

Безопасность в РС

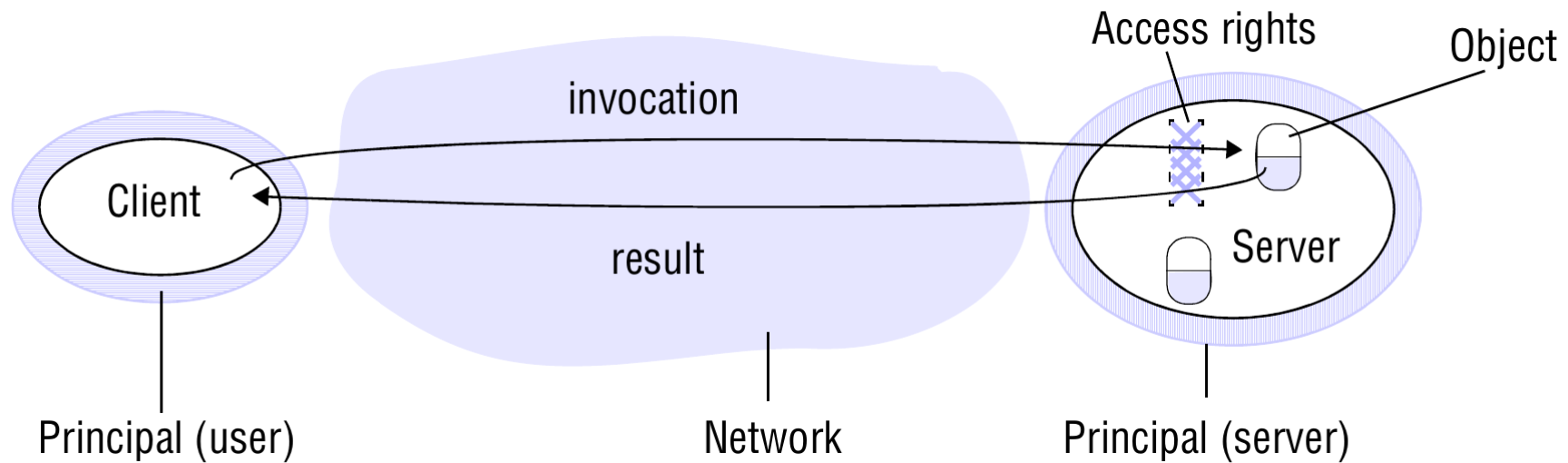
Сухорослов Олег Викторович

Распределенные вычисления

Факультет компьютерных наук НИУ ВШЭ

12.12.2020

Возможные угрозы?



Угрозы

- Interception
- Modification
- Fabrication
- Interruption

Атаки

- Подслушивание (eavesdropping)
- Фальсификация данных (data tampering)
- Человек посередине (man-in-the-middle)
- Подмена (masquerading, spoofing, phishing)
- Повтор (replaying)
- Отказ в обслуживании (denial-of-service)
- Вредоносное ПО (malware, вирус, сетевой червь, spyware)

Требования

- Конфиденциальность
- Целостность
- Аутентификация
- Невозможность отказа
- Авторизация
- Доступность
- Масштабируемость

Методика

- Анализ угроз
- Предотвращение угроз
- Валидация
- Аудит

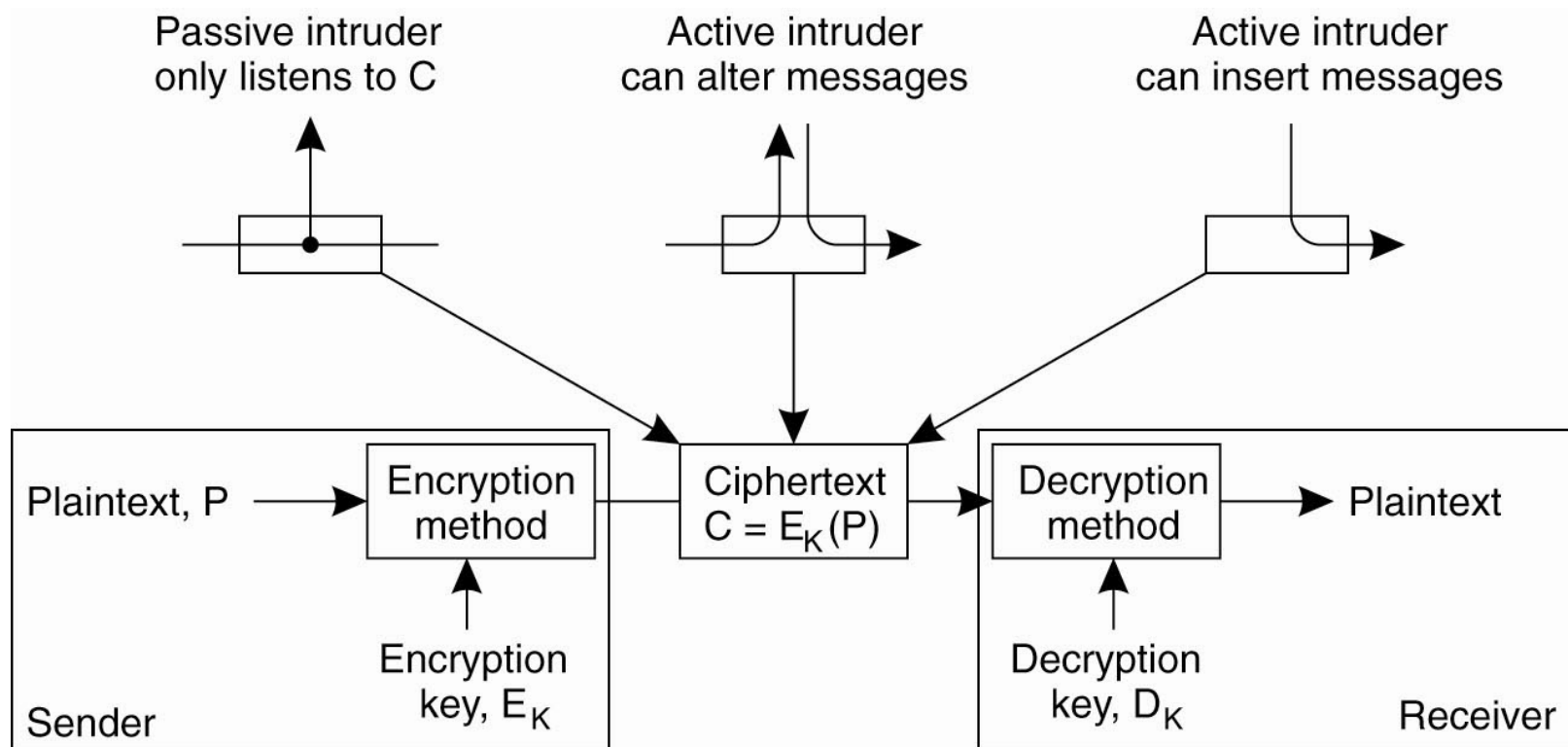
Предположения и принципы

- Интерфейсы доступны всем
- Сети не безопасны
- Время жизни и действие секретов должны быть ограничены
- Алгоритмы и код доступны атакующим
- Атакующие могут иметь доступ к большим вычислительным мощностям
- Минимизация критически важных компонентов (trusted computing base)

Базовые техники и механизмы

- Криптография (защищенный канал)
 - Конфиденциальность
 - Целостность
 - Аутентификация
 - Невозможность отказа
- Контроль доступа
 - Авторизация (ACL, capabilities, groups, roles)
 - Проверка и изолированное выполнение кода
 - Межсетевые экраны, защита от DoS-атак
- Управление безопасностью
 - Распространение ключей, цифровые сертификаты, делегирование прав...

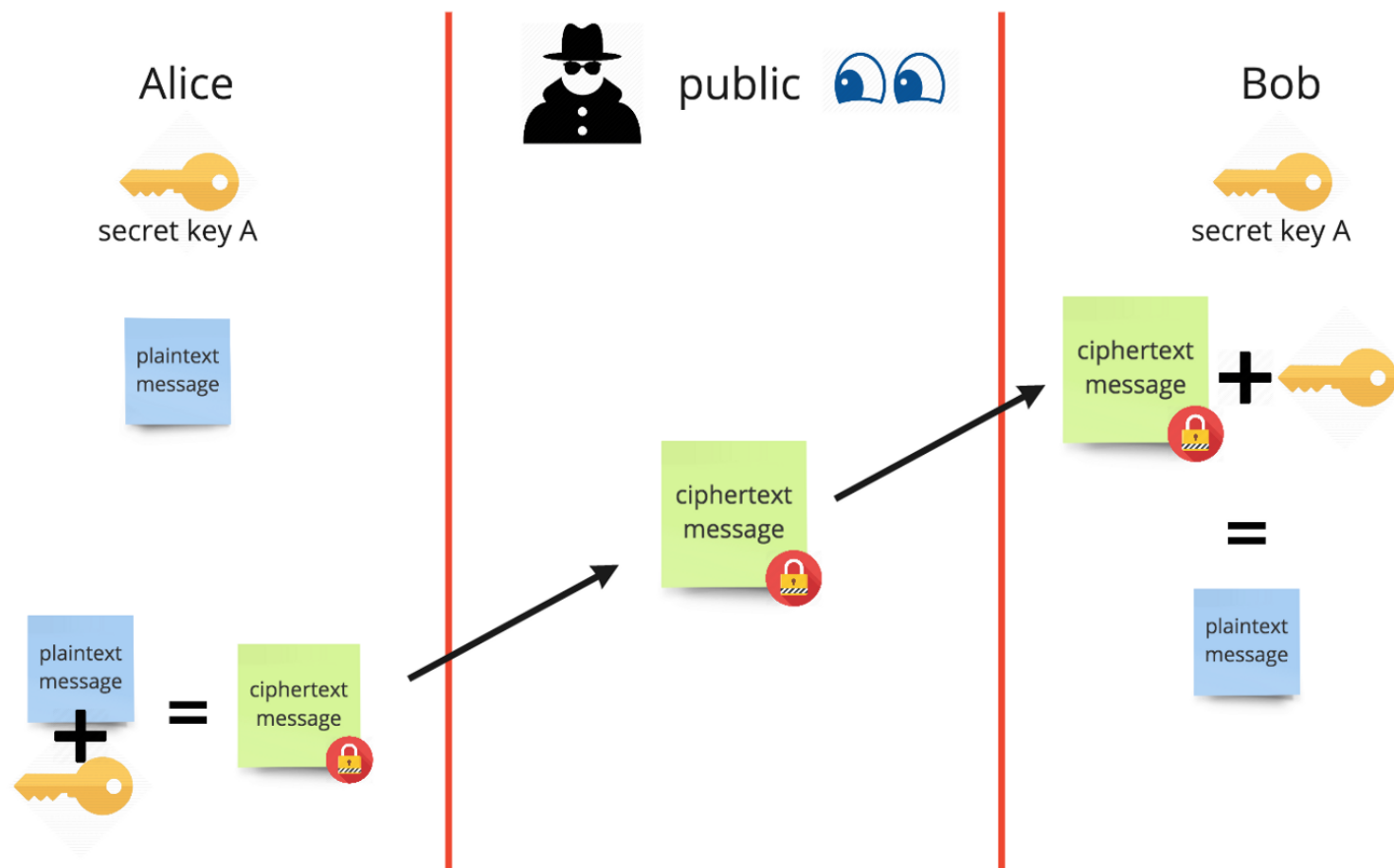
Шифрование



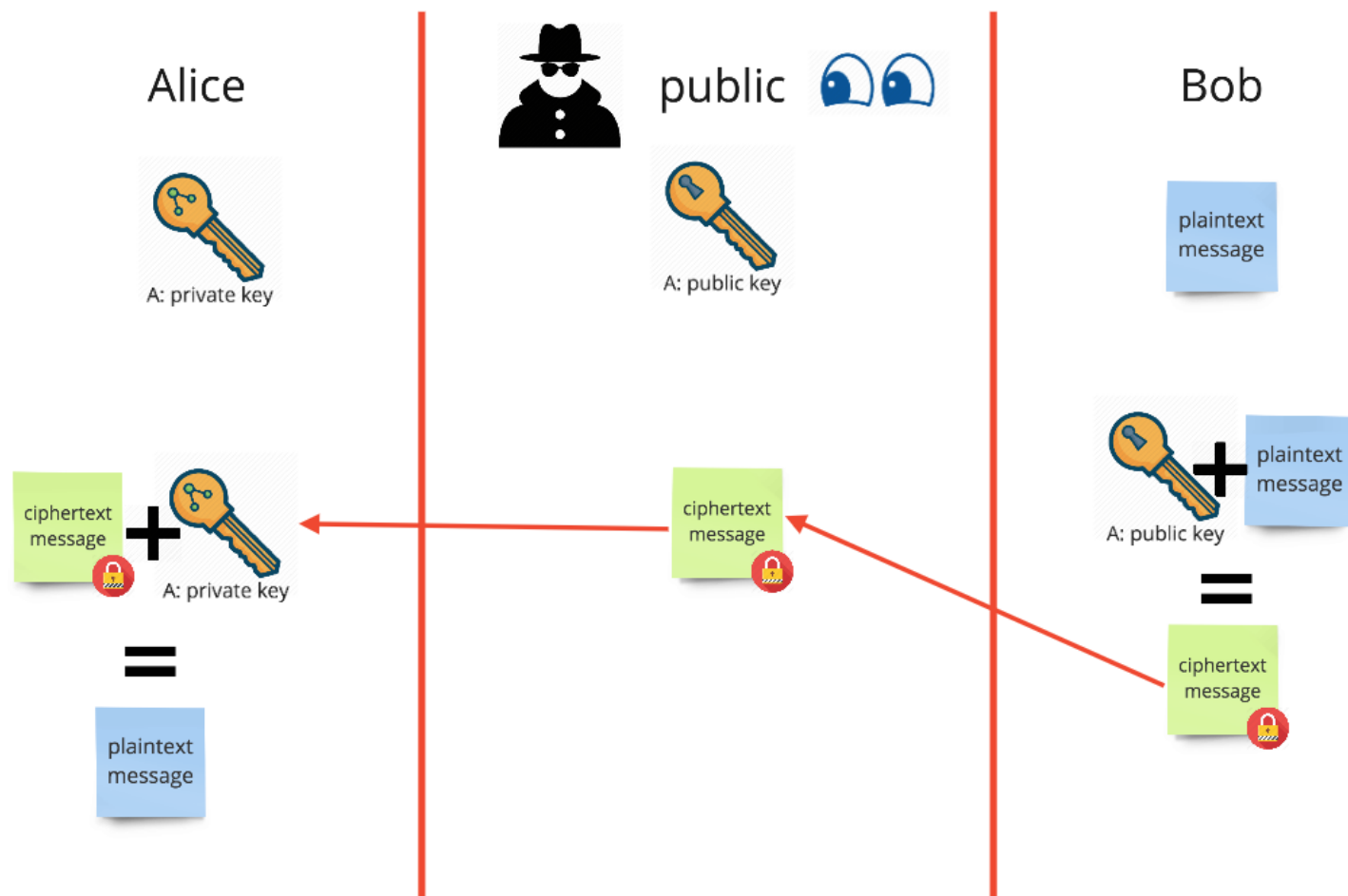
Шифрование

- Симметричное (secret-key, shared-key)
 - $P = D_K(E_K(P))$
 - $K_{A,B}$ - ключ, используемый A и B
 - Блочные шифры (DES, 3DES, TEA, IDEA, Blowfish, Twofish, AES)
 - Поточные шифры (RC4)
- Асимметричное (public-key)
 - $P = D_{K_D}(E_{K_E}(P))$
 - K_A^+ - открытый ключ A
 - K_A^- - закрытый (секретный) ключ A
 - Шифрование с открытым ключом (RSA, ElGamal, ECDSA)

Симметричное шифрование



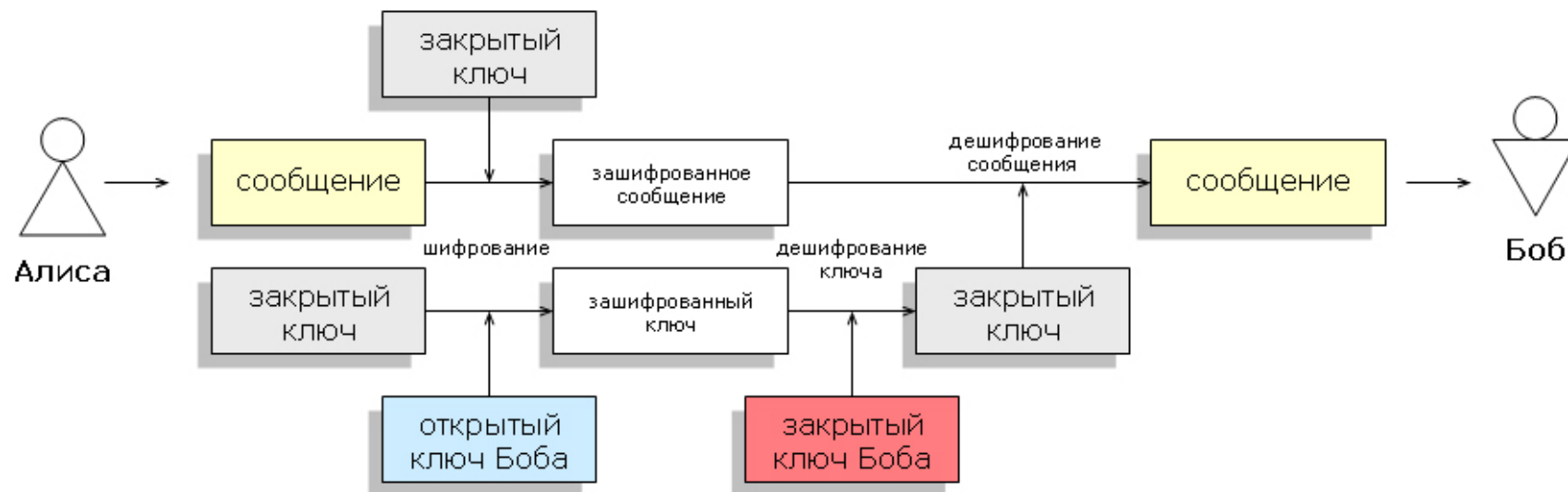
Шифрование с открытым ключом



Сравнение

- Симметричное шифрование
 - Требуется распространение ключа по защищенному каналу
 - Для каждой пары участников нужен отдельный ключ
 - В системе из N участников требуется $N(N - 1)/2$ ключей
- Шифрование с открытым ключом
 - Требуется механизм распространения и проверки открытых ключей
 - В системе из N участников требуется N пар ключей
 - Более длинные ключи и большее время работы

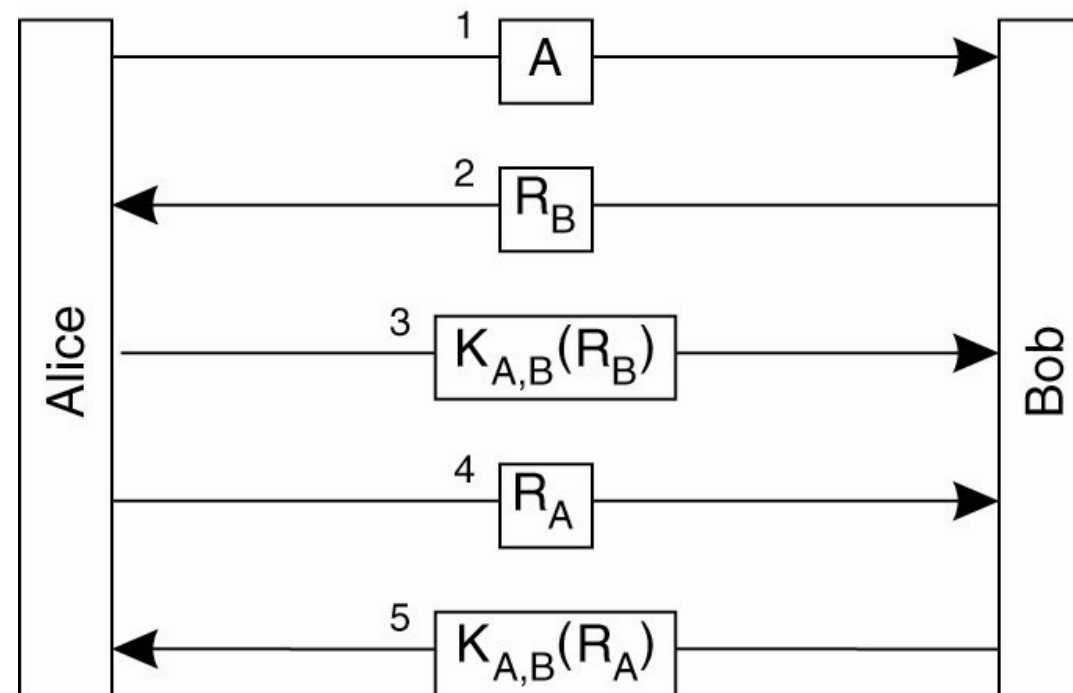
Гибридная схема



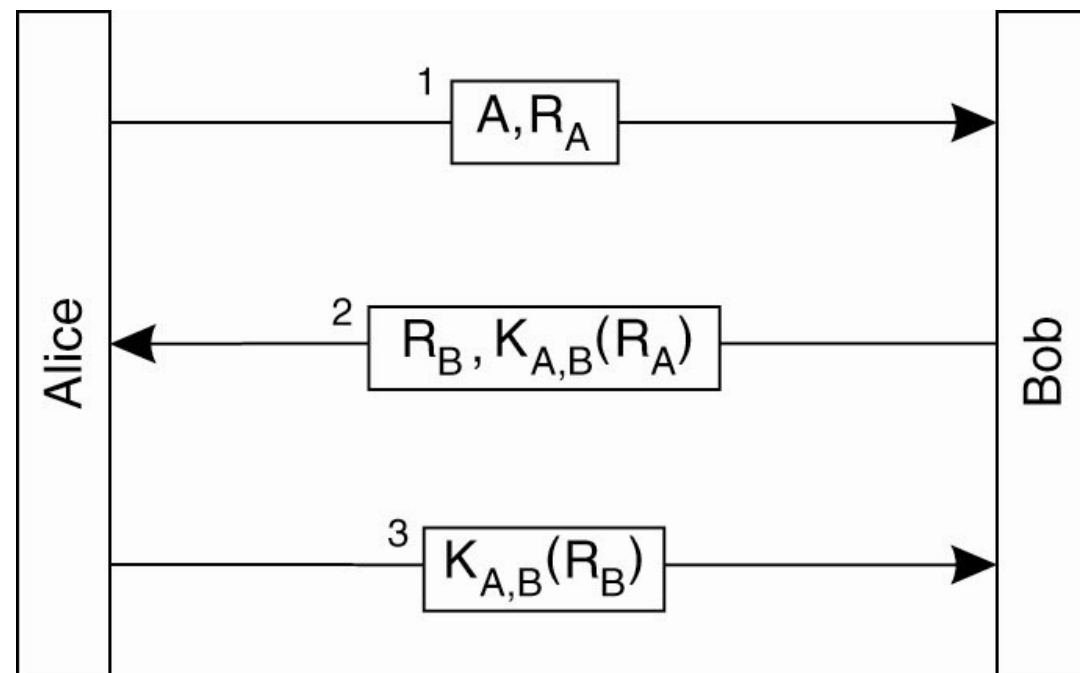
Аутентификация

- В начале взаимодействия стороны должны убедиться в подлинности друг друга
- После аутентификации между ними может быть установлен защищенный канал с использованием шифрования

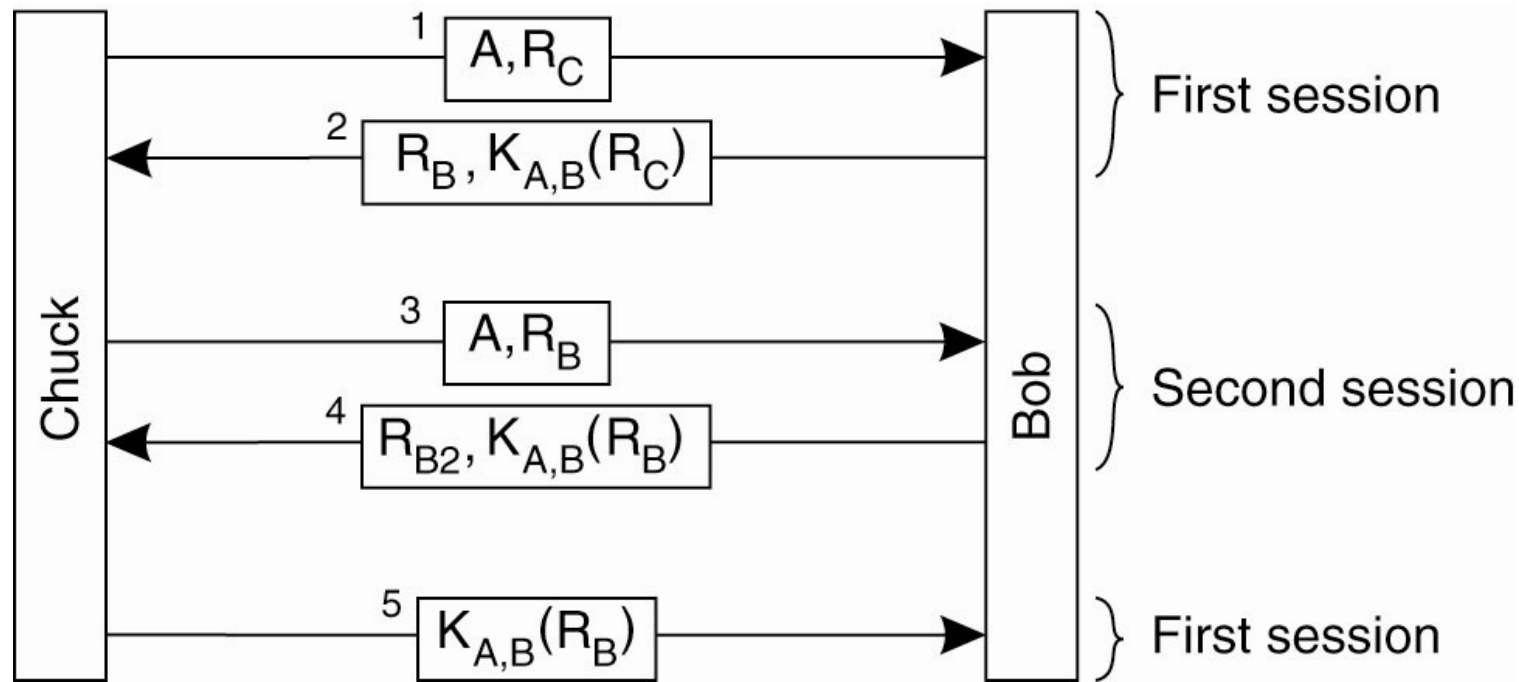
Аутентификация (shared key)



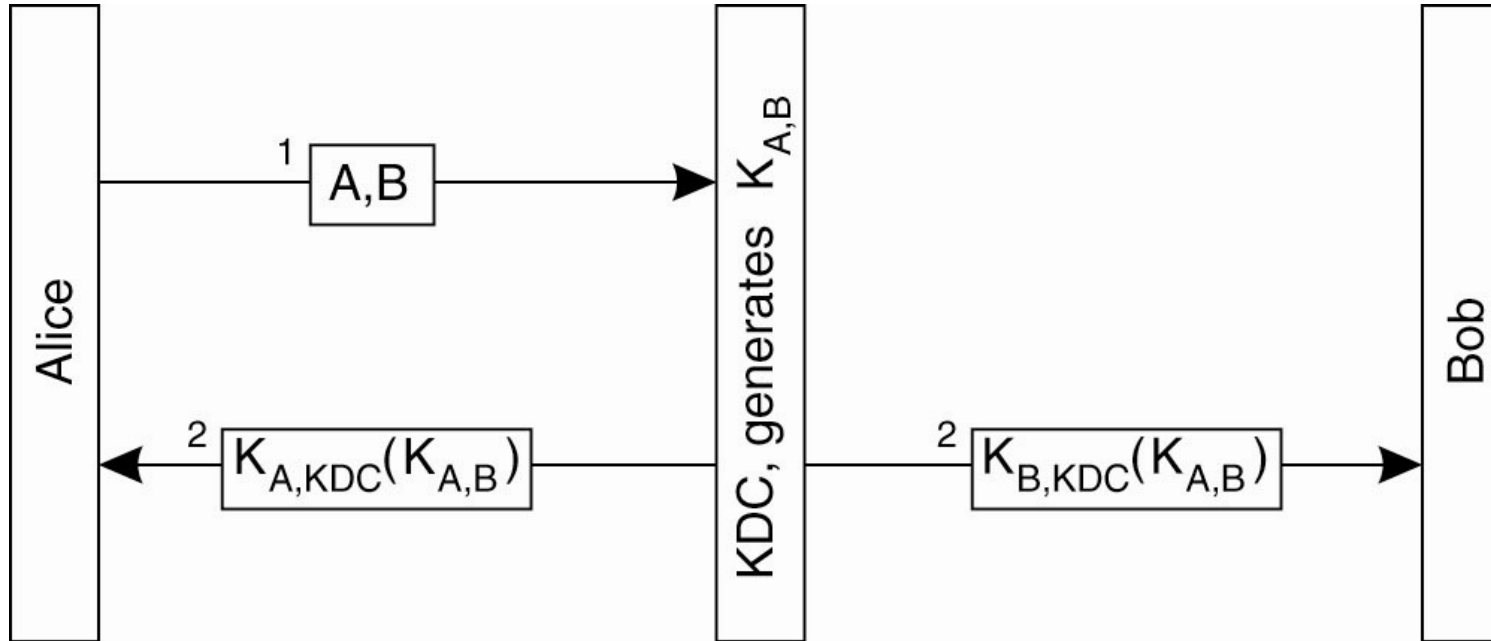
Оптимизация?



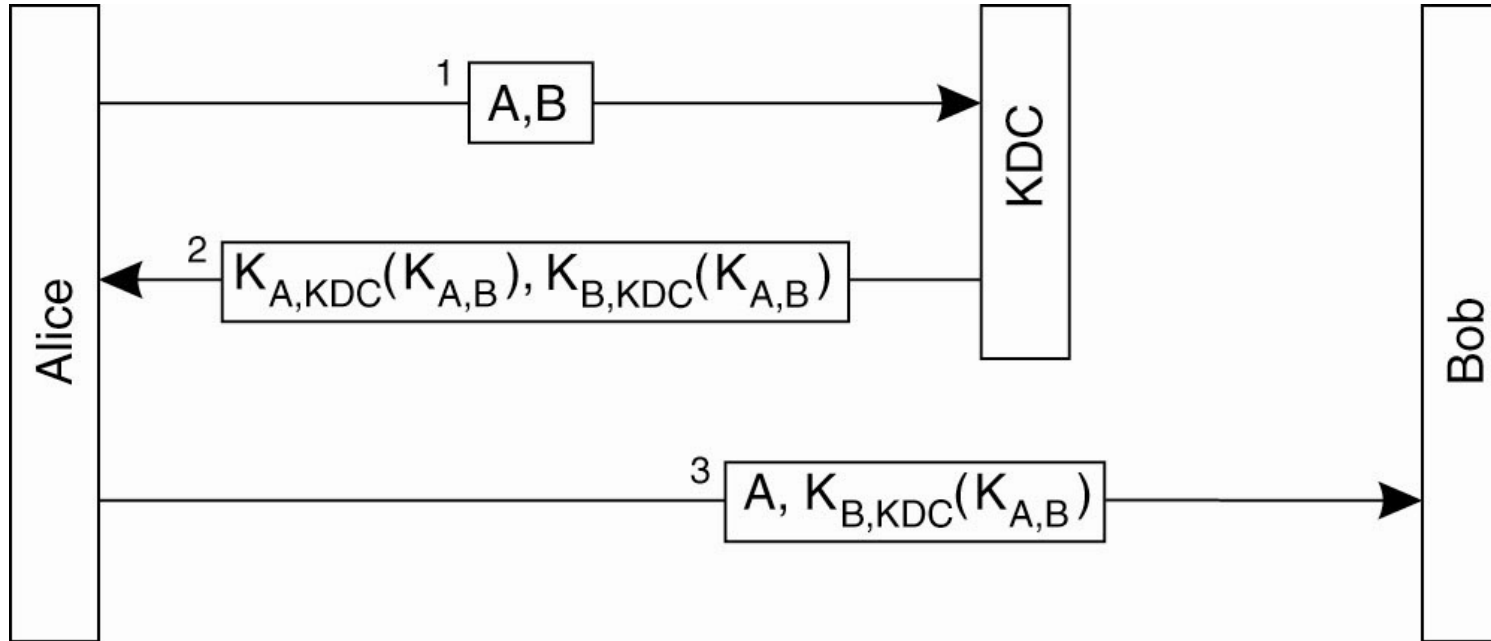
Reflection Attack



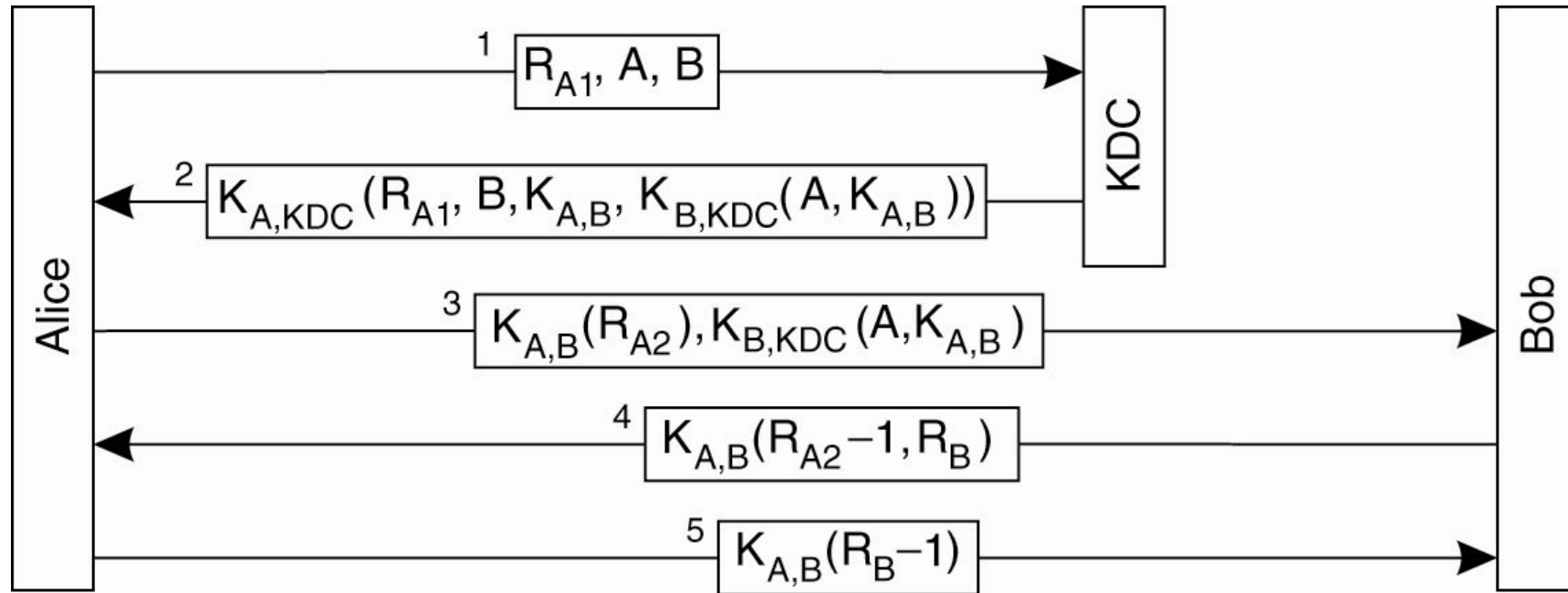
Key Distribution Center



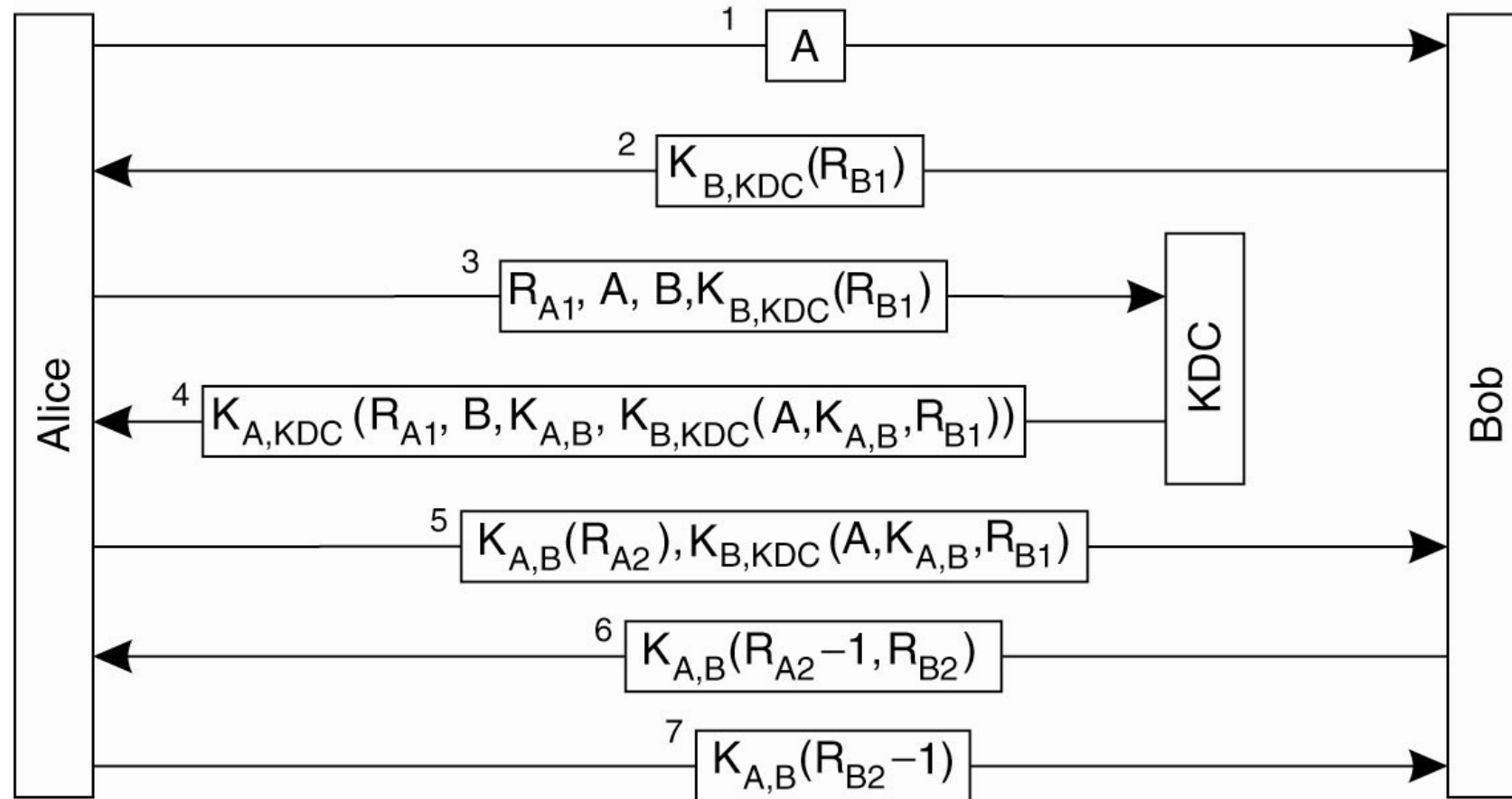
Key Distribution Center + Ticket



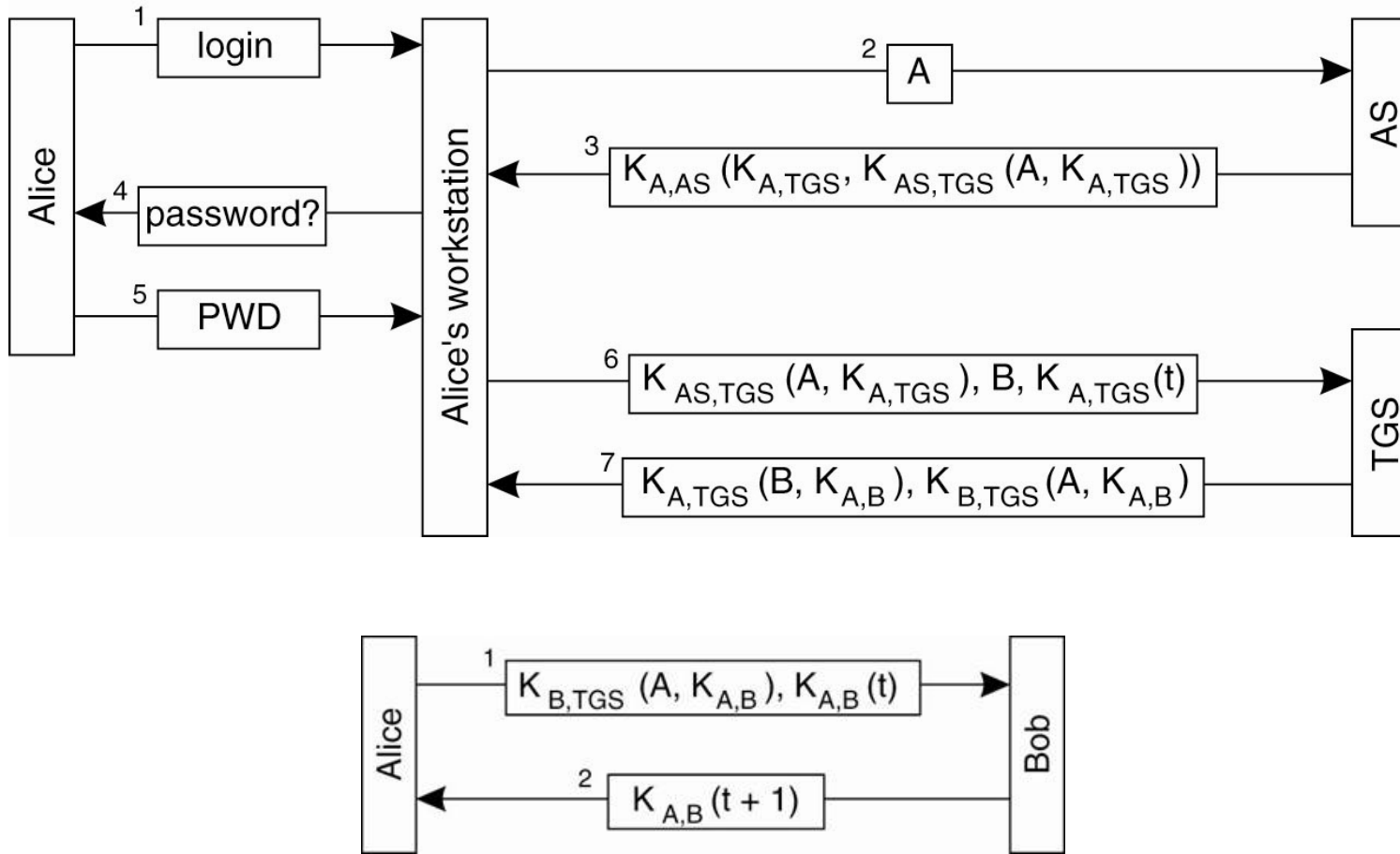
Протокол Нидхема-Шрёдера



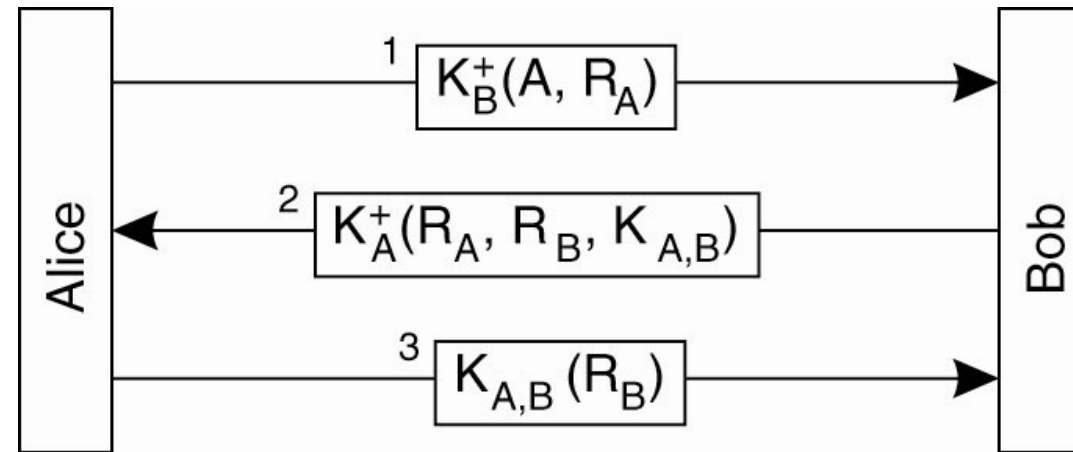
Протокол Нидхема-Шрёдера (fixed)



Single Sign-on (Kerberos)



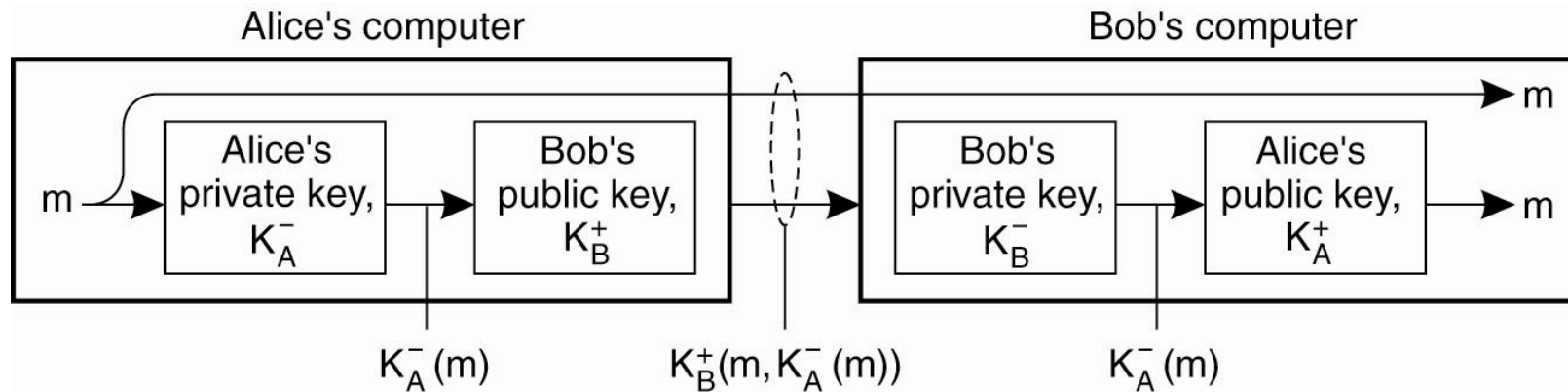
Аутентификация (public key)



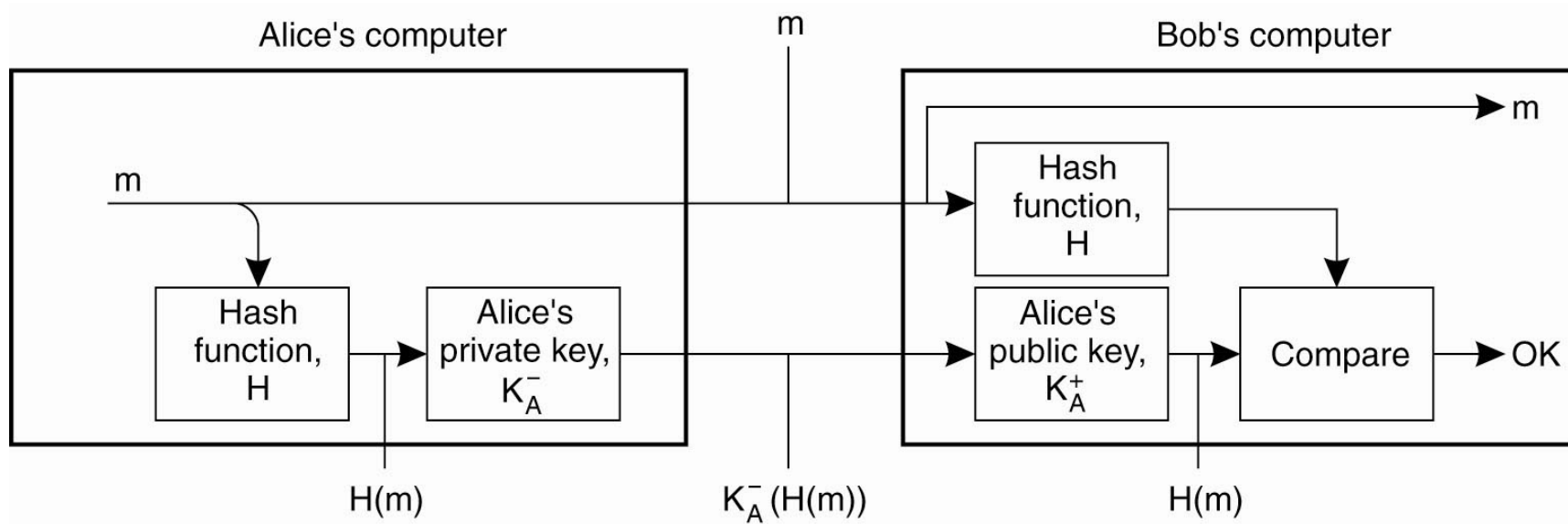
Цифровая подпись

- Как в процессе взаимодействия обеспечить
 - проверку подлинности сообщений
 - невозможность их фальсификации
 - невозможность отказа
- Для этого используются цифровые подписи

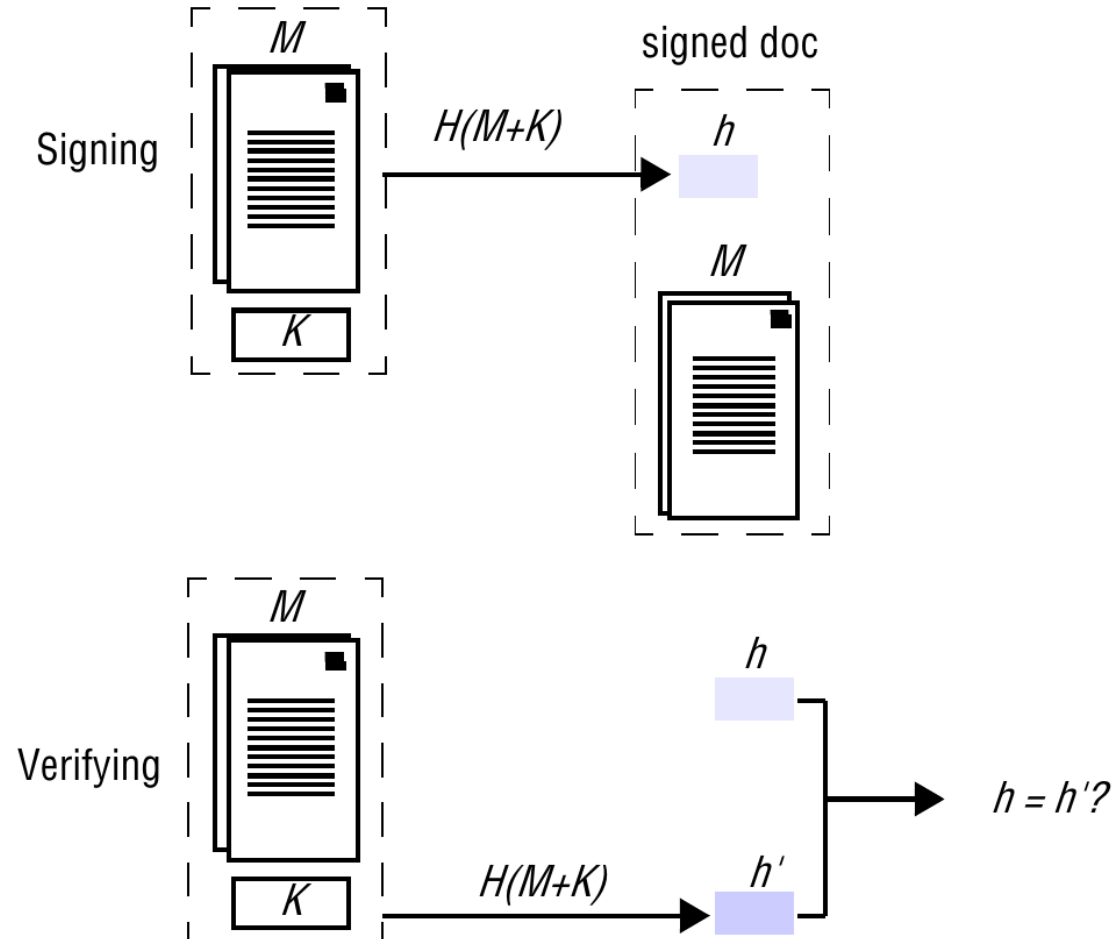
Подпись (шифр. с открытым ключом)



Подпись (message digest)



Message Authentication Code (MAC)



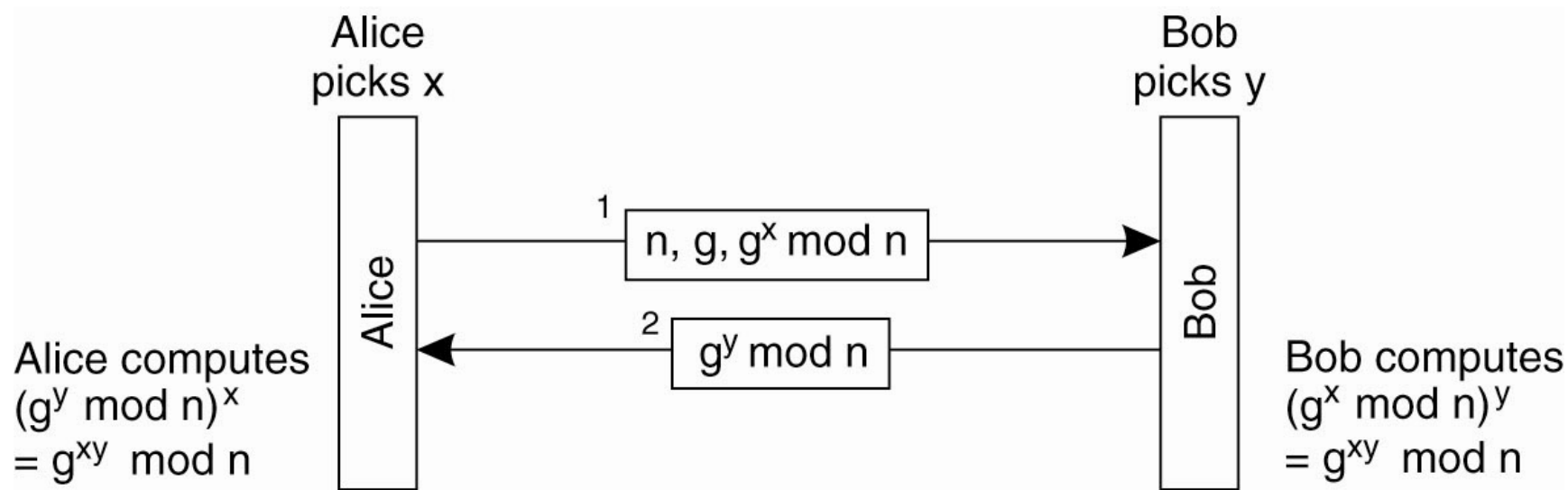
Хеширование

- Сообщение произвольной длины → строка фиксированной длины
- Свойства криптографических хеш-функций
 - сопротивление поиску первого прообраза
 - сопротивление поиску второго прообраза
 - стойкость к коллизиям
- Примеры
 - MD5, SHA-1, bcrypt, Whirlpool, SHA-2, SHA-3

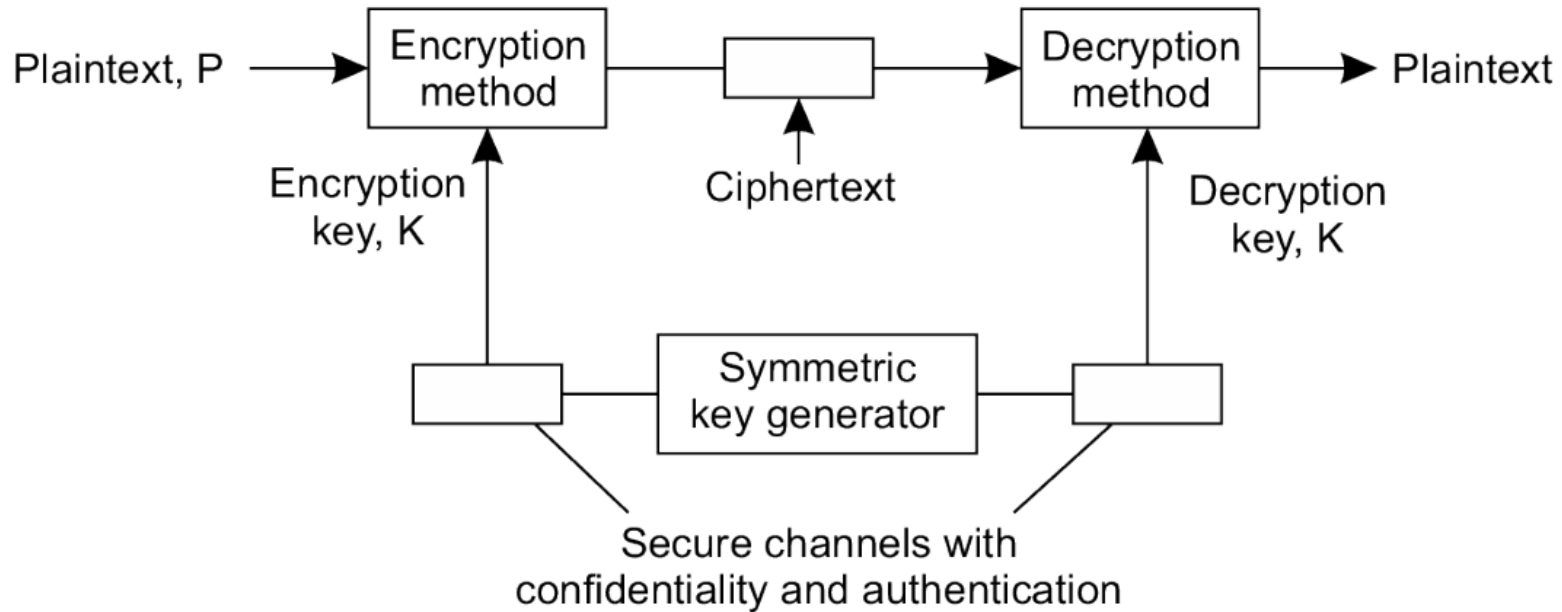
Управление ключами

- Как сторонам договориться об используемом ключе?
- Как убедиться в подлинности открытого ключа?
- Как уменьшить риски при компрометации ключа?

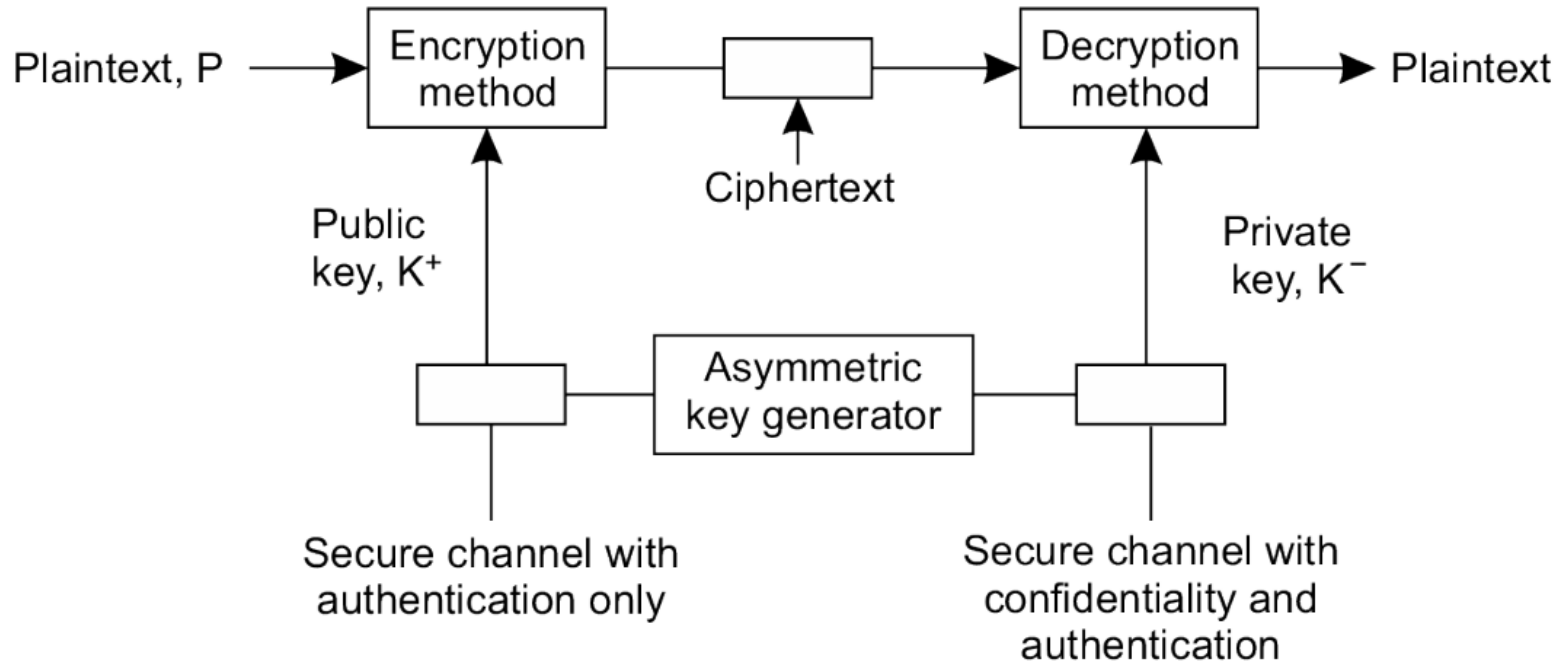
Получение общего ключа (Diffie-Hellman)



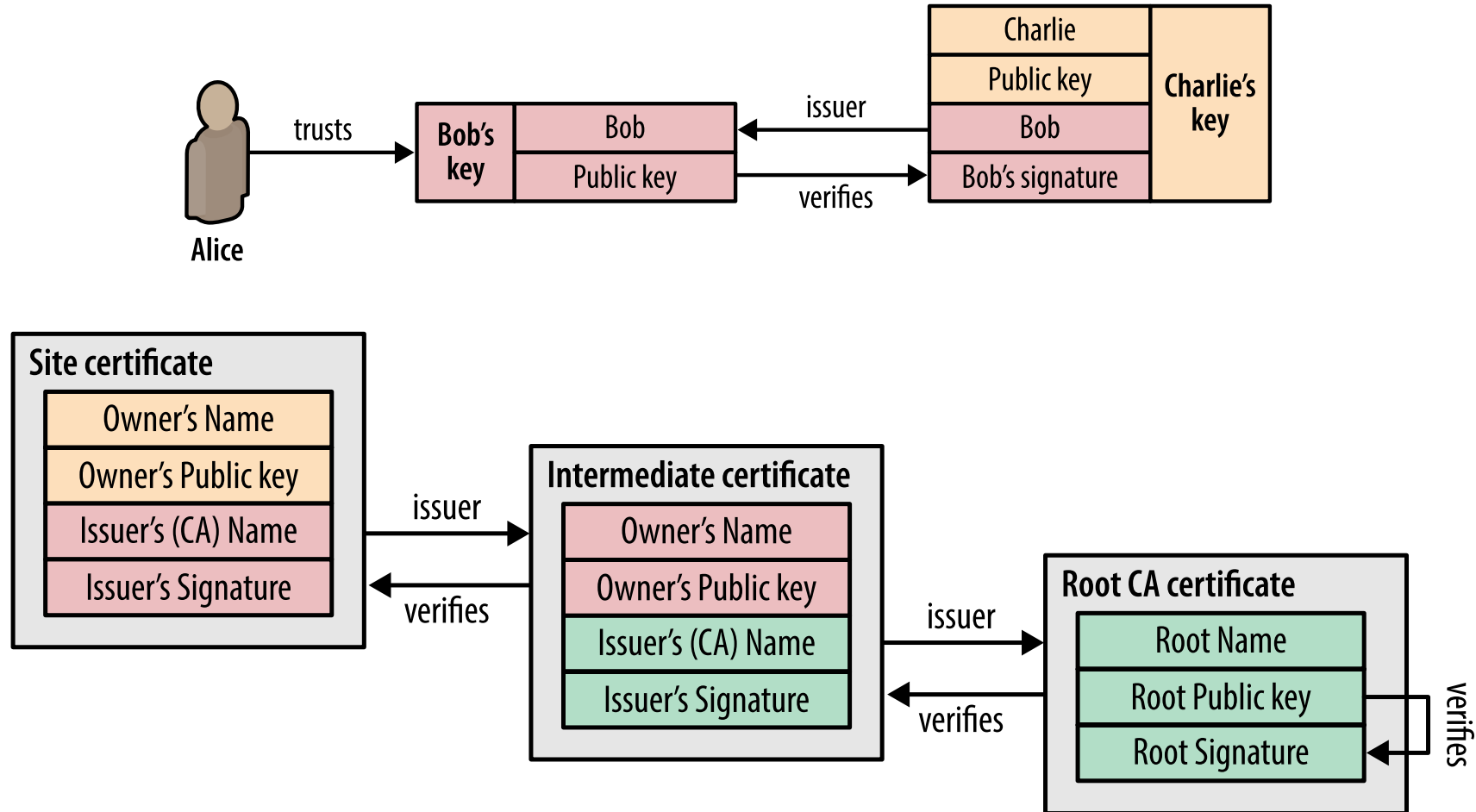
Распространение ключей (shared)



Распространение ключей (public/private)

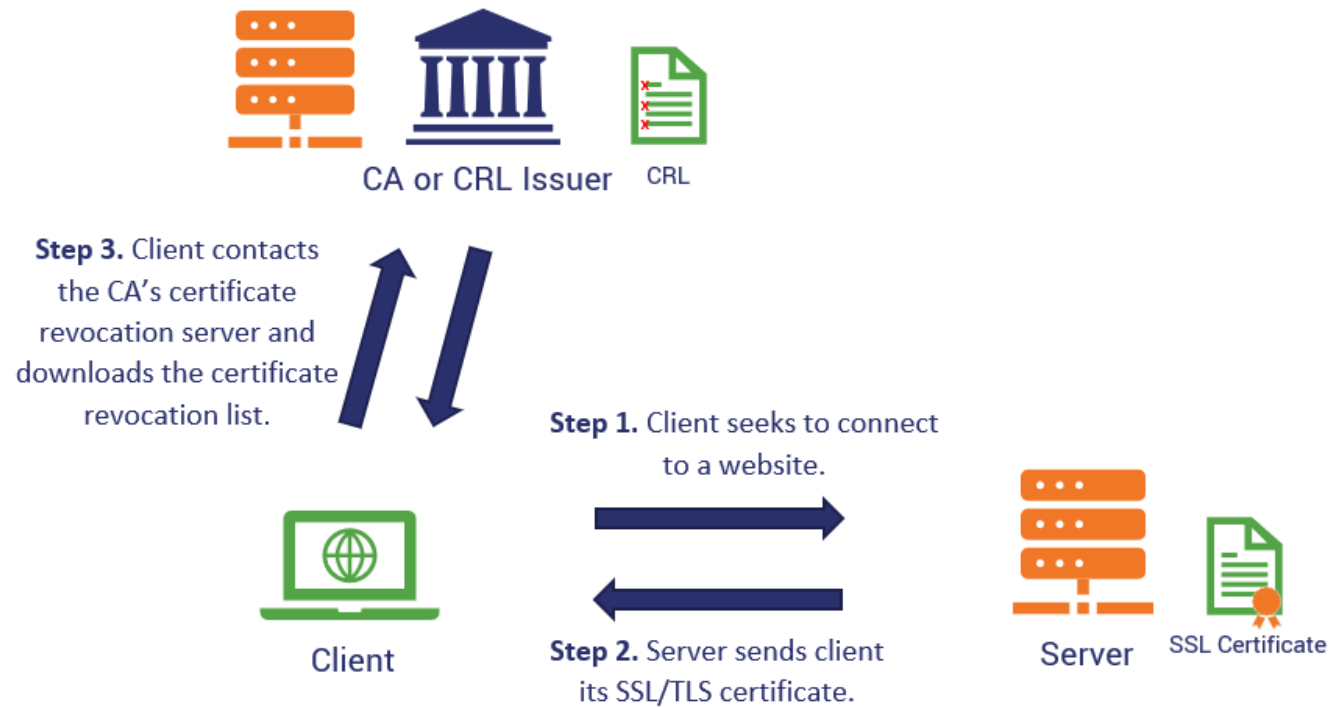


Цифровой сертификат

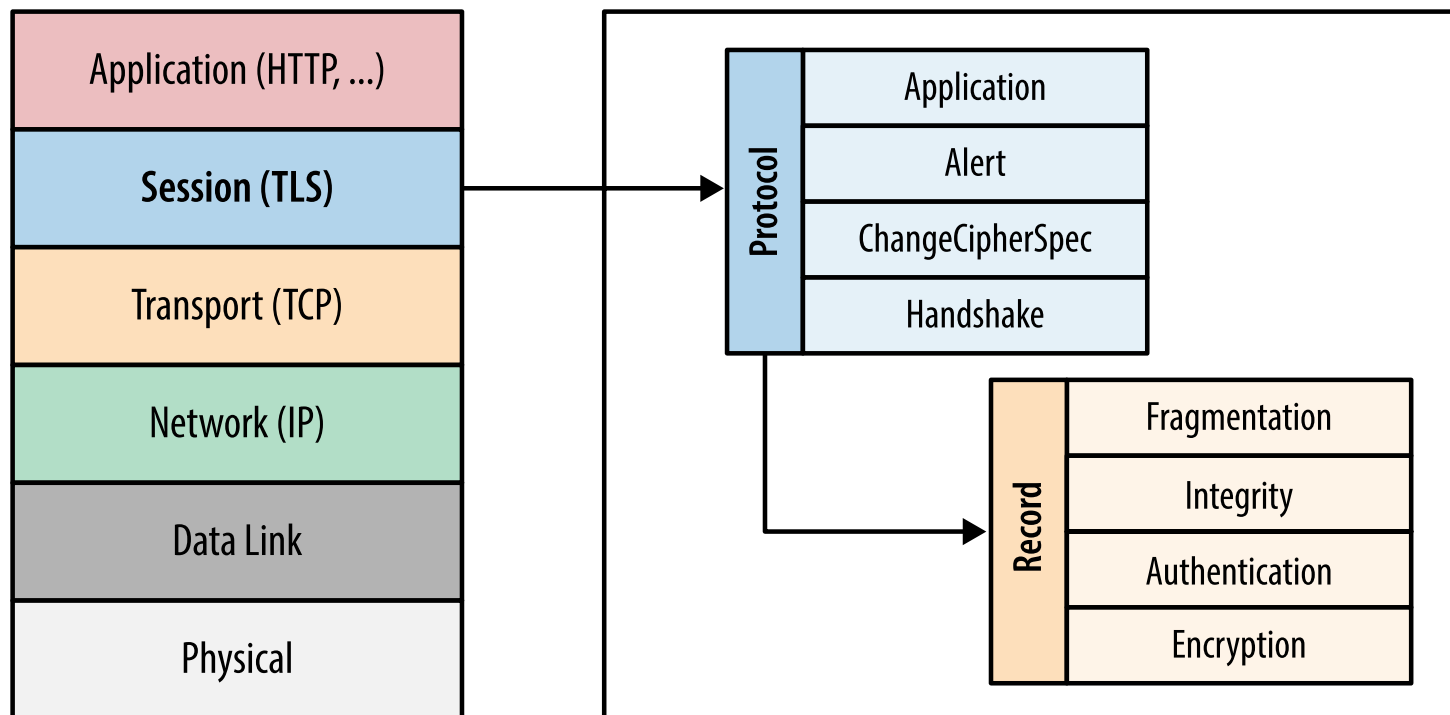


Отзыв сертификата

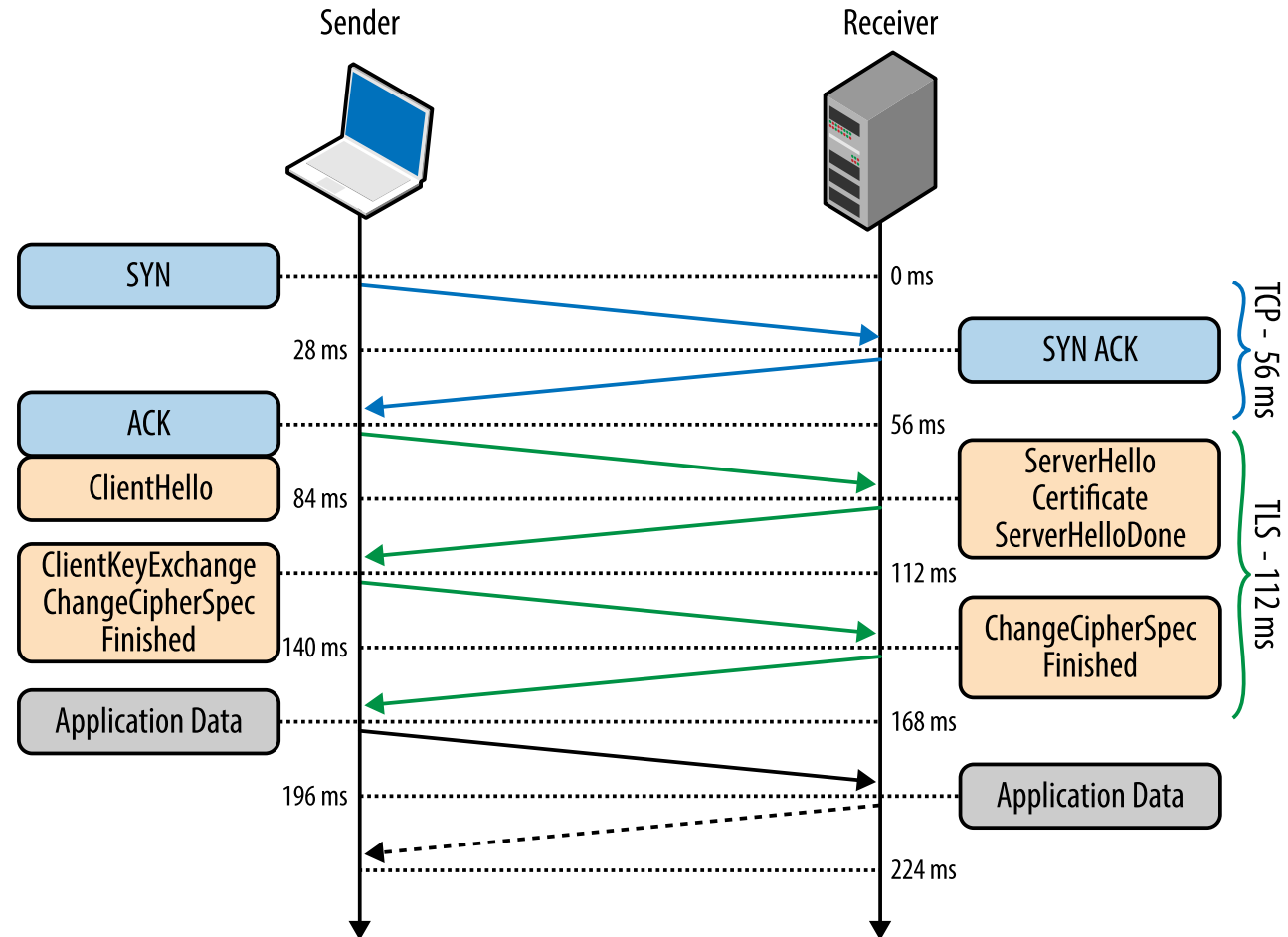
How to Check a Certificate's Revocation Status Using a CRL



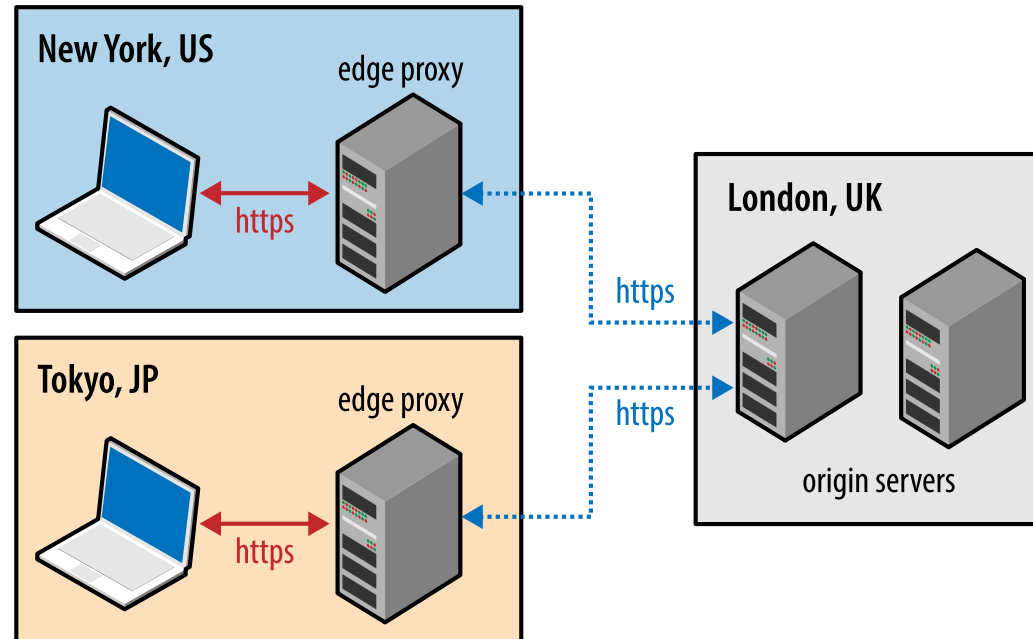
Протокол SSL/TLS



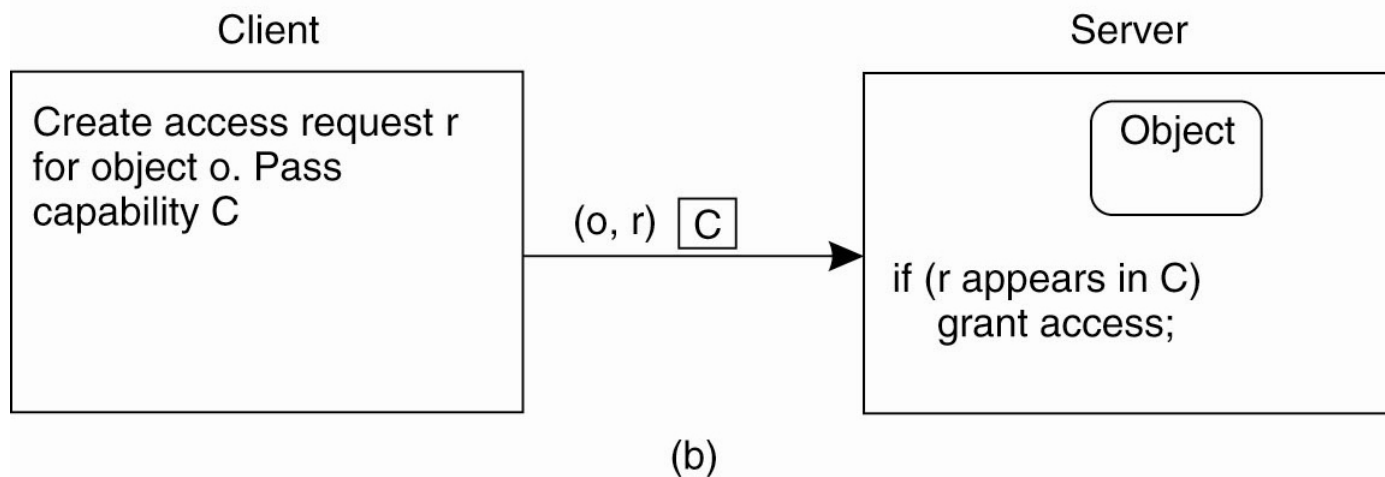
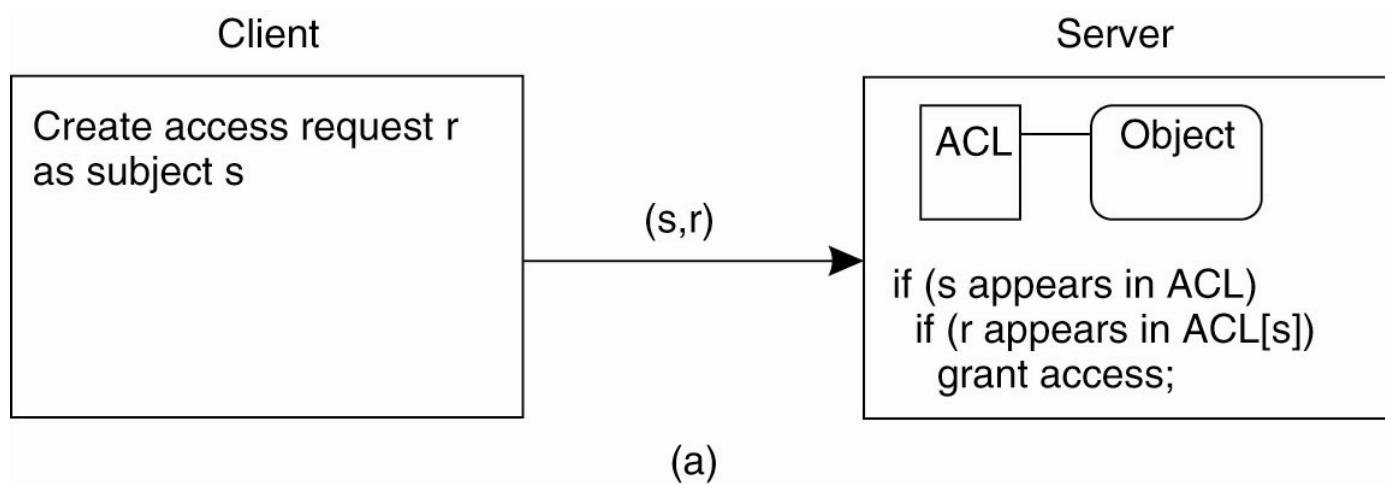
TLS Handshake



TLS Termination и CDN



Авторизация: ACL vs capabilities



Литература

- van Steen M., Tanenbaum A.S. Distributed Systems: Principles and Paradigms (глава 9)
- Coulouris G.F. et al. Distributed Systems: Concepts and Design (глава 11)
- Grigorik I. High Performance Browser Networking (глава 4)