

Отчет по лабораторной работе 8

Дисциплина: Информационная безопасность

Савченков Дмитрий Андреевич, НПИбд-02-18

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	8
	Список литературы	9

List of Figures

2.1	Функции	6
2.2	Переменные	7
2.3	Вывод программы	7

List of Tables

1 Цель работы

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

2 Выполнение лабораторной работы

1. Для выполнения данной лабораторной работы использовал язык программирования Python. Написал функции для последующей работы. (рис. -fig. 2.1)

- Функция `generate_key` берет на вход размер строки (`size`) в виде целового числа и строку символов с помощью которых мы будем генерировать ключ (в нашем случае мы будем использовать буквы английского алфавита и числа). А возвращает сгенерированный ключ в строковом формате (`string`).
- Функция `hex_form` берет на вход строку и возвращает её 16-ный вид данной строки.
- Функция `gamming` берет на вход строку и сгенерированный ключ. А возвращает зашифрованную строку методом однократного гаммирования.

```
import random
import string

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(text, key):
    text_list = [ord(t) for t in text]
    key_list = [ord(k) for k in key]
    return ''.join(chr(t ^ k) for t,k in zip(text_list, key_list))
```

Figure 2.1: Функции

2. Использовал функции выше для определения новых переменных для дальнейшей работы. (рис. -fig. 2.2)

- Переменная P_1 - это исходная строка (телеграмма) из лабораторной работы “НаВашисходящийот1204”
- Переменная P_2 - это исходная строка (телеграмма) из лабораторной работы “ВСеверныйфилиалБанка”
- Переменная gen_key - это сгенерированный ключ, который мы получили из функции generate_key.
- Переменная hex_key - это 16-ная форма сгенерированного ключа.
- Переменная C_1 - это шифротекст для первой телеграммы P_1.
- Переменная C_2 - это шифротекст для второй телеграммы P_2.
- Переменная sum_C - это сумма шифротекстов по модулю 2.

```
P_1 = "НаВашисходящийот1204"
P_2 = "ВСеверныйфилиалБанка"
print(f"Source data: {P_1} {P_2}\n")

gen_key = generate_key(len(P_1))
hex_key = hex_form(gen_key)
print(f"Key: {gen_key}")
print(f"16_key: {hex_key}\n")

C_1 = gamming(P_1, gen_key)
C_2 = gamming(P_2, gen_key)
print(f"Ciphertext {C_1} for the 1-st telegram {P_1}")
print(f"Ciphertext {C_2} for the 2-nd telegram {P_2}\n")

sum_C = gamming(C_1, C_2)
print("The first text with the gamification of two ciphers and the second text.")
print(f"P_1: {gamming(sum_C, P_2)}\n")

print("The second text with the gamification of two ciphers and the first text.")
print(f"P_2: {gamming(sum_C, P_1)}")
```

Figure 2.2: Переменные

3. Давайте изучим вывод программы. Вначале выводятся исходные телеграммы, ключ и его 16-ная форма. Затем выводиться шифротекст для двух исходных телеграмм, которые получены с помощью этой формулы $C_{12} = P_{12} (+) K$. В конце нам выводятся уже исходные телеграммы, которые получены с помощью суммирования C_1 и C_2 по модулю 2 и исходных телеграмм. (рис. -fig. 2.3)

```
Source data: НаВашисходящийот1204 ВСеверныйфилиалБанка

Key: Pb1wKlK68DPFluZmTbK
16_key: 506231774B4E0B384450466C755A4D7754624B

Ciphertext зНУчГŸœIWŸЦєѲJfFR for the 1-st telegram НаВашисходящийот1204
Ciphertext тѲхŸŸiŸŸœŸœкѲкjo for the 2-nd telegram ВСеверныйфилиалБанка

The first text with the gamification of two ciphers and the second text.
P_1: НаВашисходящийот1204

The second text with the gamification of two ciphers and the first text.
P_2: ВСеверныйфилиалБанка
```

Figure 2.3: Вывод программы

3 Выводы

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

Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов