Лабораторная работа №7

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

19 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Волчок Кристина Александровна, студентка кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- [1032215007@rudn.ru]

Вводная часть

Вводная часть

Однократное гаммирование, или метод Вернама, — это симметричный способ шифрования, основанный на сложении по модулю 2 между текстом и случайным ключом. При соблюдении всех условий метод гарантирует абсолютную криптостойкость. В данной работе изучается применение этого метода для защиты данных.

Актуальность

Однократное гаммирование является одним из методов симметричного шифрования, обеспечивающих абсолютную стойкость при соблюдении строгих условий использования. В современном мире информационной безопасности важно использовать эффективные методы защиты данных, что делает изучение однократного гаммирования актуальной задачей для криптографии.

Объект и предмет исследования

Объектом исследования является криптографический метод однократного гаммирования.

Предмет исследования — процесс шифрования и дешифрования информации с использованием гаммы, а также условия абсолютной стойкости шифра.

Цели и задачи

Целью работы является освоение метода однократного гаммирования и проверка его криптографической стойкости на практике. Для достижения этой цели требуется разработать приложение, которое будет шифровать и дешифровать данные, используя метод наложения гаммы.

Материалы и методы

Для выполнения работы использовался метод однократного гаммирования, предложенный Г. С. Вернамом. Шифрование и дешифрование данных выполнялись с помощью операции сложения по модулю 2 (XOR) между элементами открытого текста и ключа. Программа была реализована для выполнения этих операций с текстом и ключом, представленными в шестнадцатеричном формате.

Результаты

1. Было разработано приложение, которое позволяет зашифровать и дешифровать данные с использованием однократного гаммирования.
2. Шифрование текста и последующее его дешифрование с известным ключом подтвердили теоретические основы метода.
3. Подтверждена абсолютная стойкость шифра при соблюдении условий полной случайности и однократного использования ключа .

Итоговый слайд

Однократное гаммирование демонстрирует абсолютную стойкость, если выполняются строгие условия. Правильное использование этого метода способно обеспечить надежную защиту информации, что делает его важным инструментом в криптографии. Главное — понимать, что безопасность данных зависит от уникальности и случайности ключа.