

Презентация по лабораторной работе №3

Шифрование гаммированием

Саргсян А. Г.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель: Изучить метод шифрования гаммированием

Задачи: Реализовать алгоритм шифрования конечной гаммой.

Гаммирование — это наложение на открытые данные последовательности элементов других данных.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2.

$$0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0.$$

```
: message = "приказ"
  gamma = "гамма"
  println("Исходное сообщение: ", message, ";\nКонечная гамма шифрования: ", gamma)

  ciphertext = Cipher_Gamma(message, gamma)
  println("Результат шифрования: ", ciphertext)

  decrypted_message = Decipher_Gamma(ciphertext, gamma)
  println("Результат дешифрования: ", decrypted_message)
```

Исходное сообщение: приказ;
Конечная гамма шифрования: гамма
Результат шифрования: усхчбл
Результат дешифрования: приказ

Рис. 1: Результат работы алгоритма

Я реализовал алгоритм шифрование конечной гаммой.