Skillbox

Security

TLS/SSL

Симметричное и асимметричное шифрование

Чернухин Максим

Software Architect АО Альфа-Банк

На этом уроке мы узнаем

- Что такое SSL
- Чем он отличается от TLS
- Какими способами шифруются данные

Skillbox

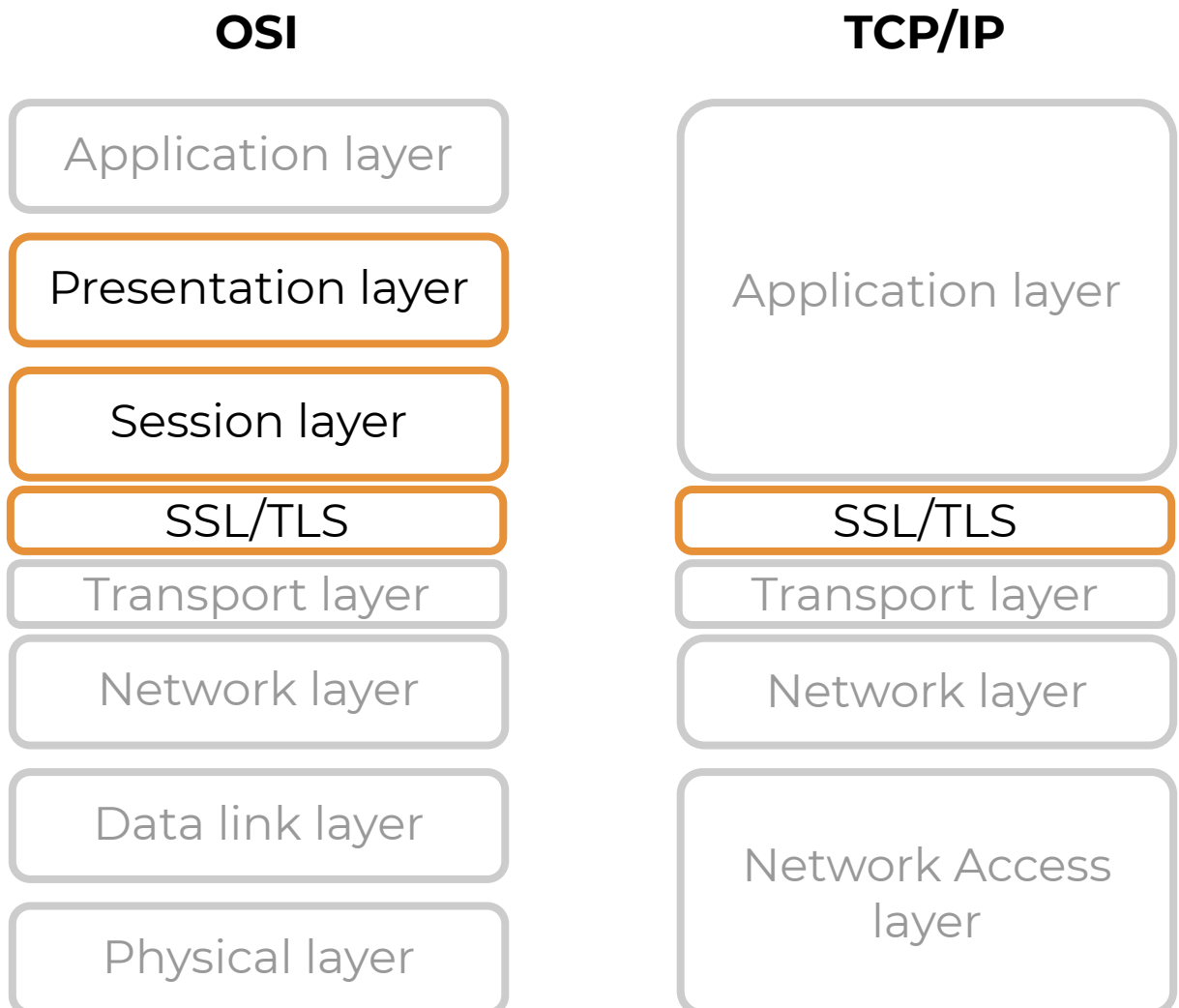
Протоколы безопасной передачи данных

- **SSL** — Secure Sockets Layer (уровень защищённых сокетов)
- **TLS** — Transport Layer Security (протокол защиты транспортного уровня)

Использование **TLS/SSL**: HTTP**S**, SMTP**S**, POP3**S**

Skillbox

Место в модели OSI и TCP/IP



История протоколов

- **SSL 1.0** — 1994 не опубликован
- **SSL 2.0** — 1995
- **SSL 3.0** — 1996 RFC 6101

- **TLS 1.0** — 1999 RFC 2246
- **TLS 1.1** — 2006 RFC 4346
- **TLS 1.2** — 2008 RFC 5246
- **TLS 1.3** — 2018 RFC 8446

История протоколов

- **SSL 1.0** — 1994 не опубликован
- **SSL 2.0** — 1995
- **SSL 3.0** — 1996 RFC 6101

- **TLS 1.0** — 1999 RFC 2246
- **TLS 1.1** — 2006 RFC 4346
- **TLS 1.2** — 2008 RFC 5246
- **TLS 1.3** — 2018 RFC 8446

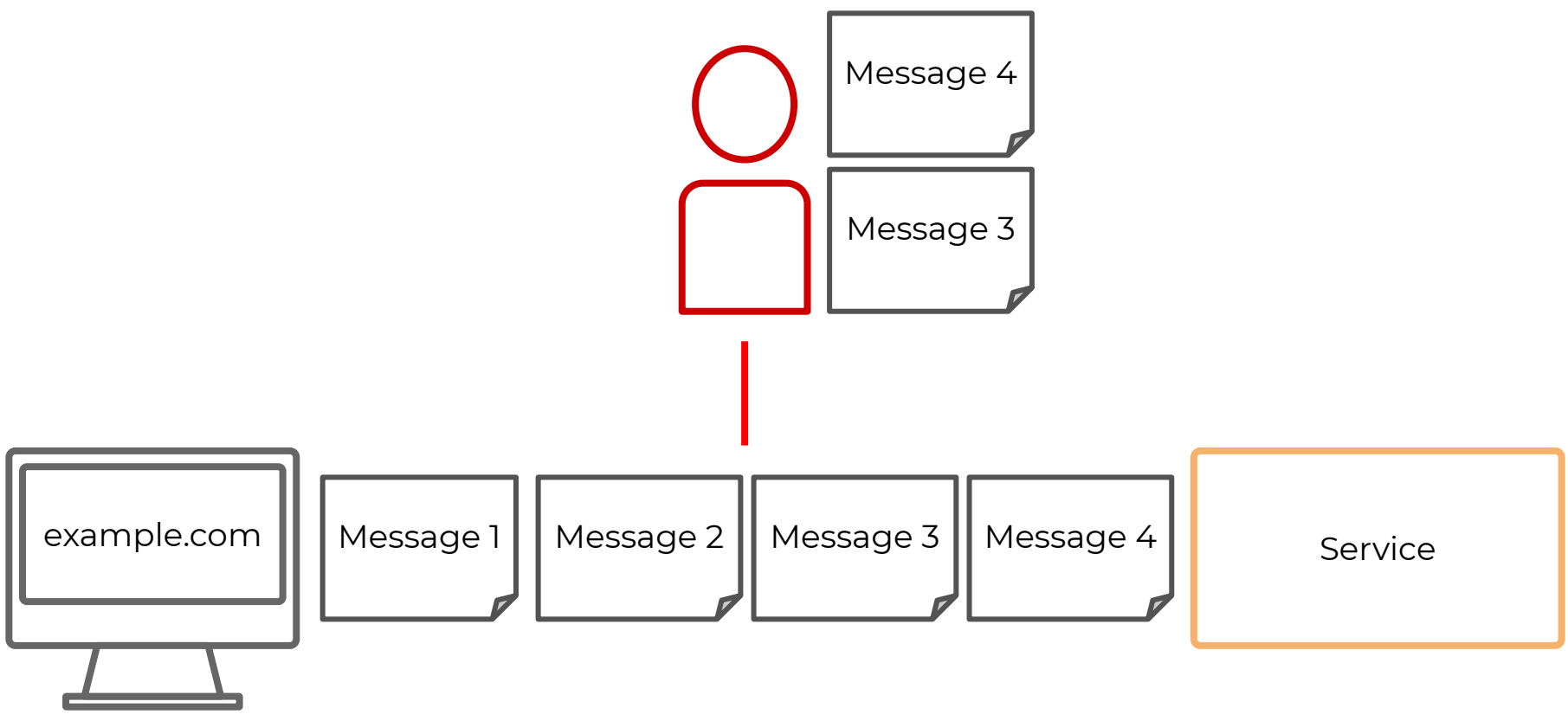
Что гарантирует TLS/SSL?

- Приватность (Privacy)
- Целостность (Integrity)
- Аутентификацию (Authentication)

Skillbox

Приватность (Privacy)

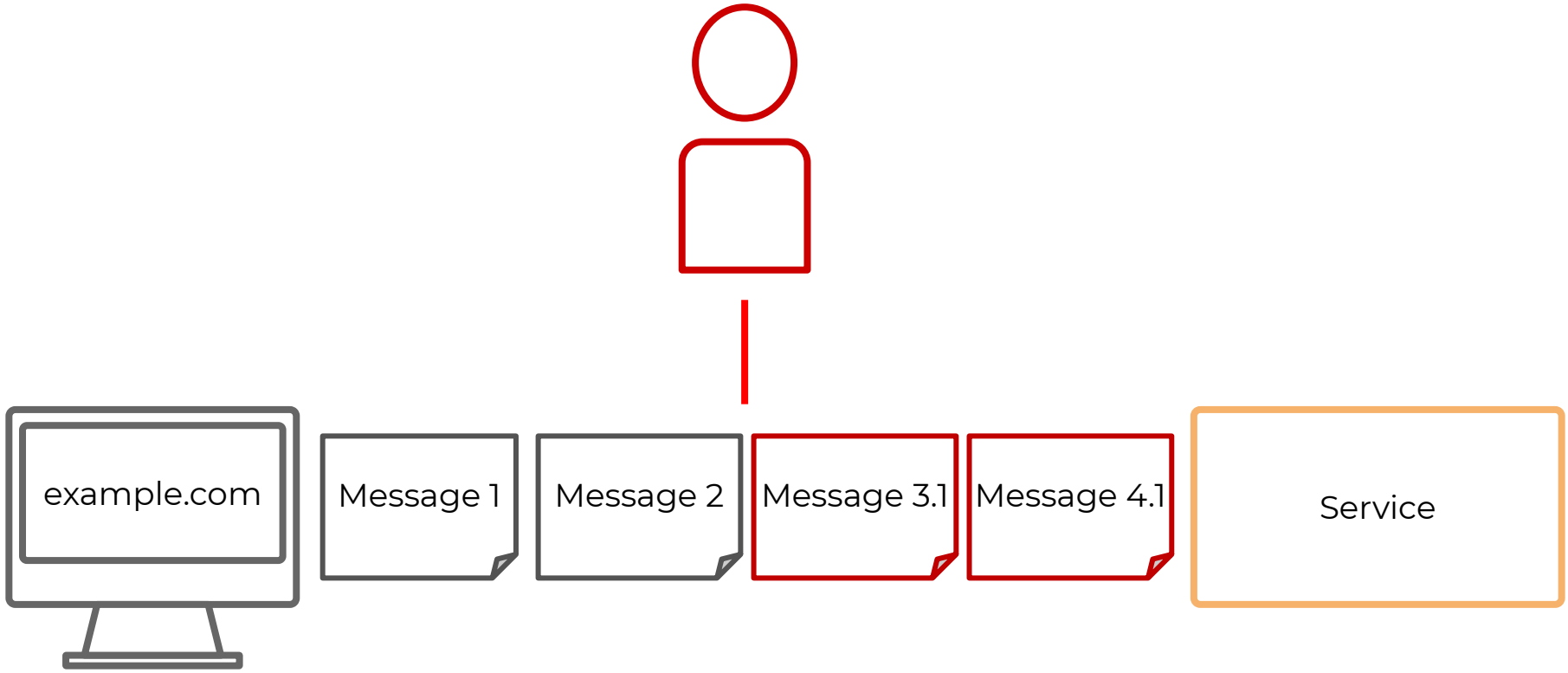
Шифрование для защиты.



Skillbox

Целостность (Integrity)

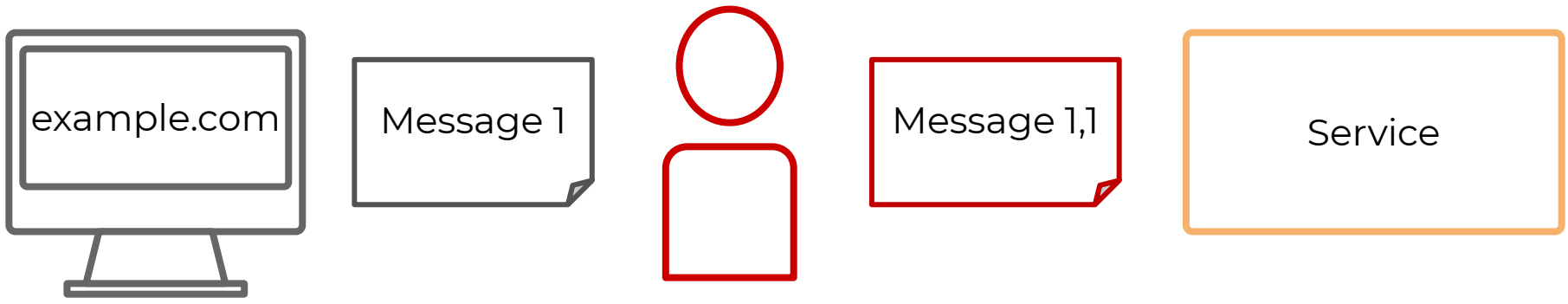
Хеш-функции для защиты.



Skillbox

Аутентификация (Authentication)

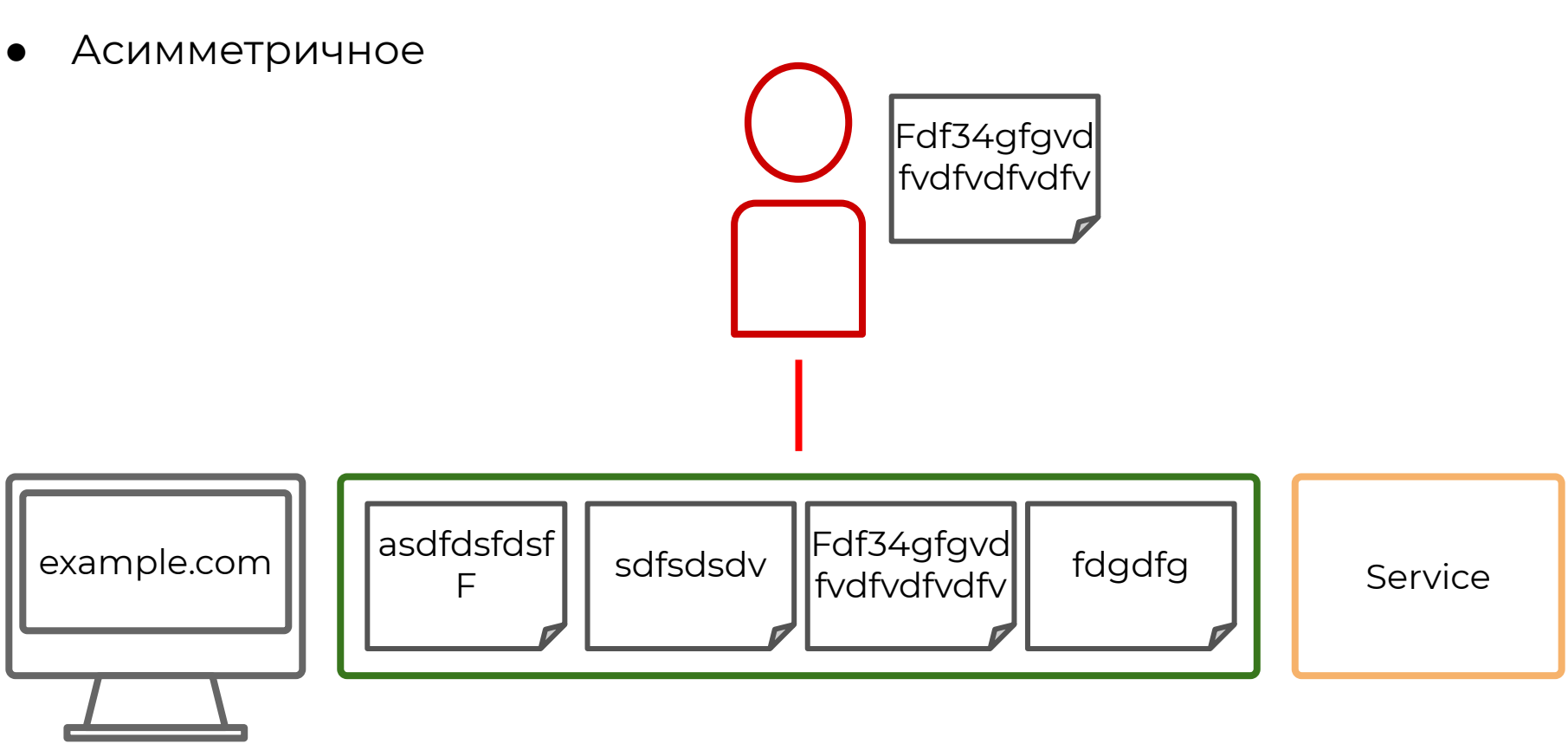
Цифровая подпись для защиты.



Man in the middle

Шифрование

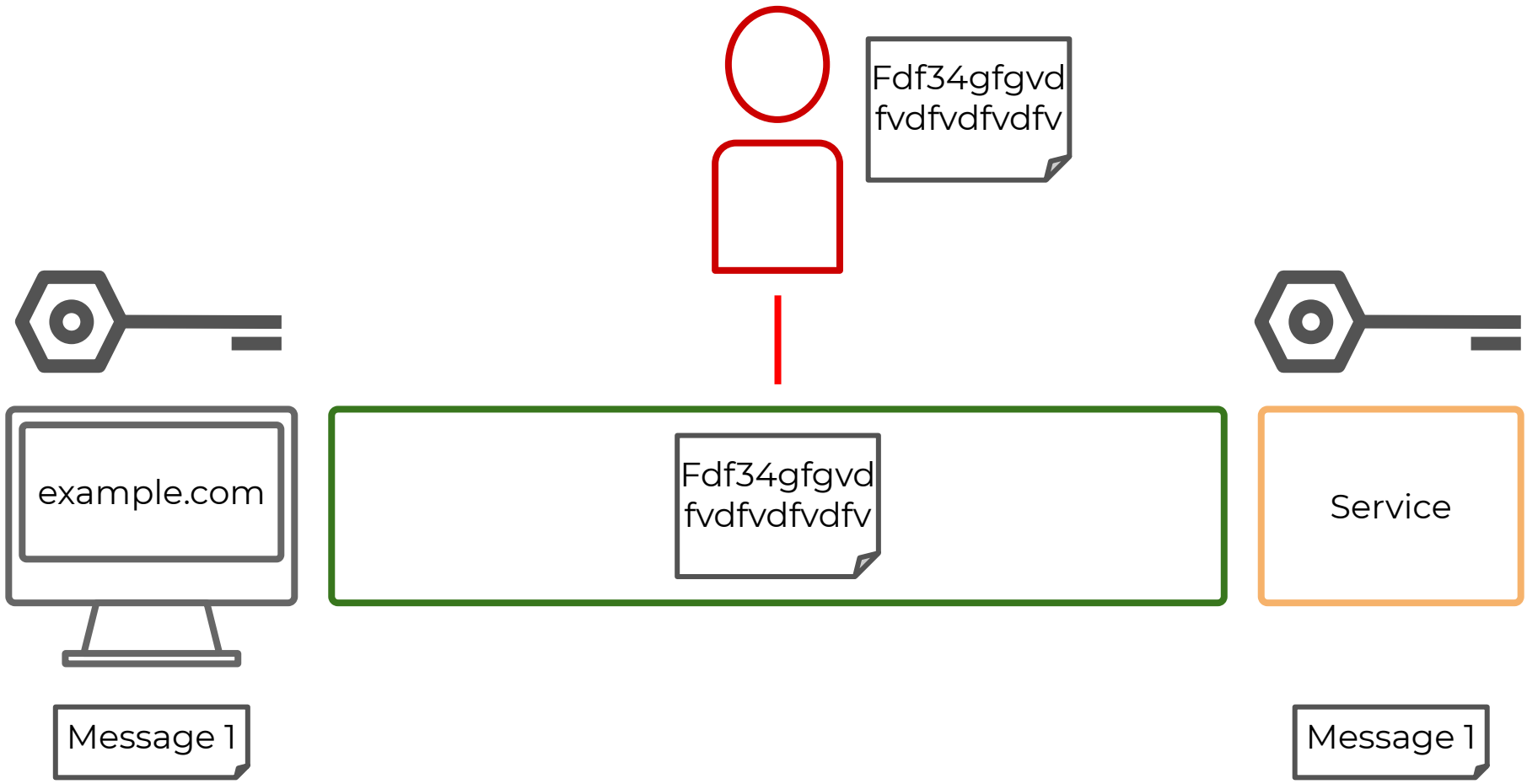
- Симметричное
- Асимметричное



Skillbox

Симметричное шифрование

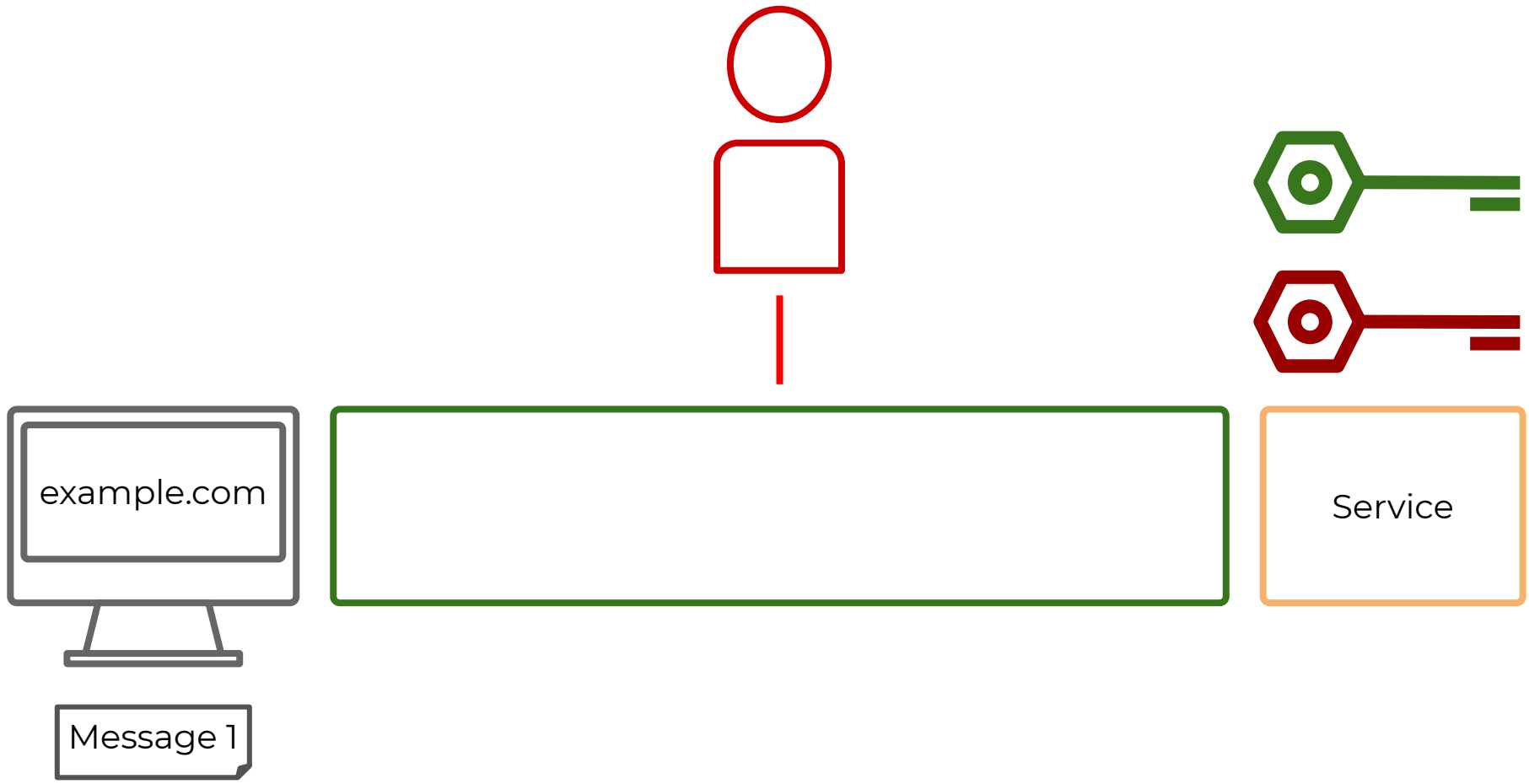
AES, 3DES6 RC6 и т. д.



Skillbox

Асимметричное шифрование

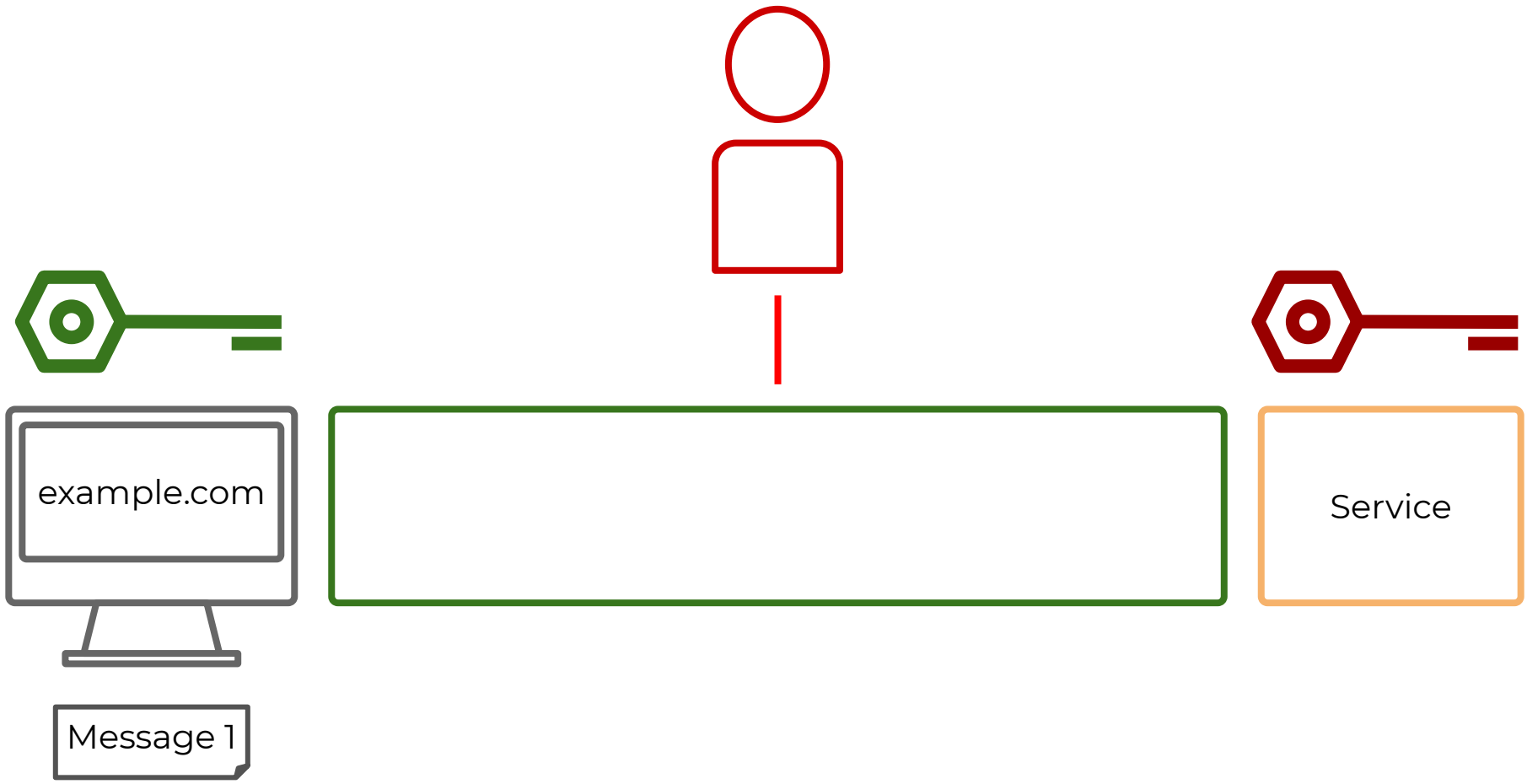
AES, 3DES6 RC6 и т. д.



Skillbox

Асимметричное шифрование

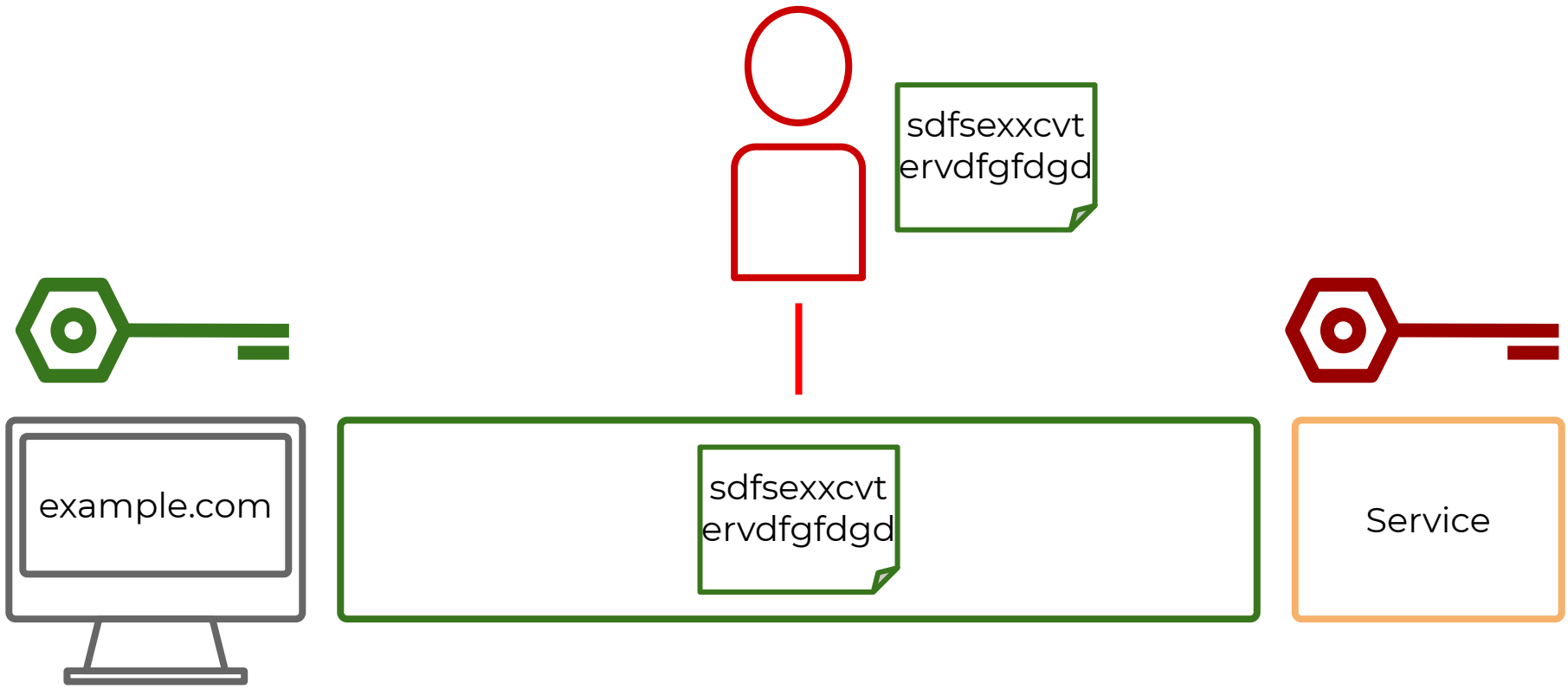
AES, 3DES6 RC6 и т. д.



Skillbox

Асимметричное шифрование

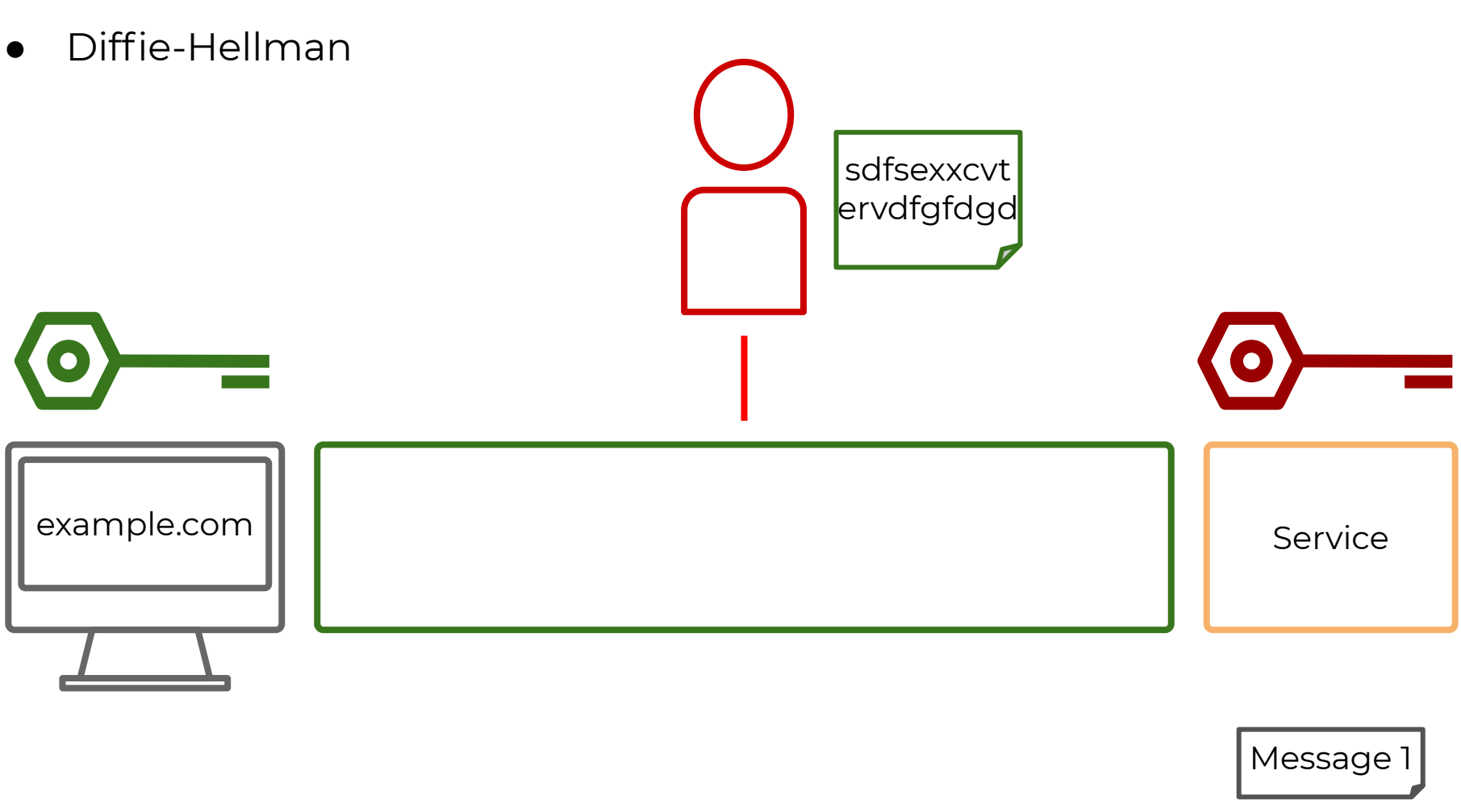
AES, 3DES6 RC6 и т. д.



Skillbox

Асимметричное шифрование

- RSS, DSA, DSS
- Diffie-Hellman

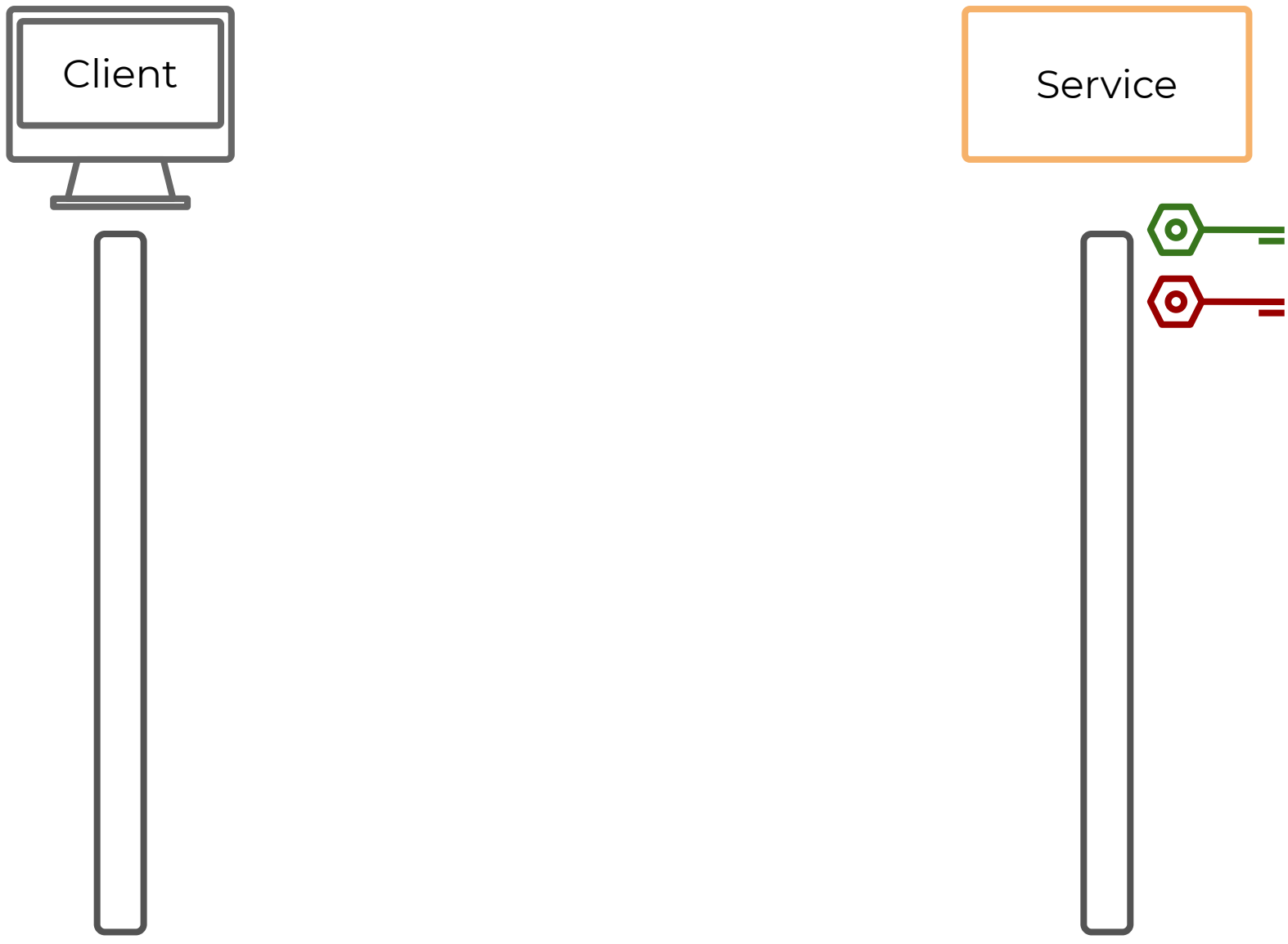


Шифрование

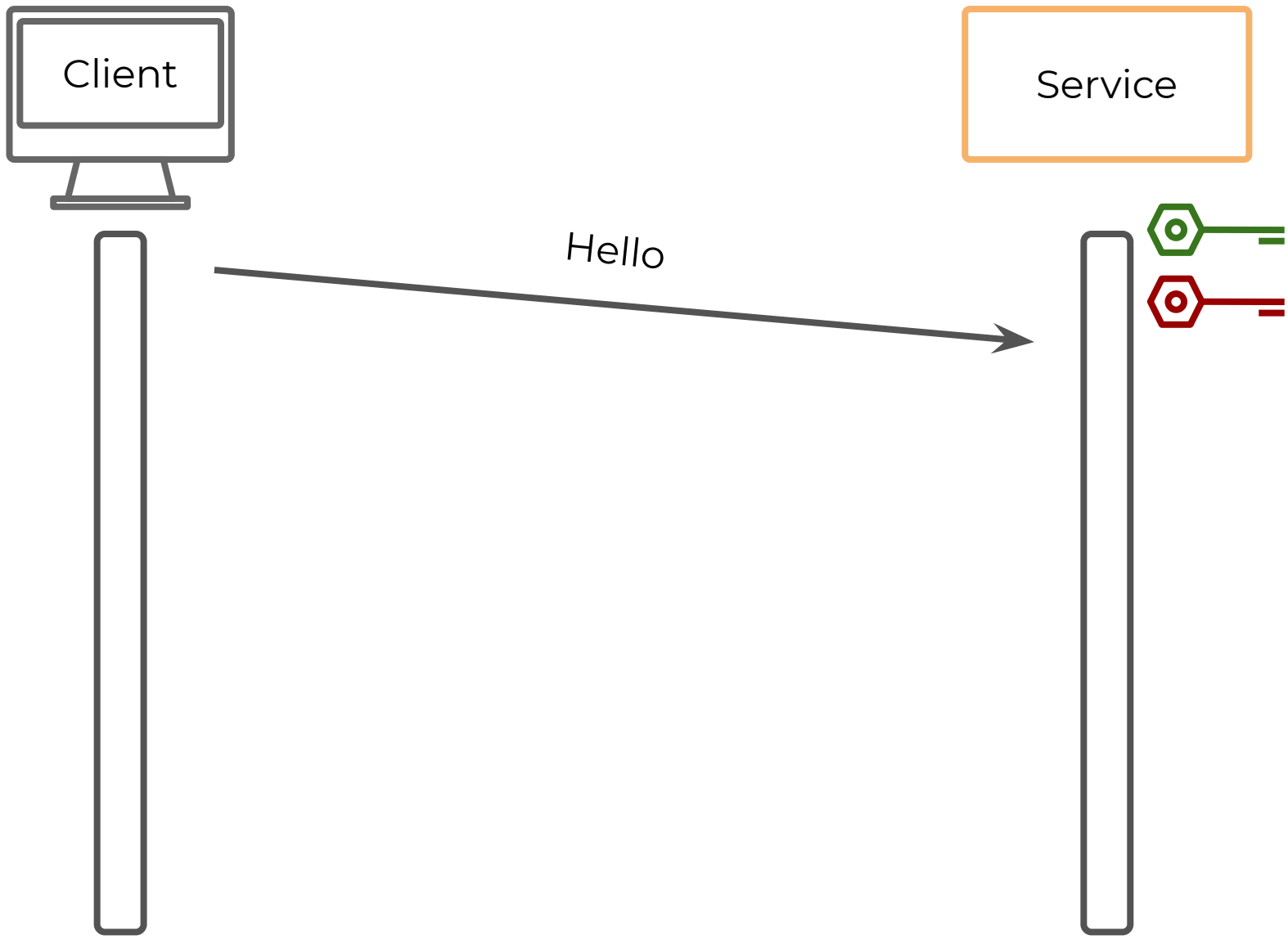
- Симметричное:
  - быстро работает
  - хранение и передача ключей
- Асимметричное:
  - работает медленнее
  - открытый ключ может передаваться по сети
- Гибридное шифрование TLS/SSL:
  - для передачи синхронных ключей — асинхронное шифрование
  - для передачи данных — синхронное шифрование

Skillbox

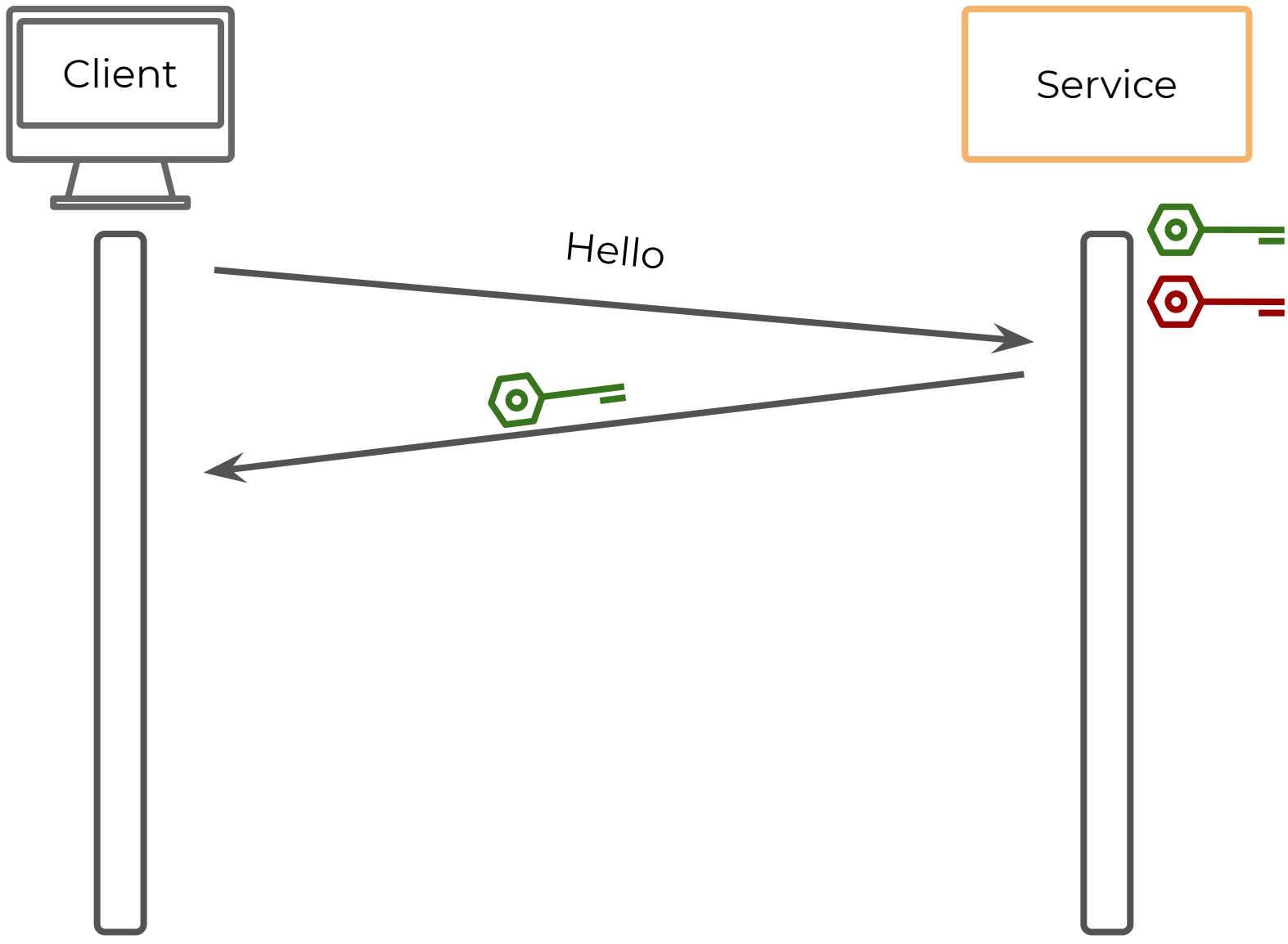
RSA-алгоритм



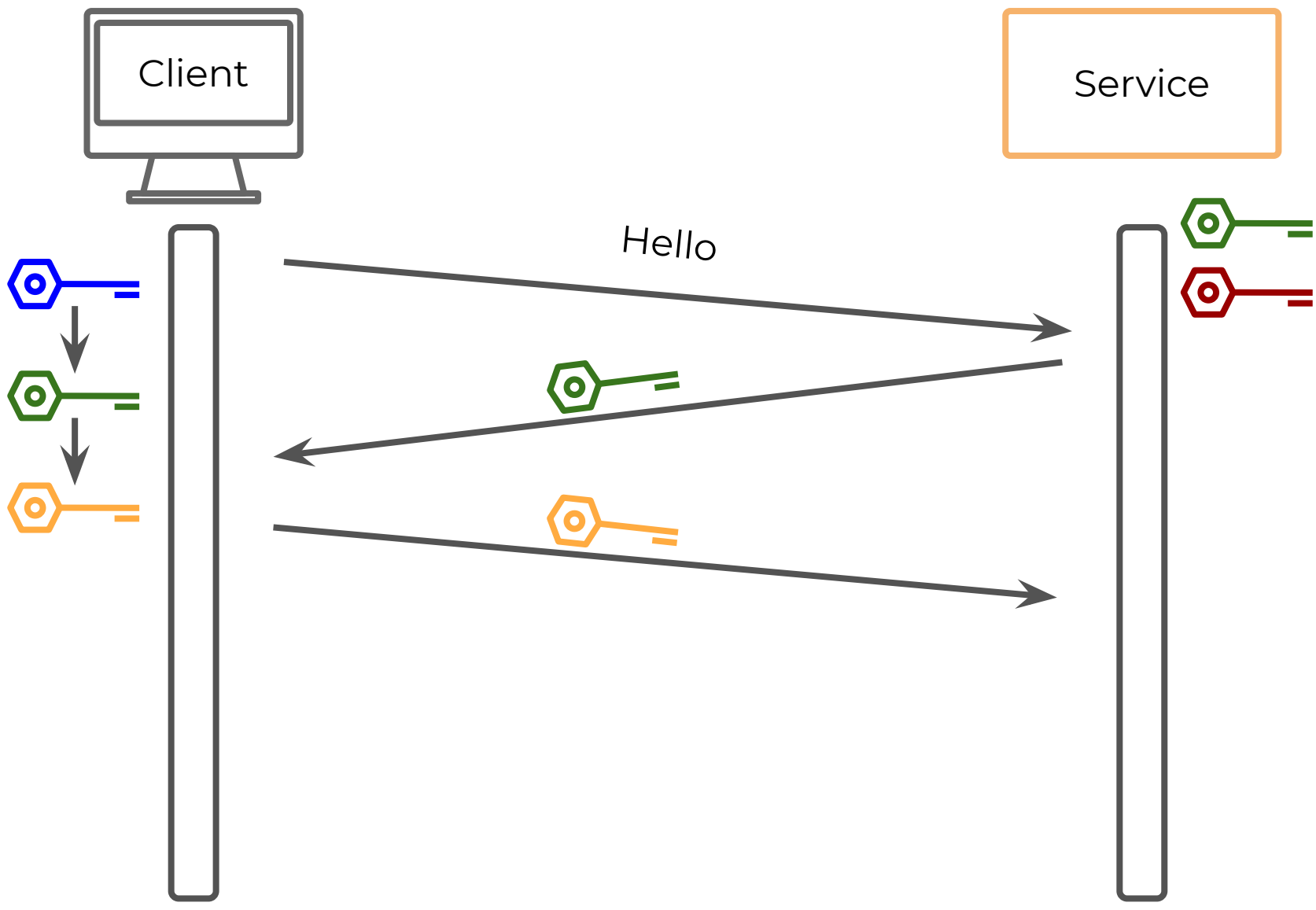
RSA-алгоритм



RSA-алгоритм

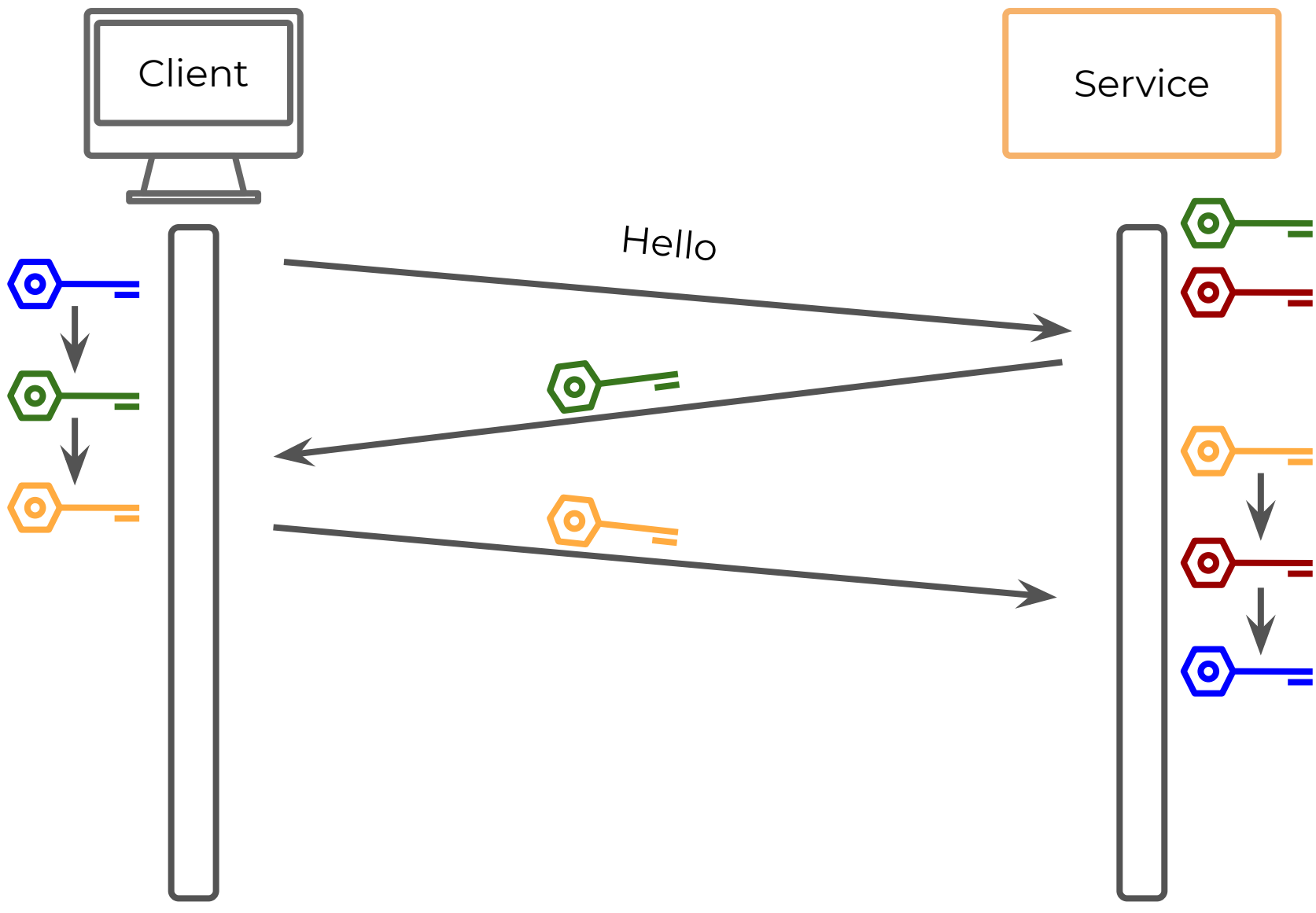


RSA-алгоритм



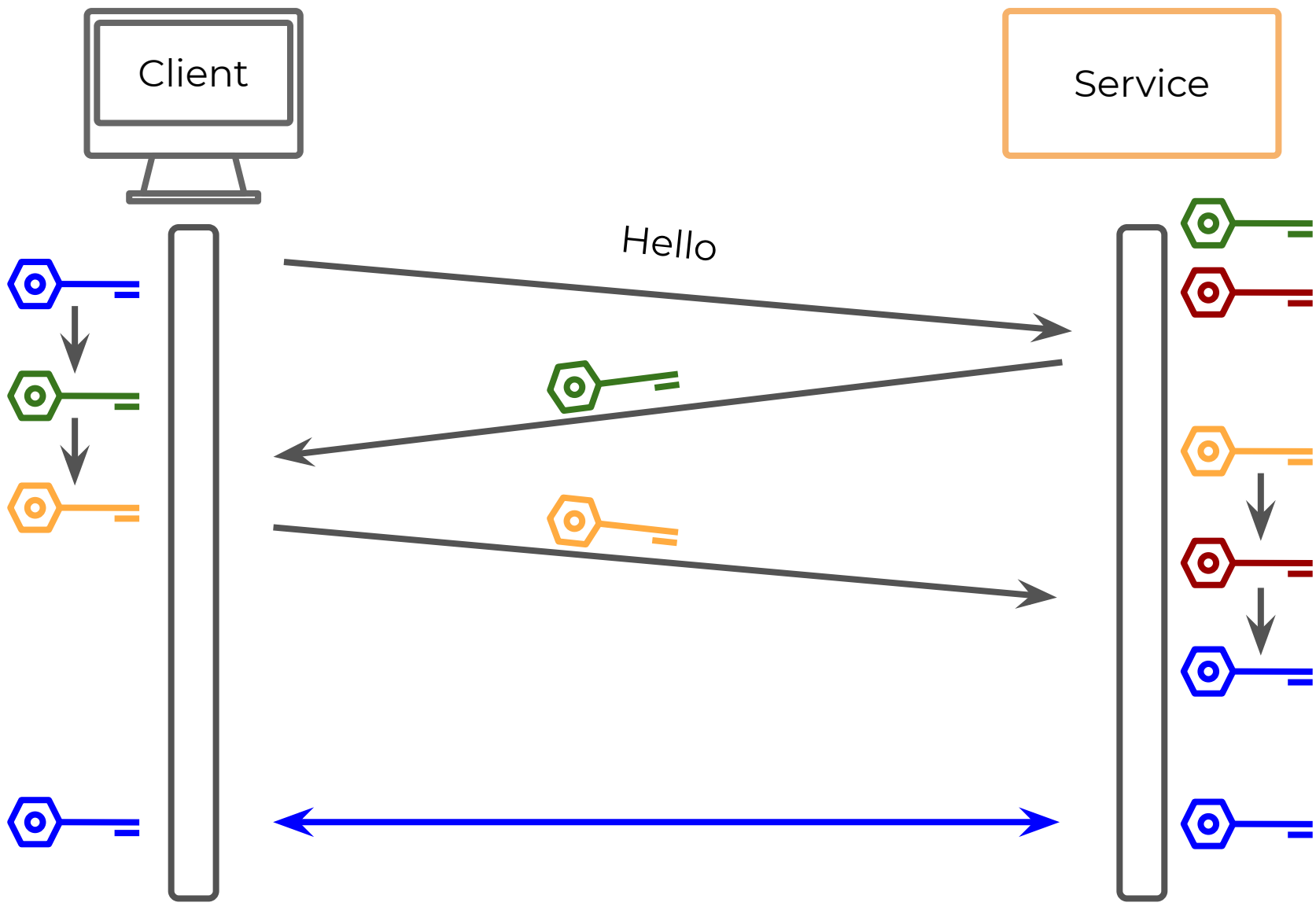
Skillbox

RSA-алгоритм



Skillbox

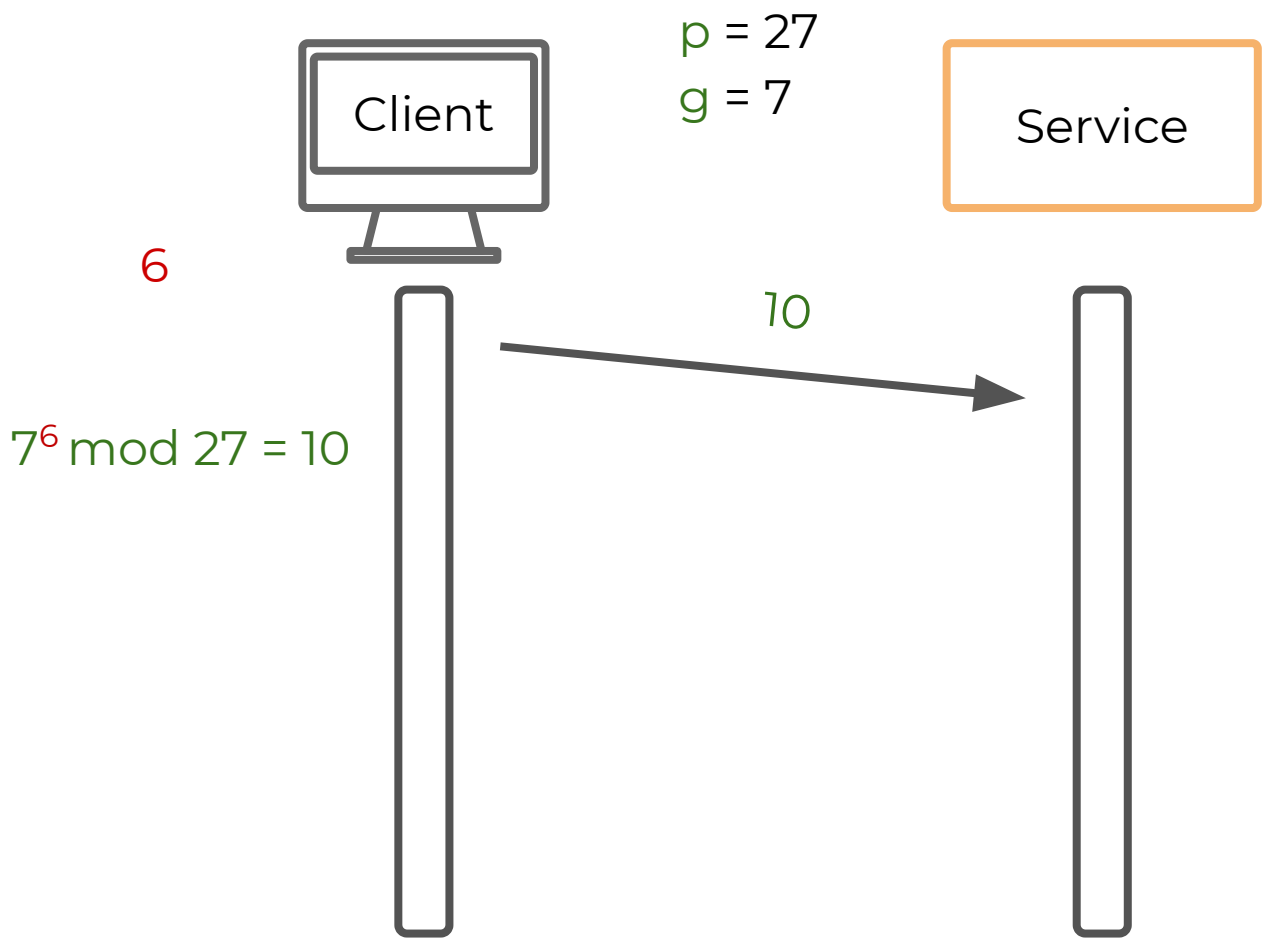
RSA-алгоритм



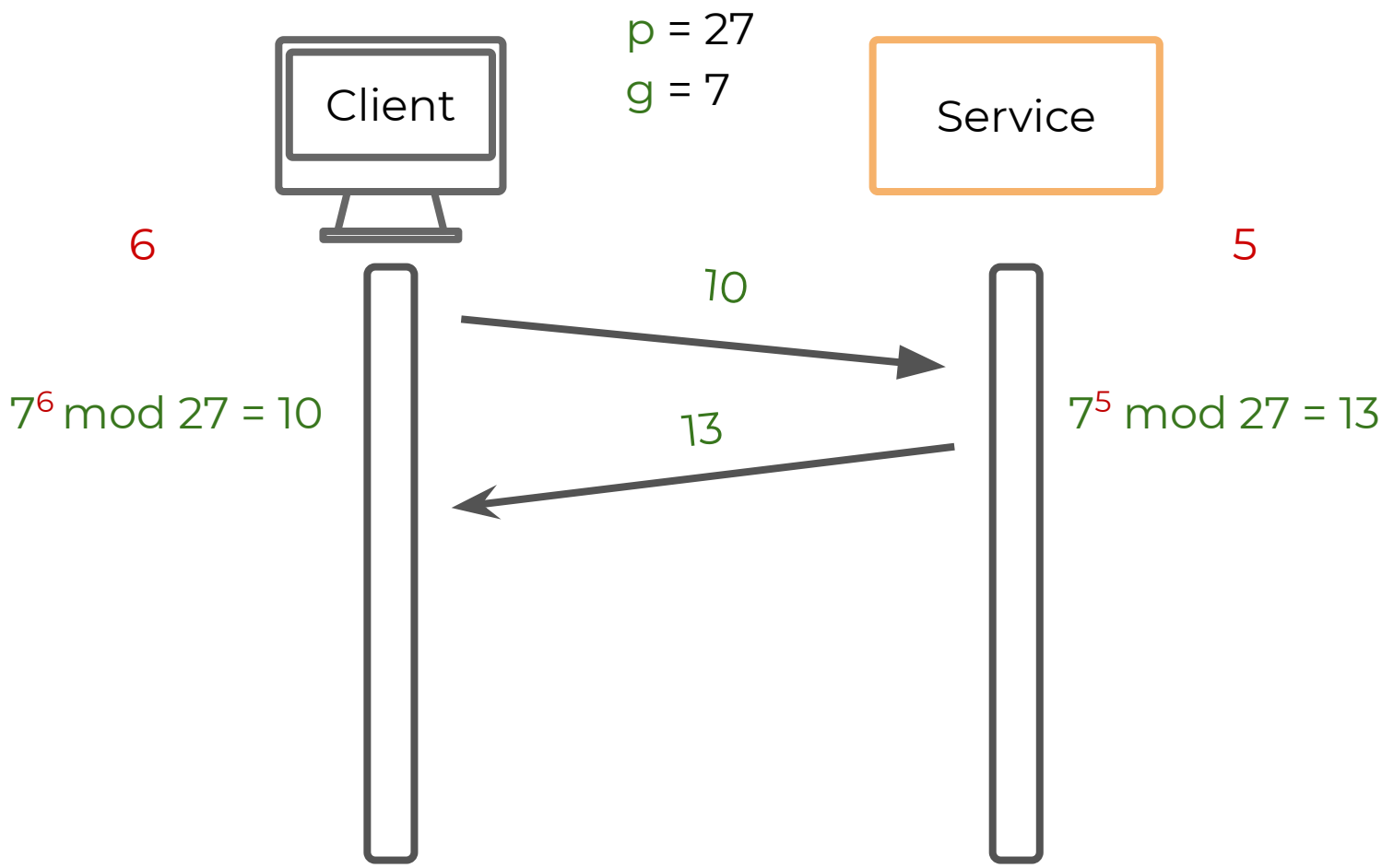
Шифрование

- RSA не обеспечивает Perfect Forward Secrecy
- Уязвимости RSA:
  - Million Message Attack, Bleichenbacher, 1998
  - ROBOT 2017 — Return of Bleichenbacher Oracle Threat
- TLS 1.3 запрещает использование RSA

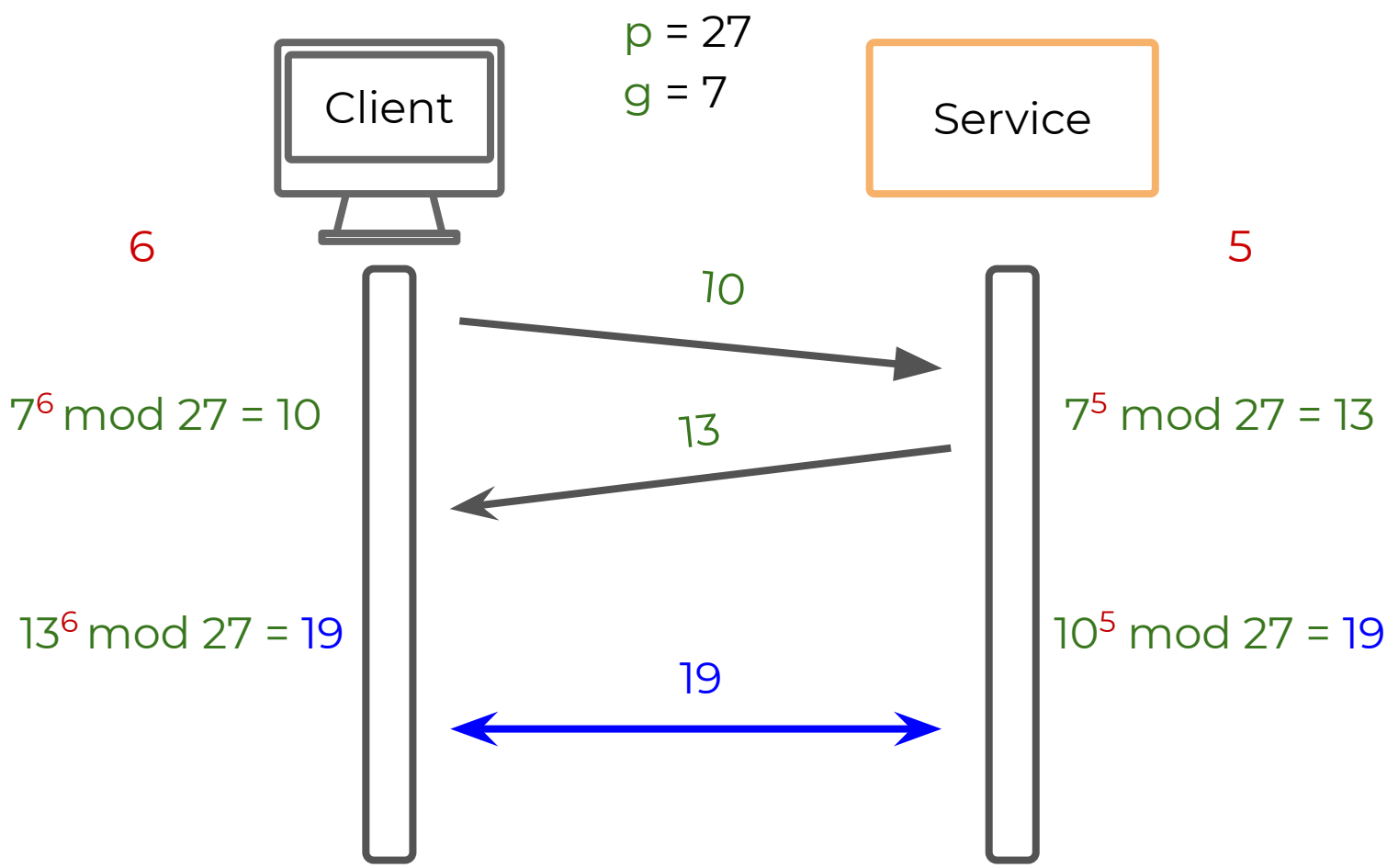
Алгоритм Diffie — Hellman



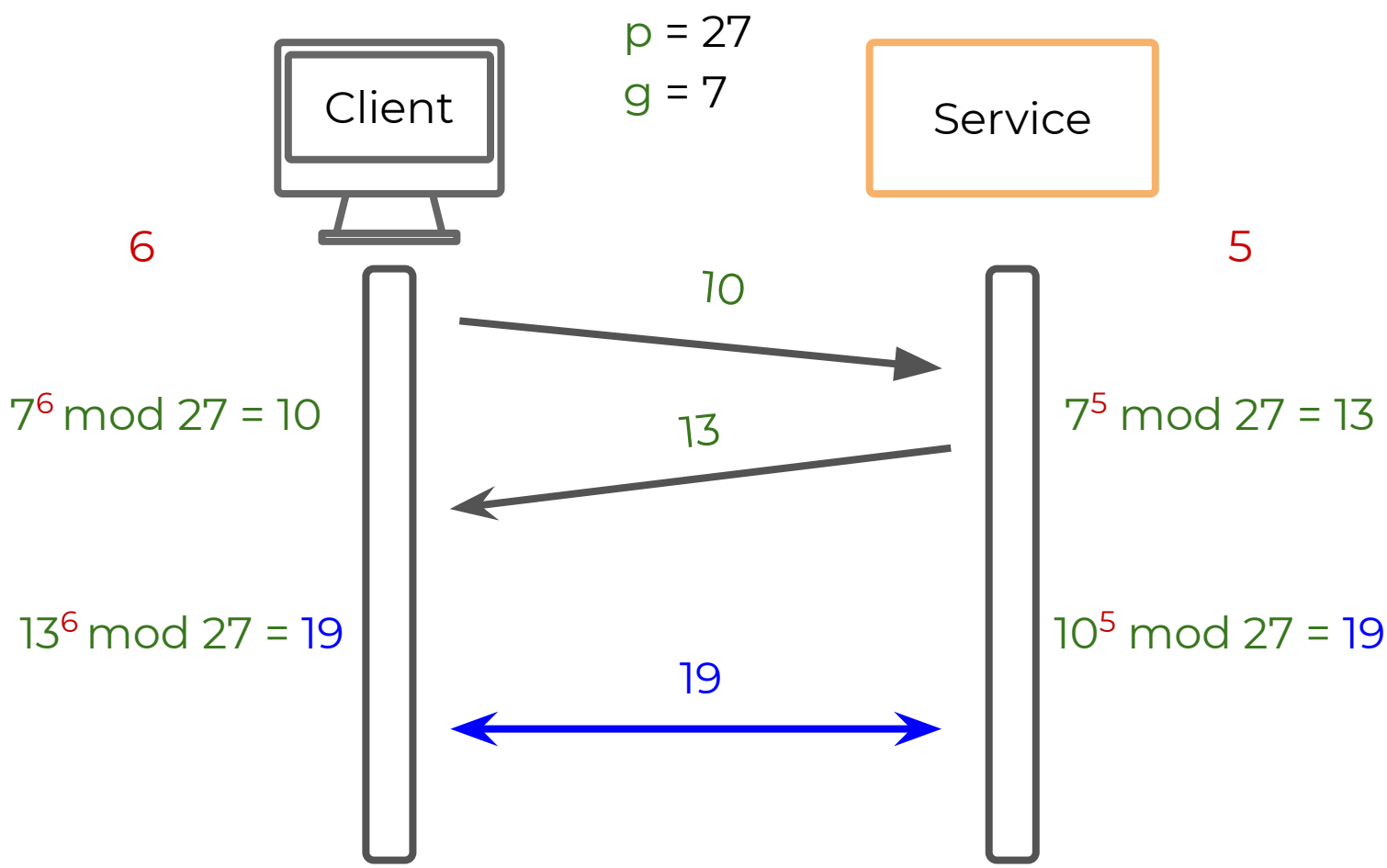
Алгоритм Diffie — Hellman



Алгоритм Diffie — Hellman



Алгоритм Diffie — Hellman



$$(7^6 \bmod 27)^5 \bmod 27 = (7^5 \bmod 27)^6 \bmod 27$$

Итоги

- Мы познакомились с SSL и TLS
- Узнали, чем отличается симметричное шифрование от асимметричного
- Узнали, как работают RSA- и Diffie — Hellman-алгоритмы

Что дальше?

- Что такое аутентификация?
- Где используется авторизация?
- Какие бывают способы построения ролевых моделей?

Skillbox

Спасибо за внимание!