Презентация Лаб 8

Лаб 8

Аристид Ж. Л.

26 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

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

Вводная часть

Объект и предмет исследования

- Криптография
- Однократное гаммирование
- Сложение по моделю 2
- другой метод дешифрования

Цели и задачи

- Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Определение

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

Этапы алгоритмы криптографии

- Представить Открытый тектс на двойчном представлении
- Генеровать ключ шифрования случайном образом
- Сложение по модулью 2

Другой метод дешифрование

Другой метод дешифрование

- 1 сложиться по модулью 1 равно 0.
- 1 сложиться по модулью 0 равно 1.
- C1 сложиться по модулью C2 сложиться по модулью P1 равно P2.

Итоговый слайд

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