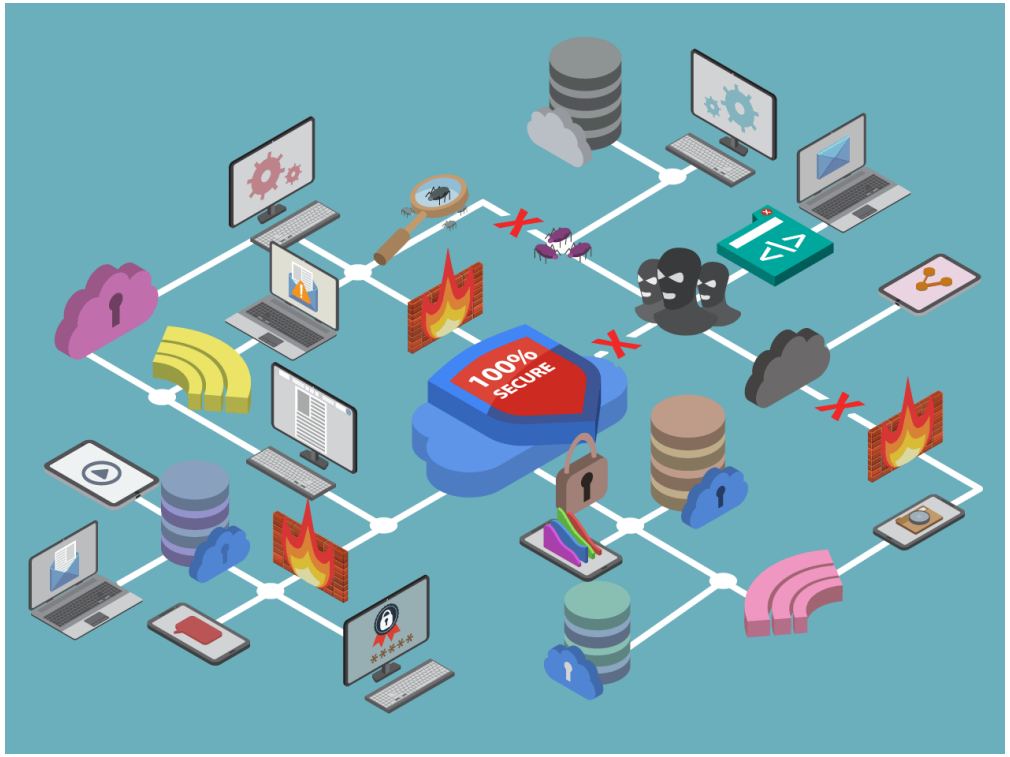
13. Безопасность в распределенных системах

Сухорослов Олег Викторович

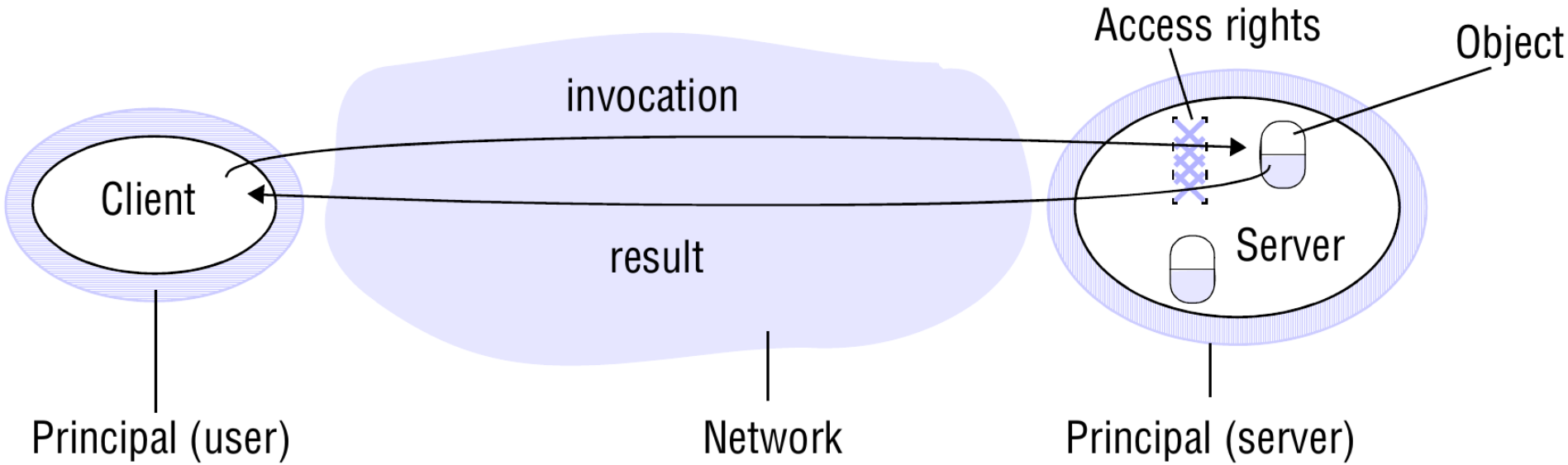
04.12.2023

План лекции

- Требования к безопасности в PC
- Базовые техники и механизмы
  - Шифрование
  - Аутентификация
  - Цифровая подпись
  - Управление ключами
  - Авторизация

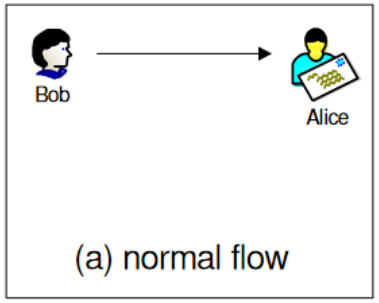


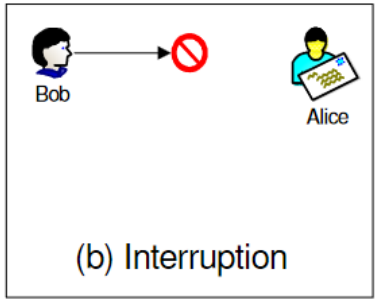
Возможные угрозы?

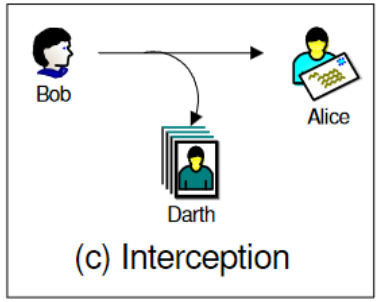


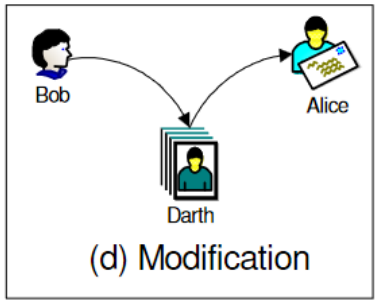
Угрозы

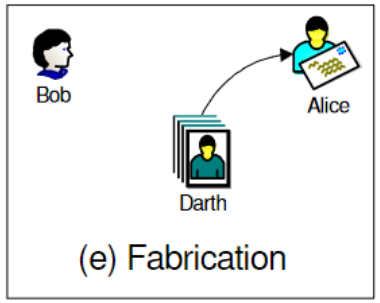
- **Interception**
  несанкционированный доступ к данным
- **Modification**
  несанкционированное изменение данных
- **Fabrication**
  вставка поддельных данных и действий
- **Interruption**
  нарушение доступности системы





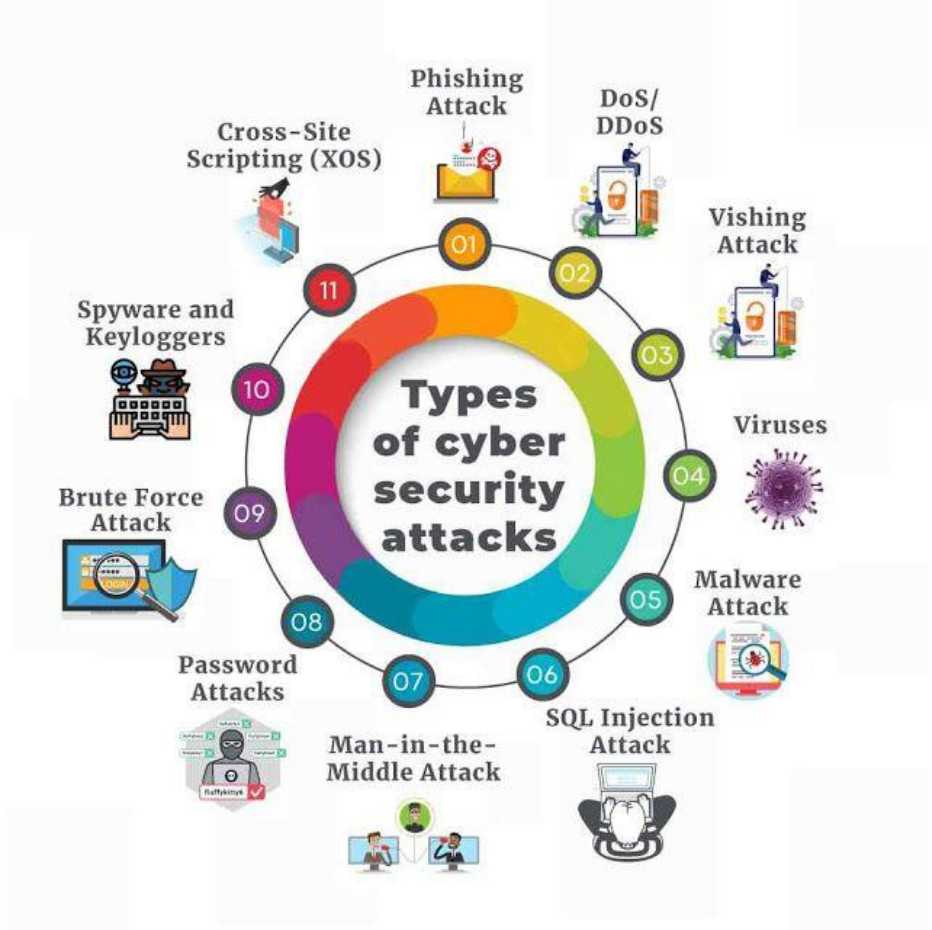






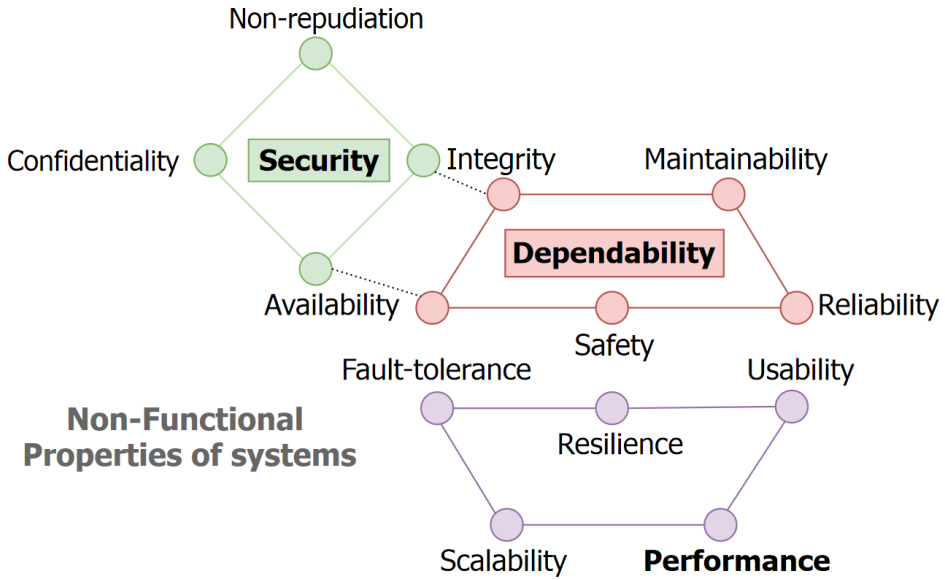
Атаки

- 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

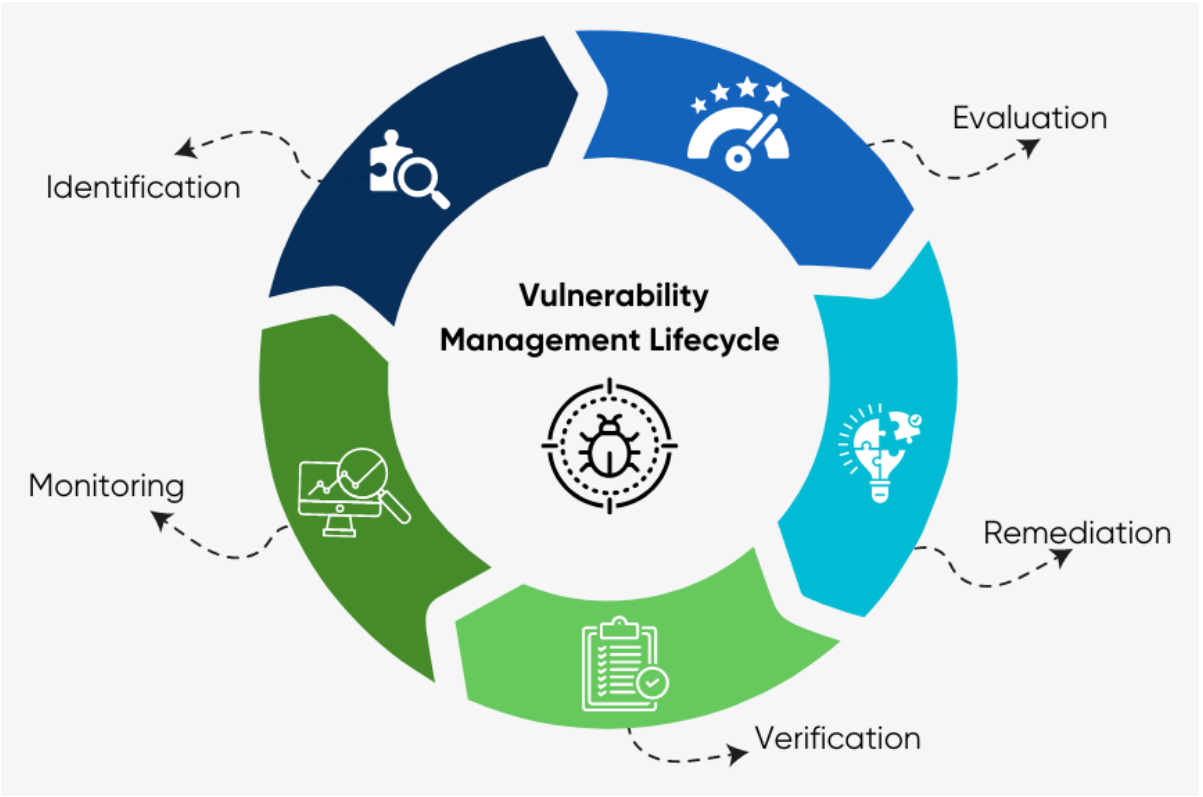
- Конфиденциальность
- Целостность
- Доступность
- Невозможность отказа
- Аутентификация
- Авторизация
- Масштабируемость



[Introduction to Performance Evaluation of Systems]

Методика

- Анализ угроз
- Предотвращение угроз
- Валидация
- Аудит



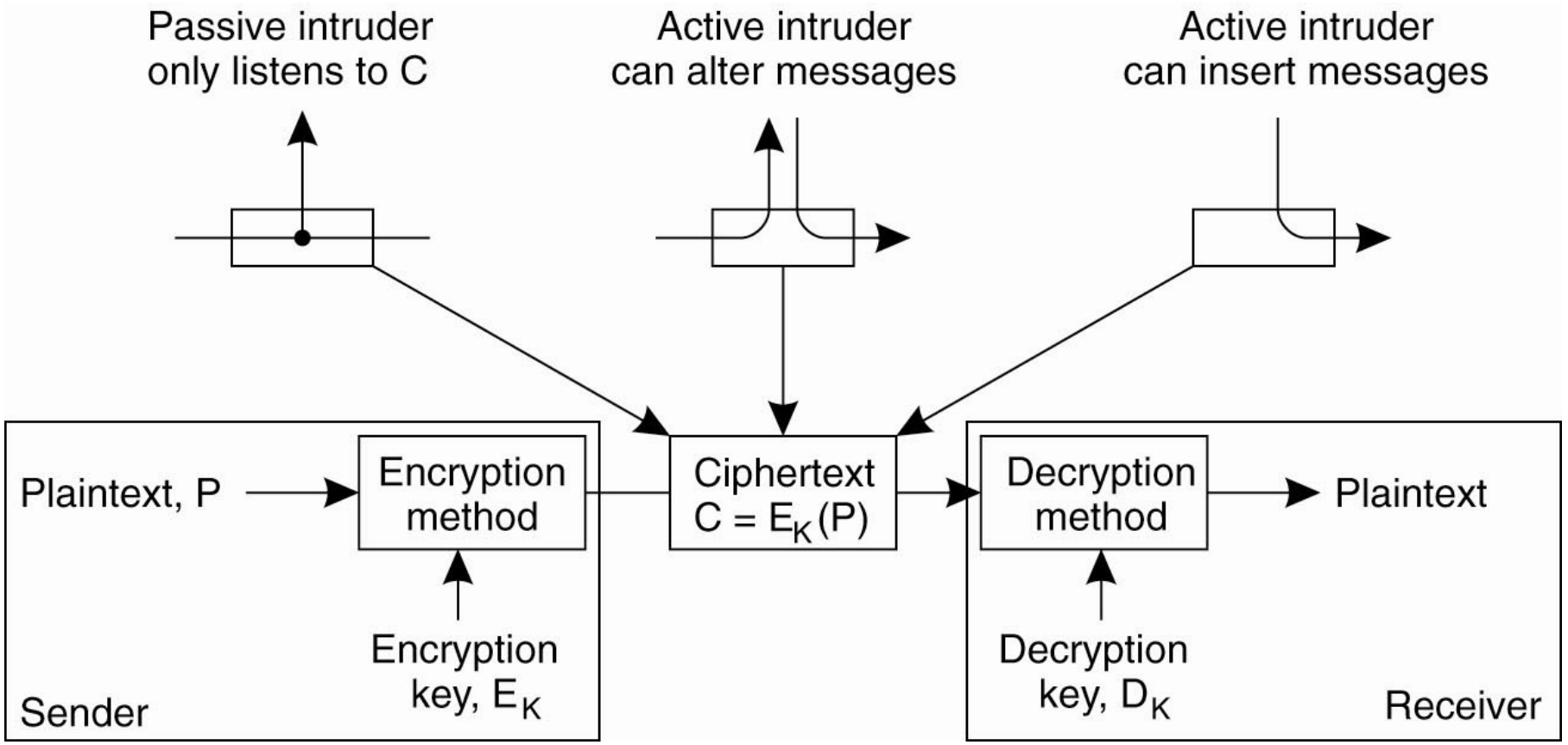
Предположения и принципы

- Интерфейсы доступны всем
- Сети сами по себе не обеспечивают безопасность
- 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...

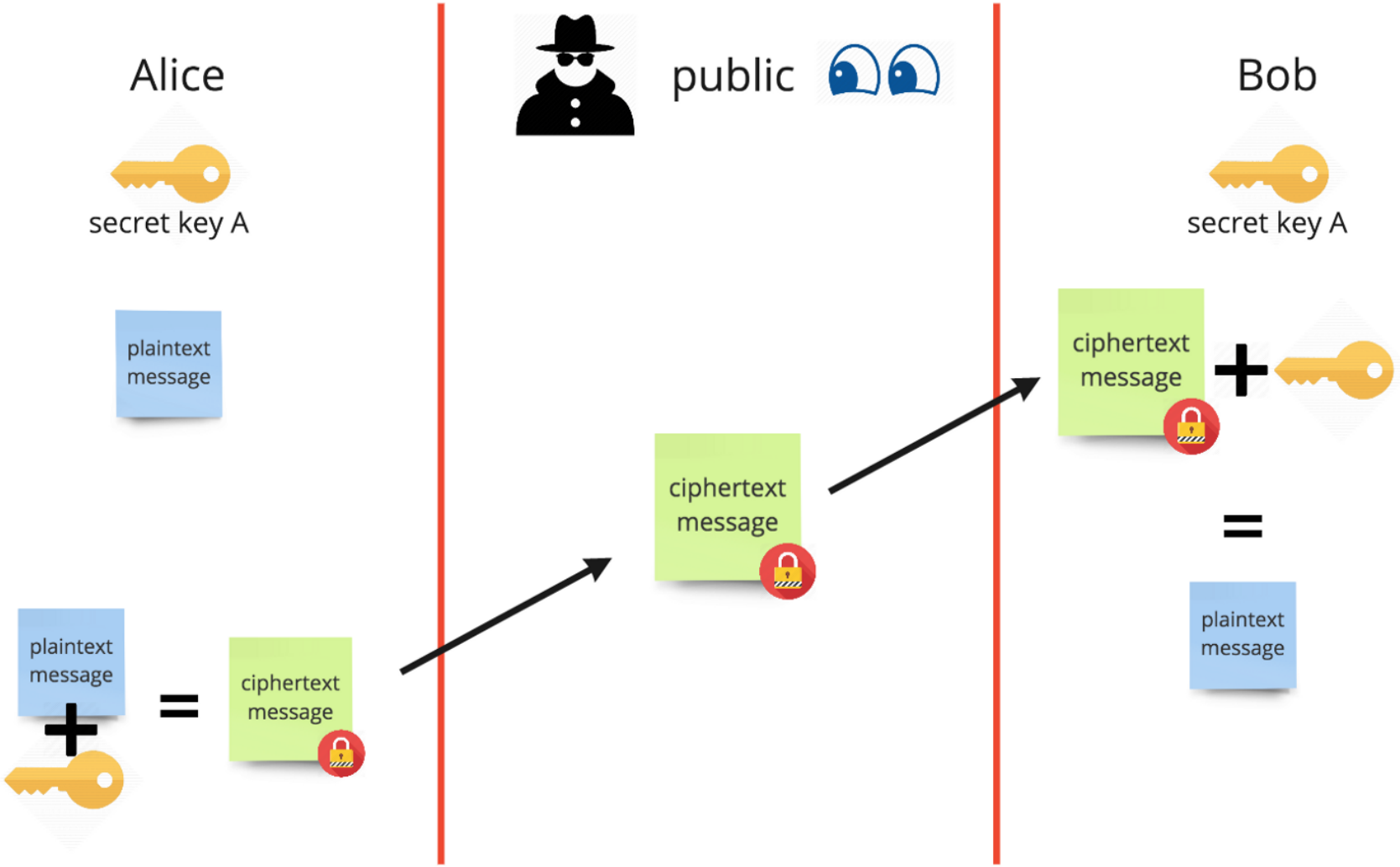
Шифрование


Passive intruder
only listens to C
Active intruder
can alter messages
Active intruder
can insert messages
Plaintext, P
Encryption
method
Encryption
key, E_K
Sender
Ciphertext
$C = E_K(P)$
Decryption
method
Decryption
key, D_K
Plaintext
Receiver

Шифрование

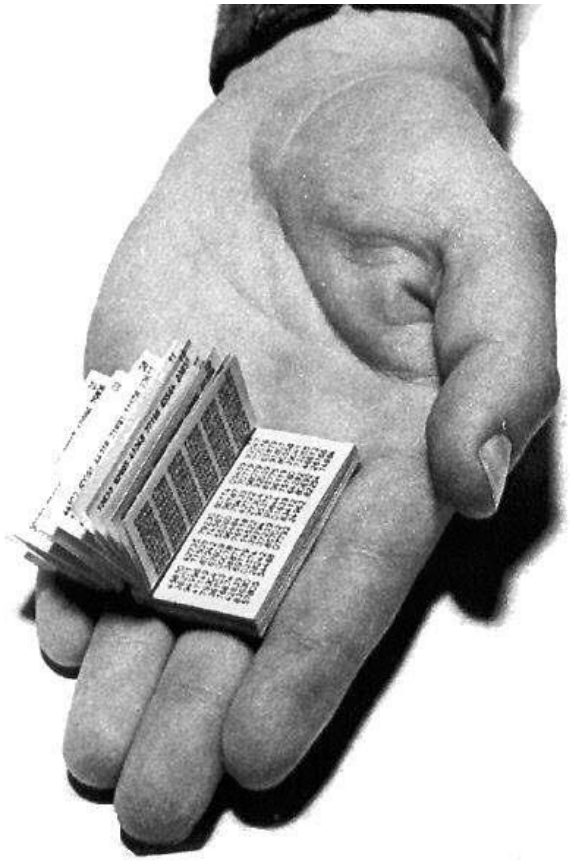
- Симметричное (secret-key, shared-key)
  - $P = D_K(E_K(P))$
  - $K_{A,B}$ – ключ, используемый A и B
  - Блочные шифры (DES, 3DES, TEA, IDEA, Blowfish, Twofish, AES)
  - Поточные шифры (RC4)
- Асимметричное (public-key)
  - $P = D_{K_D}(E_{K_E}(P))$
  - K_A^+ – открытый ключ A
  - K_A^- – закрытый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

Симметричное шифрование

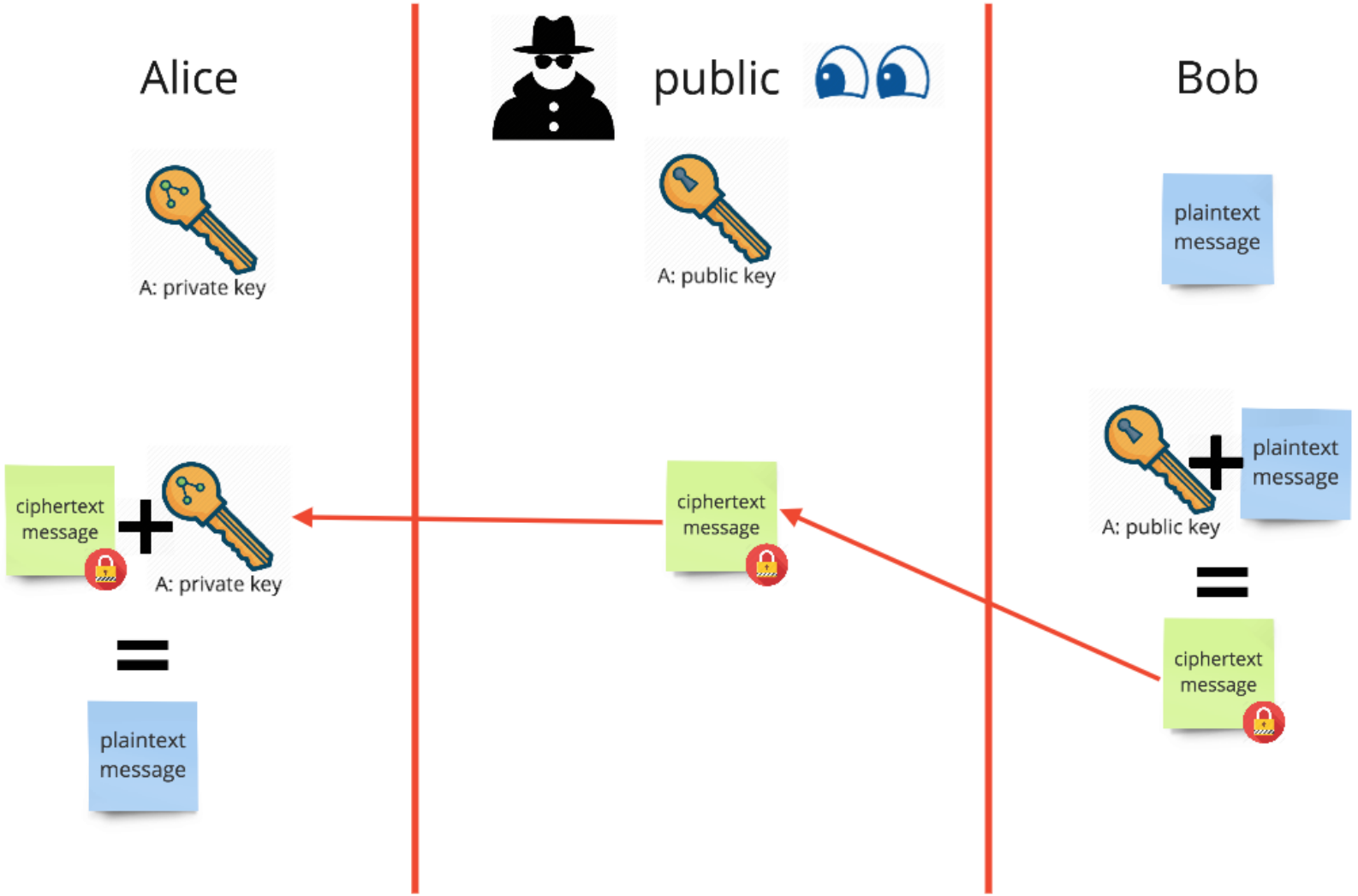


Шифр Вернама (одноразовый блокнот)

Plain text:	**H**	**O**	**W**	**A**	**R**	**E**	**Y**	**O**	**U**
	7	14	22	0	17	4	24	14	20
+									
OTP:	**13**	**2**	**1**	**19**	**25**	**16**	**0**	**17**	**23**
	N	C	B	T	Z	Q	A	R	X
Initial total:	**20**	**16**	**23**	**19**	**42**	**20**	**24**	**31**	**43**
Mod 26:	**20**	**16**	**23**	**19**	**16**	**20**	**24**	**5**	**17**
Ciphertext:	**U**	**Q**	**X**	**T**	**Q**	**U**	**Y**	**F**	**R**



Шифрование с открытым ключом



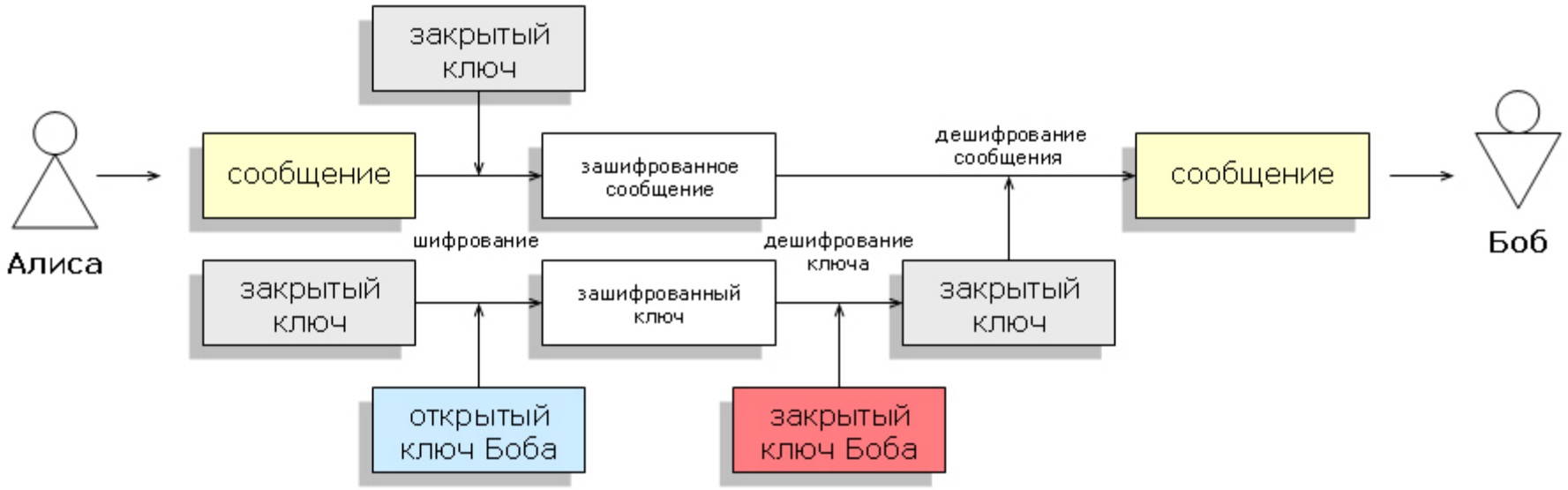
Односторонние функции

- Разложение больших чисел на простые множители
  - RSA (Rivest-Shamir-Adleman)
- Дискретное логарифмирование в конечном поле
  - Криптосистема Эль-Гамаля
- Вычисление корней алгебраических уравнений (на основе эллиптических уравнений)
  - ECDSA (Elliptic Curve Digital Signature Algorithm)

Сравнение

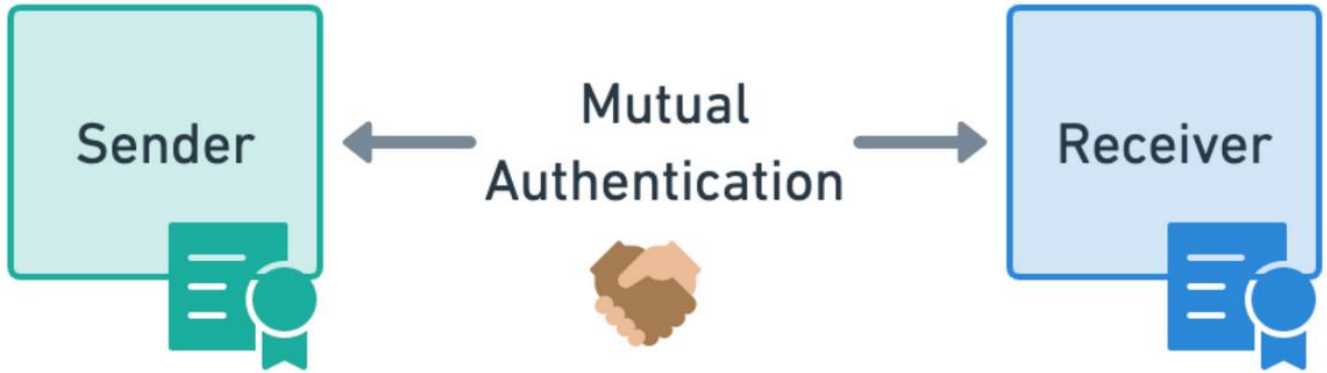
- Симметричное шифрование
  - Требуется распространение ключа по защищенному каналу
  - Для каждой пары участников нужен отдельный ключ
  - В системе из N участников требуется $N(N-1)/2$ ключей
- Шифрование с открытым ключом
  - Требуется механизм распространения и проверки открытых ключей
  - В системе из N участников требуется N пар ключей
  - Более длинные ключи и значительно большее (x10-100) время работы

Гибридная схема

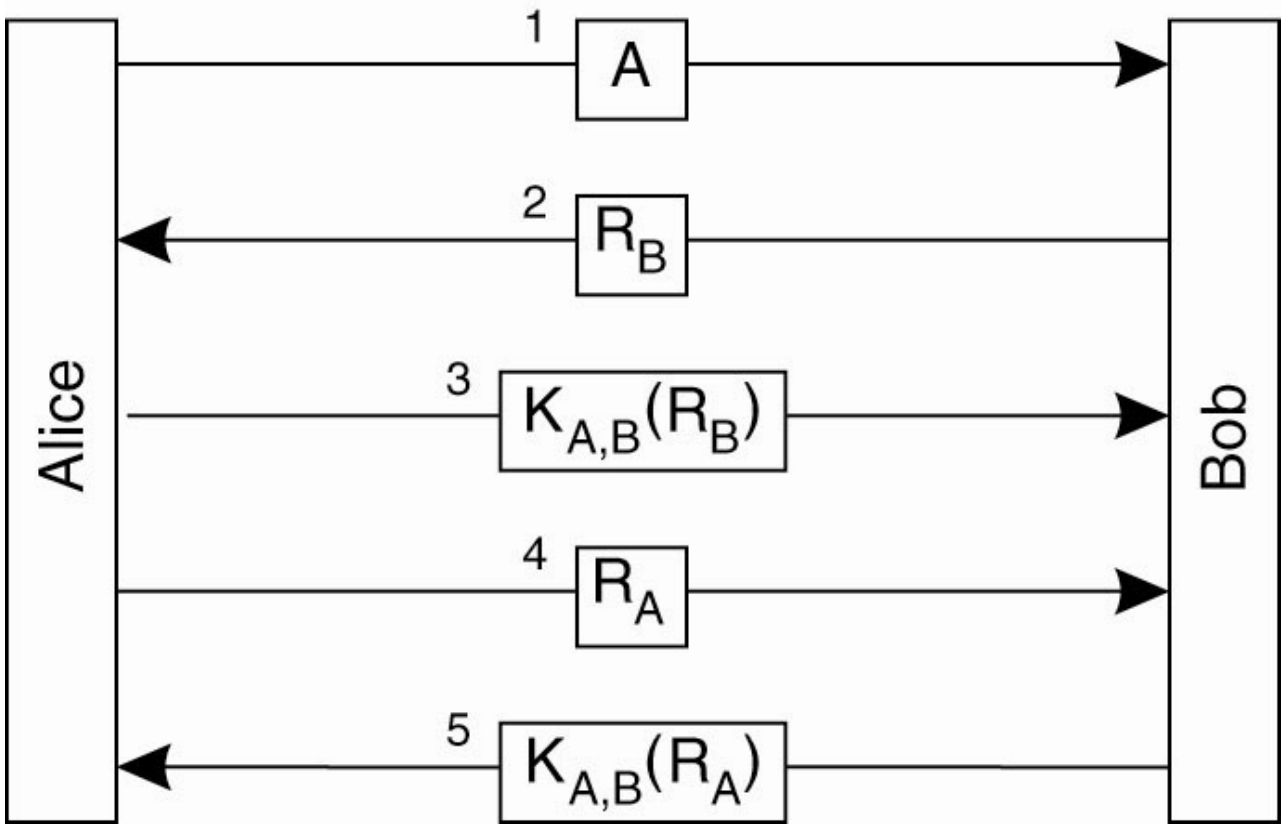


Аутентификация

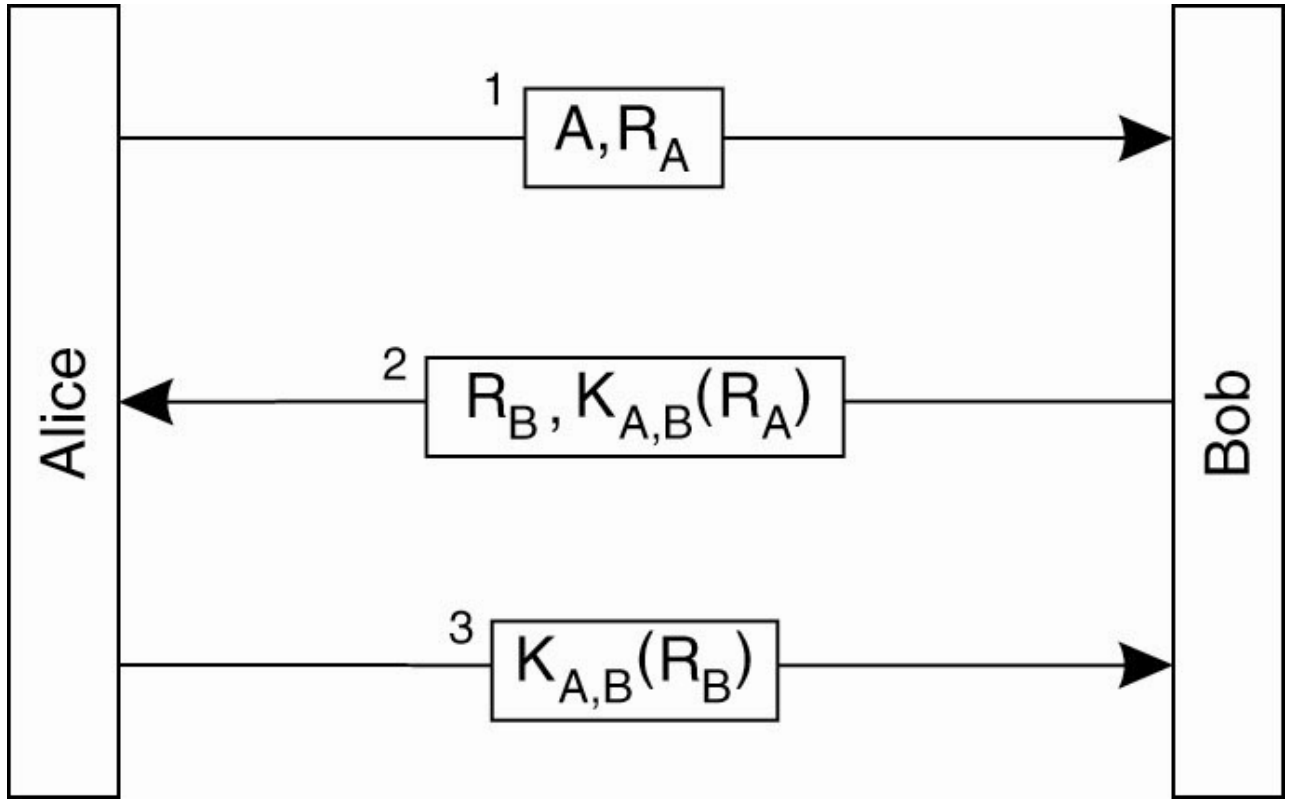
- В начале взаимодействия стороны должны убедиться в подлинности друг друга
- После взаимной аутентификации между ними может быть установлен защищенный канал с использованием шифрования



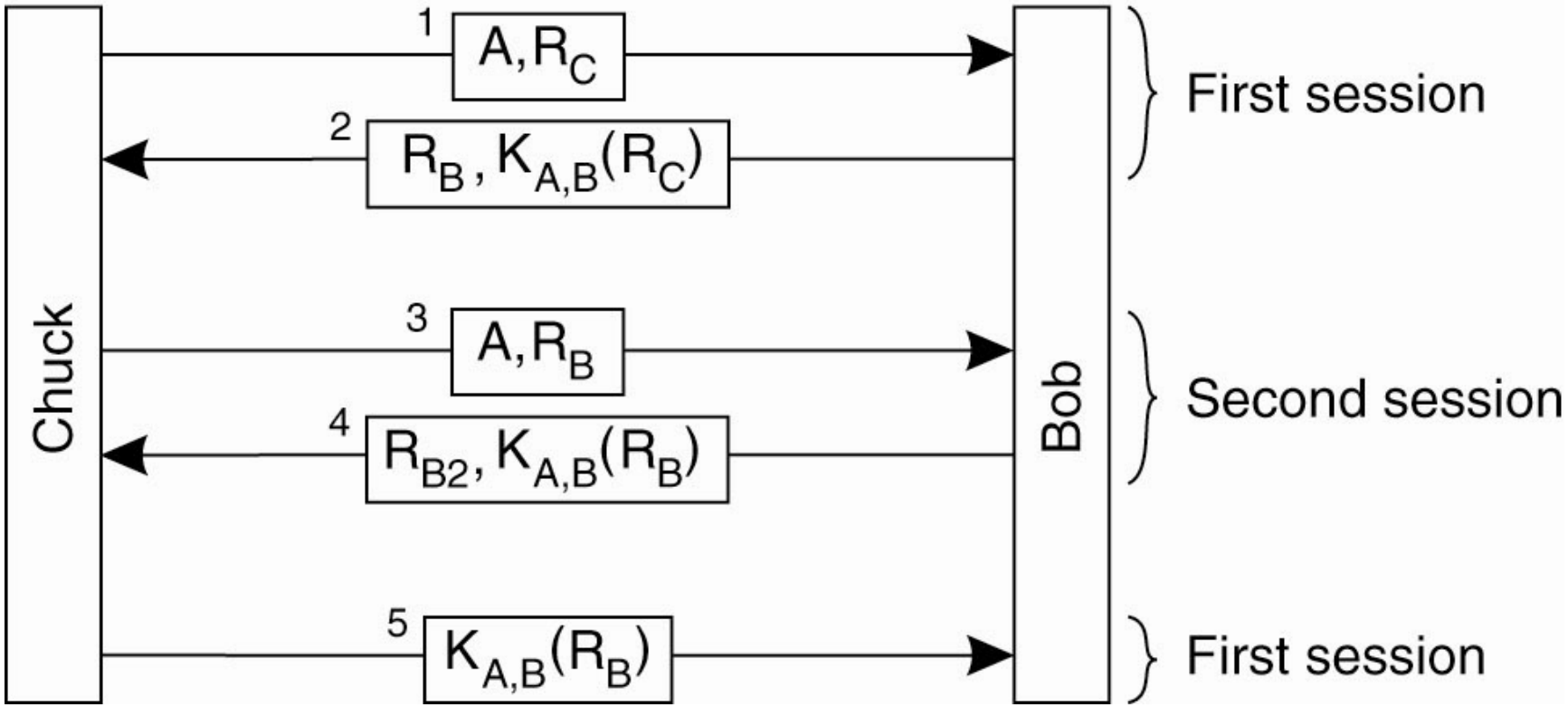
Аутентификация (shared key)



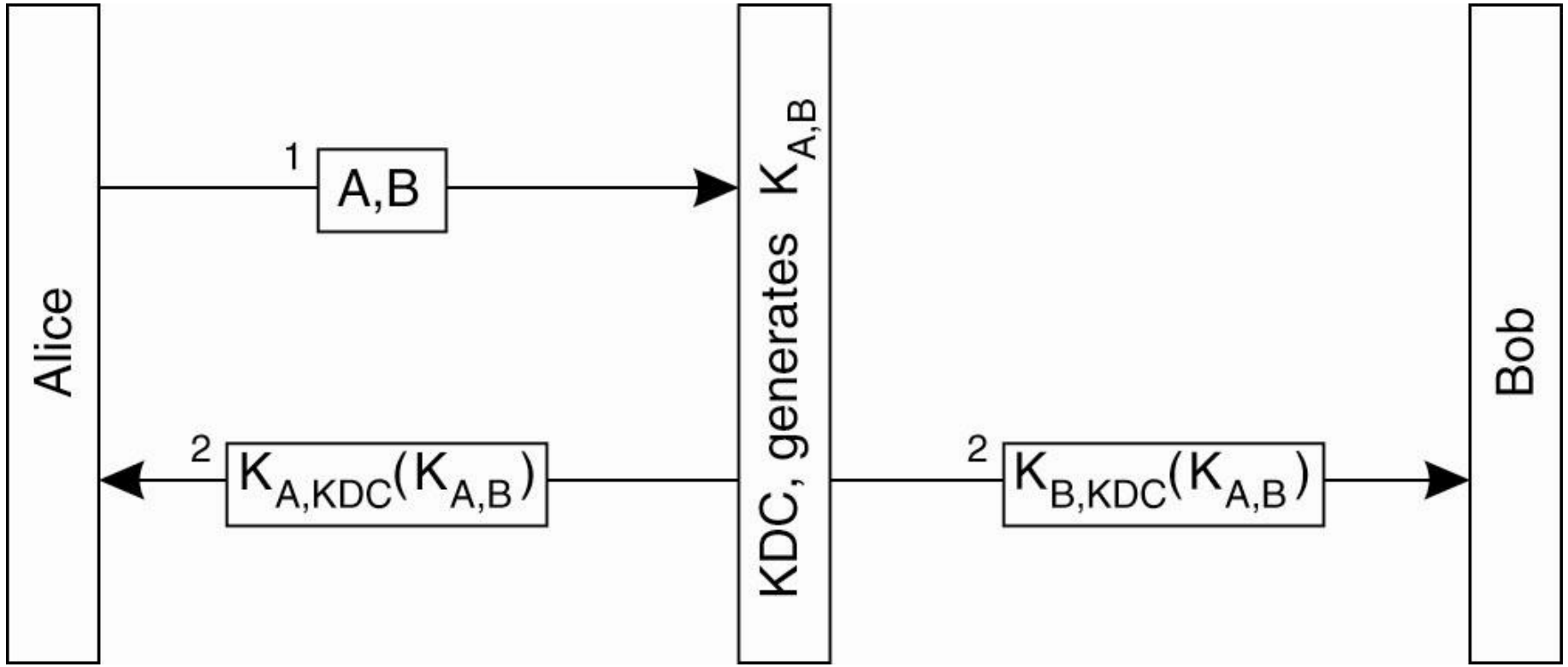
Оптимизация?



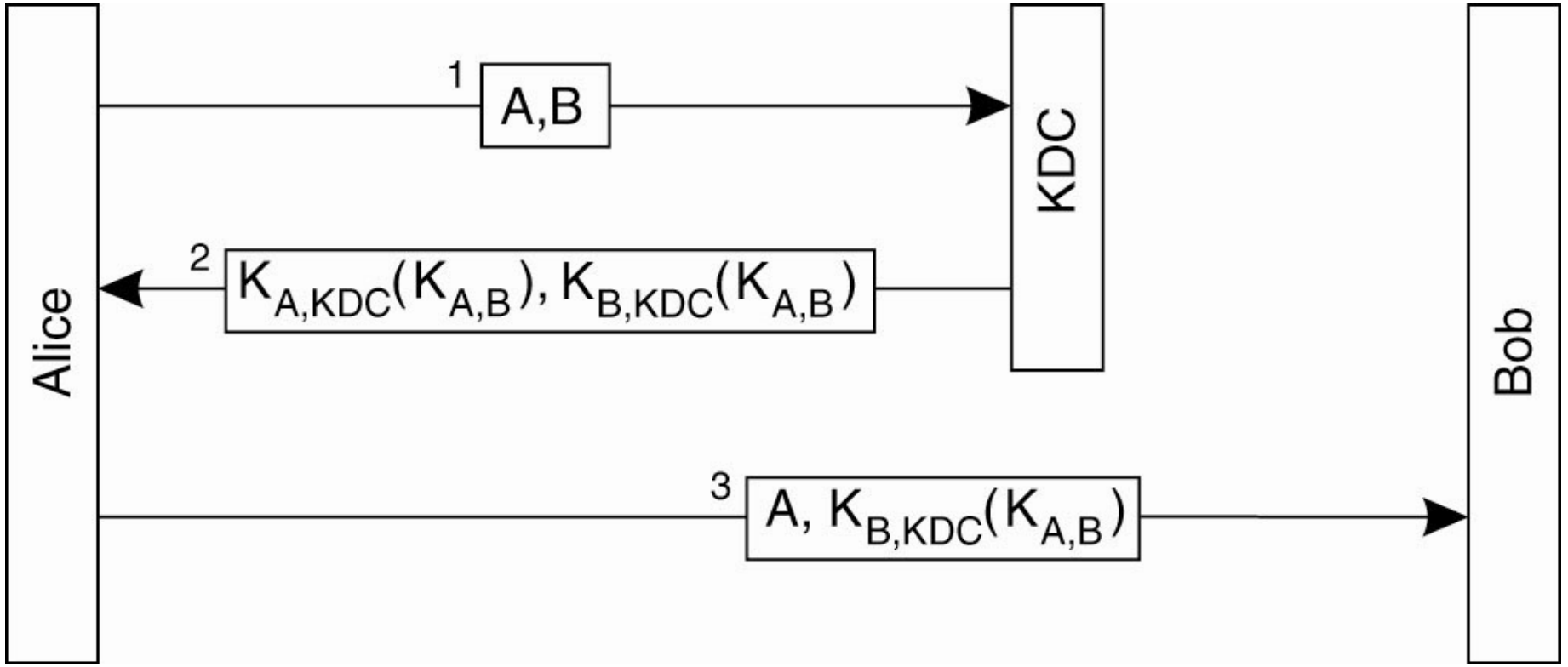
Reflection Attack



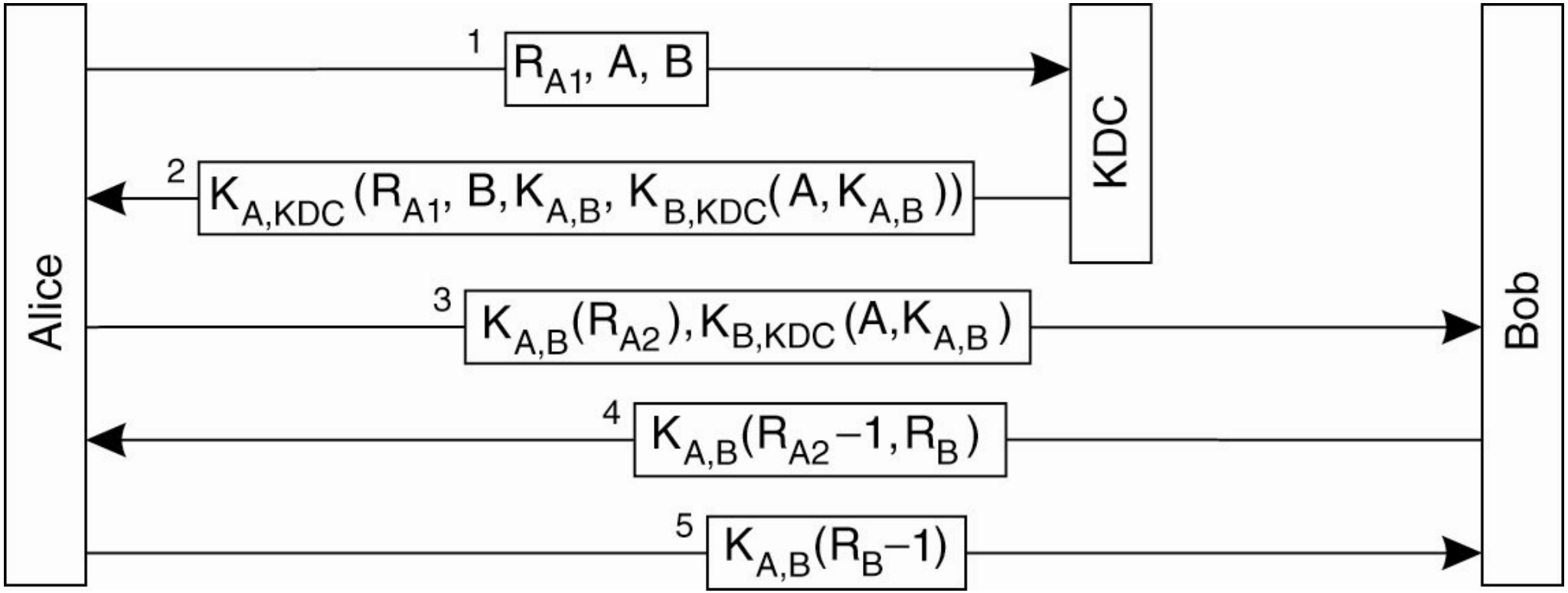
Key Distribution Center



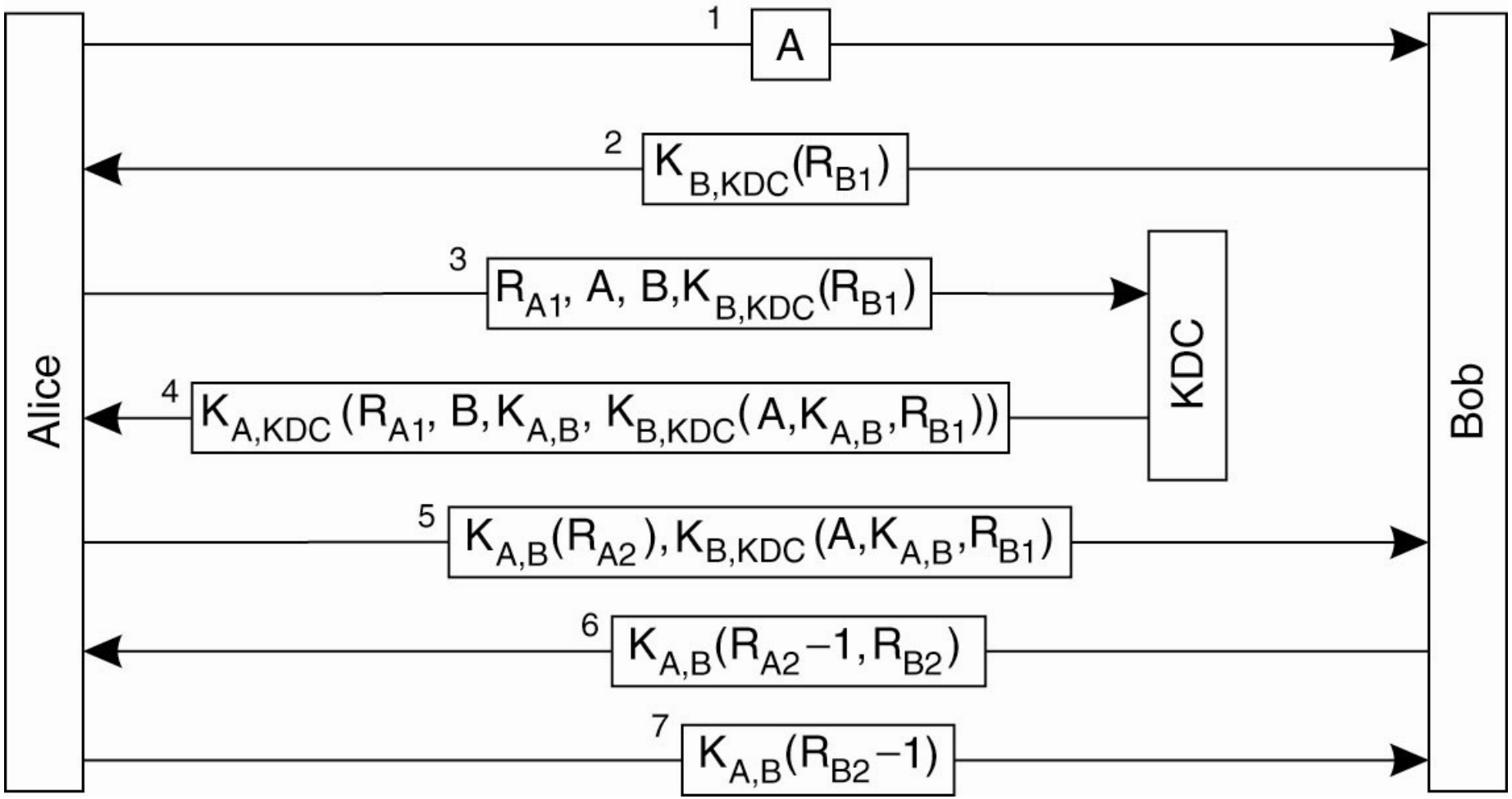
Key Distribution Center + Ticket



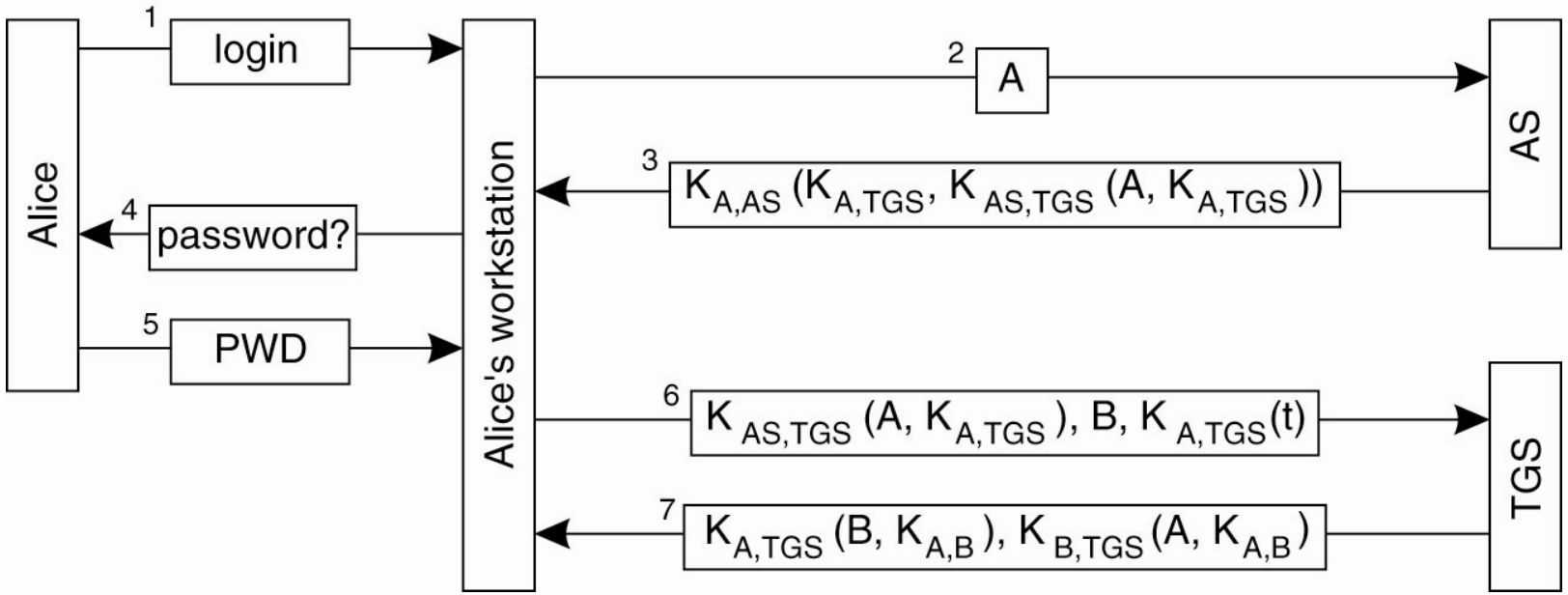
Протокол Нидхема-Шрёдера

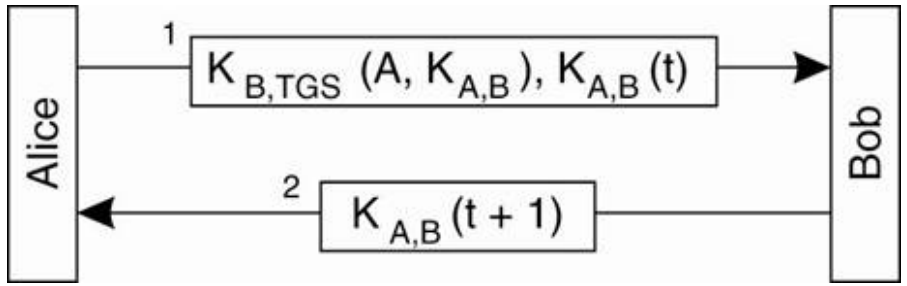


Протокол Нидхема-Шрёдера (fixed)

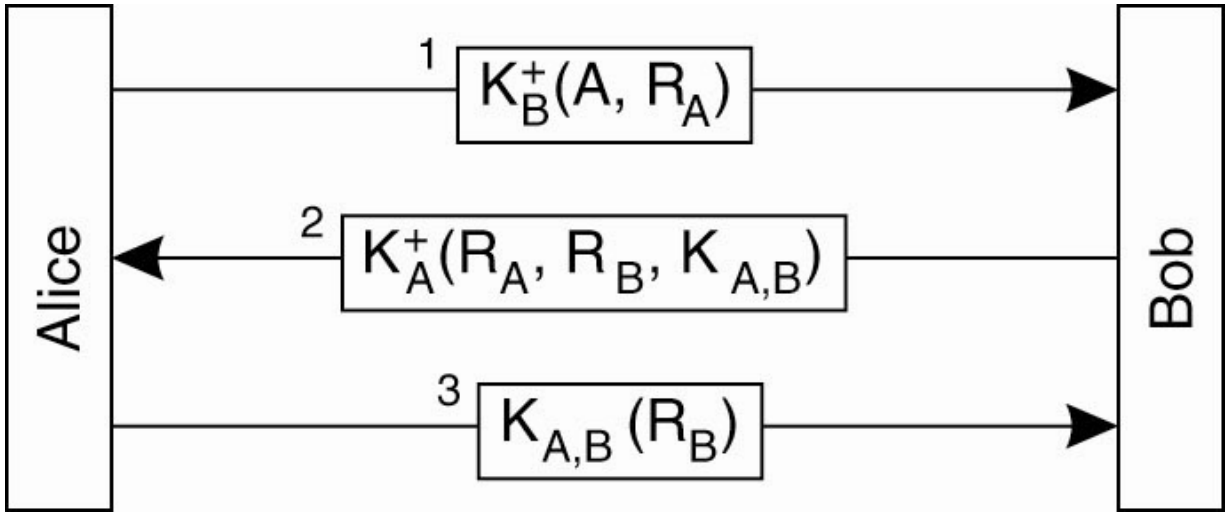


Single Sign-on (Kerberos)





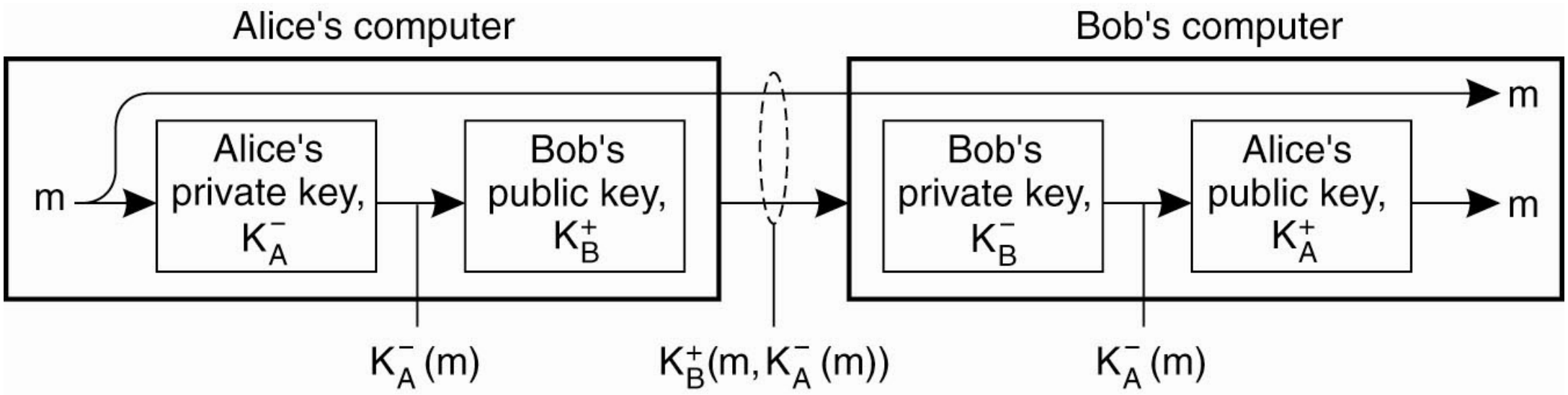
Аутентификация (public key)



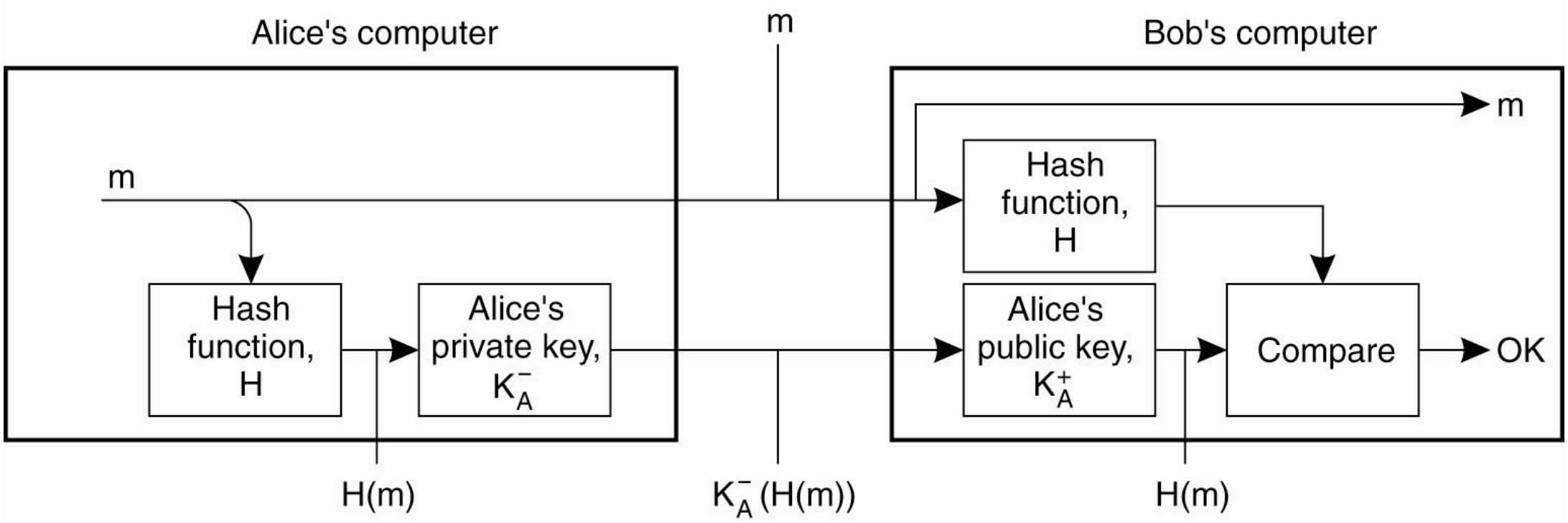
Цифровая подпись

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

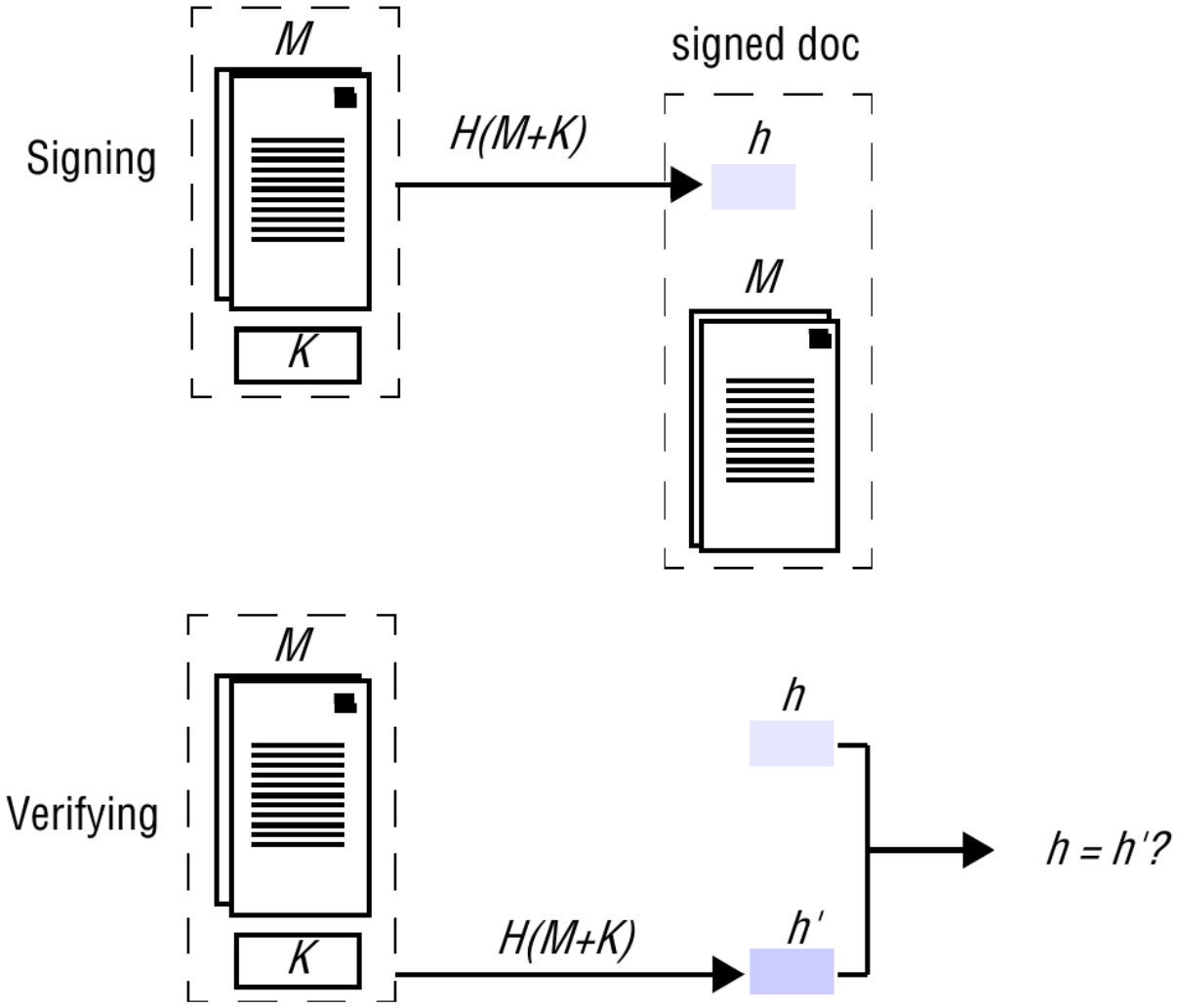
Подпись (шифр. с открытым ключом)



Подпись (message digest)



Message Authentication Code (MAC)



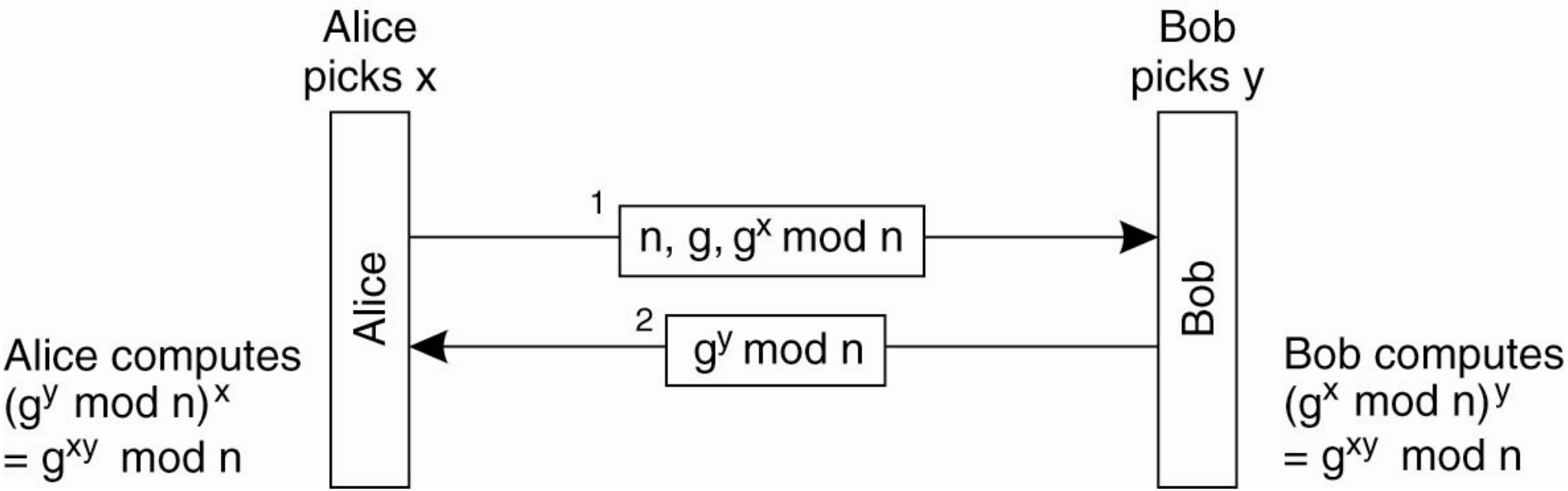
Хеширование

- 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

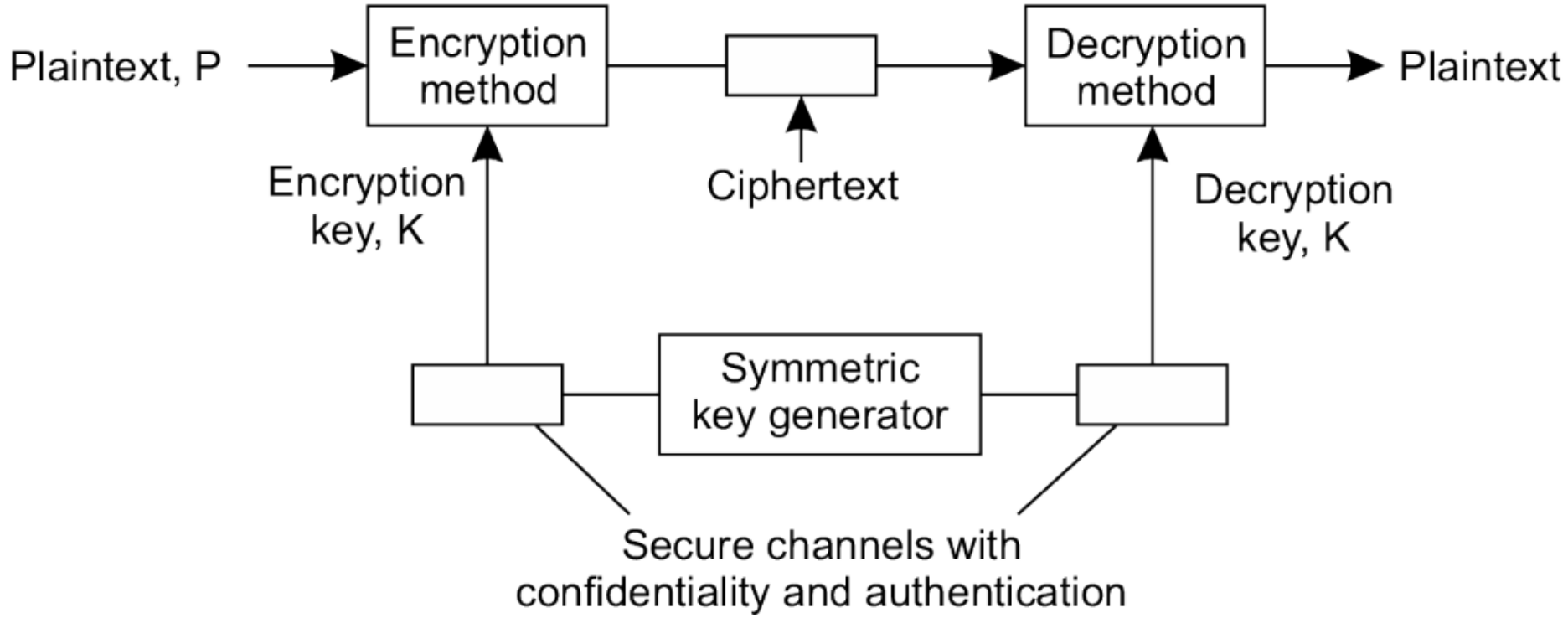
Управление ключами

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

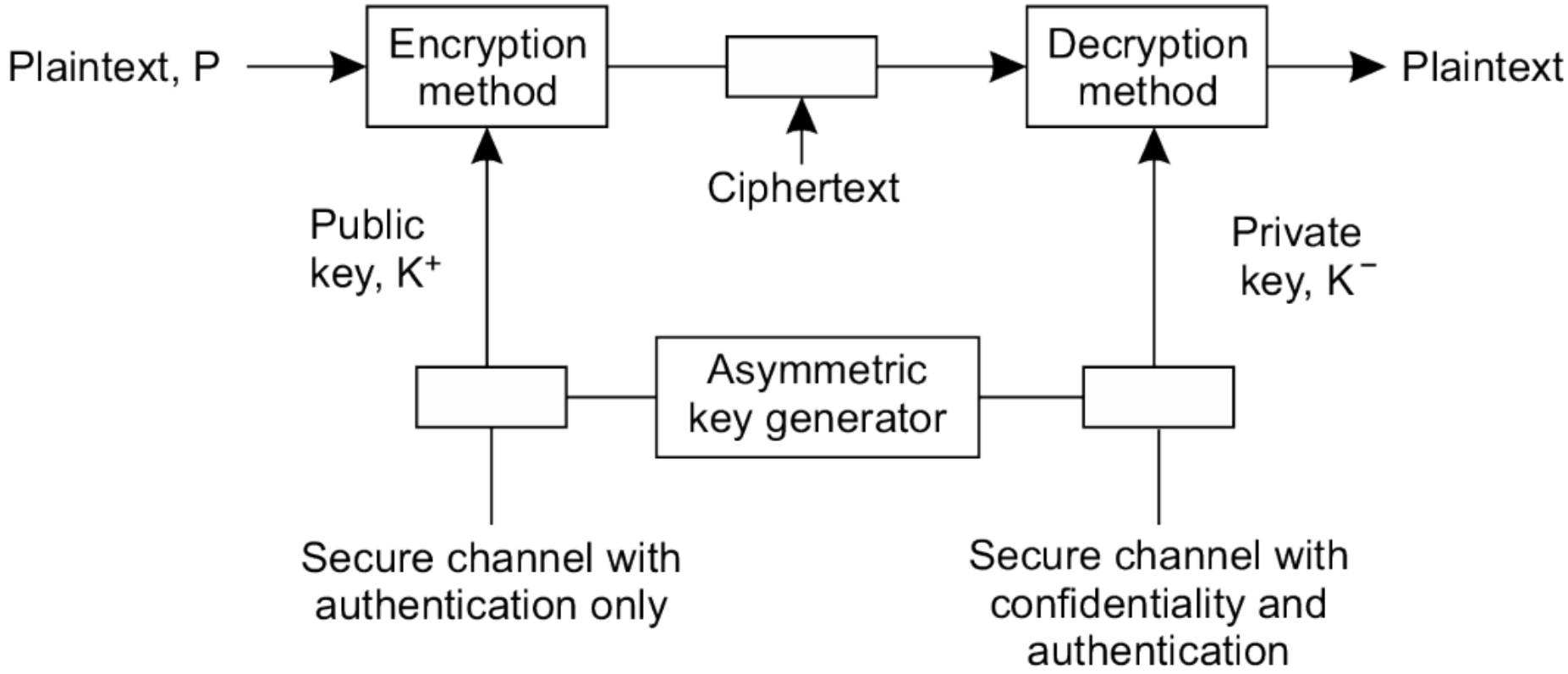
Получение общего ключа (Diffie-Hellman)



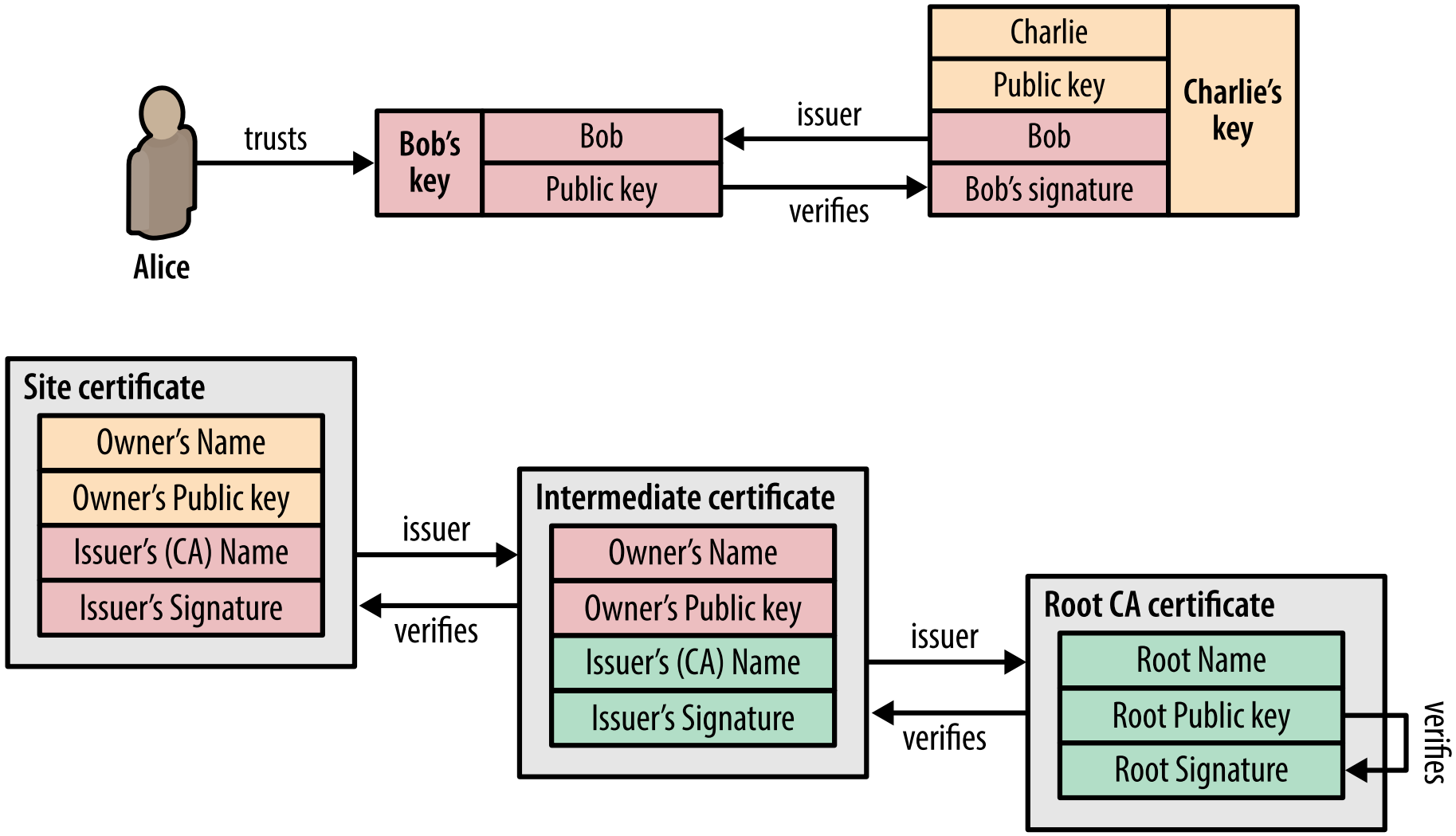
Распространение ключей (shared)



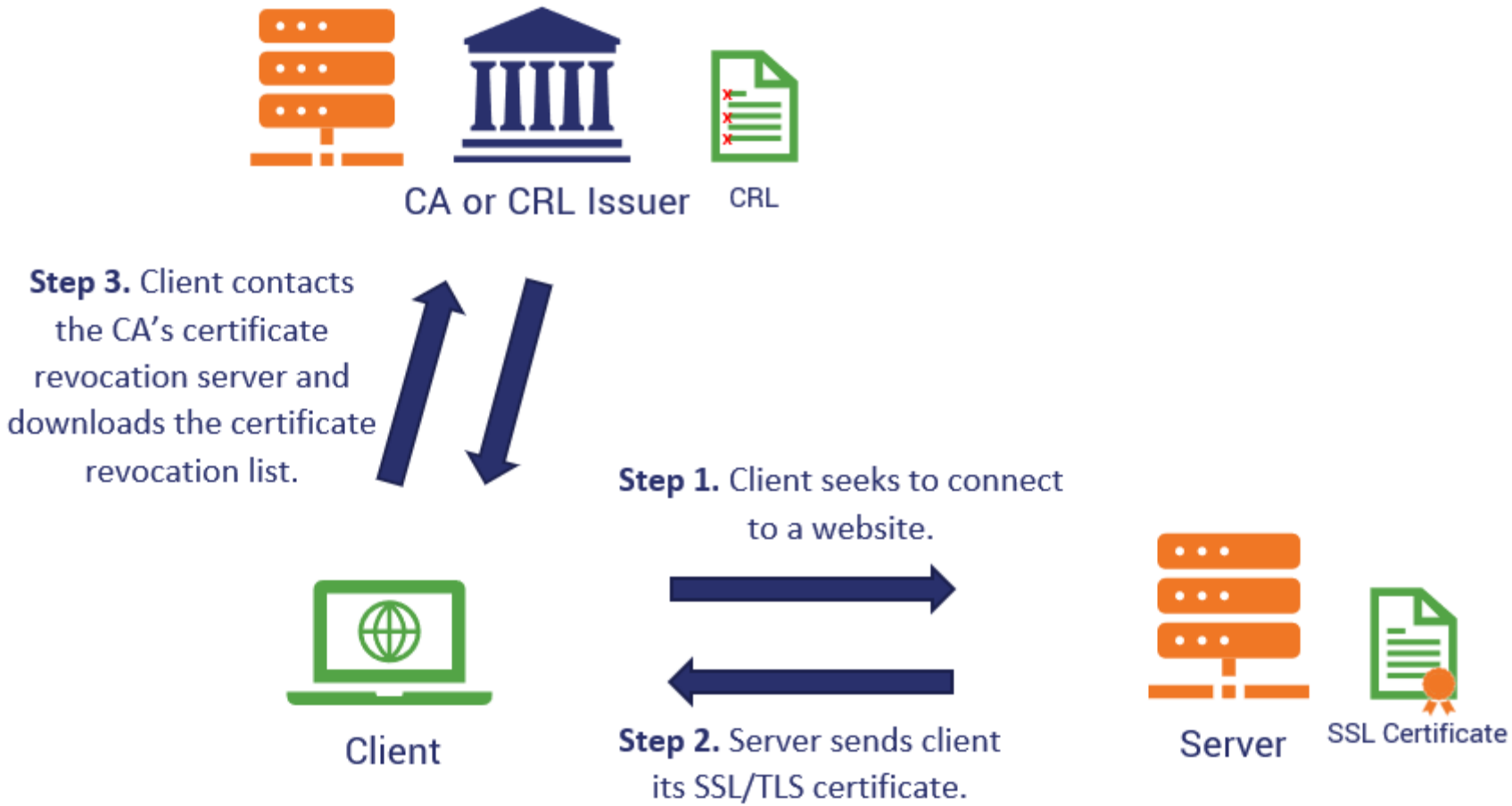
Распространение ключей (public/private)



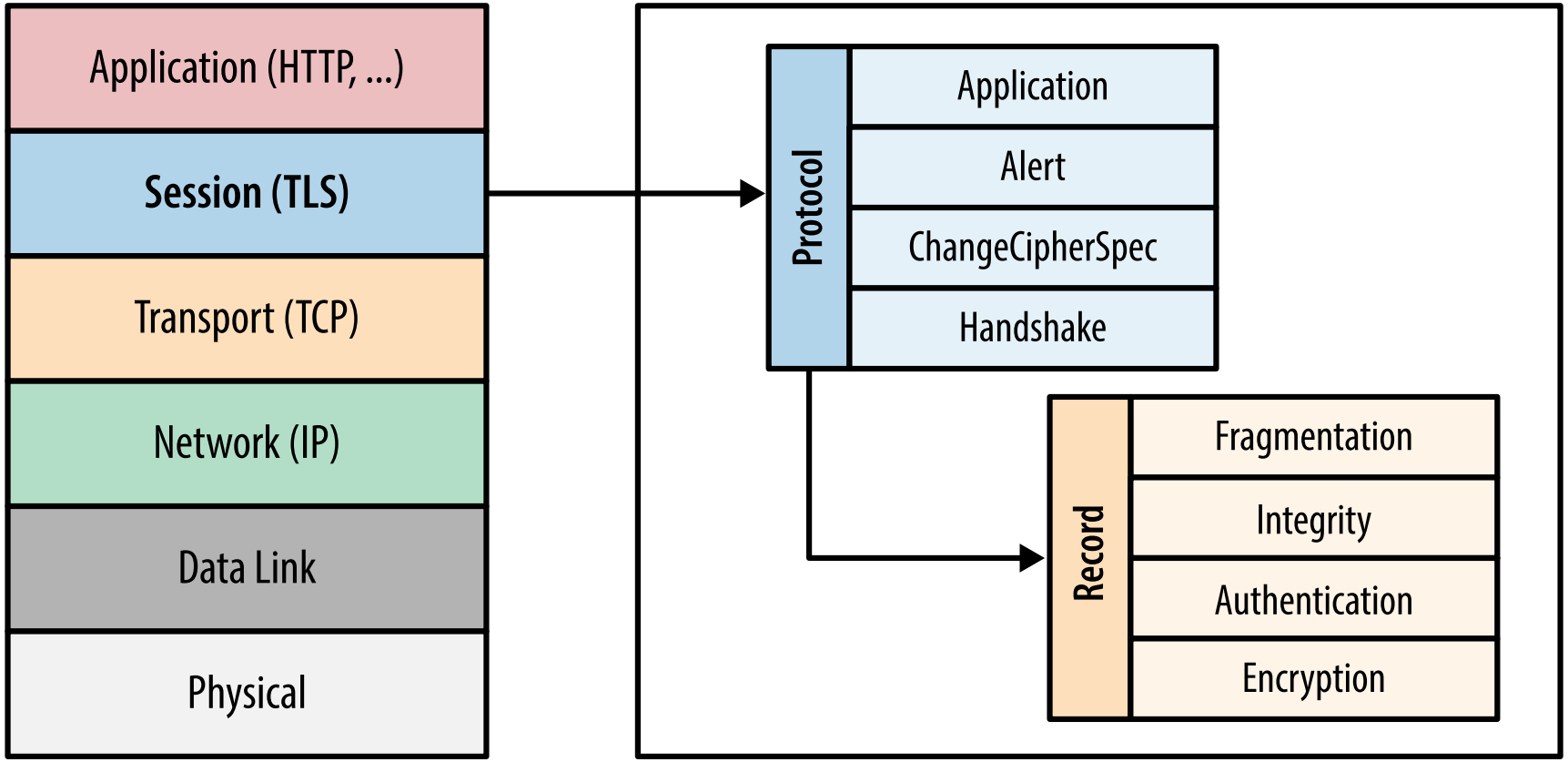
Цифровой сертификат



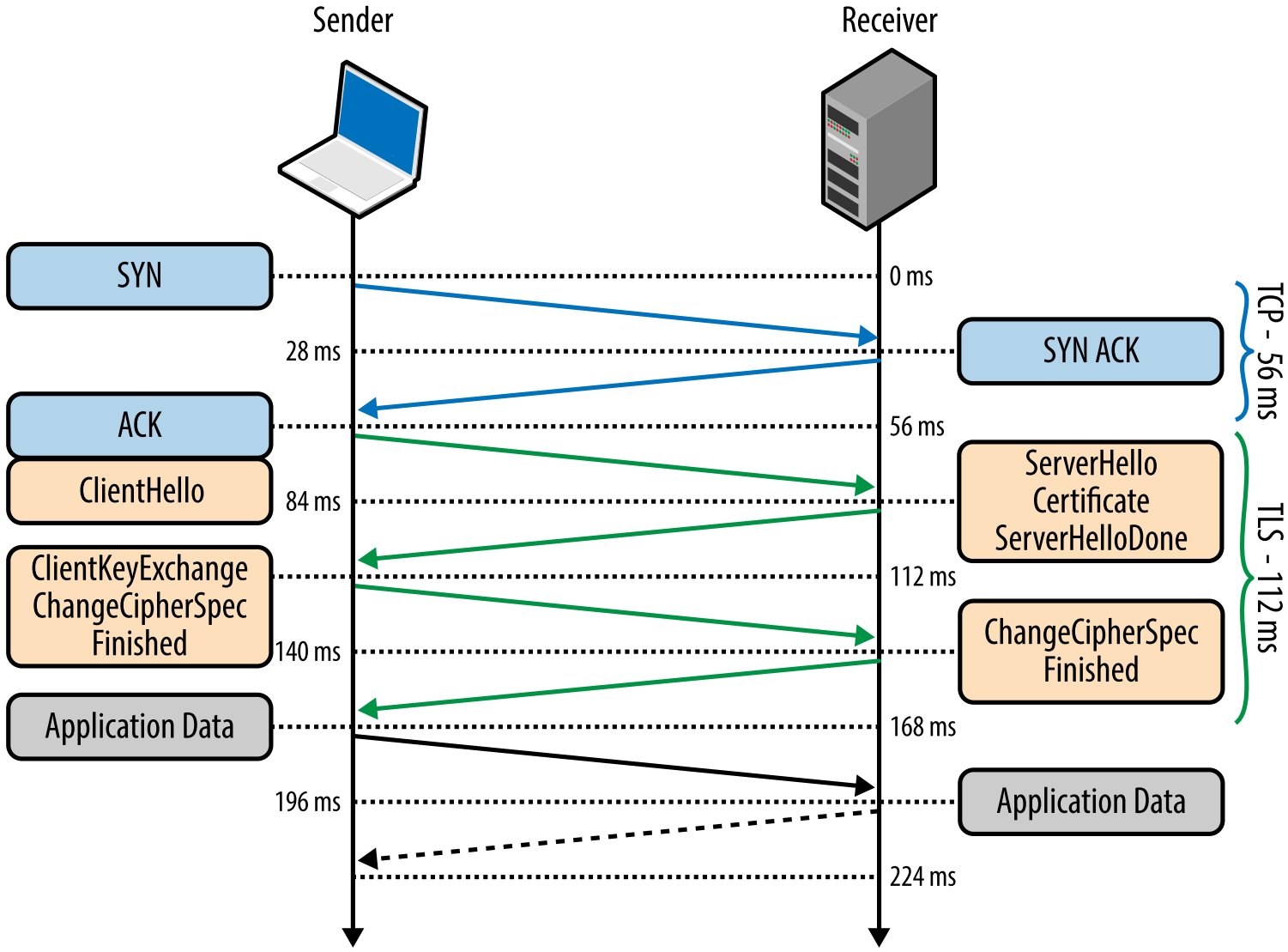
Отзыв сертификата



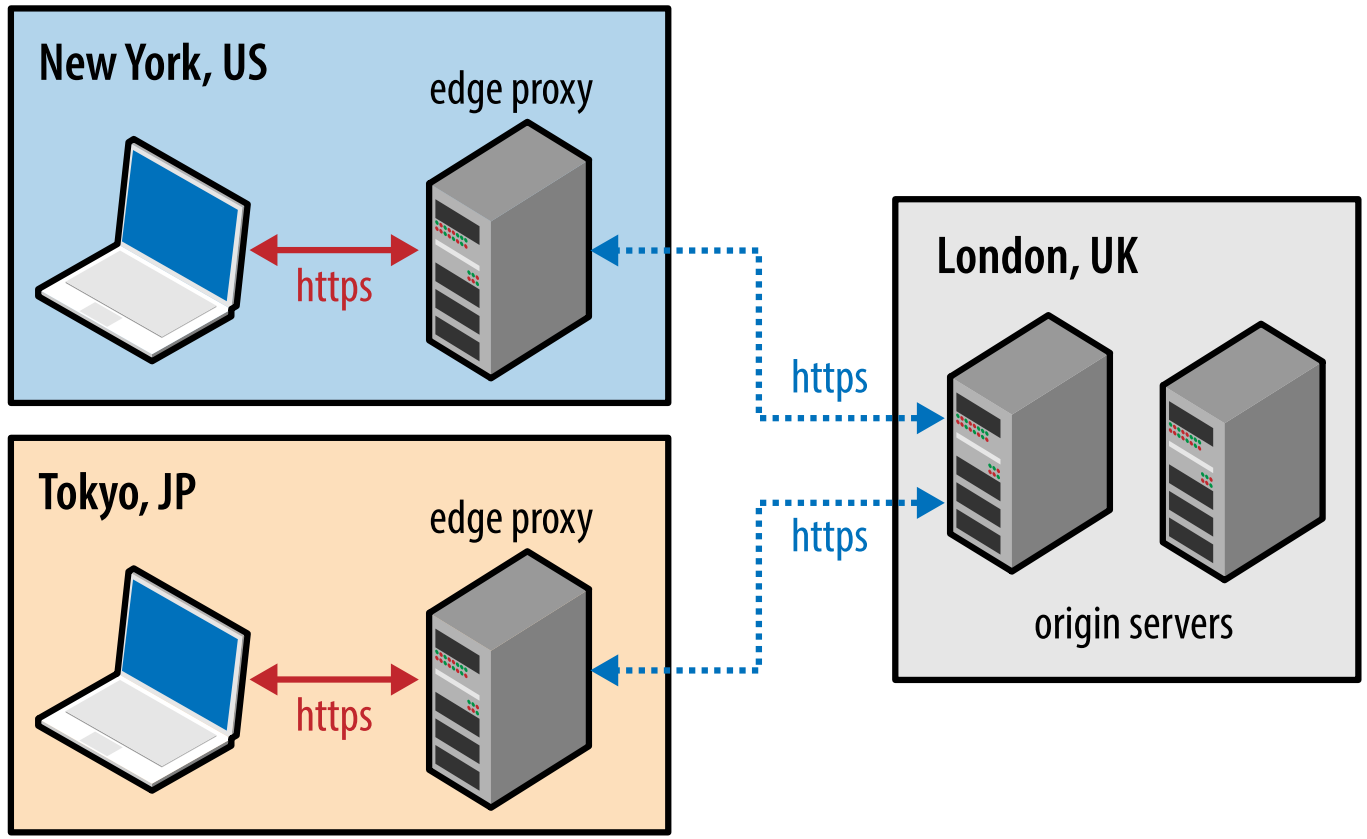
Протокол SSL/TLS



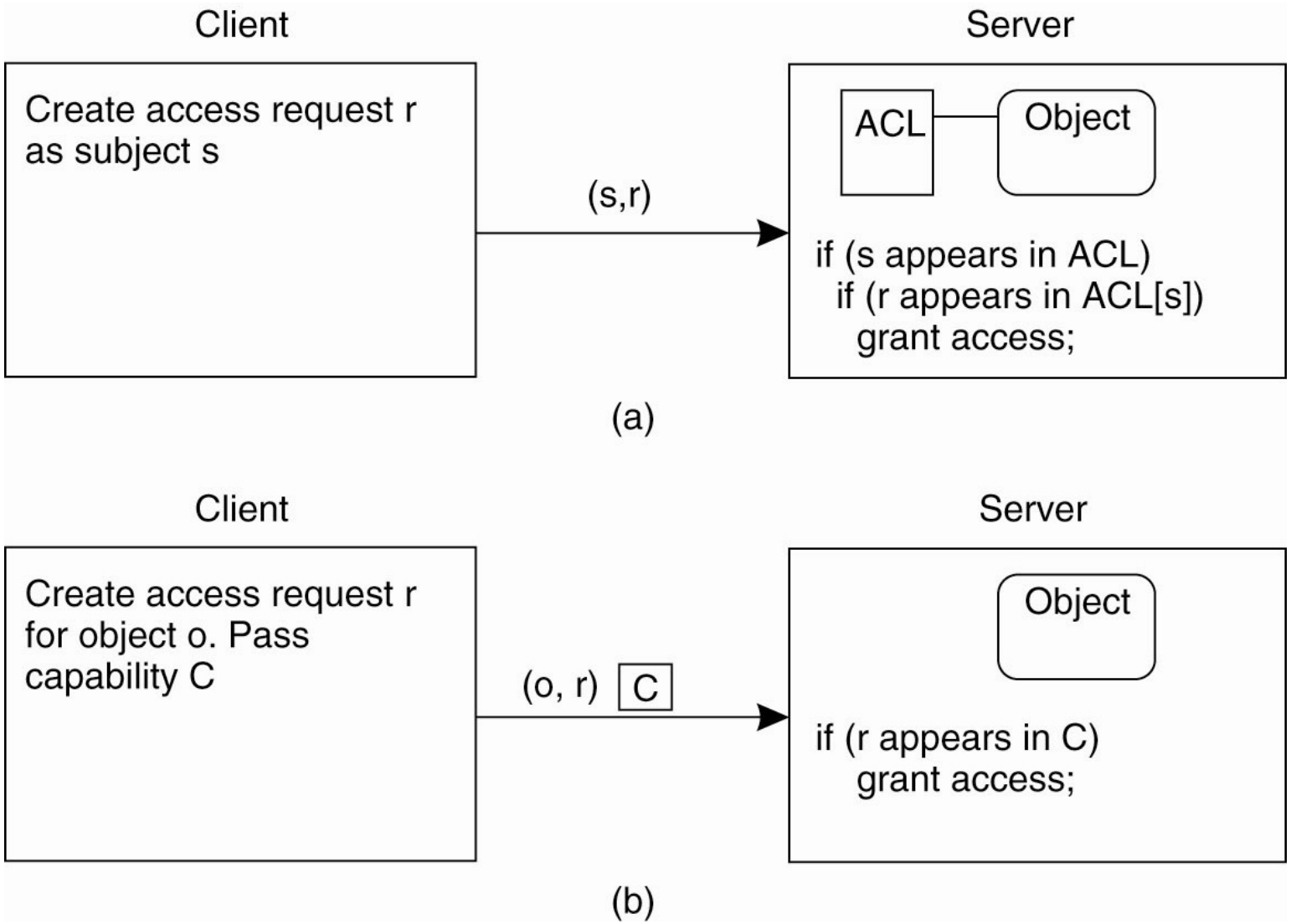
TLS Handshake



TLS Termination и CDN



Авторизация: ACL vs capabilities



Материалы

- Distributed Systems: Principles and Paradigms (глава 9)
- Distributed Systems: Concepts and Design (глава 11)
- High Performance Browser Networking (глава 4)