Шифр гаммирования

Савченко Елизавета НБИ-01-20

28 октября, 2023. Россия, Москва

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Алгоритм взлома

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K$$
$$C_2 = P_2 \oplus K$$

Алгоритм взлома

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Алгоритм взлома

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C_1 \oplus C_2$ (известен вид обеих шифровок). Тогда зная P_1 имеем:

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

Пример 1 работы программы

```
import string
import random

def hexx(text):
    return ' '.join(hex(ord(i))[2:] for i in text)
def gen_key(size):
    return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
def encrypted(firstText,secondText):
    first_text=[ord(i) for i in firstText]
    second_text=[ord(i) for i in secondText]
    return ''.join(chr (a^b) for a,b in zip(first_text,second_text))
```

Figure 1: алгоритм работы

Пример 2 работы программы

```
p1 = "Восходящийот1222"
p2 = "Верныйфайл"

key=gen_key(len(p1))
print(key)
hex_key=hexx(key)
print("Ключ в шестнадцатиричном виде: ",hex_key)

c1 = encrypted(p1,key)
c2 = encrypted(p2,key)

print("Зашифрованный текст: ",c1)
print("Зашифрованный текст: ",c2)

decrypt=encrypted(c1,c2)
print("Расшифрованный текст: ",encrypted(decrypt,p2) )
print("Расшифрованный текст: ",encrypted(decrypt,p1) )
```

```
xvjgKvcPPqZlCpkY
Ключ в шестнадцатиричном виде:  78 76 6a 67 4b 76 63 50 50 71 5a 6c 43 70 6b 59
Зашифрованный текст:  ЖшЫTvтЬЙИшЊЮrBYk
Зашифрованный текст:  ЖуЪњЁяЧЏмъ
Расшифрованный текст:  Восходящий
Расшифрованный текст:  Верныйфайл
```

Figure 2: алгоритм работы взлома ключа

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.