import string
import random

def generate_key(size, chars = string.ascii_letters + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))

def hex_form(input_string):
    return ''.join('{:02X}'.format(ord(a)) for a in input_string)

def gamming(input_string, key):
    key_list = [ord(k) for k in key]
    input_list = [ord(s) for s in input_string]
    return ''.join(chr(k ^ s) for k,s in zip(key_list,input_list))

def unencrypt(cipher_text, key):
    cipher_list = [ord(c) for c in cipher_text]
    key_list = [ord(k) for k in str(key)]
    return ''.join(chr(c ^ k) for c,k in zip(cipher_list, key_list))

def open_text(cipher_text,input_string):
    input_list = [ord(i) for i in input_string]
    cipher_list = [ord(c) for c in cipher_text]
    return ''.join(chr(c ^ i) for c,i in zip(cipher_list,input_list))
```

Figure 1: Функции

```
input_string = input("Введите строку: \n")
gen_key = generate_key(len(input_string))
hex_key = hex_form(gen_key)
print(f"Полученный ключ: {gen_key}")
print(f"16-ная форма ключа: {hex_key}")

encrypted_string = gamming(input_string, gen_key)

new_key = generate_key(len(encrypted_string))
unencrypted_key = unencrypt(encrypted_string, new_key)
input_key = open_text(encrypted_string, input_string)
unencrypted_input_key = unencrypt(encrypted_string, input_key)
```

Введите строку:
С Новым Годом, друзья!
Полученный ключ: Fa5lXWsjJaX355UeljtNYbb
16-ная форма ключа: 466153317857736A615833355355656C6A744E596262

Figure 2: Переменные

```
print(f"Полученный шифрованный текст: {encrypted_string}")  
print(f"16-ная форма: {hex_form(encrypted_string)}")
```

Полученный шифрованный текст: AAdUyMaJbAIfyEjbaqE9C
16-ная форма: 4674144E40F44A41C44F4A47246640740B46F794545842A43747941542D43

Figure 3: 1 задание


```
print(f"Новый ключ: {new_key}")  
print(f"Незашифрованный ключ: {unencrypted_key}")  
print(f"Исходный ключ: {input_key}")  
print(f"Расшифрованный текст: {unencrypted_input_key}")
```

Новый ключ: vPxVxnbXyUtoHqJ03NHTYv
Незашифрованный ключ: БжэввВгёкЗЙгбсV5
Исходный ключ: FaS1xWsjaX35Sue1jtNYbb
Расшифрованный текст: С Новым Годом, друзья!

Figure 4: 2 задание

Выводы по работе

Освоил на практике применение режима однократного гаммирования.

Спасибо за внимание!