Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Логинов Егор Игоревич

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Логинов Егор Игоревич
- студент НФИбд-01-20
- Российский университет дружбы народов
- 1032201661@pfur.ru
- https://github.com/Y0gu4t

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).

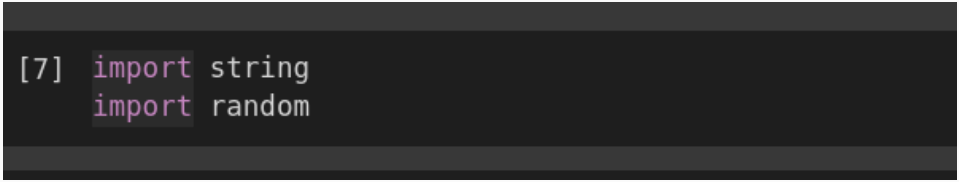

Рис. 1: Импорт модулей

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

```
[8]  def to_hex(text):
         return " ".join(hex(ord(i))[2:] for i in text)

     def generate_key(size):
         key = "".join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
         return key

     def encoder(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).

```
msg = "С Новым годом, друзья!"
key = generate_key(len(msg))
hex_key = to_hex(key)

enc_text = encoder([ord(i) for i in msg], [ord(i) for i in key])
hex_text = to_hex(enc_text)
decr_text = encoder([ord(i) for i in enc_text], [ord(i) for i in key])
```

```
[11] print("Ключ: ", hex_key)
     print("Зашифрованное сообщение: ", hex_text)
     print("Расшифрованный текст: ", decr_text)
```

```
Ключ:  69 46 55 50 74 41 75 61 6f 59 6d 41 46 45 50 69 6a 6a 39 32 52 64
Зашифрованное сообщение:  448 66 448 46e 446 40a 449 41 45c 467 459 47f 47a 69 70 45d 42a 429 40e 47e 41d 45
Расшифрованный текст:  С Новым годом, друзья!
```

Рис. 3: Кодирование и декодирование строки

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

```
[12] new_msg = "С Новым годом, Логинов Егор!"

     key = encoder([ord(i) for i in enc_text], [ord(i) for i in new_msg])
     print("Ключ: ", to_hex(key))

     Ключ:  69 46 55 50 74 41 75 61 6f 59 6d 41 46 45 50 46 14 1a 36 43 23 477
```

Рис. 4: Получение ключа для другого прочтения открытого текста

Вывод

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