Современные методы криптографии

Презентация

Подхалюзина Виолетта Михайловна НКАбд-04-24 1132246761

Российский университет дружбы народов, Москва, Россия

Введение

Что такое криптография?

Криптография — это наука о защите информации путем ее преобразования таким образом, чтобы несанкционированные лица не могли ее прочитать.

Рис. 1: Криптография

Ключевые цели криптографии: - Конфиденциальность — защита данных от несанкционированного доступа. - Целостность — предотвращение изменений данных без ведома отправителя. - Аутентификация — проверка подлинности отправителя и получателя. - Неотрекаемость — невозможность отрицания факта отправки или получения данных.

Эволюция криптографии

- Античность: Цезарево шифрование (замена букв с фиксированным сдвигом).
- Средневековье: Полиграфические шифры (например, шифр Виженера).
- XX век: Механизированные шифры (Enigma, SIGABA).
- Современность: Компьютерные криптографические алгоритмы (AES, RSA, ECC).
- Будущее: Квантовая криптография, гомоморфное шифрование.

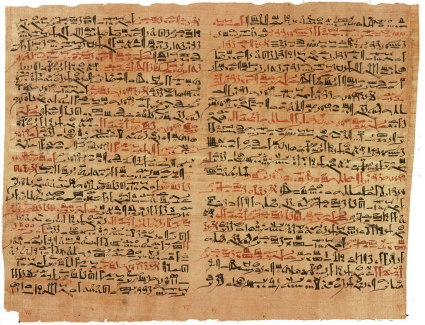


Рис. 2: Эволюция криптографии

Симметричное шифрование

Основные принципы

Симметричное шифрование использует один ключ как для шифрования, так и для расшифровки.

Преимущества: - Высокая скорость работы. - Простая реализация.

Недостатки: - Проблема безопасного обмена ключами. - Уязвимость при компрометации ключа.

Основные алгоритмы

- AES (Advanced Encryption Standard) – современный стандарт шифрования, используемый во многих системах.
- DES (Data Encryption Standard) – устаревший алгоритм, замененный на AES.
- ChaCha20 – более быстрый и безопасный алгоритм, используемый в мобильных устройствах.

Асимметричное шифрование

Основные принципы

Использует два ключа: - Открытый ключ (public key) — используется для шифрования. - Закрытый ключ (private key) — используется для расшифровки.

Преимущества: - Безопасная передача данных через незащищенные каналы. - Поддержка цифровых подписей.

Недостатки: - Более низкая скорость по сравнению с симметричными алгоритмами. - Высокая нагрузка на вычислительные ресурсы.

Основные алгоритмы

- RSA – один из первых алгоритмов асимметричного шифрования, основанный на факторизации больших чисел.
- ECC (Elliptic Curve Cryptography) – использует эллиптические кривые, обеспечивает высокий уровень безопасности при меньших размерах ключей.

Рис. 4: Асимметричное шифрование

Хеш-функции

Что такое хеширование?

Хеш-функция – это алгоритм, который преобразует данные в уникальный фиксированный цифровой отпечаток (хеш).

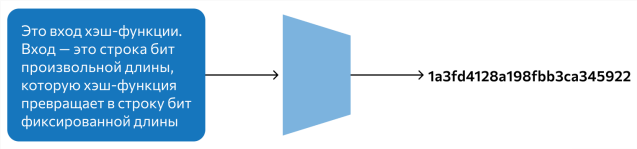


Рис. 5: Хеш-функция

Свойства хеш-функций: - Односторонность: невозможно восстановить исходные данные. - Коллизионная устойчивость: маловероятно найти два разных сообщения с одинаковым хешем. - Эффективность вычисления.

Применение хеш-функций

- Проверка целостности данных (контрольные суммы).
- Хранение паролей (в базах данных вместо пароля хранится его хеш).
- Цифровые подписи и аутентификация.

Основные алгоритмы

- SHA-256 – широко используется в блокчейне и цифровых подписях.
- MD5 – устаревший алгоритм, не рекомендуется из-за уязвимости к коллизиям.
- BLAKE2 – более быстрый и безопасный, чем SHA.

Криптография на эллиптических кривых (ECC)

Основные идеи

ECC использует математические свойства эллиптических кривых над конечными полями для создания криптографических алгоритмов.

Преимущества ECC: - Высокая безопасность при меньшем размере ключа. - Более эффективные вычисления по сравнению с RSA.

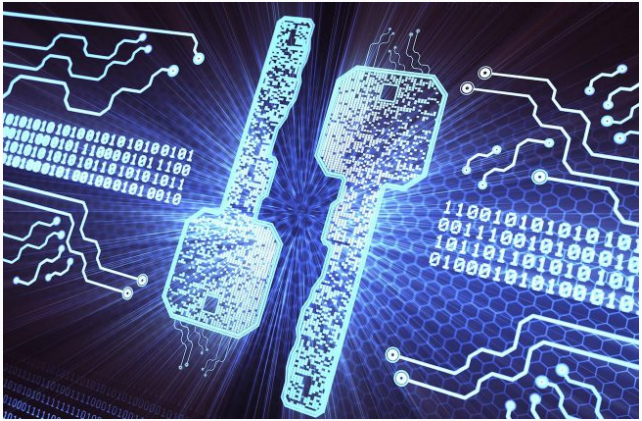
Применение

- Используется в HTTPS, блокчейне, мобильных устройствах.
- Популярные алгоритмы: ECDSA, EdDSA.

Квантовая криптография

Что это такое?

Квантовая криптография использует принципы квантовой механики для передачи ключей без возможности перехвата.



Преимущества:

- Невозможно перехватить квантовый ключ без его изменения.
- Устойчивость к атакам квантовых компьютеров.

Основные методы:

- Квантовое распределение ключей (QKD) – передача ключа через квантовые каналы связи.
- Алгоритмы постквантовой криптографии – защита от атак квантовых компьютеров.

Гомоморфное шифрование

Что это такое?

Гомоморфное шифрование позволяет выполнять вычисления над зашифрованными данными без их расшифровки.

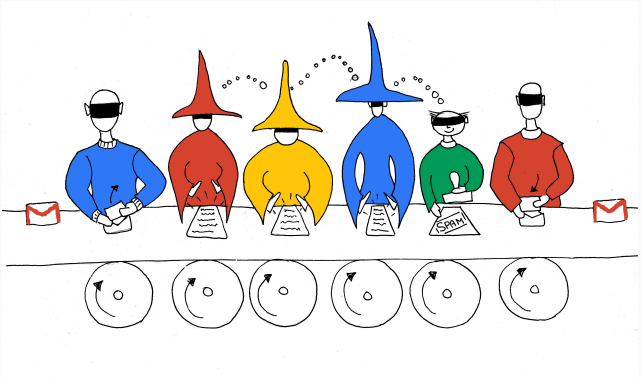


Рис. 7: Гомоморфное шифрование

Применение: - Облачные вычисления с конфиденциальными данными. - Приватные медицинские и финансовые расчеты.

Основные типы: - Частично гомоморфное шифрование (PHE) – поддерживает только один тип операций (сложение или умножение). - Полностью гомоморфное шифрование (FHE) – поддерживает любые арифметические операции.

Итоги

- Криптография — основа цифровой безопасности.
- Современные методы позволяют надежно защищать данные.
- Будущее – квантовые и гомоморфные технологии.

Список литературы

1. Katz J., Lindell Y. *Introduction to Modern Cryptography*. – CRC Press, 2020.
2. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. – CRC Press, 1996.
3. Stallings W. *Cryptography and Network Security: Principles and Practice*. – Pearson, 2016.