Отчет по лабораторной работе 8

Savchenkov Dmitriy Andreevich[1]

18 December, 2021 Moscow, Russian Federation

[1]RUDN University, Moscow, Russian Federation

Цель выполнения работы

Цель работы

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

Результаты выполненной работы

Результаты выполненной работы

- Написал программу на языке программирования Python для выполнения данной лабораторной работы.
- Зашифровал две телеграммы одним ключом с помощью шифрования однократного гаммирования. С помощью формул C1 = P1 (+) K, C2 = P2 (+) K.
- Вывел открытый текст, зная шифротекст двух телеграмм и сумму C_1 и C_2 по модулю 2. C1 (+) C2

Программа

```python
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 1: Функции

Программа

```
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: Переменные

```
Source data: НаВашисходящийот1204 ВСеверныйфилиалБанка

Key: Pb1wKNk68DPFluZMwTbK
16_key: 506231774B4E6B36384450466C755A4D7754624B

Ciphertext эђУчЃЎъѳІѰПЏєьЌЏFfR  for the 1-st telegram НаВашисходящийот1204
Ciphertext туЄхѾЎіὄЁЀӎὄєхѡќчѩјо 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 3: Вывод программы

Выводы по работе

Выводы

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

Спасибо за внимание!