

Защита лабораторной работы №8

Информационная безопасность

Шатохина В. С.

2024

Российский университет дружбы народов, Москва, Россия

- Шатохина Виктория Сергеевна
- Студентка группы НФИбд-02-21
- Студ. билет 1032217046
- Российский университет дружбы народов

Цель лабораторной работы

- Освоить на практике применение режима однократного гаммирования

Предложенная Г.С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных. [0]

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком \oplus) между элементами гаммы и элементами подлежащего сокрытию текста.

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Ход выполнения лабораторной работы

Задача лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Решение задачи лабораторной работы

Для решения задачи написан программный код:

```

10 [1]: import random

11 [2]: from random import randint

12 [3]: import string

13 [4]: if __name__ == '__main__':
14     # Генерация случайного пароля
15     def generate_password(length):
16         """Генерация пароля заданной длины"""
17         password = ''
18         for i in range(length):
19             password += chr(randint(97, 122))
20         return password

21 [5]: # Ввод количества паролей
22 count = int(input('Введите количество паролей: '))

23 [6]: # Генерация паролей
24 for i in range(count):
25     password = generate_password(10)
26     print(f'Пароль {i+1}: {password}')

27 [7]: # Вывод паролей в файл
28 with open('passwords.txt', 'w') as file:
29     for i in range(count):
30         password = generate_password(10)
31         file.write(f'{password}\n')

32 [8]: # Проверка паролей
33 def check_password(password):
34     """Проверка пароля на соответствие требованиям"""
35     if len(password) < 8:
36         return False
37     if not any(char.isdigit() for char in password):
38         return False
39     if not any(char.islower() for char in password):
40         return False
41     if not any(char.isupper() for char in password):
42         return False
43     return True

34 [9]: # Проверка паролей
35 for i in range(count):
36     password = generate_password(10)
37     if check_password(password):
38         print(f'Пароль {i+1}: {password} - подходит')
39     else:
40         print(f'Пароль {i+1}: {password} - не подходит')

```

Рис. 1: (рис. 1. Программный код приложения, реализующего режим однократного гаммирования)

Вывод

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

Список литературы.

Библиография

0] Методические материалы курса