Симметричные криптосистемы. Обзор, виды применение

Ощепков Дмитрий, Нкабд-02-22,
1132226442

Содержание

Два вида криптосистем

1. Симметричная криптосистема
   - В симметричной криптосистеме используется один и тот же секретный ключ для шифрования и расшифрования данных.
   - Ключ является секретным и должен быть известен как отправителю, так и получателю сообщения.
   - Примеры симметричных алгоритмов включают DES, AES, идея шифрования, RC4 и т. д.

2. Несимметричная криптосистема (также известная как асимметричная криптосистема

Концептуальное устройство симметричной криптосистемы

1. Генерация ключа
2. Канал передачи ключа
3. Обмен ключами
4. Защита ключа
5. Использование ключа и шифрование собщений

Алгоритмы шифрования

1. Алгоритм DES

DES (Data Encryption Standard) - это симметричный блочный шифр, разработанный в 1970-х годах.

2. Алгоритм AES

AES (Advanced Encryption Standard) - это симметричный блочный шифр, который является одним из самых распространенных алгоритмов шифрования данных. Он был разработан как стандарт шифрования для защиты конфиденциальной информации и обеспечения безопасности в различных информационных системах

3. Алгоритм RC4

RC4 (Rivest Cipher 4) - это алгоритм поточного шифрования, разработанный Рональдом Ривестом в 1987 году. Он широко использовался в различных протоколах безопасности, таких как SSL и WEP (Wired Equivalent Privacy)

Отличия алгоритмов

- **Длина ключа**:
  - DES: Использует фиксированный ключ длиной 56 бит.
  - AES: Поддерживает ключи длиной 128, 192 и 256 бит.
  - RC4: Поддерживает переменную длину ключа от 40 до 2048 бит
- **Скорость работы**:
  - DES: DES характеризуется сравнительно низкой скоростью работы на современных устройствах из-за своей сложной структуры и небольшой длины блока.
  - AES: AES обычно работает быстрее DES благодаря более эффективным алгоритмам и большему размеру блока.
  - RC4: RC4 обычно работает быстрее DES и AES из-за своего поточного характера и относительной простоты алгоритма.

Отличия алгоритмов

- **Тип шифрования**:
  - DES (Data Encryption Standard): DES является блочным шифром с длиной блока 64 бита. Он работает по принципу замены и перестановки битов.
  - AES (Advanced Encryption Standard): AES также является блочным шифром, но с более длинными блоками - 128 бит. Он также работает на основе замены и перестановки битов, но использует более сложные алгоритмы и большее количество раундов для шифрования данных.
  - RC4 (Rivest Cipher 4): RC4 является алгоритмом поточного шифрования, что означает, что он шифрует данные байт за байтом на основе псевдослучайной последовательности. Длина ключа может варьироваться от 40 до 2048 бит

Методы атак

1. Подбор ключа (Brute Force)

- Этот метод атаки предполагает перебор всех возможных комбинаций ключей для расшифровки зашифрованных данных.
- Для DES с его относительно коротким ключом в 56 бит, атака полным перебором ключа является практически выполнимой задачей при использовании современных вычислительных ресурсов.
- Для AES с более длинными ключами (128, 192 или 256 бит), метод полного перебора ключа становится намного более сложным и требует огромных вычислительных ресурсов и времени.

2. Атака по известному открытому тексту (Known Plaintext Attack):

- В этом типе атаки злоумышленник имеет доступ к зашифрованным данным и соответствующим открытым текстам.
- Злоумышленник использует эту информацию для анализа и атаки на шифр, пытаясь выявить закономерности или слабости в процессе шифрования.

Методы атак

3. Атака по выбранному открытому тексту

- В этом типе атаки злоумышленник может выбирать определенные открытые тексты и наблюдать за соответствующими зашифрованными данными.
- После этого злоумышленник пытается анализировать полученные данные и искать уязвимости в шифре

4. Дифференциальный криптоанализ

- Этот метод атаки направлен на нахождение характерных различий между зашифрованными текстами, полученными при разных входных данных.
- Злоумышленник анализирует различия в выходных данных для выявления корреляций и слабостей в алгоритме шифрования.

5. Линейный криптоанализ

- Этот метод атаки основан на поиске линейных аппроксимаций между входными и выходными данными алгоритма шифрования.
- Злоумышленник использует статистические методы для поиска линейных зависимостей, которые могут помочь в раскрытии ключа

Заключение

В заключении, симметричные криптосистемы играют важную роль в обеспечении безопасности информации путем шифрования и защиты конфиденциальности данных. Они предоставляют эффективные и быстрые методы шифрования, позволяя защищать информацию на различных уровнях, включая хранение, передачу и обработку данных.

Однако существуют некоторые ограничения и проблемы, с которыми сталкиваются симметричные криптосистемы. **Одним из главных ограничений является необходимость безопасного обмена секретным ключом между отправителем и получателем перед использованием шифрования.** Это может быть сложной задачей, особенно при обмене данными через открытые сети.