Шифрование в TLS/SSL

Компьютерные сети

Шифрование в TLS/SSL

TLS/SSL – протоколы безопасной передачи данных по небезопасной сети:

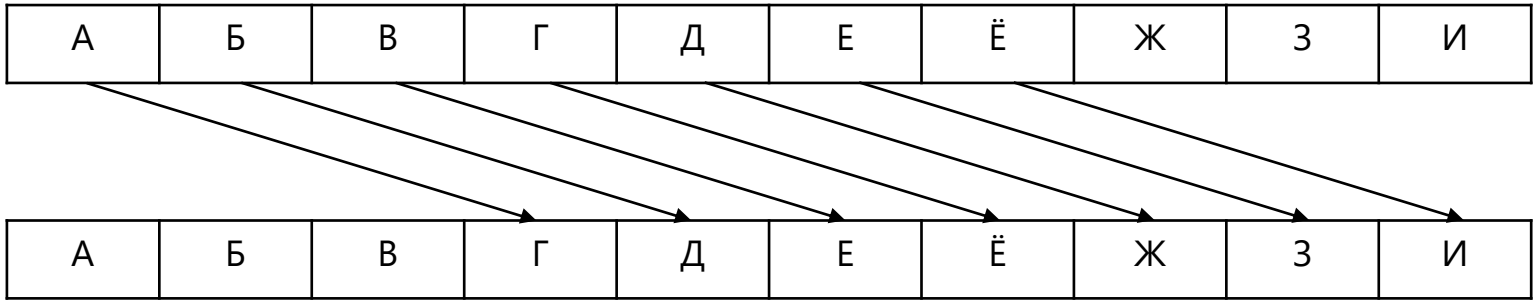
- Приватность
- Целостность
- Аутентификация

Шифр Цезаря

Простой шифр сдвига:

- Использовался в Древнем Риме Юлием Цезарем

Метод шифрования:

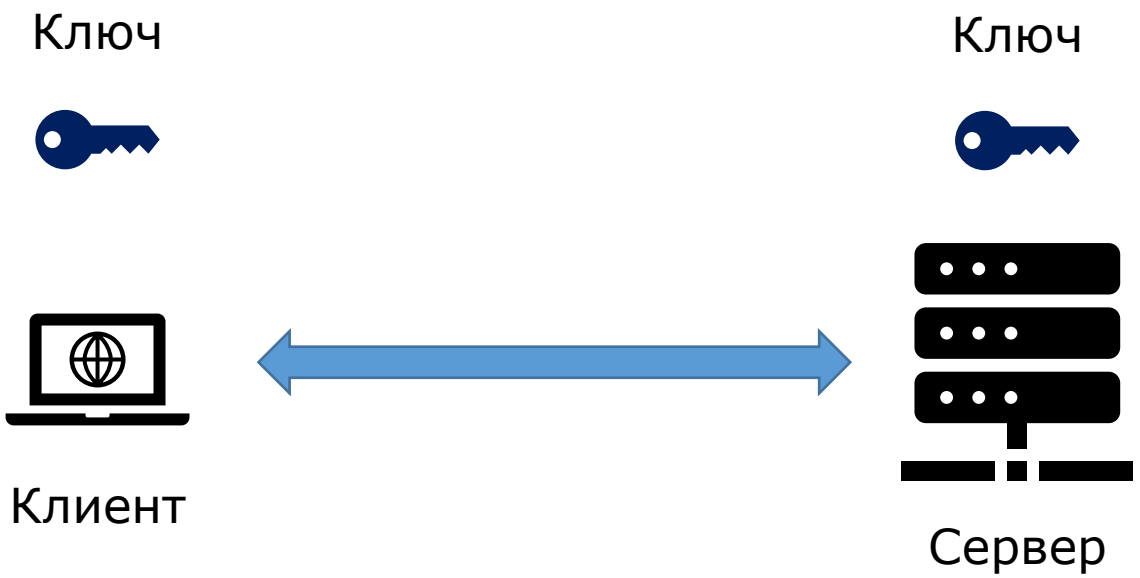


Ключ шифрования:

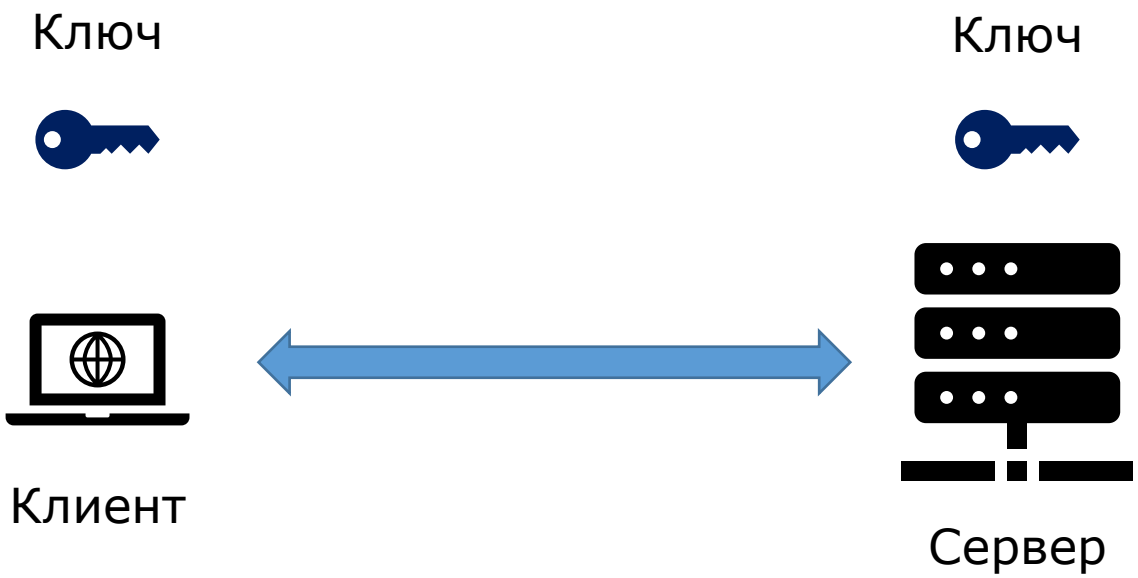
- Величина и направление сдвига

Шифр очень легко взломать

Симметричное шифрование



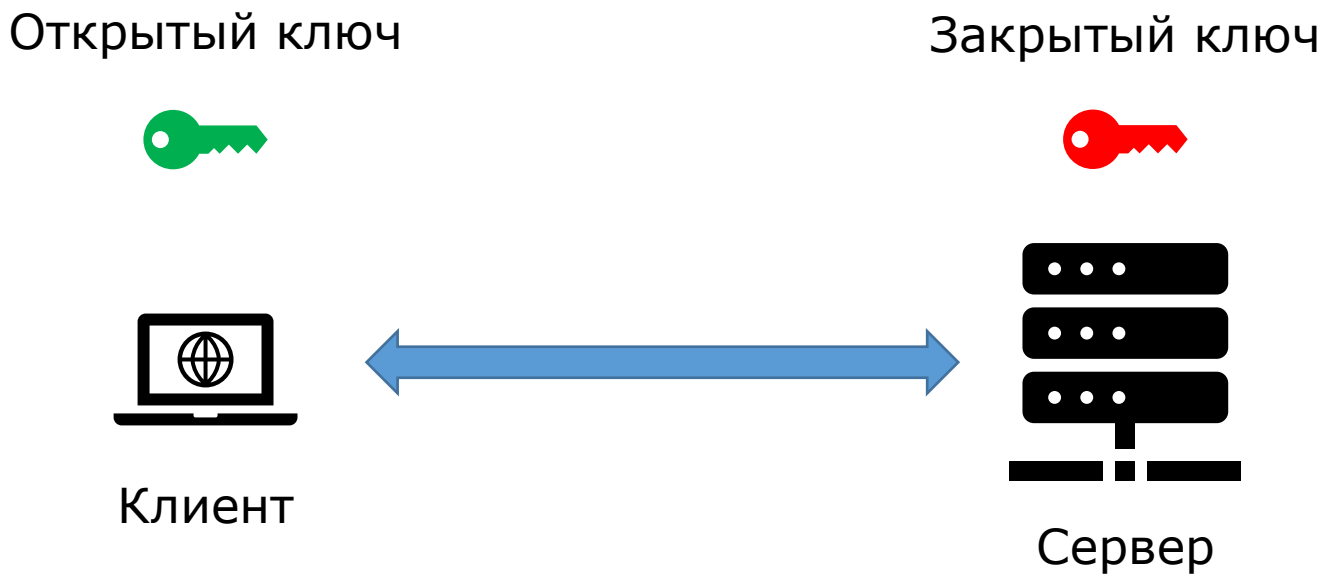
Симметричное шифрование



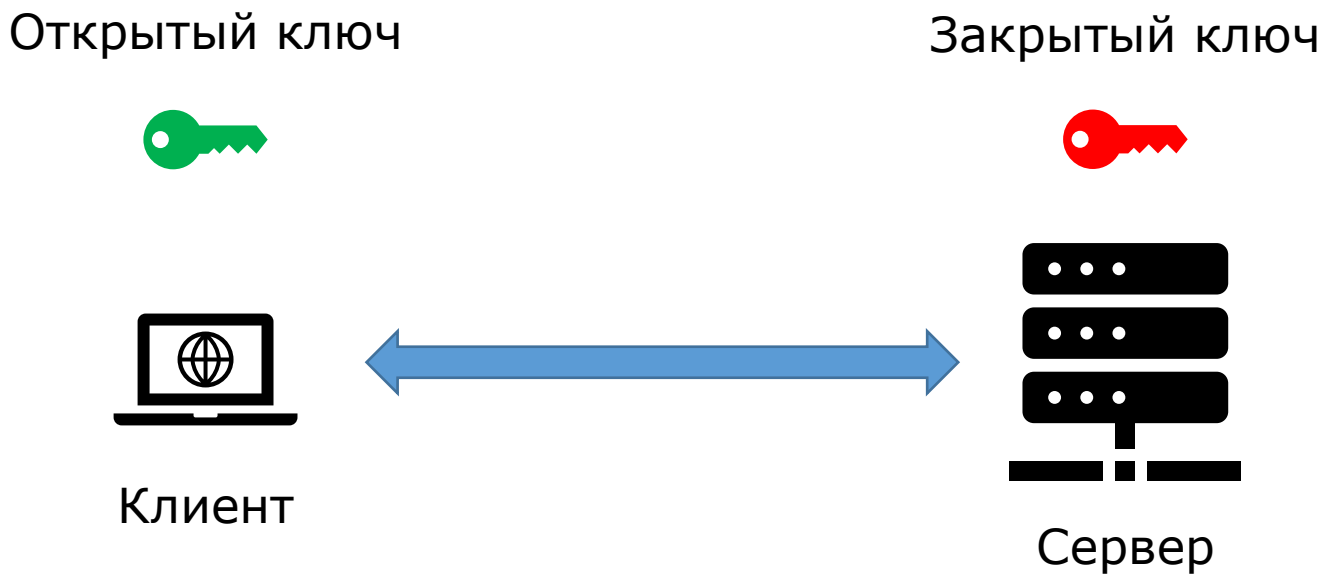
Алгоритмы симметричного шифрования:

- AES (Advanced Encryption Standard)
- 3DES (Triple Data Encryption Algorithm)
- RC4, RC5, RC6 (Rivest cipher)

Асимметричное шифрование



Асимметричное шифрование



Алгоритмы асимметричного шифрования:

- RSA (Rivest–Shamir–Adleman)
- DSA (Digital Signature Algorithm), DSS (Digital Signature Standard)
- Diffie–Hellman

Симметричное vs Асимметричное шифрование

Асимметричное шифрование:

- Открытый ключ может распространяться без ограничений
- Работает медленно

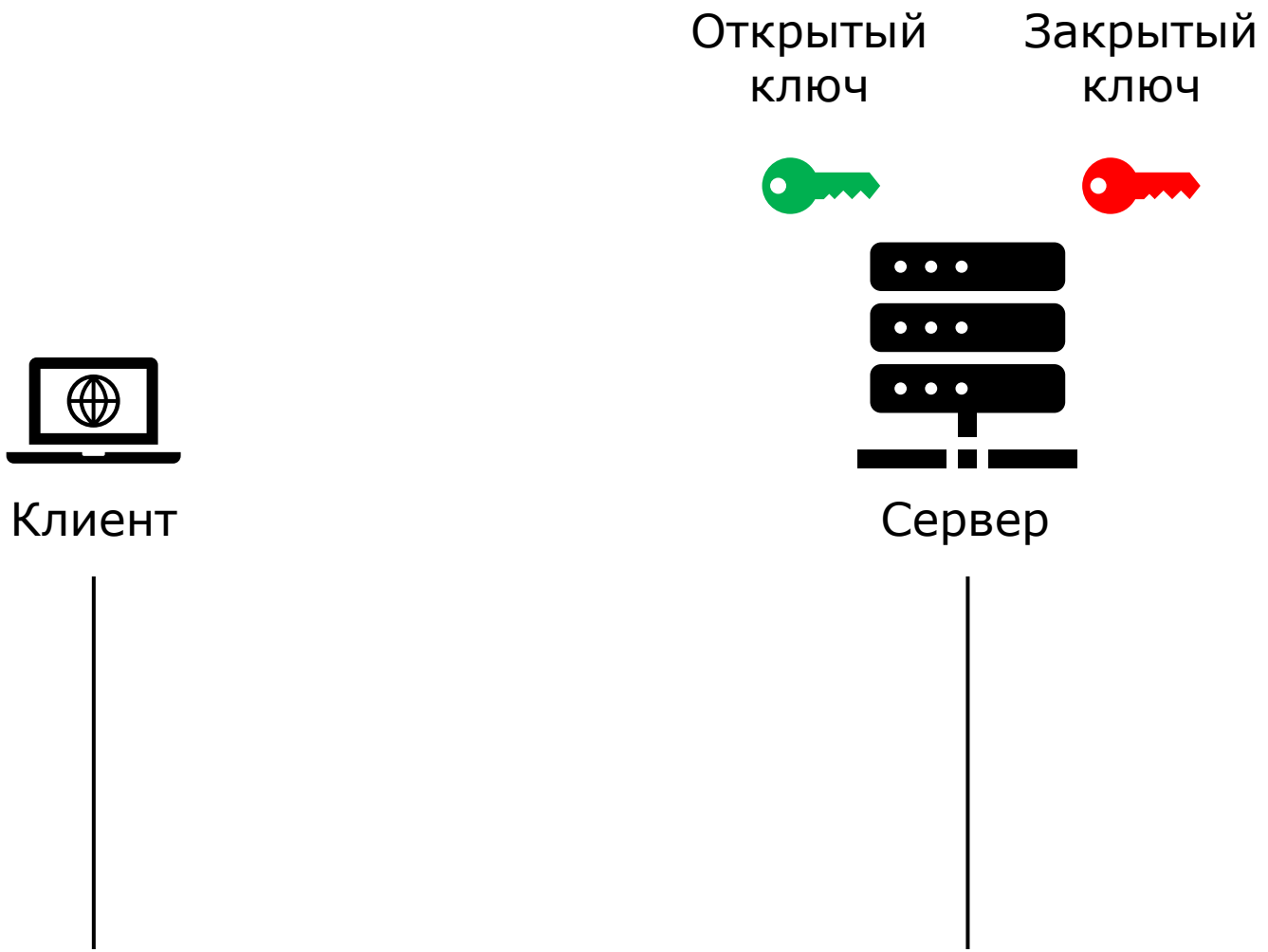
Симметричное шифрование:

- Ключ должен храниться в тайне
- Работает быстро

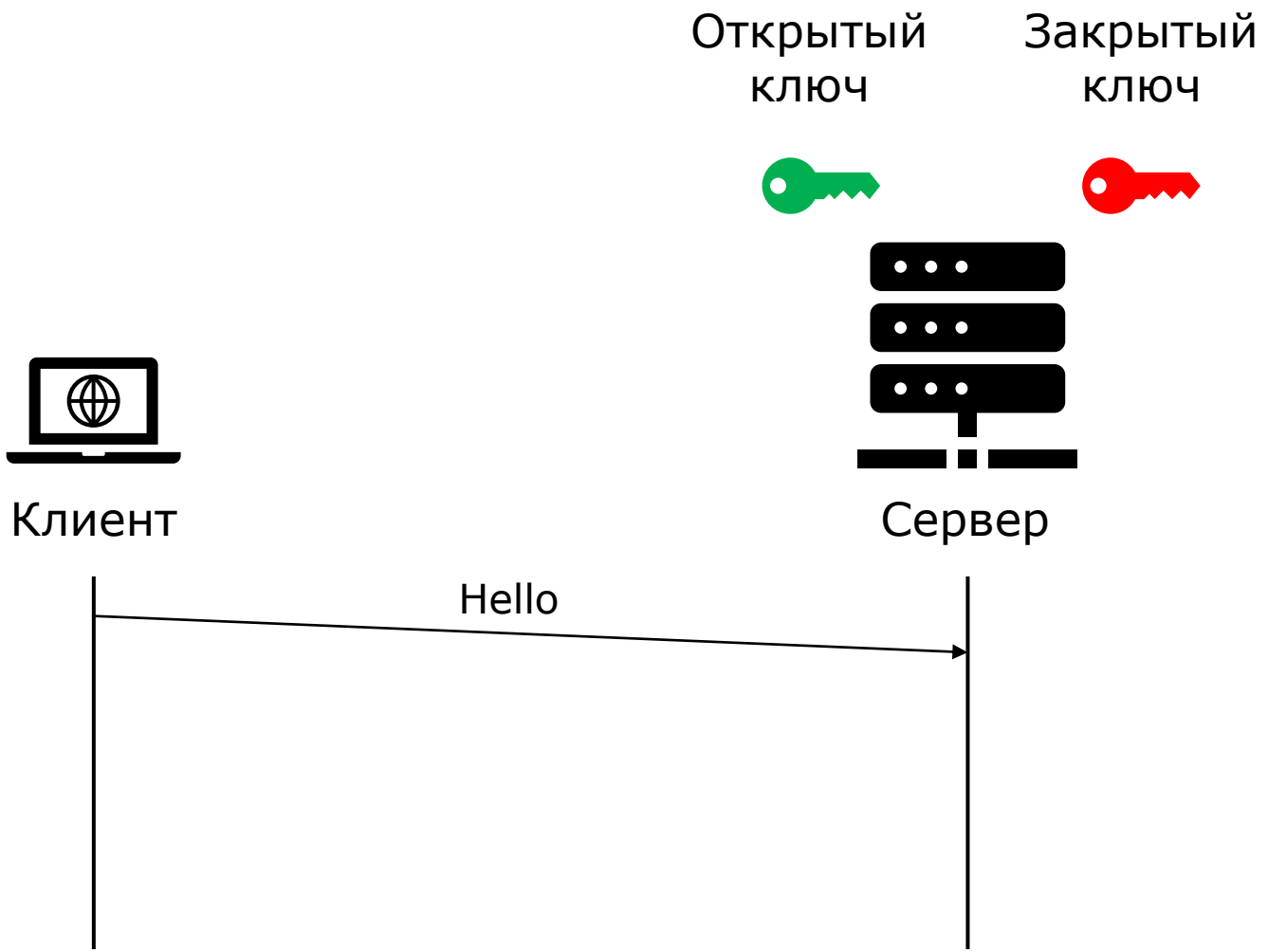
Гибридное шифрование в TLS/SSL:

- Ассиметричное шифрование для передачи ключа симметричного шифрования
- Симметричное шифрование для передачи данных

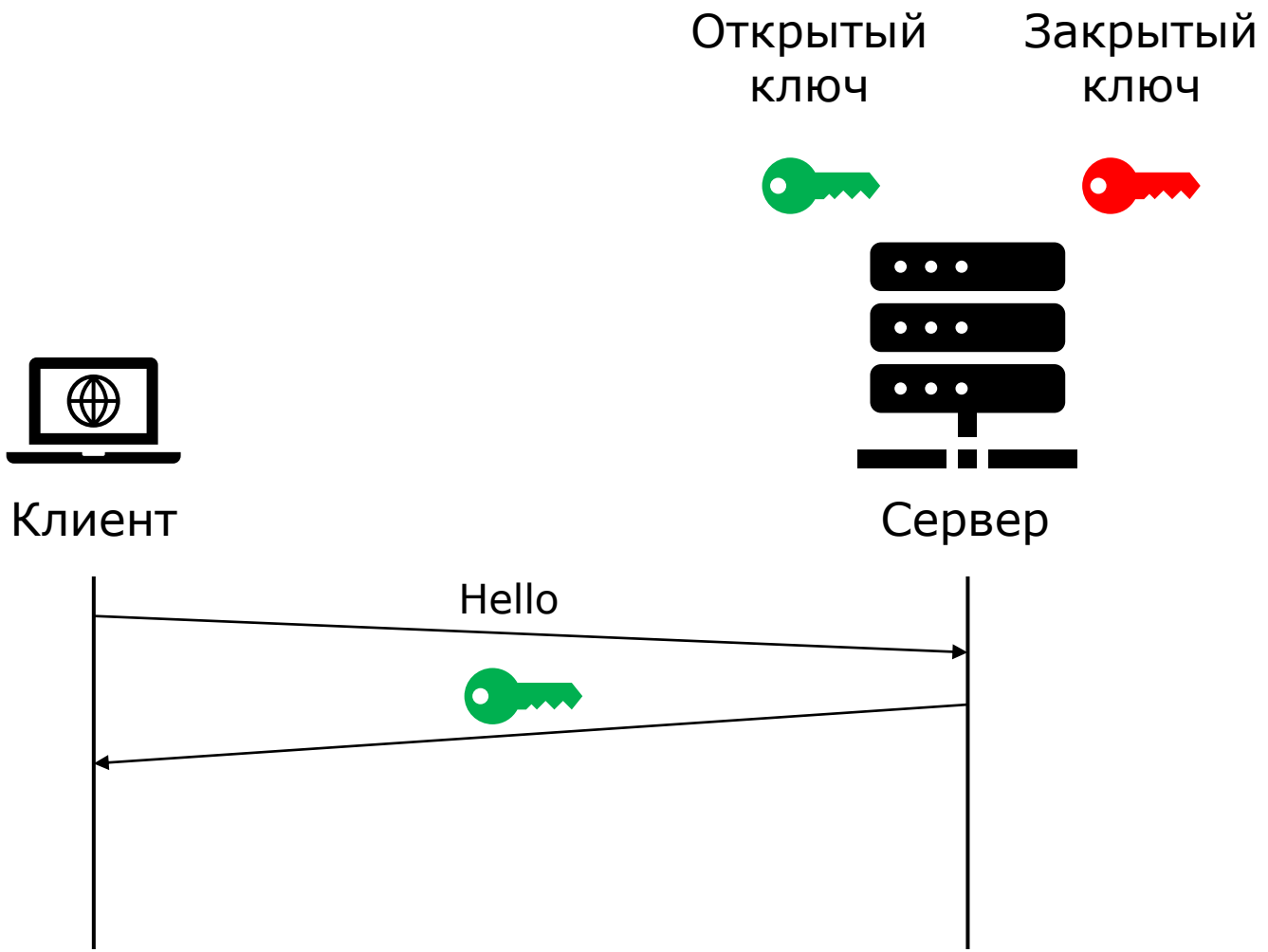
Алгоритм обмена ключами RSA



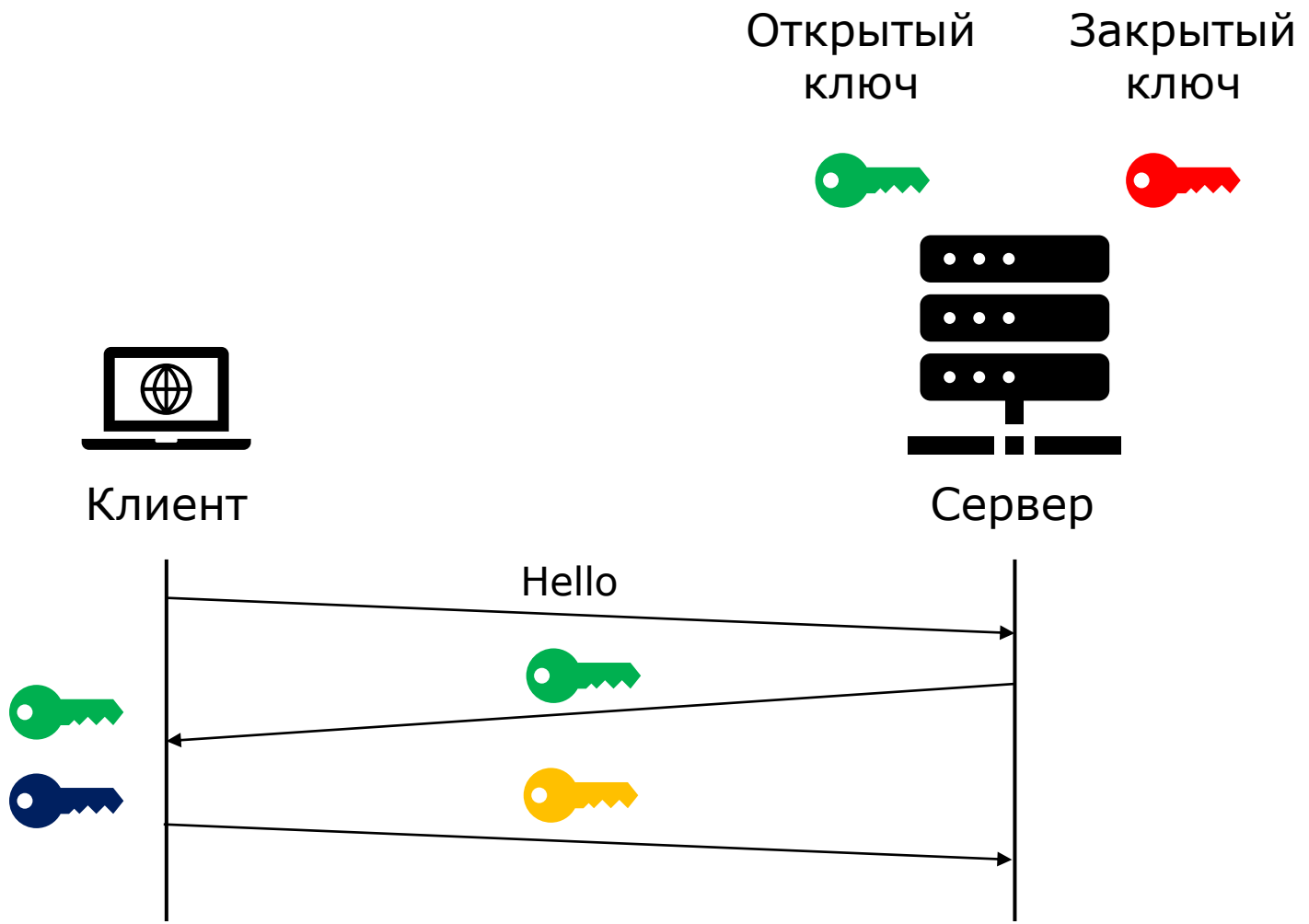
Алгоритм обмена ключами RSA



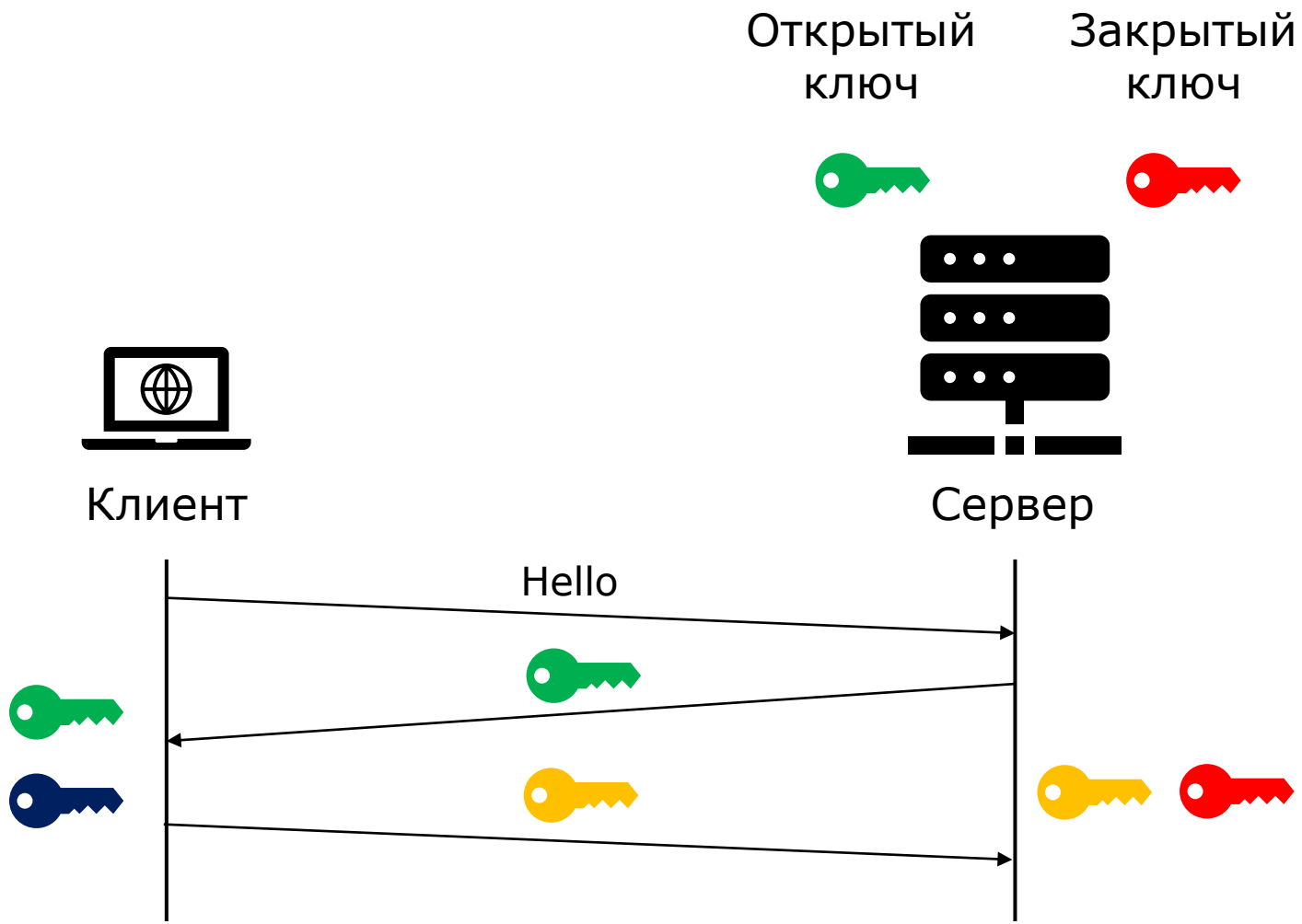
Алгоритм обмена ключами RSA



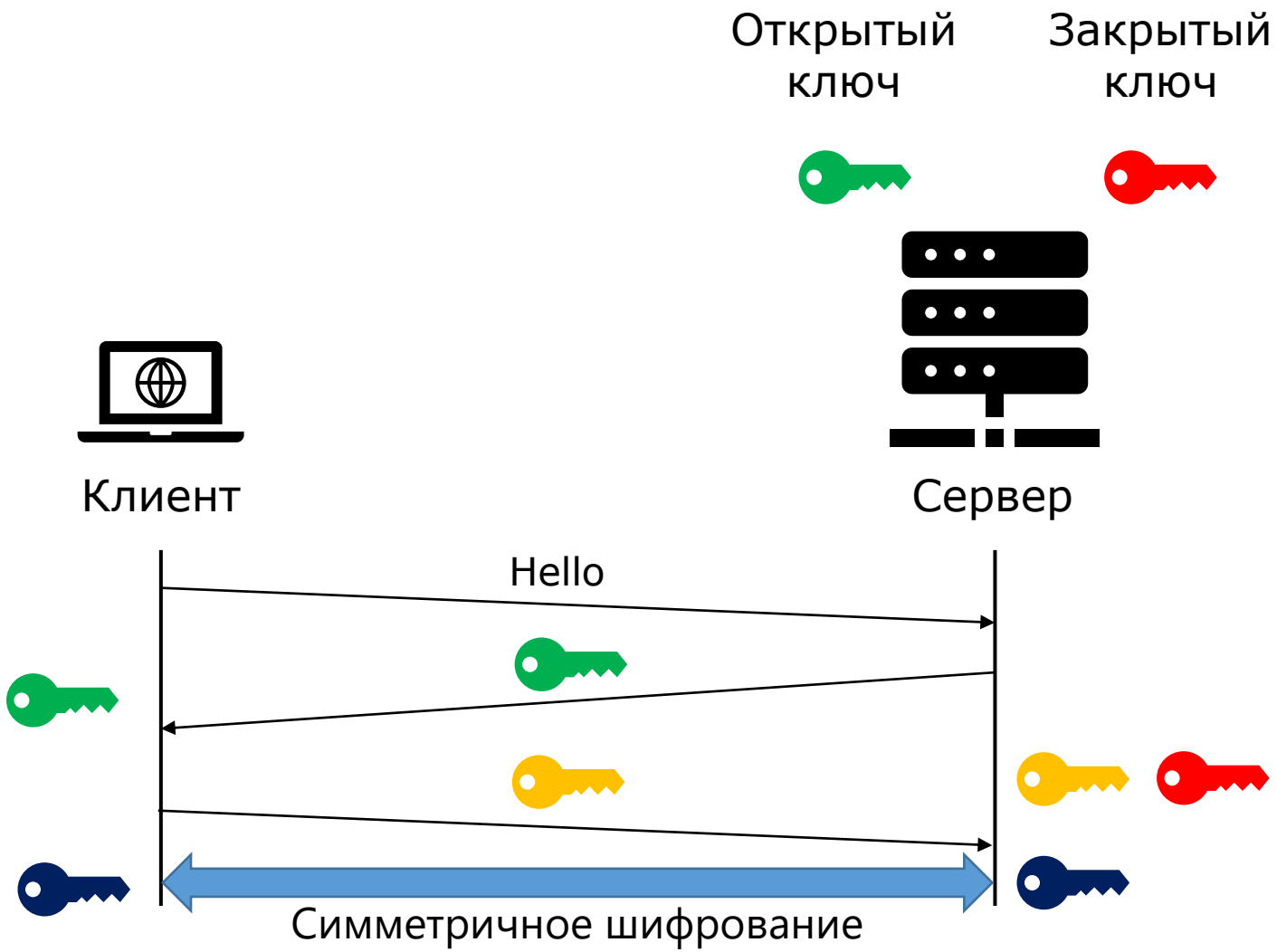
Алгоритм обмена ключами RSA



Алгоритм обмена ключами RSA



Алгоритм обмена ключами RSA



Недостатки алгоритма обмена ключами RSA

Не обеспечивается совершенная прямая секретность (Perfect forward secrecy):

- Доступ к закрытому ключу сервера позволит расшифровать все передаваемые данные

Уязвимости RSA:

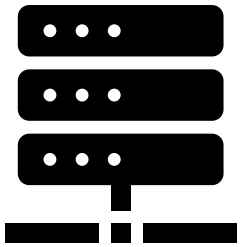
- Атака миллиона сообщений (million message attack, Bleichenbacher, 1998)
- ROBOT (Return Of Bleichenbacher's Oracle Threat, 2017)

Алгоритм обмена ключами RSA запрещено использовать начиная с TLS 1.3

Алгоритм обмена ключами Диффи-Хеллмана

p = 29
g = 3

Клиент

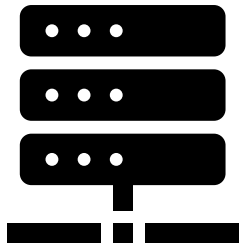


Сервер

Алгоритм обмена ключами Диффи-Хеллмана

p = 29
g = 3

Клиент



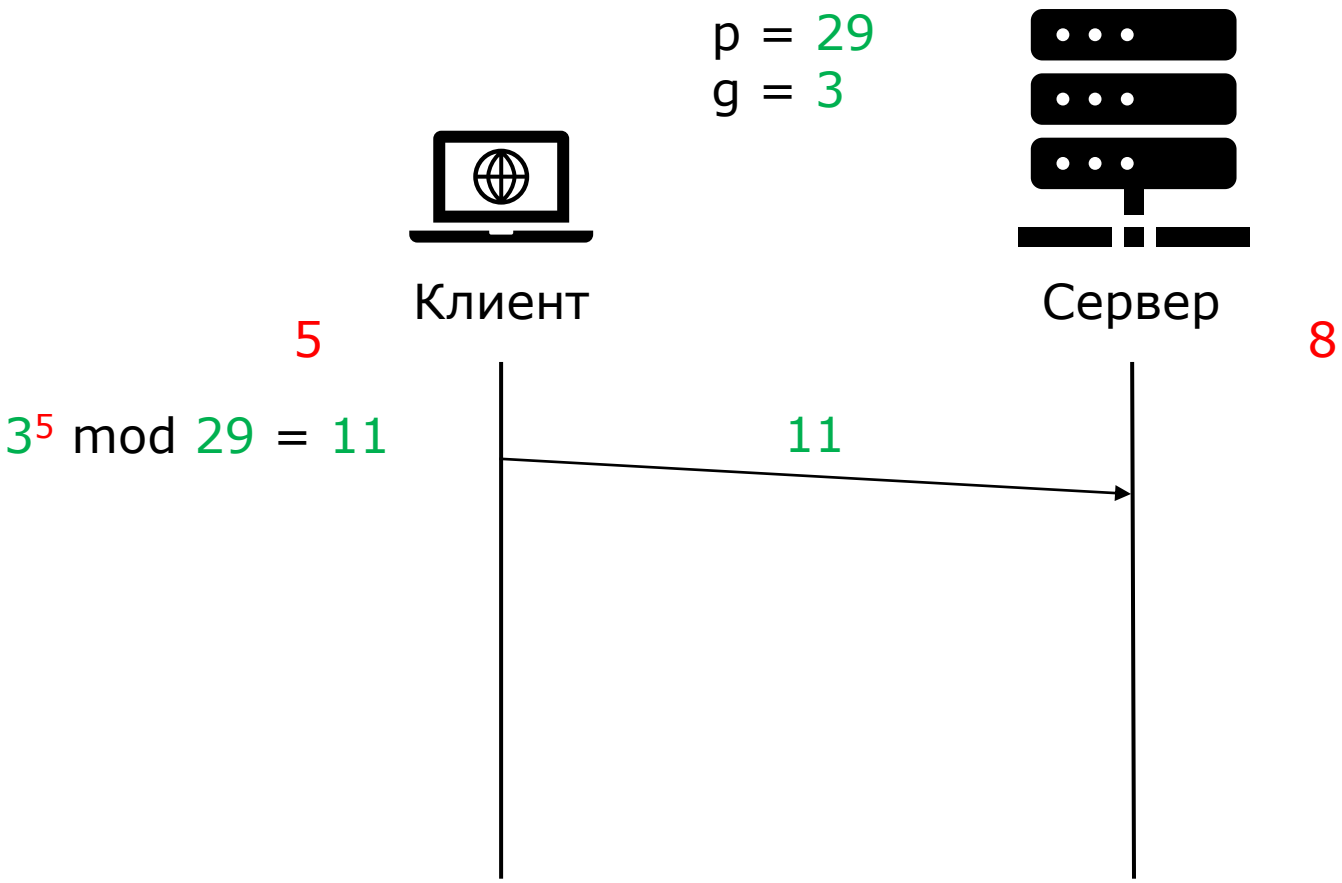
Сервер

5

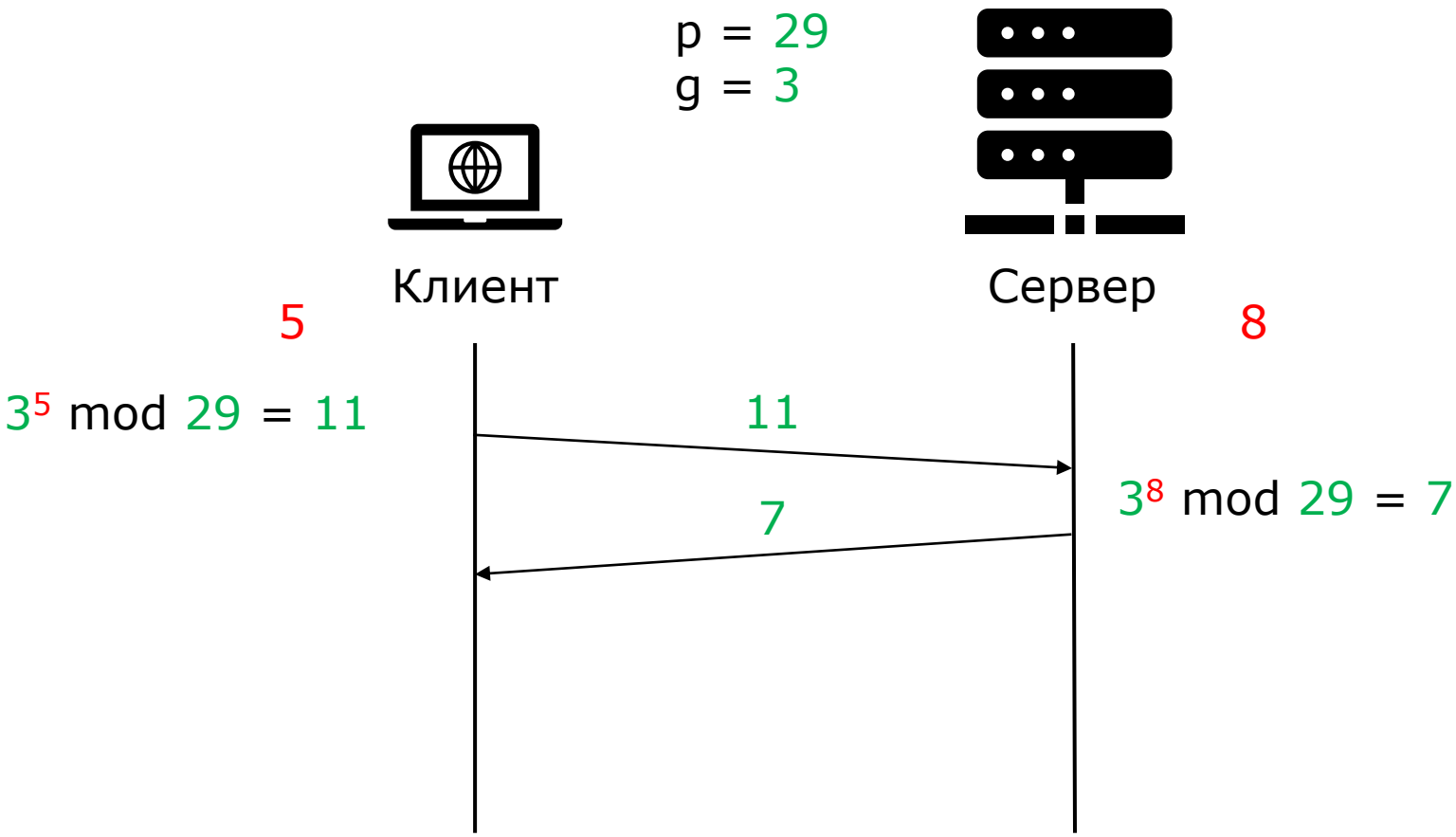
$3^5 \bmod 29 = 11$

8

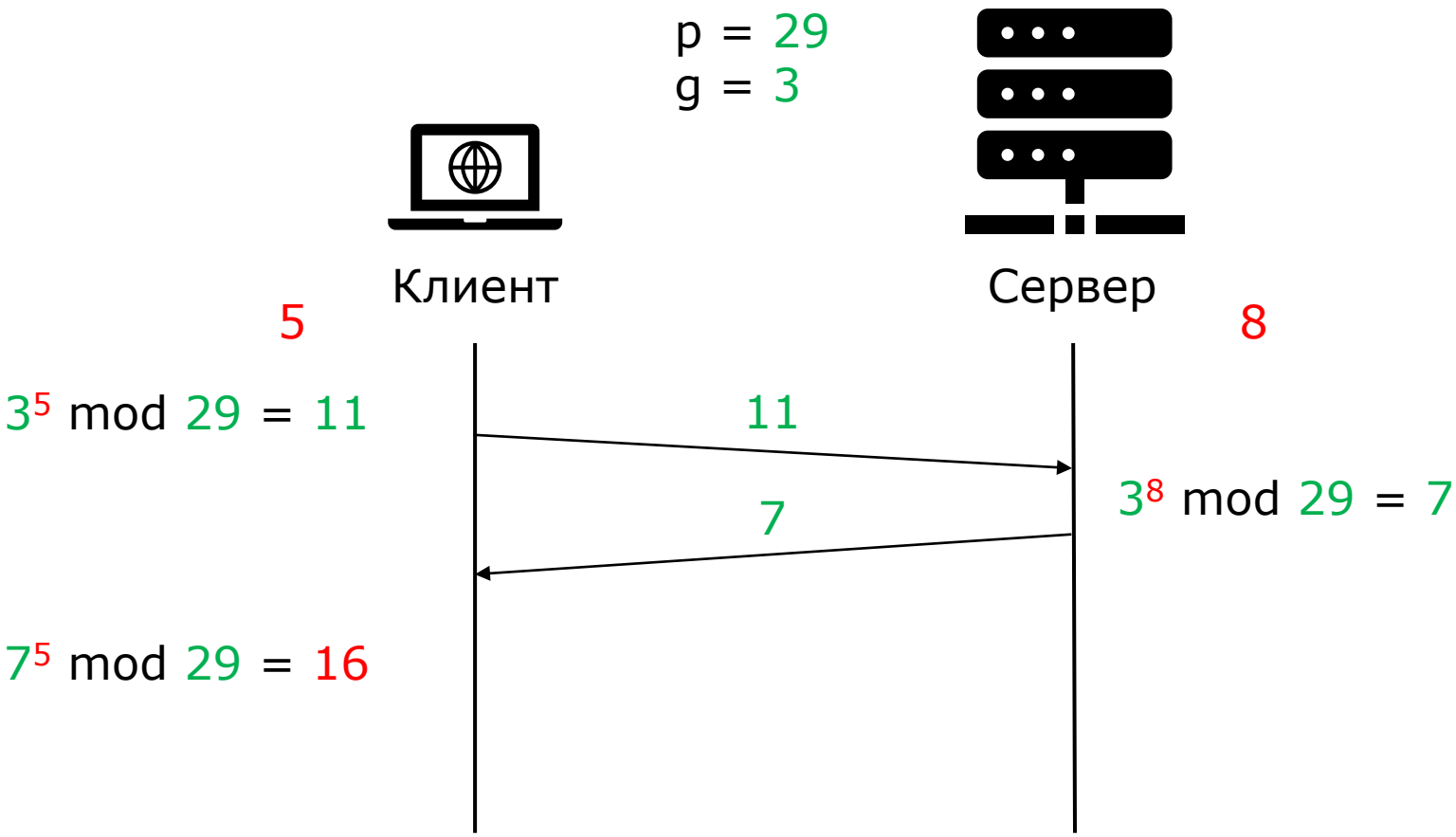
Алгоритм обмена ключами Диффи-Хеллмана



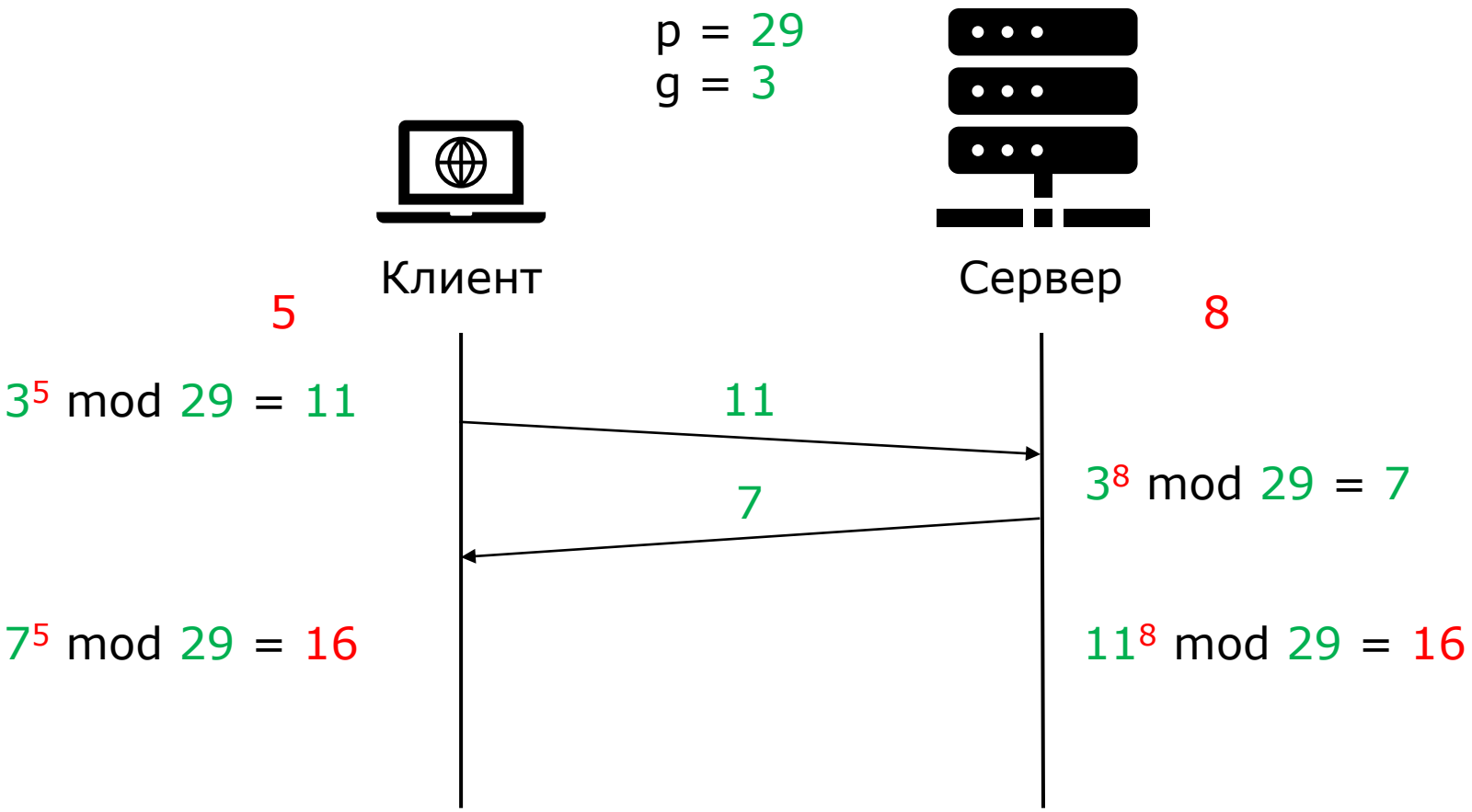
Алгоритм обмена ключами Диффи-Хеллмана



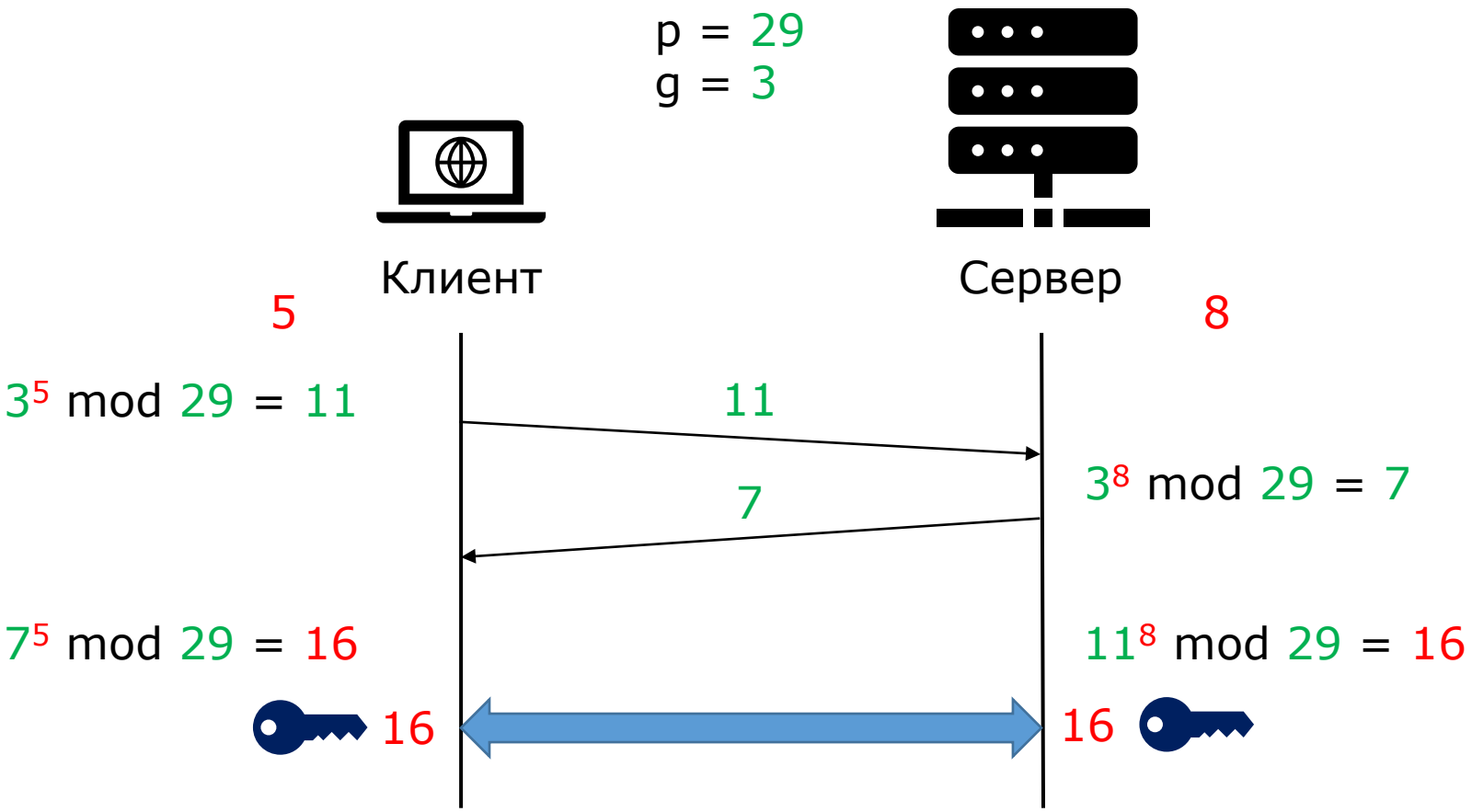
Алгоритм обмена ключами Диффи-Хеллмана



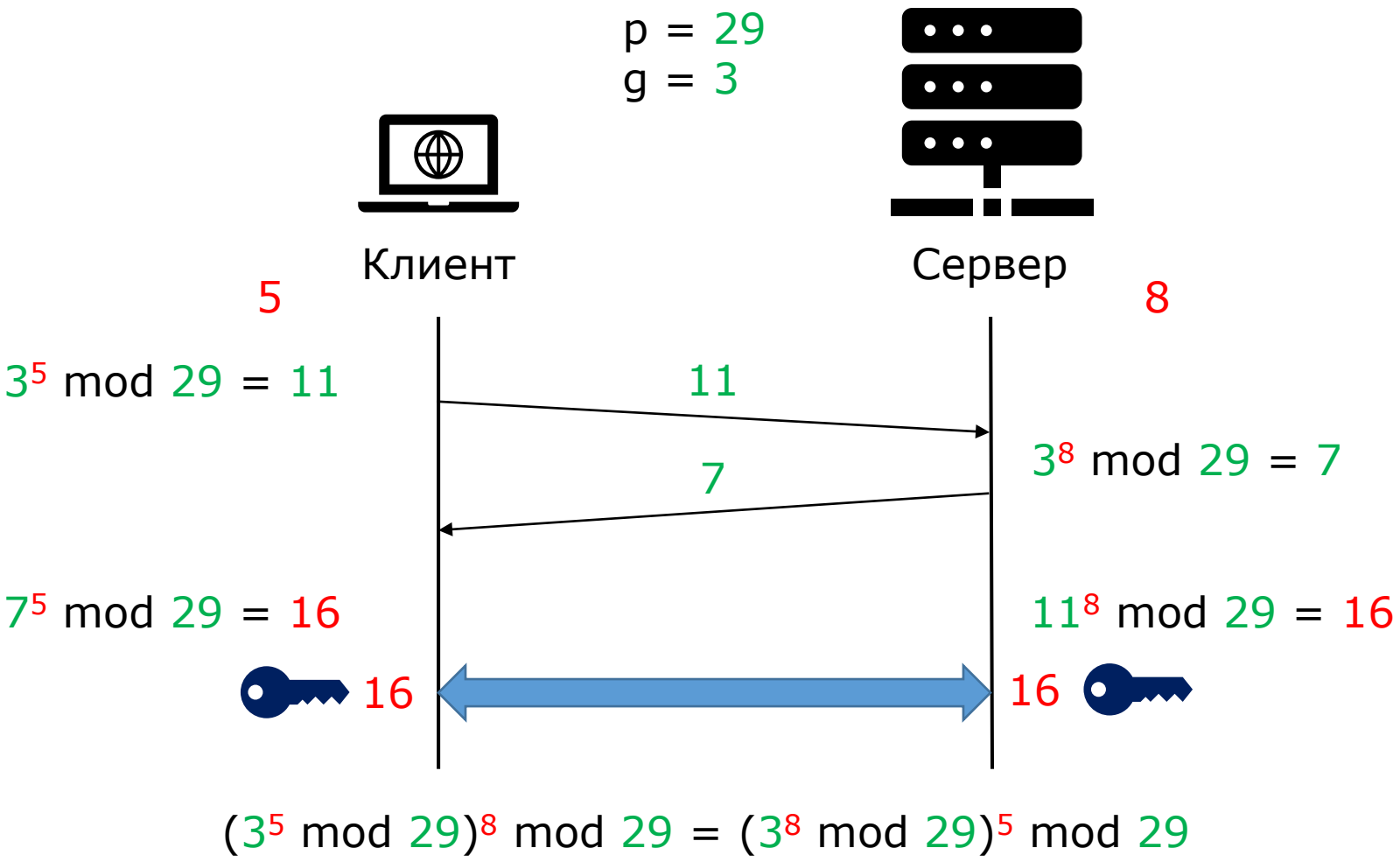
Алгоритм обмена ключами Диффи-Хеллмана



Алгоритм обмена ключами Диффи-Хеллмана



Алгоритм обмена ключами Диффи-Хеллмана



Алгоритм обмена ключами Диффи-Хеллмана

Условия работы алгоритма Диффи-Хеллмана:

- p – большое простое число, минимум 1024 бита
- g – первообразный корень по модулю p, небольшое целое число
- Невозможно вычислить ключ даже на современных суперкомпьютерах

Совершенная прямая секретность:

- Невозможно раскодировать зашифрованные данные, даже если есть доступ к серверу

Более совершенный вариант алгоритма:

- Диффи-Хеллман на эллиптических кривых

Итоги

Гибридное шифрование в TLS/SSL:

- Симметричное шифрование для передачи данных
- Ассиметричное шифрование для обмена ключами

Набор шифров TLS (cipher suite):

- Алгоритм обмена ключами (RSA, DH)
- Алгоритм симметричного шифрования (AES, 3DES и др.)

Установка соединения TLS:

- Выбор поддерживаемого набора шифров TLS
- Обмен ключами для симметричного шифрования

Совершенная прямая секретность:

- Невозможность расшифровать переданные данные при получении доступа к серверу