Лабораторная работа №8

Алибаева Данагуль [1]

2021 Moscow, Russia

[1]RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной работы

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

Задачи выполнения лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется, не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Результаты выполнения лабораторной работы

1. Успешное создание приложения.

```python
import random
import string
P1 = " НаВашисходящийот1204"
P2 = " ВСеверныйфилиалБанка"

def hex1(a):
    return ' '.join(hex(ord(i))[2:] for i in a)

def key1(lenn):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(lenn))

def gamming(first, second):
    first = [ord(i) for i in first]
    second = [ord(i) for i in second]
    return ''.join(chr (a^b) for a,b in zip(first, second))

key = key1(len(P1))
print("Ключ: ", key)
hex_key = hex1(key)
print("Шеснадцатиричный ключ: ", hex_key)
C1 = gamming(P1, key)
C2 = gamming(P2, key)
gamming2 = gamming(C1,C2)
print("Открый 1 текст: ", gamming(gamming2,P1))
print("Открый 2 текст: ", gamming(gamming2,P2))
print("Зашифрованное 1 послание: ", C1)
print("Зашифрованное 2 послание: ", C2)
```

```
Ключ:  y70Zts2kcnTksBzubtAH2
Шеснадцатиричный ключ:  79 37 30 5a 74 73 32 6b 63 6e 54 6b 73 42 7a 75 62 74 41 48 32
Открый 1 текст:   ВСеверныйфилиалБанка
Открый 2 текст:   НаВашисходящийот1204
Зашифрованное 1 послание:  YЪЁшфлЊЪЦёЏФkQуыPEsx
Зашифрованное 2 послание:  YXБ ццѲiШїAґшQъюефЎѲЂ
```

Figure 1: Разработка приложения

Вывод

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

Спасибо за внимание!