Лабораторная работа №8

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

Шифрование данных является одним из ключевых аспектов информационной безопасности. Однократное гаммирование, также известное как шифр Вернама, представляет собой симметричный метод шифрования, основанный на операции XOR между открытым текстом и ключом. При правильном использовании этот метод может обеспечивать высокую степень защиты данных.

Актуальность

Повторное использование одного и того же ключа для шифрования нескольких сообщений представляет собой уязвимость, которая может быть использована для взлома шифра. В условиях быстрого роста объемов передаваемой и хранимой информации важно понимать не только методы шифрования, но и риски, связанные с неправильным их использованием. В частности, однократное гаммирование представляет собой метод, который при нарушении правил применения может быть легко скомпрометирован.

Объект и предмет исследования

Объект исследования — однократное гаммирование, используемое для шифрования данных.

Предмет исследования — процесс шифрования и дешифрования сообщений с использованием одного и того же ключа и выявление уязвимостей, связанных с повторным использованием ключа для двух сообщений.

Цели и задачи

Цель работы — продемонстрировать уязвимости метода однократного гаммирования при повторном использовании ключа для шифрования разных сообщений и научиться восстанавливать одно сообщение, зная другое.

Задачи: 1. Реализовать шифрование двух различных сообщений одним ключом. 2. Продемонстрировать возможность восстановления одного сообщения на основе другого. 3. Оценить риски, связанные с повторным использованием ключа.

В качестве материалов используются два сообщения, которые шифруются с помощью заранее определенного 20-байтного ключа. Для выполнения шифрования и дешифрования используется операция XOR.

Метод исследования — шифрование данных с использованием однократного гаммирования (XOR), а также математический анализ, позволяющий восстановить один текст, зная другой и имея доступ к шифротекстам.

Результаты

1. **Шифрование двух сообщений**: Два текста зашифрованы с использованием одного ключа методом XOR.
2. **Восстановление второго сообщения**: Восстановлен текст P2, зная P1 и шифротексты, без использования ключа.
3. **Оценка рисков**: Повторное использование ключа ослабляет безопасность шифрования, позволяя восстановить исходные данные.

Итоговый слайд

- “Использование одного и того же ключа — шаг к раскрытию тайны.” © Криптограф
- Повторное использование одного ключа для шифрования нескольких сообщений создает серьёзную уязвимость, позволяя злоумышленнику восстановить данные.
- Уникальные ключи для каждого сообщения — это залог безопасности. Даже самый надёжный метод шифрования становится уязвимым при неправильном использовании ключей.