Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Ван И

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ван И
- студент НФИбд-02-20
- Российский университет дружбы народов
- 1032198069@pfur.ru
- https://github.com/WangYi157

Вводная часть

Объект и предмет исследования

- Атрибуты файлов
- Дистрибутив Rocky
- Дискреционное разграничение доступа

Цели

Освоить на практике применение режима однократного гаммирования

Импортируем необходимые модули (@fig:001).

Рис. 1: Импорт модулей

Выполнение работы

Создадим функции для преобразования данных в шестнадцатеричный формат, генерации ключа и кодирования, декодирования данных (@fig:002).

```
>>> def hex_text(text):
...     return " ".join(hex(ord(i))[2:] for i in text)
...
>>> def generate(size):
...     key = "".join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
...     return key
...
>>> def enc(text, key):
...     return "".join(chr(a^b) for a, b in zip(text, key))
```

Рис. 2: Функции

Закодируем и декодируем строку “С Новым годом, друзья!” (@fig:003).

```
>>> mess = "С Новым годом, друзья!"
>>> key = generate(len(mess))
>>> hex_key = hex_text(key)
>>>
>>> enc_text = enc([ord(i) for i in mess], [ord(i) for i in key])
>>> hex_text = hex_text(enc_text)
>>> decr_text = enc([ord(i) for i in enc_text], [ord(i) for i in key])
>>>
>>> print("Ключ: ", hex_key, "\nЗашифрованное сообщение: ", hex_text, "\nРасшифрованный текст: ", decr_text)
Ключ:  57 42 55 76 70 49 75 48 6c 72 34 6a 4e 59 71 64 52 7a 73 45 61 44
Зашифрованное сообщение:  476 62 448 448 442 402 449 68 45f 44c 400 454 472 75 51 450 412 439 444 409 42e 65
Расшифрованный текст:  С Новым годом, друзья!
```

Рис. 3: Кодирование и декодирование строки

Получим ключ, с помощью которого получим сообщения “С Новым годом, друг” вместо “С Новым годом, друзья!” при декодировании. Воспользуемся симметричностью кодирования(@fig:004).

```
>>> new_msg = "С Новым годом, друг!"
>>>
>>> key = encoder([ord(i) for i in enc_text], [ord(i) for i in new_msg])
>>> print("Ключ: ", to_hex(key))
Ключ:  48 71 6c 6d 7a 77 36 6c 5a 70 51 58 34 4f 36 73 65 56 72 438
>>>
```

Рис. 4: Получение ключа для другого прочтения открытого текста

Вывод

В рамках данной лабораторной работы было освоено на практике применение режима однократного гаммирования