Отчет по лабораторной работе №8

Valery A. Dinkiev[1]

17 December 2021 Moscow, Russia

[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

```
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"Исходные данные: {P_1} {P_2}")

gen_key = generate_key(len(P_1))
hex_key = hex_form(gen_key)

print(f"Ключ: {gen_key}")
print(f"16-ная форма ключа: {hex_key}\n")

C_1 = gamming(P_1,gen_key)
C_2 = gamming(P_2,gen_key)

print(f"Шифротекст {C_1} для первой телефеграммы {P_1}")
print(f"Шифротекст {C_2} для второй телеграммы {P_2}\n")

sum_C = gamming(C_1,C_2)
print("Первый текст путем гаммирования двух шифровок и второго текста")
print(f"P_1: {gamming(sum_C, P_2)}\n")

print("Второй текст путем гаммирования двух шифровок и первого текста")
print(f"P_2: {gamming(sum_C, P_1)}")
```

Figure 2: Переменные

Программа

```
Исходные данные: НаВашисходящийот1204 ВСеверныйфилиалБанка
Ключ: Suz9BPo69YuiXUZGC2jp
16-ная форма ключа: 53 75 7A 39 42 50 6F 36 39 59 75 69 58 55 5A 47 43 32 6A 70

Шифротекст љѠўѠбѰзљћѻЎКЋѪъиh⍰w[ для первой телефеграммы НаВашисходящийот1204
Шифротекст сєяђѶАђѽÈНэђѠкwіөЏѐр для второй телеграммы ВСеверныйфилиалБанка

Первый текст путем гаммирования двух шифровок и второго текста
P_1: НаВашисходящийот1204

Второй текст путем гаммирования двух шифровок и первого текста
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!