

Презентация по лабораторной работе № 7

Информационная безопасность

Адоле Фейт

19.10.2023

Российский университет дружбы народов, Москва, Россия

Информация

- Адоле Фейт Эне
- студент группы НПМбд-02-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Освоить на практике применение режима однократного гаммирования.

Я начала процесс с импорта необходимых библиотек, неотъемлемых для криптографических операций, которые последовали. Впоследствии я разработала специализированную функцию, способную выполнять операции побитового XOR на двух строках, облегчая процессы шифрования и дешифрования. Исходный текст, служащий оригинальным незашифрованным текстом, играл ключевую роль в последующих шагах. Ключ, тщательно созданный для соответствия длине исходного текста, генерировался для внесения дополнительного уровня безопасности в механизм шифрования.

Применяя ранее разработанную функцию, я легко получила шифротекст, предполагая знание как исходного текста, так и созданного ключа. Этот шифротекст, представляющий собой зашифрованную форму оригинального текста, служил важным посредником в криптографических процедурах. Кроме того, я продемонстрировала обратимость процесса, используя ту же функцию для получения исходного текста при наличии информации как о шифротексте, так и о ключе.

Интригующим образом, криптографический процесс не ограничивался лишь шифрованием и дешифрованием, но также распространялся на восстановление ключа. Снова воспользовавшись той же функцией, я успешно извлекла ключ, обладая информацией как о исходном тексте, так и соответствующем шифротексте. Этот всесторонний подход к криптографическим операциям подчеркивает взаимосвязанную природу шифрования, дешифрования и управления ключами в обеспечении целостности и конфиденциальности чувствительной информации.

Выполнение лабораторной работы 4

```
File Edit View Insert Cell Kernel Help
In [1]: import random
        from random import seed
        import string

In [7]: def cipher_text_function(text, key):
        if len(key) != len(text):
            return "Ключ и текст должны быть одной длины!"
        cipher_text = ""
        for i in range(len(key)):
            cipher_text_symbol = ord(text[i]) ^ ord(key[i])
            cipher_text += chr(cipher_text_symbol)
        return cipher_text

In [8]: text = "С Новым годом, друзья!"

In [9]: key = ""
        seed(23)
        for i in range(len(text)):
            key += random.choice(string.ascii_letters + string.digits)
        print(key)
        7X8s51fbt8yHdUmrCao

In [11]: cipher_text = cipher_text_function(text, key)
         print("Шифротекст:", cipher_text)
         Шифротекст: K0x010u8RvW-v[1w6V3P

In [12]: print("Открытый текст:", cipher_text_function(cipher_text, key))
         Открытый текст: С Новым годом, друзья

In [13]: print("Ключ:", cipher_text_function(text, cipher_text))
         Ключ: 7X8s51fbt8yHdUmrCao
```

Рис. 1: Приложение, реализующее режим однократного гаммирования

```
File Edit View Insert Cell Kernel Help
In [1]: import random
        from random import seed
        import string

In [7]: def cipher_text_function(text, key):
        if len(key) != len(text):
            return "Ключ и текст должны быть одной длины!"
        cipher_text = ""
        for i in range(len(key)):
            cipher_text_symbol = ord(text[i]) ^ ord(key[i])
            cipher_text += chr(cipher_text_symbol)
        return cipher_text

In [8]: text = "С Новым годом, друзья!"

In [9]: key = ""
        seed(23)
        for i in range(len(text)):
            key += random.choice(string.ascii_letters + string.digits)
        print(key)
        7X8s51fbt8yHdUmrCao

In [11]: cipher_text = cipher_text_function(text, key)
         print("Шифротекст:", cipher_text)
         Шифротекст: K0x010u8RvW-v[1w6V3P

In [12]: print("Открытый текст:", cipher_text_function(cipher_text, key))
         Открытый текст: С Новым годом, друзья

In [13]: print("Ключ:", cipher_text_function(text, cipher_text))
         Ключ: 7X8s51fbt8yHdUmrCao
```

Рис. 2: Код

Вывод

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.