Доклад

Асимметричные криптосистемы: обзор, виды, применение

Беличева Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- https://dmbelicheva.github.io/ru/

Цель работы

Целью данного доклада является представление основного принципа работы асимметричных криптосистем, их видов и применения в современных информационных системах.

Задачи

- Дать определение асимметрическим криптосистемам;
- Рассмотреть историю развития асимметричных криптосистем и их вклад в криптографию;
- Описать основные принципы работы асимметричных криптосистем;
- Представить основные виды асимметричных криптосистем;
- Проанализировать преимущества и недостатки асимметричной криптографии в сравнении с симметричными методами;
- Рассмотреть примеры применения асимметричных криптосистем в различных областях.

Теоретическое введение

Рис. 1: Ассиметричное шифрование

Основы асимметричных криптосистем

- **Открытый ключ** используется для шифрования данных. Он может быть свободно передан по открытому каналу.
- **Закрытый ключ** используется для расшифровки зашифрованной информации. Он остается известным только владельцу.

Сравнение симметрических и асимметричных криптосистем

Характеристика	Симметричное шифрование	Асимметричное шифрование
Принцип работы	Один и тот же ключ используется для шифрования и расшифровки	Используются два разных ключа: открытый для шифрования, закрытый для расшифровки
Скорость	Быстрое шифрование и расшифровка	Медленное шифрование и расшифровка
Вычислительные затраты	Низкие вычислительные затраты	Высокие вычислительные затраты
Передача ключа	Требует безопасного обмена секретным ключом	Не требует передачи секретного ключа, только открытого
Безопасность	Зависит от секретности ключа, уязвимо при утечке	Безопаснее, закрытый ключ остается в секрете
Примеры алгоритмов	AES, DES, 3DES, Blowfish	RSA, Диффи-Хеллман, DSA, Эллиптическая криптография

Сравнение симметрических и асимметричных криптосистем

Характеристика	Симметричное шифрование	Асимметричное шифрование
Область применения	Шифрование больших объемов данных	Шифрование ключей, цифровые подписи, аутентификация
Преимущества	Высокая скорость, низкая сложность	Высокая безопасность, отсутствие необходимости передачи секретного ключа
Недостатки	Необходимость безопасного обмена ключом	Медленная работа с большими объемами данных
Типичные применения	Шифрование файлов, баз данных	HTTPS, цифровые подписи, обмен ключами, блокчейн

Виды асимметричных криптосистем

1. RSA (Ривест-Шамир-Адлеман)
2. Алгоритм Диффи-Хеллмана
3. Эллиптическая криптография (ECC)
4. DSA (Алгоритм цифровой подписи)

Зашифруем и расшифруем сообщение “CAB” по алгоритму RSA.

- Выберем p=3 and q=11.
- Определим n= 3*11=33.
- Найдем (p-1)*(q-1)=20. Следовательно, d будет равно, например, 3: (d=3).
- Выберем число e по следующей формуле: (e*3) mod 20=1. Значит e будет равно, например, 7: (e=7). -Представим шифруемое сообщение как последовательность чисел в диапозоне от 0 до 32. Буква A =1, B=2, C=3.

RSA (Ривест-Шамир-Адлеман)

Теперь зашифруем сообщение, используя открытый ключ {7,33}

C1 = (3^7) mod 33 = 2187 mod 33 = 9;

C2 = (1^7) mod 33 = 1 mod 33 = 1;

C3 = (2^7) mod 33 = 128 mod 33 = 29;

Теперь расшифруем данные, используя закрытый ключ {3,33}.

M1=(9^3) mod 33 =729 mod 33 = 3(C);

M2=(1^3) mod 33 =1 mod 33 = 1(A);

M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

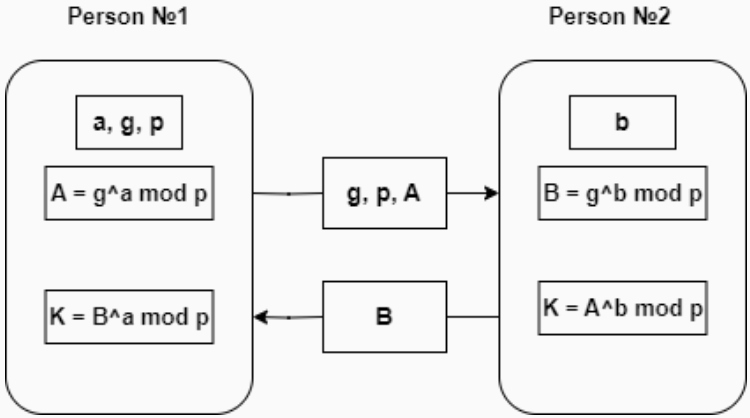

Рис. 2: Алгоритм Диффи – Хеллмана, где K – итоговый общий секретный ключ

Применение асимметричных криптосистем

1. HTTPS и SSL/TLS
2. Электронная почта (PGP, S/MIME)
3. Цифровые подписи
4. Блокчейн и криптовалюты
5. Мобильные платежные системы

Заключение

Асимметричные криптосистемы играют важную роль в защите информации в современном мире. Они обеспечивают высокую безопасность при передаче данных, позволяют проверять подлинность документов и сообщений, а также используются в критически важных приложениях, таких как защита веб-сайтов, электронная почта и блокчейн.

Список литературы

1. Адигеев М.Г. Введение в криптографию. Часть 1 // Ростов-на-Дону: Издательство РГУ. 2002.
2. Асимметричное шифрование [Электронный ресурс]. 2024. URL: https://encyclopedia.kaspersky.ru/glossary/asymmetric-encryption/.
3. RSA: Алгоритм асимметричного шифрования [Электронный ресурс]. 2024. URL: https://e-nigma.ru/stat/rsa/.