

Презентация Лаб 7

Лаб 7

Аристид Ж. Л.

19 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Аристид Жан Л. А.
- Студент
- Российский университет дружбы народов

Вводная часть

- Криптография
- Однократное гаммирование
- Сложение по модулю 2

-Освоить на практике применение режима однократного гаммирования¹

Определение

- Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Этапы алгоритмы криптографии

- Представить Открытый текст на двойчном представлении
- Генеровать ключ шифрования случайном образом
- Сложение по модулю 2

- В ходе этой лабораторной работы мы изучили хороший метод криптографии для отправки сообщений, которые могут быть поняты только теми, у кого есть ключ дешифрования.