
CRYPTO
PARTY

Приватность

Право на выбор самовыражения

Личное пространство

лаборатория мыслей

Фундаментальное право

Пренебрежение личным правом влечет ограничение права других

Культура массовой слежки

Контроль

Приватность опирается на безопасность

Безопасность

То, что находится между представлением того, как работают вещи и как они работают *на самом деле*.

Безопасность нельзя
купить, скачать или установить

Безопасность - это процесс

Для безопасных коммуникаций нет бизнес модели

Интернет

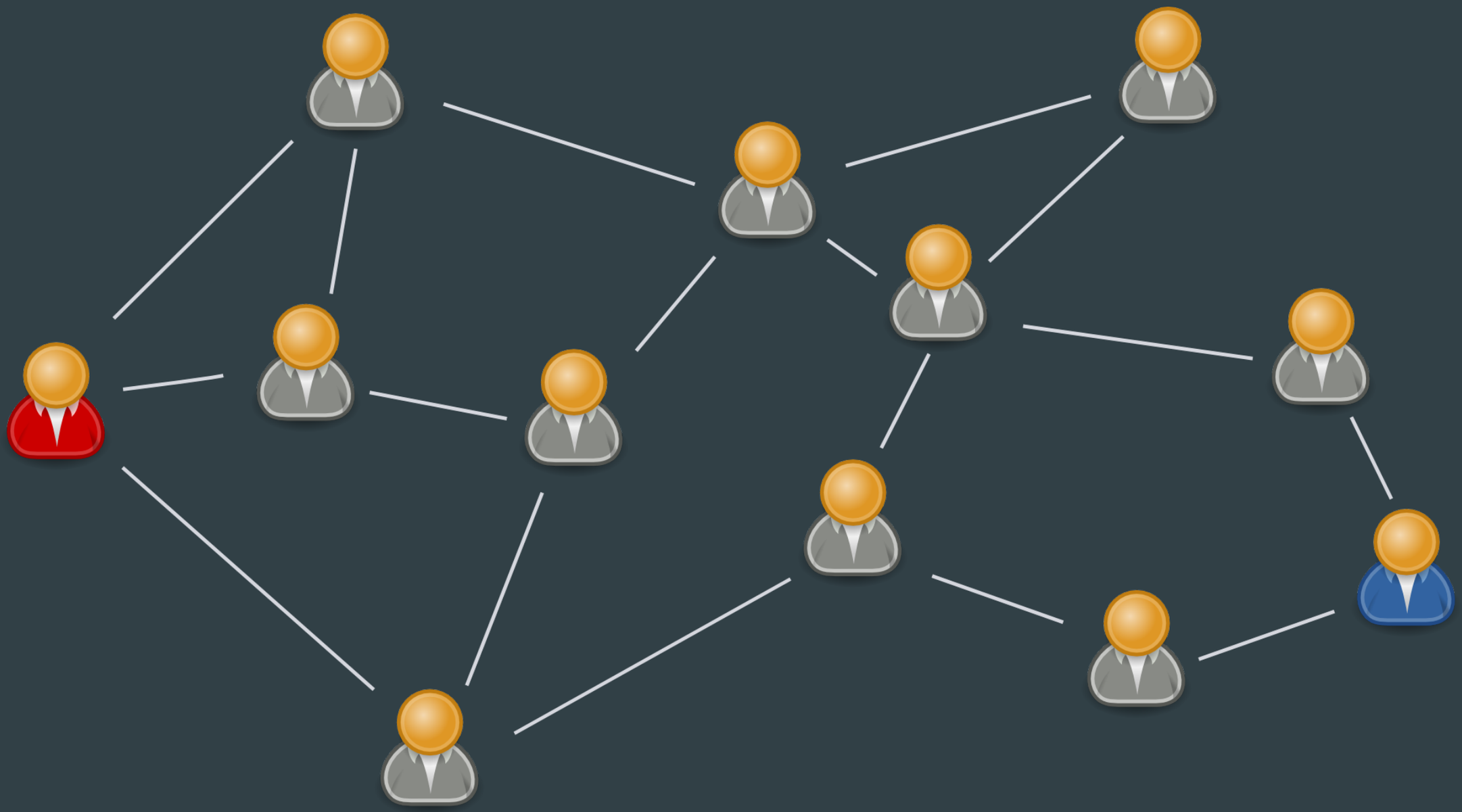
Интернет вошел в нашу жизнь

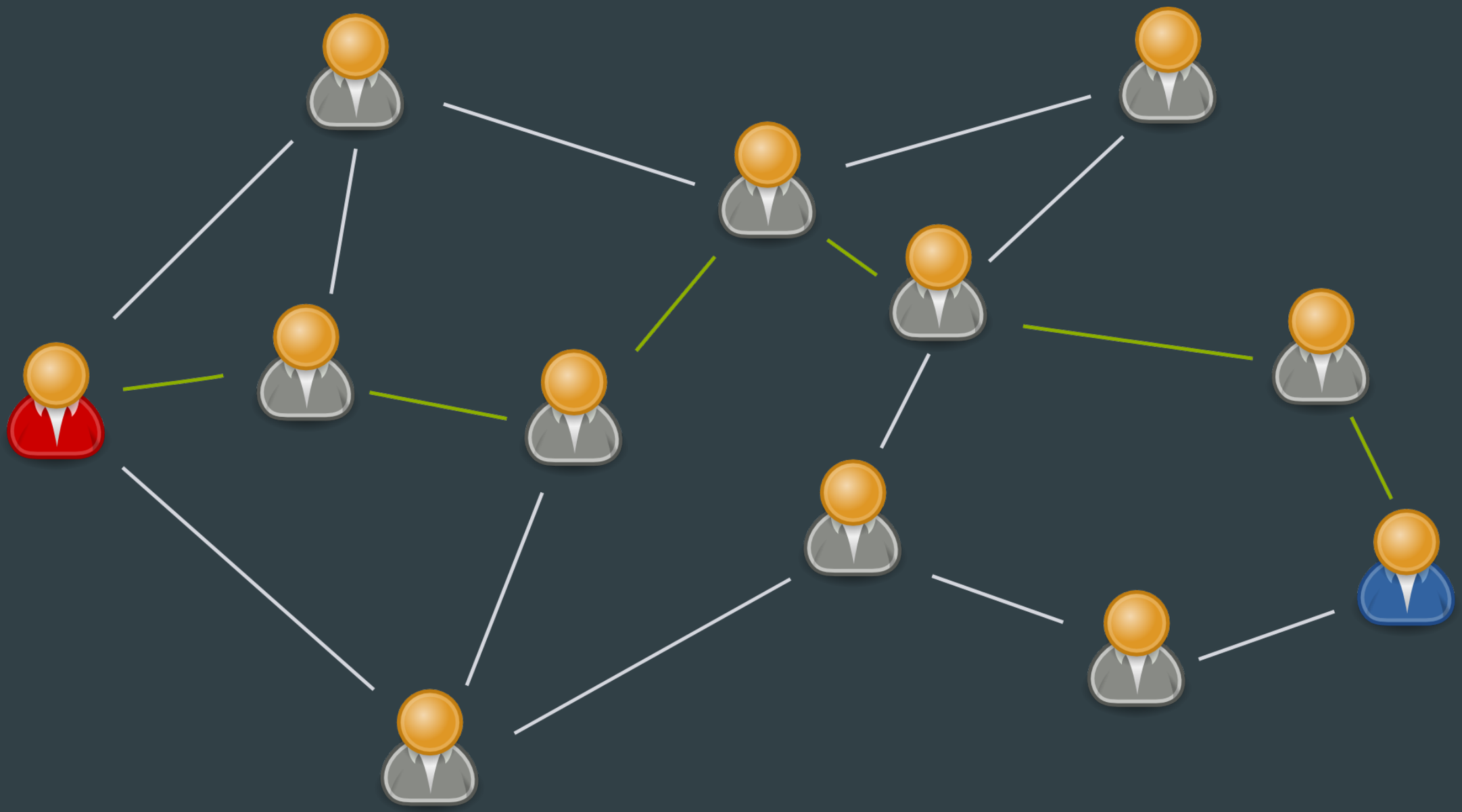
Как передается информация через Интернет?

Интернет - сеть сетей

Передача из одной сети в другую

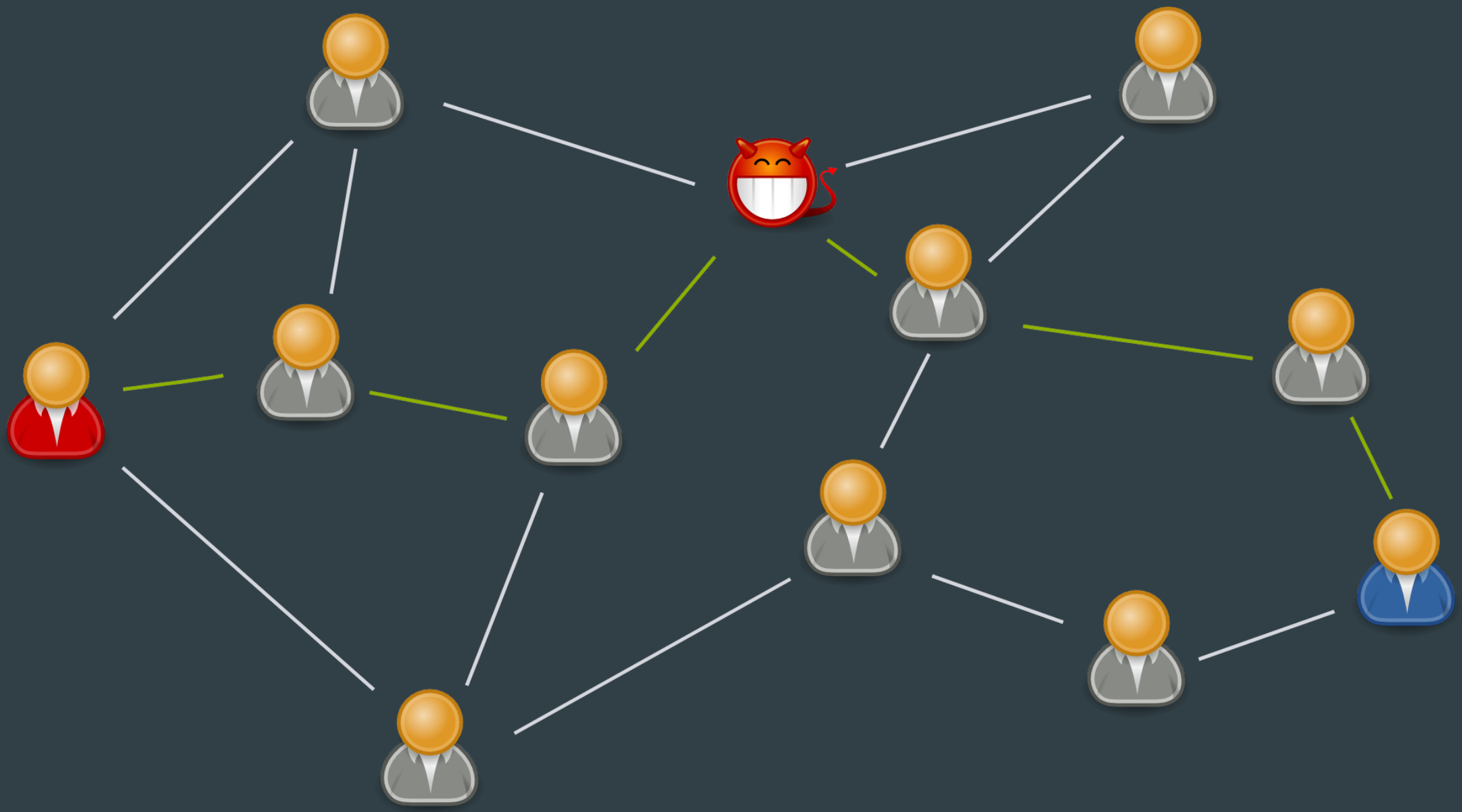
Через множество посредников

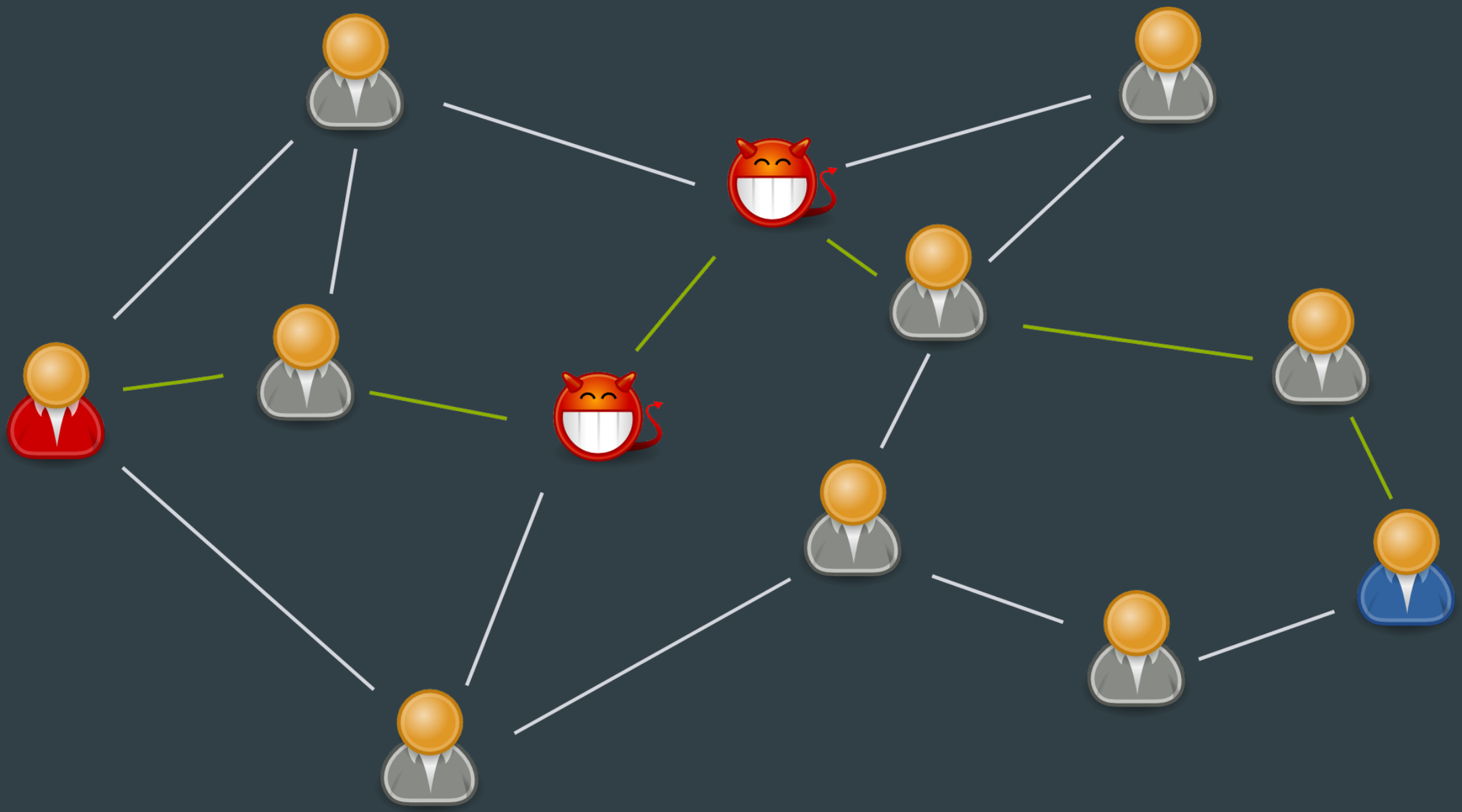


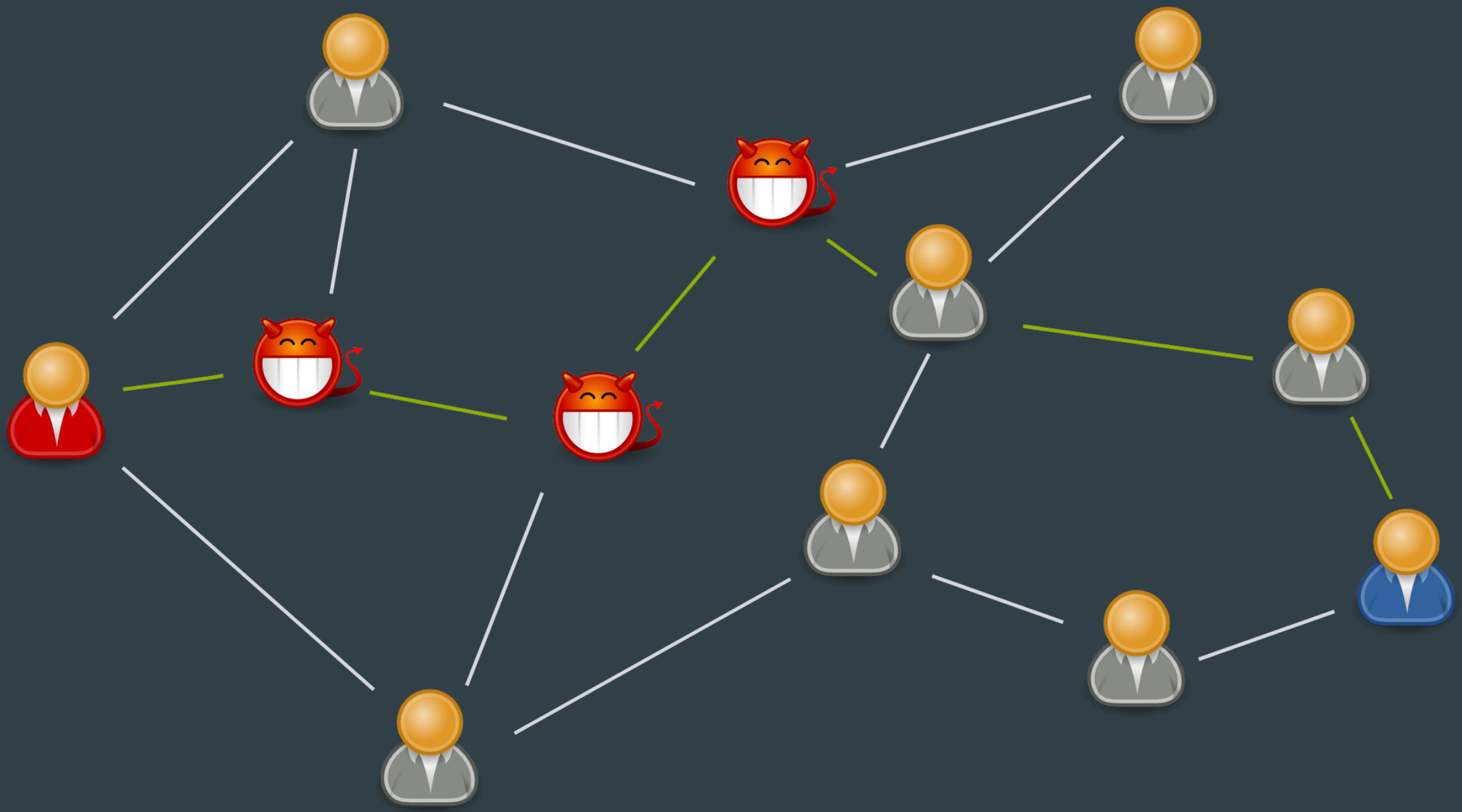


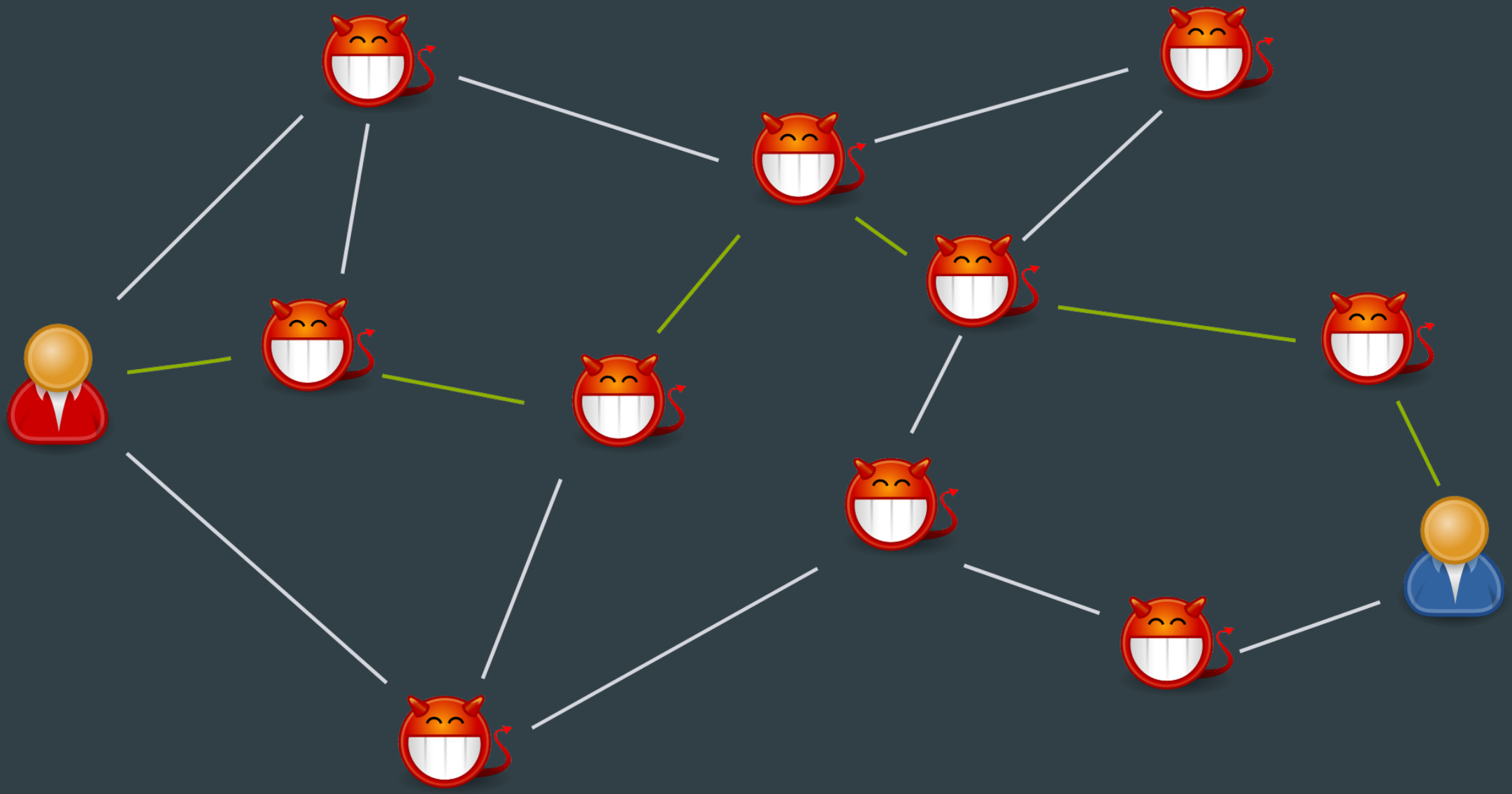
Интернет - *просто* сеть передачи данных

Посредниками могут быть *кто-угодно*









Криптография -
методы безопасных коммуникаций

Что такое шифрование?

Методы превращения полезной информации в бессмыслицу

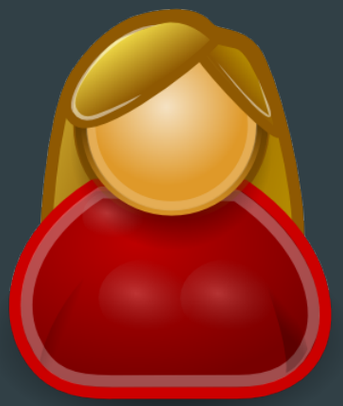
Бессмыслицу, которая ”понятна” только вам

было: cu at cryptoparty
стало: 9d23fb0afafa37a57dafa

Какое бывает шифрование?

Симметричное

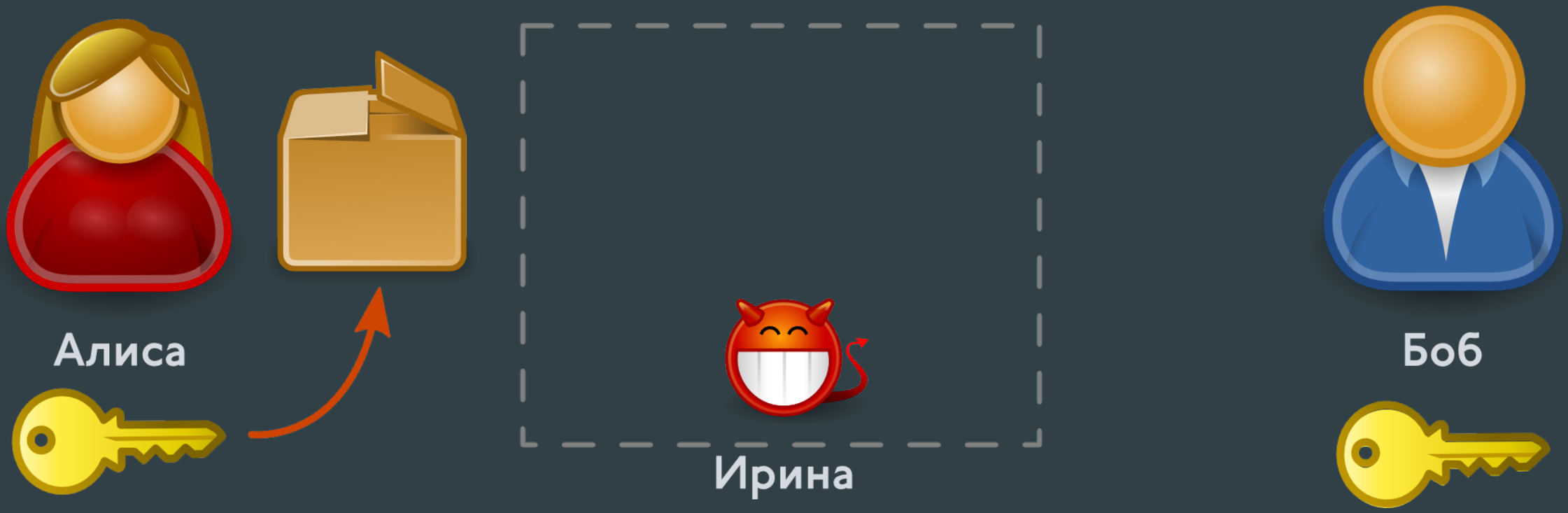
Единый ключ на зашифровку и на расшифровку

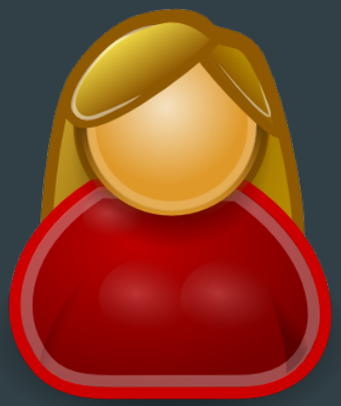


Алиса

Ирина

Боб

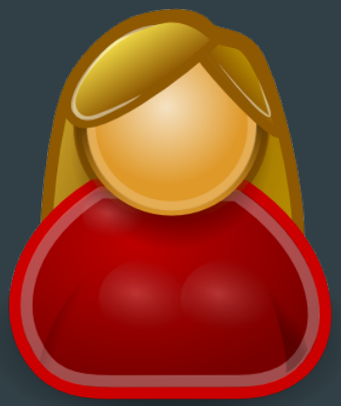

Алиса
Ирина
Боб



Алиса

Ирина

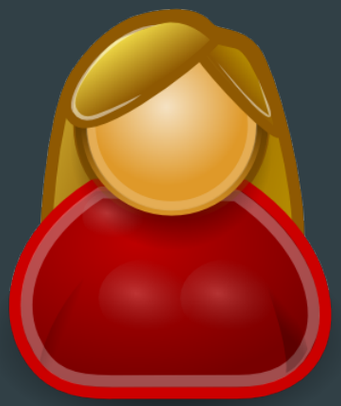
Боб



Алиса

Ирина

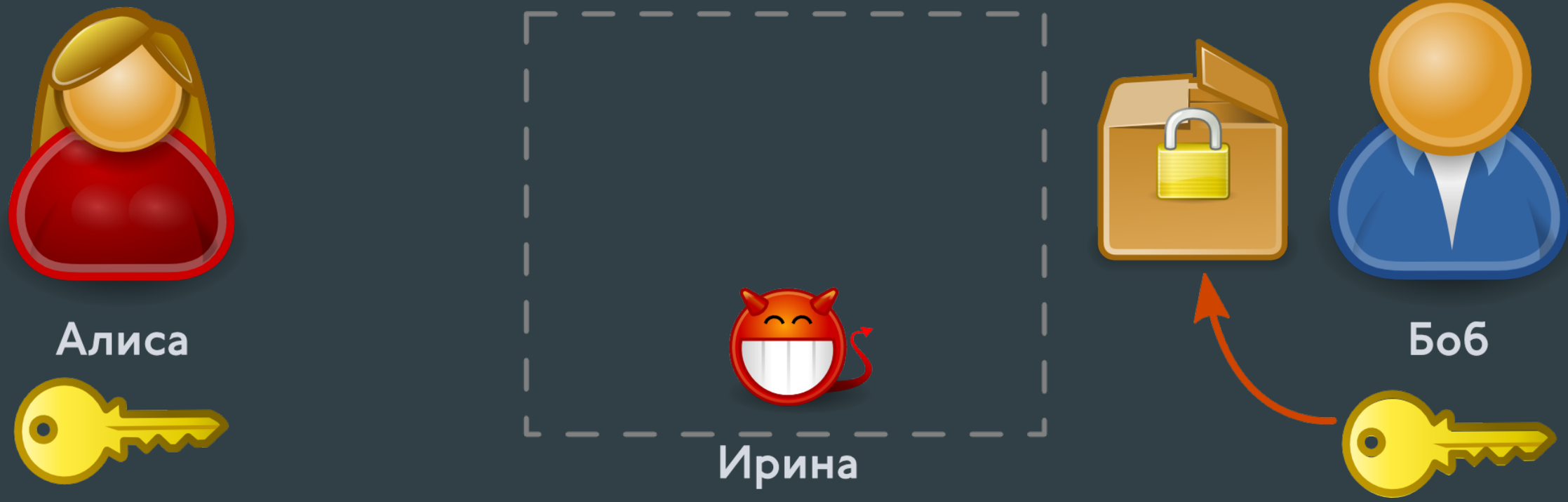
Боб

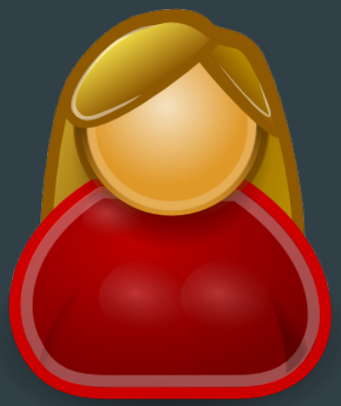


Алиса

Ирина

Боб


Алиса
Ирина
Боб



Алиса

Ирина

Боб

Например, симметричный ключ выглядит так:
e3594d0ce14fd79425921123d8ec81ea

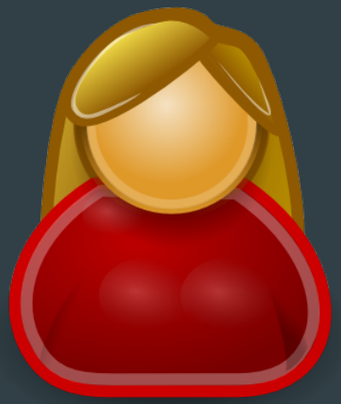
Например, шифрование паролем

Как безопасно передать ключ публично?

Асимметричное

Криптосистема с публичным ключом

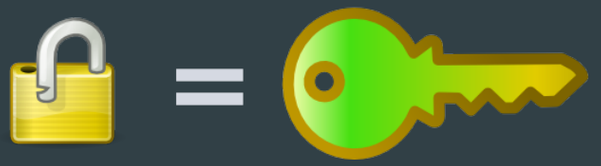
Публичный ключ
для зашифровки
Закрытый ключ
для расшифровки

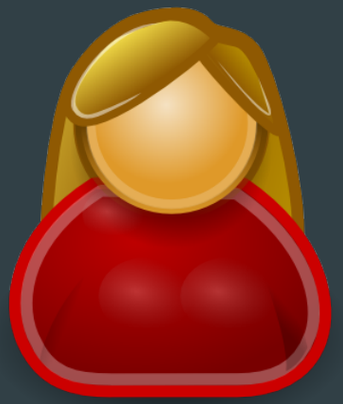


Алиса

Ирина

Боб

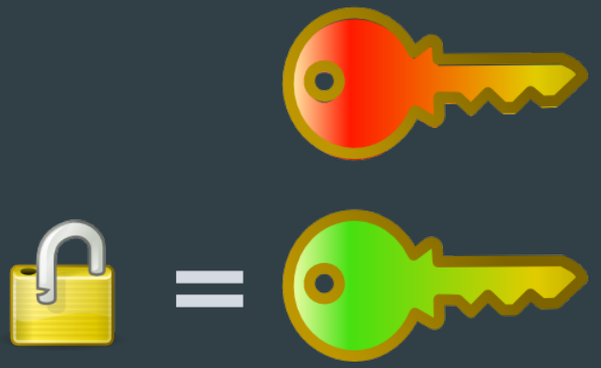


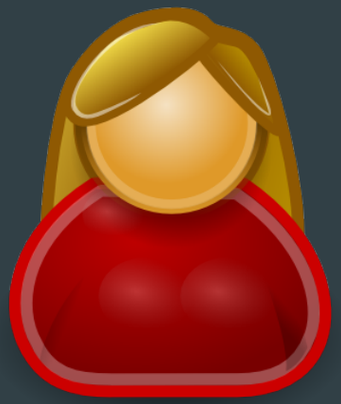


Алиса

Ирина

Боб

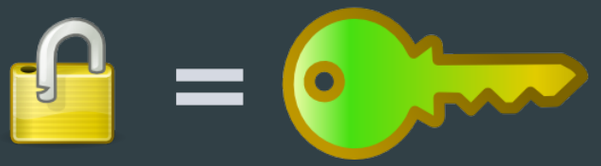


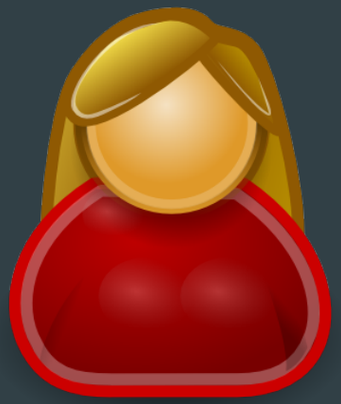


Алиса

Ирина

Боб

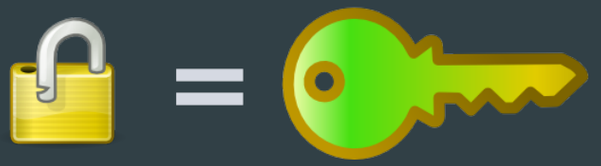


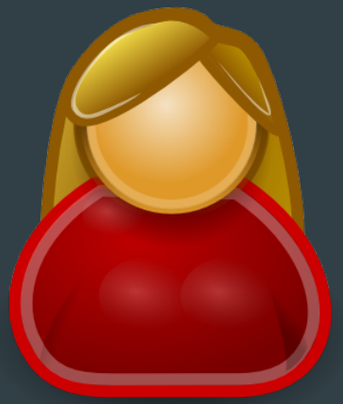


Алиса

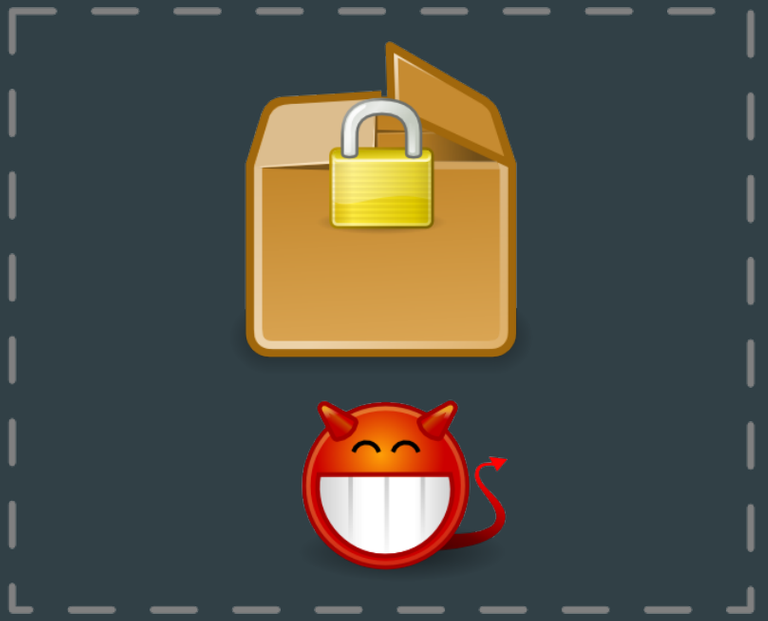
Ирина

Боб



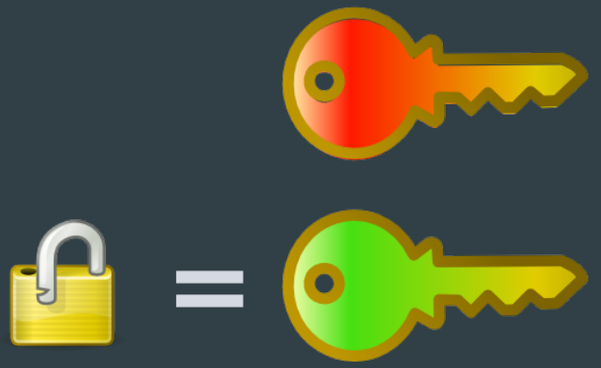


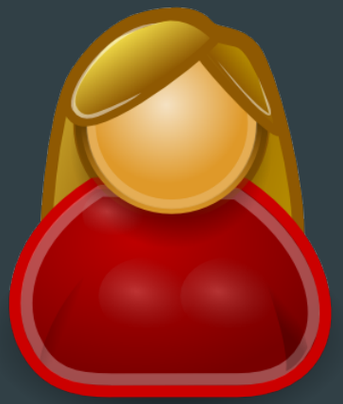
Алиса



Ирина

Боб

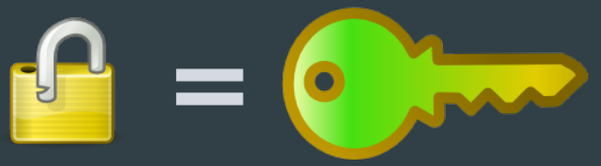


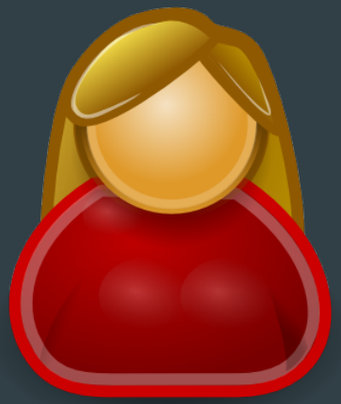


Алиса

Ирина

Боб

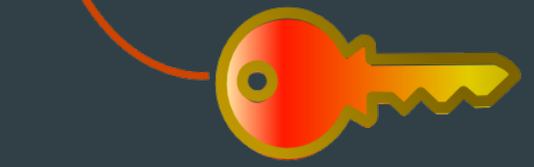


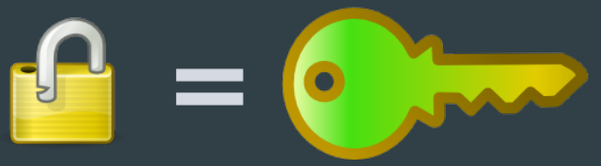


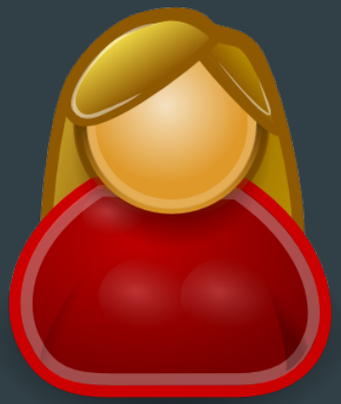
Алиса

Ирина

Боб



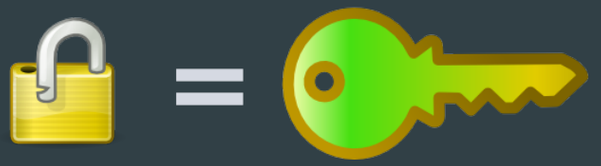




Алиса

Ирина

Боб



Например, публичный ключ выглядит так:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mI0EV+8yFwEEAOygoNBKEPl/SiNxPb3Uq5W75cX9B2TmwYagLboifZdiCxozj7XX
b39QPmjeHnoxWKYGSfshGbKGW+RpqjNJkUwyjlJp5lH70Kj3JjLy36h3fJ963vcg
Ur0UKyTn+QIs5ePogSVyHhfC45RPwkZRmd4/HPhMBuNDFUIw/AN0XRYfABEBAAG0
C0NyeXB0bIBhcnR5iLgEEwECACIFAlfvMhcCGwMGCwkIBwMCBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEIwmVKbI7KOs/UAD/IaZYs7gaEUtnhERkh05mRIH8xTDnPFdIdv9
bTiqrdtyIOLnSuI7P8XoUvxjkvlyI/NMgENS8WOYXK+iDXvikZ9MqnRjhM/NErNI
05apOJ0/JoTw+Ks0bUhUcfZSbjNOC0VakNKY74HEKffV3e+c/igIJzUAyEkM+sIM
A+d0XwZx
=3/wJ
-----END PGP PUBLIC KEY BLOCK-----

Например, закрытый ключ выглядит так:

-----BEGIN PGP PRIVATE KEY BLOCK-----
lQHYBFfvMhcBBADsoKDQShD5f0ojcT29IKuVu+XF/Qdk5sGGoC26In2XYgsaM4+I
I29/UD5o3h56MVimBkn7IRmyhlvkaaozSZFMMo5SaeZR+9Co9yYy8t+od3yfet73
IFK9FCsk5/kCLOXj6IElch4XwuOUT8JGUZnePxz4TAbjQxVNcPwDdF0WHwARAQAB
AAP/XlSShzZfmfbCiWqFYH29gU2Mhece4XyUPaTxVbiWNJkjL+jKK4WcrzZACvlx
WCj/2/+50mEZq2+ghmgRL6zuPJvP38K7HY+jg5f4S87RjkIR2rP+P0X775xCNI++
v4BvJDmA98+lWEZ9DojUI8x005TMSHPfb05ah94sLWoXjyECAPIRJQRJCM7oFRrb
MkTiYBVOHjHB3O+o2KlVqirnV3n4zrfMBSBUnpRcpZ3YxHqII2Hvis9kmNDfoDBj
28LLTKkCAPo/VRNbFUs8Edtad5XaCSdoYC/r+p3UG+d5QMojpRojk5YIxRZ+ZZEC
nupThcr9CYNnREqucv6+Z7vSbAbjAYcB/RGSJOjflHQ05o+bNYaU9JeOSZ9AySoo
TeKL9b/rpS+czkzL3eyWTm97kM3bce7OeVSTP5LhOkdKHe+/jHm5RE6ni7QLQ3J5
cHRvUGFydHmluAQTAQIAIgUCV+8yFwIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgEC
F4AACgkQjCZUpvXso6z9QAP/VplizuBoRS2eERGSHTmZEgfzFMOc8V0h2/ItOKqt
23Ig4udK7Xs/xehS/GOS+XLX80yAQILxY5hcr6lNe+KRn0yqdGOEz80Ss0jTlqk4
nT8mhPD4qzRtSFRx9lJuM04LRVqQ0pjvgcQp99Xd75z+KDUnNQDISQz6zUwD53Rf
BnE=
=972B
-----END PGP PRIVATE KEY BLOCK-----

Сквозное шифрование

end-to-end encryption

Шифрование без третьих лиц

Forward Secrecy

Будущая секретность

Сообщения одноразовые

Прошлые сообщения не поддаются расшифровке

Цифровая подпись

Только Боб может создать подпись сообщения, которая связана только с этим сообщением. Её можно проверить с помощью публичного ключа Боба.

Создание подписи


Документ
Закрытый ключ
Боб
Документ
Подпись

Проверка подписи


Документ
+
Подпись
Ключ Боба
Павел
?

Например, подписанный документ выглядит так:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

OMG, Im at CryptoParty. Such privacy! So encryption! Yay!
-----BEGIN PGP SIGNATURE-----
iJwEAQEIAAYFAlfvNH8ACgkQjCZUpvXso6zBDQP/aMKOEGTMOci5Io6Za+8s+/CO
WNHDedc/xAwXpGYGAgf4VGLqES+/CIvz/OIO0k8GsWkSeTYqlZKBvKwleio6pIAK
A2wN9zeOeQ6lCOsGoE38/CVuKsXT5J6toPH6t/0lC8NNg9fVlOQfsPwtAaIju9Nx
XCgi+xFShMCm9kHJv3o
==MOAJ
-----END PGP SIGNATURE-----

А что, если замок прислал *не Боб*?

Надо убедиться, что это его ключ

Ручная сверка публичных ключей

Отпечаток ключа

Fingerprint

Короткий ”эквивалент” публичного ключа. Если отпечатки публичных ключей совпадают, значит совпадают и эти ключи.

Например, отпечаток ключа выглядит так:

4I5E 86BB A956 ID0C E5A5 2B95 8C26 54A6 F5EC A3AC

Содержание передаваемых нами данных неизвестно

Метаданные

данные о данных

Размер, время/место передачи, получатель/отправитель...

Метаданные несут очень большую опасность

”Мы убиваем людей на основе метаданных” -

Майкл Хайден, директор АНБ (1999-2005)

Наиболее интересны

Универсальны

Не зависят от языка

Малый объем

Из них можно узнать больше, чем из самих данных

Любимые места, заболевания, пристрастия, социальные связи, настроение, планы на будущее...

Теперь с обязательным хранением

по закону - ”до трех лет”

Важность свободного ПО

Приватность невозможна без безопастости

Безопасность и приватность невозможны без СПО

Доступность всех деталей и исходного кода

Отсутствие ограничений на использование

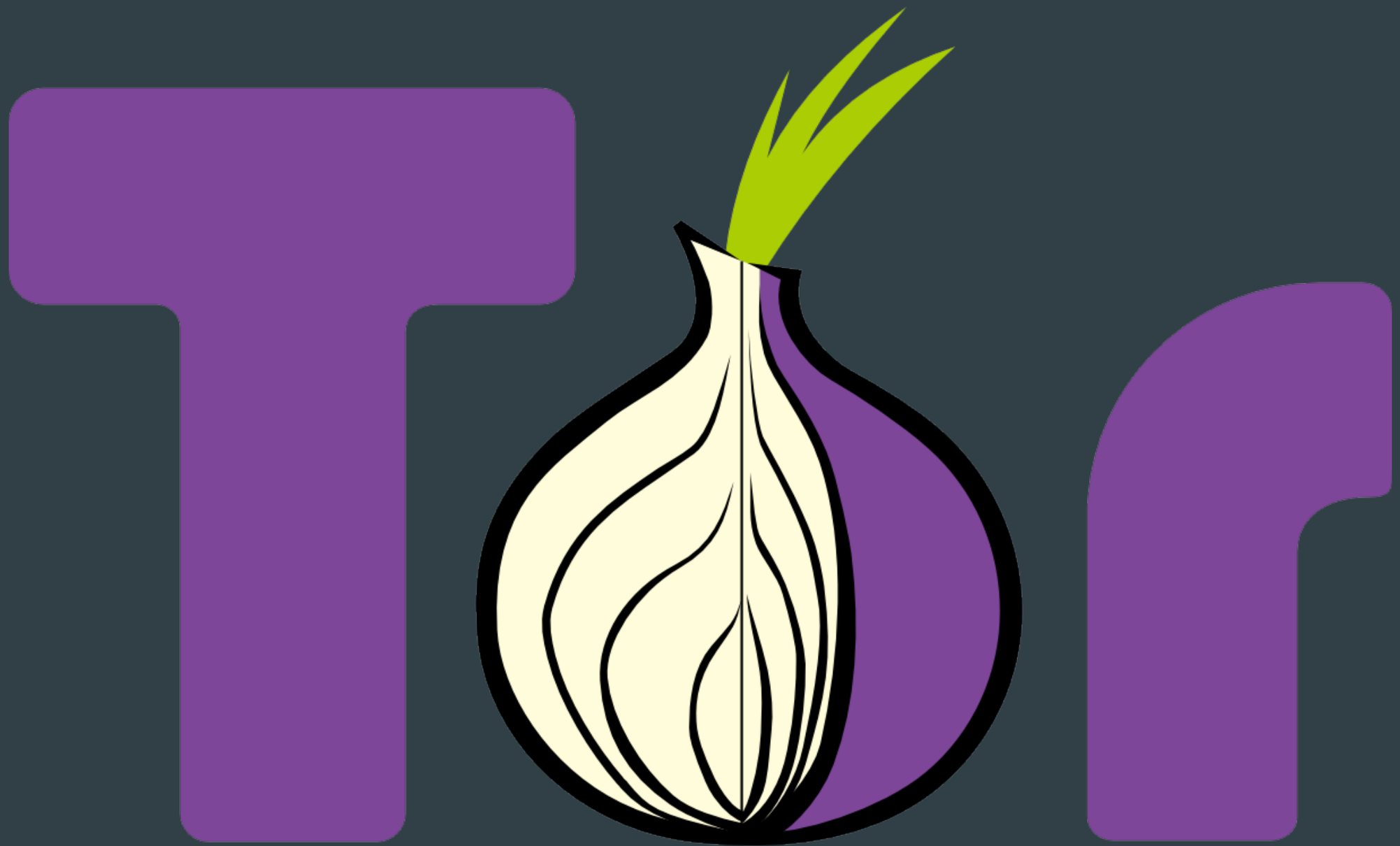
Проверяемость

очень сложно встроить лазейки

Независимость

Основные инструменты защиты приватности

Защита метаданных, сетевой активности и обход цензуры


Tor

The onion router

Луковичный маршрутизатор

Луковичная маршрутизация

Разделение маршрутизации и данных

техническая анонимность

Маршрут выбирает пользователь, а не операторы сети

”Не существует вездесущего наблюдателя”

предположение

(S//REL) Very Secure

(S//REL) Low enough latency for most *TCP* uses

(S//REL) Still the King of high secure, low latency Internet Anonymity

- (S//REL) There are no contenders for the throne in waiting

Как устроен Tor?

Без Tor

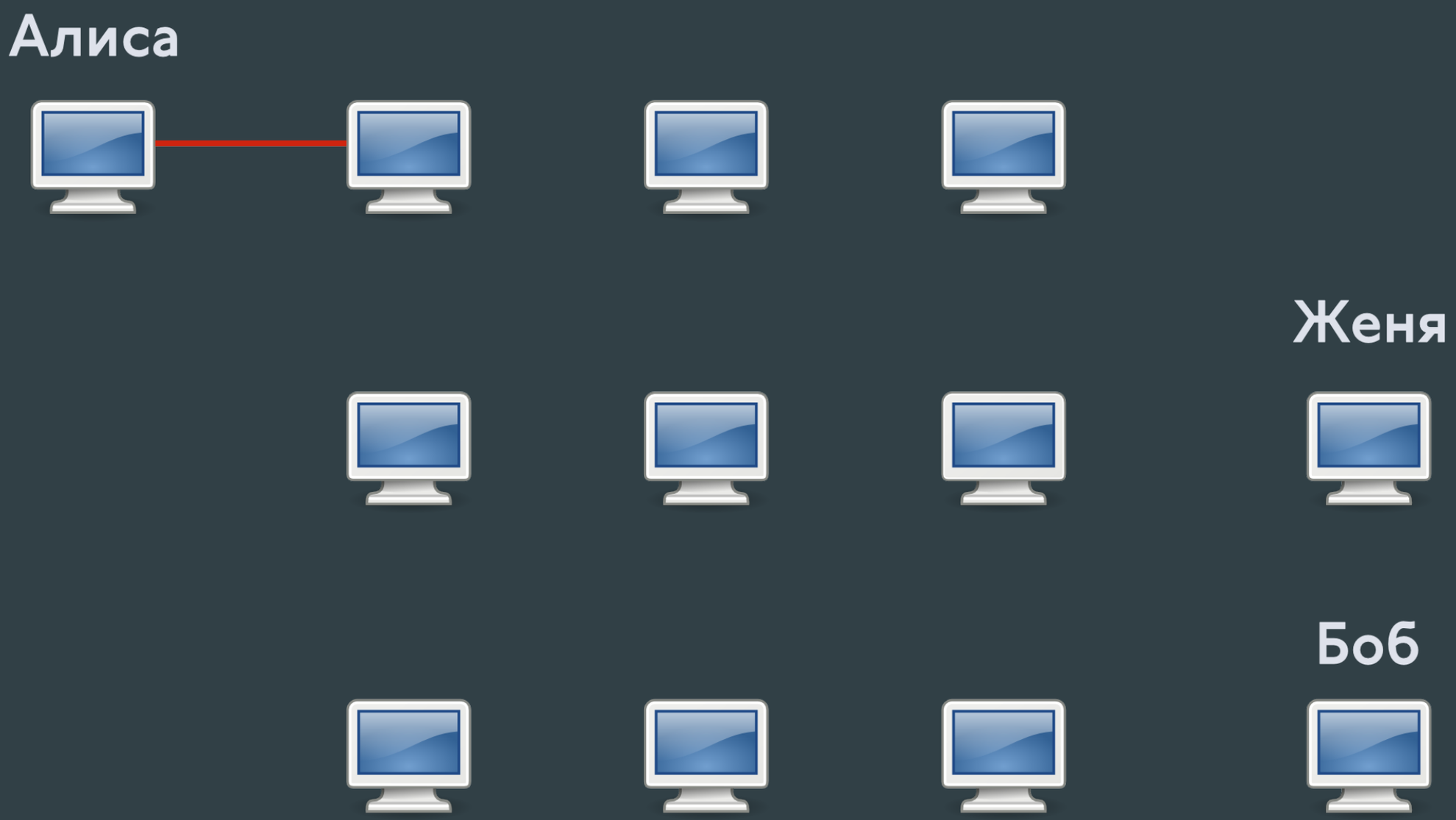
Алиса

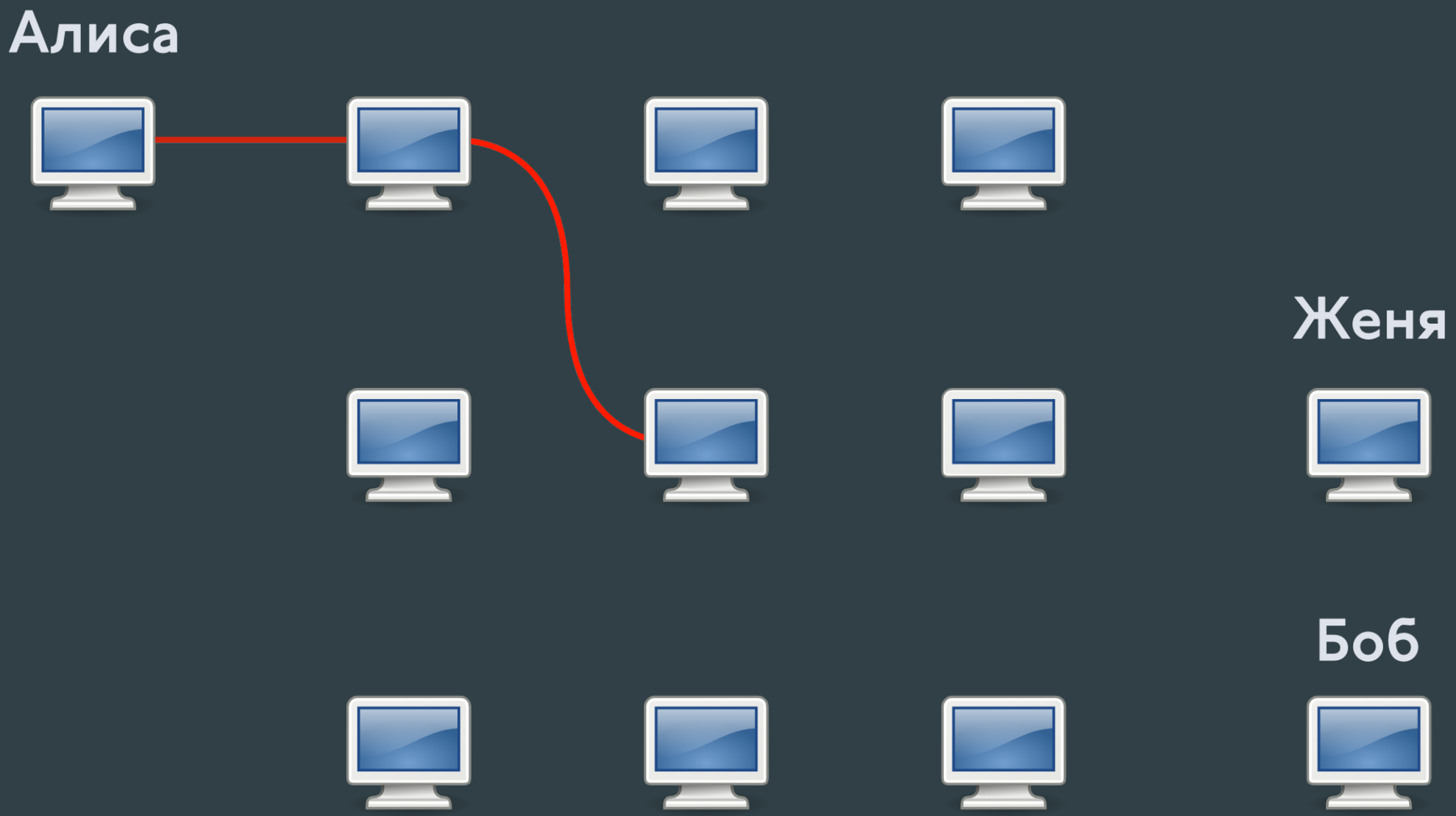
Алиса

Алиса

Женя

Боб


Алиса
Женя
Боб


Алиса
Женя
Боб


Алиса
Женя
Боб


Алиса
Женя
Боб

Выход в Интернет через Tor

Алиса

Женя

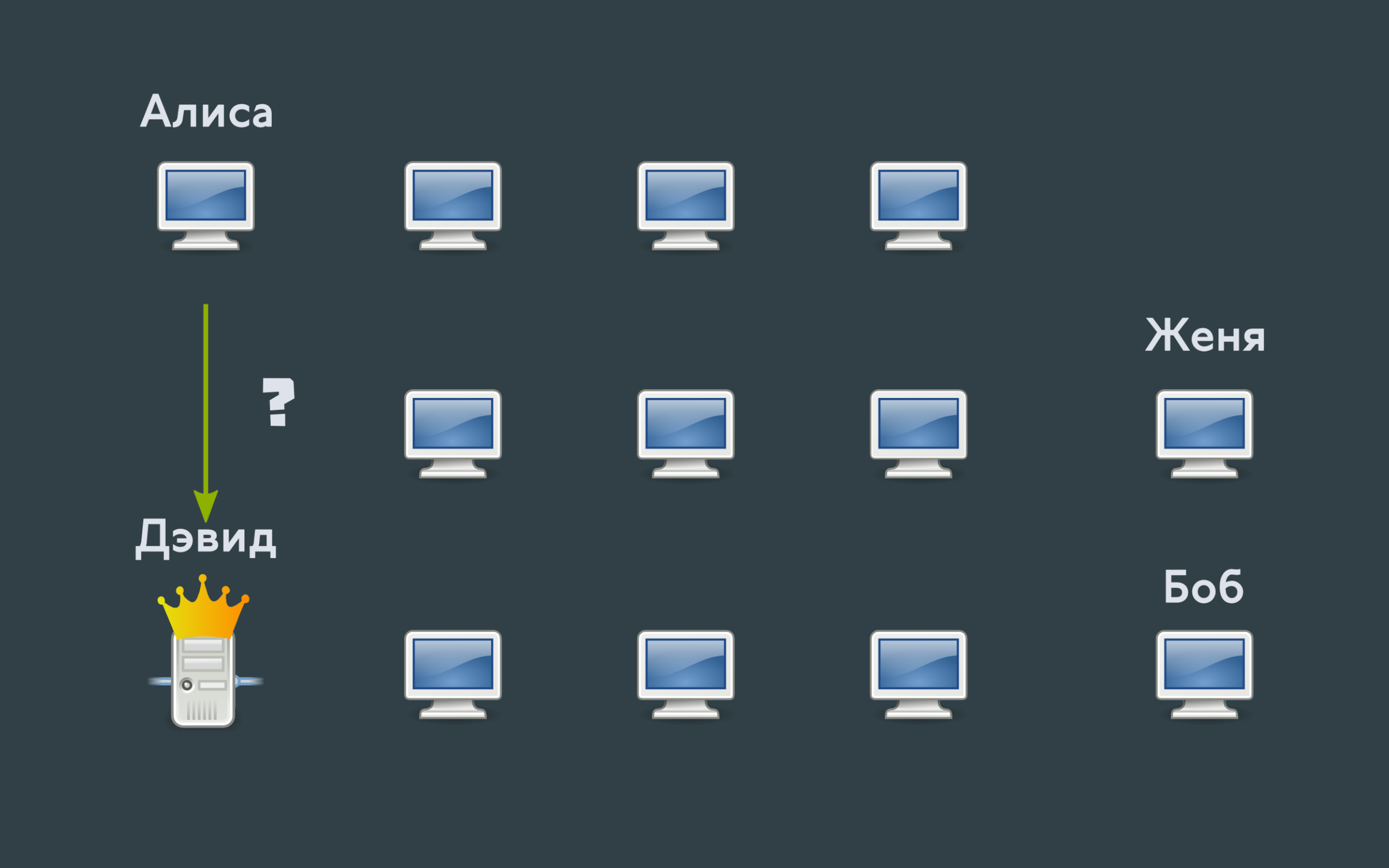
Боб

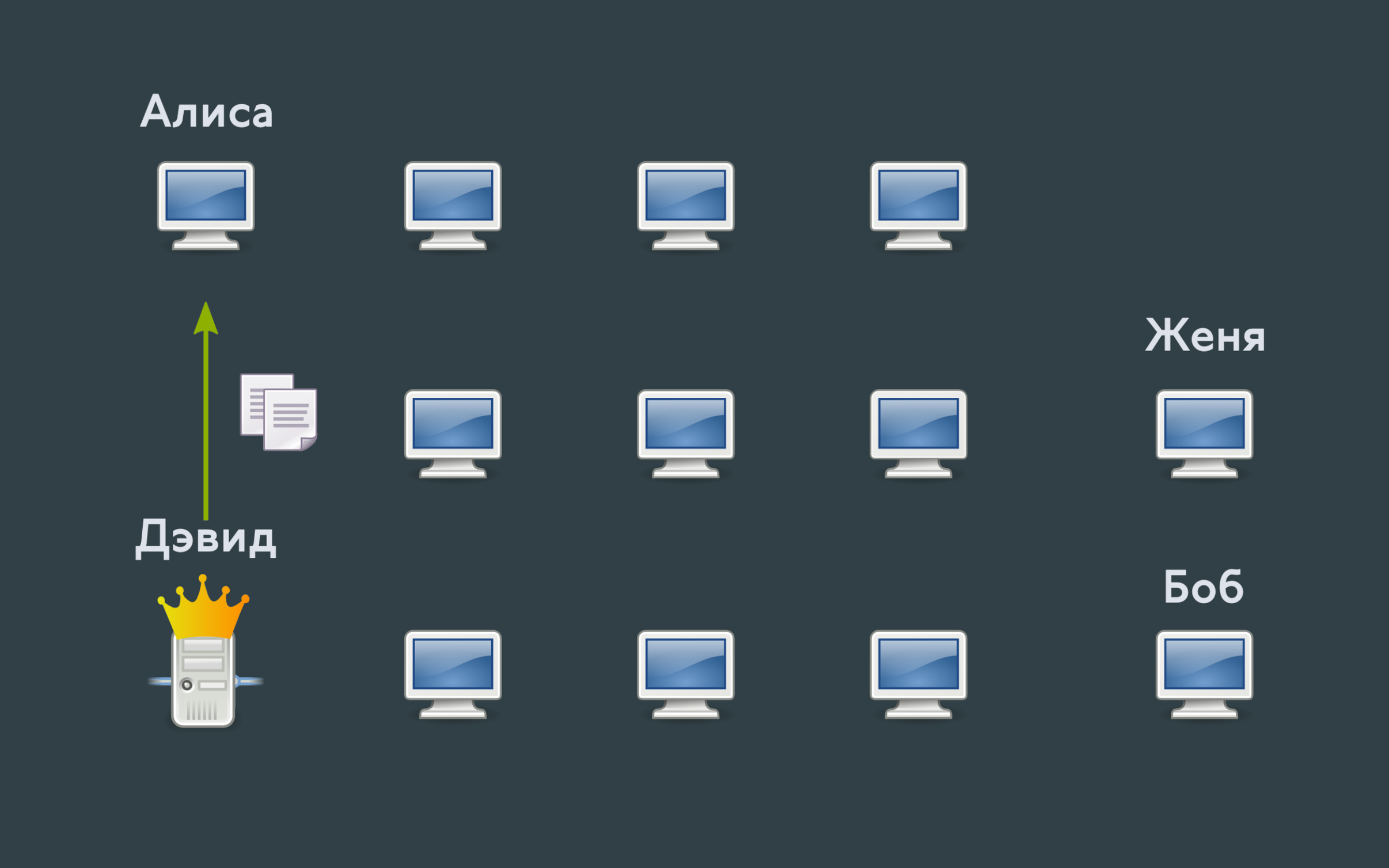
Алиса

Женя

Дэвид

Боб


Алиса
?
Женя
Дэвид
Боб

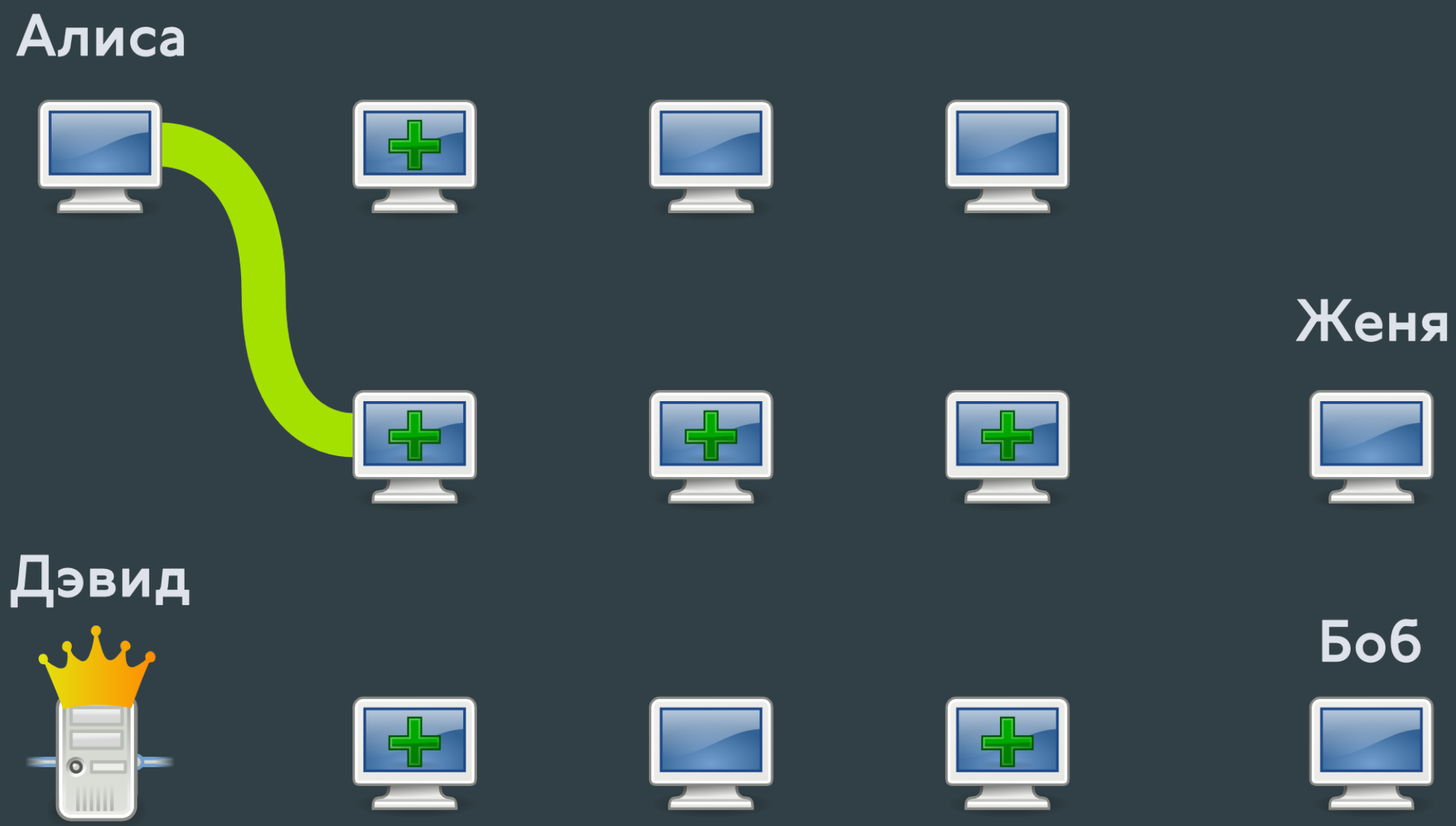

Алиса
Женя
Дэвид
Боб

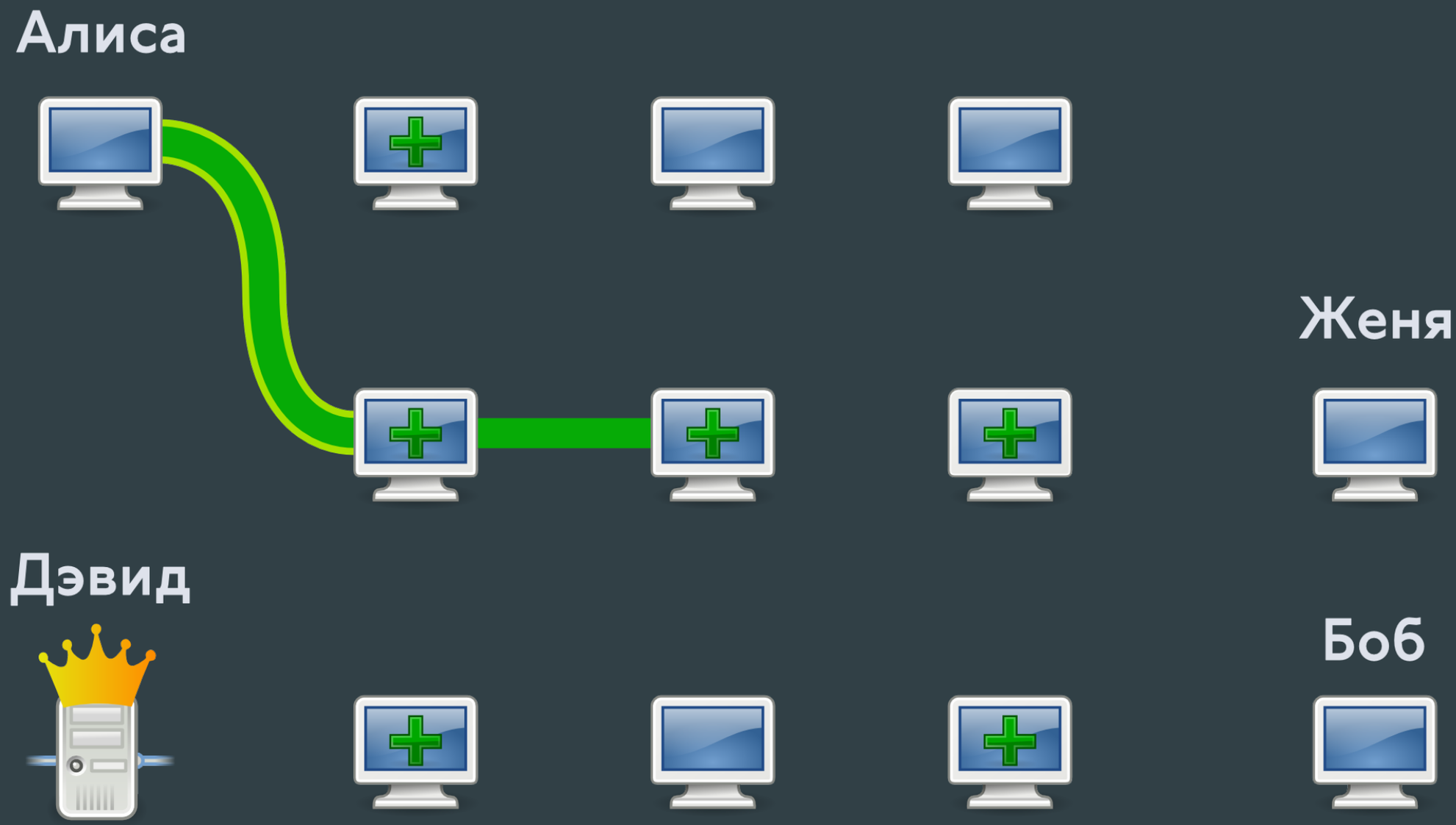
Алиса

Женя

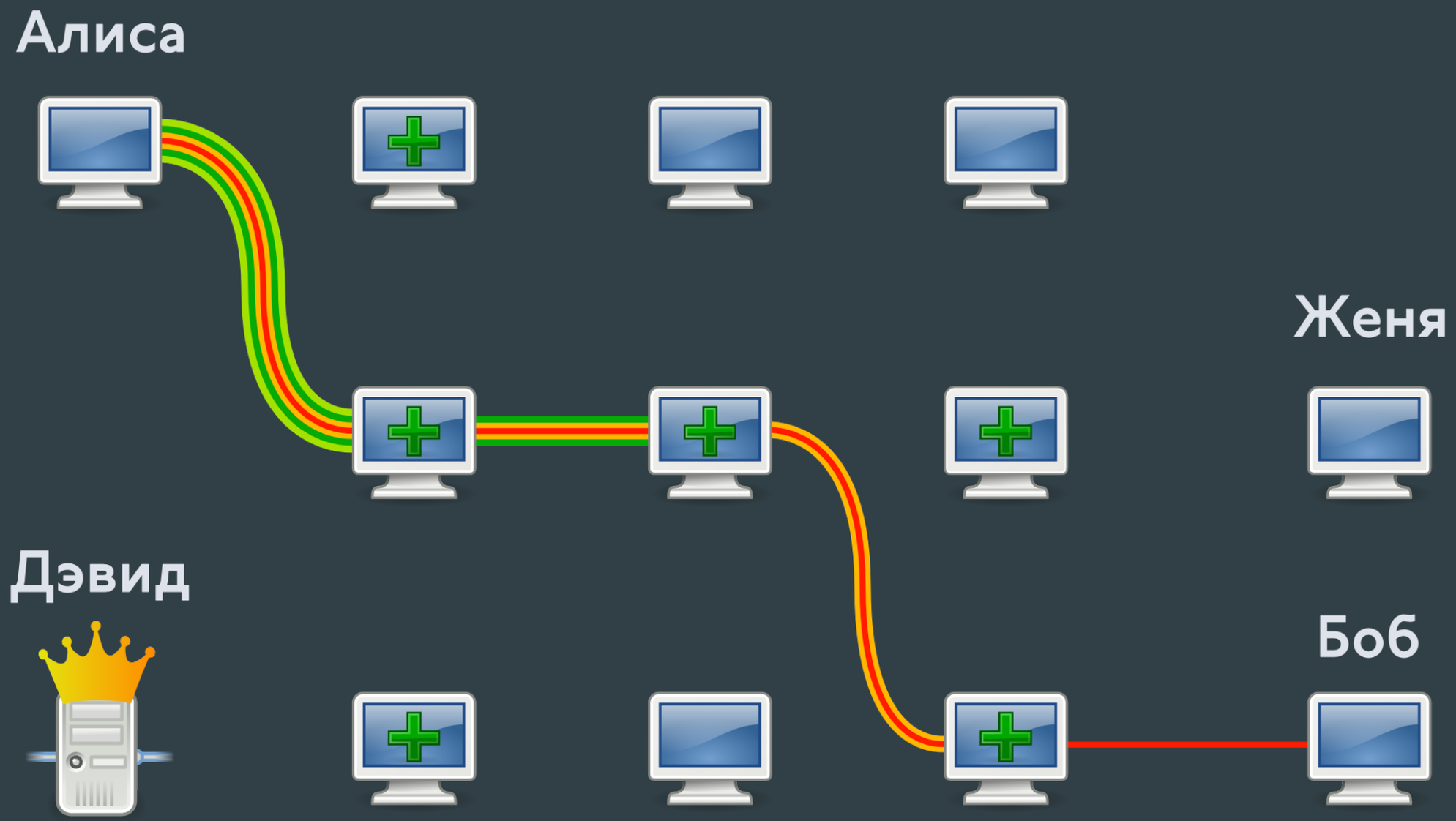
Дэвид

Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб

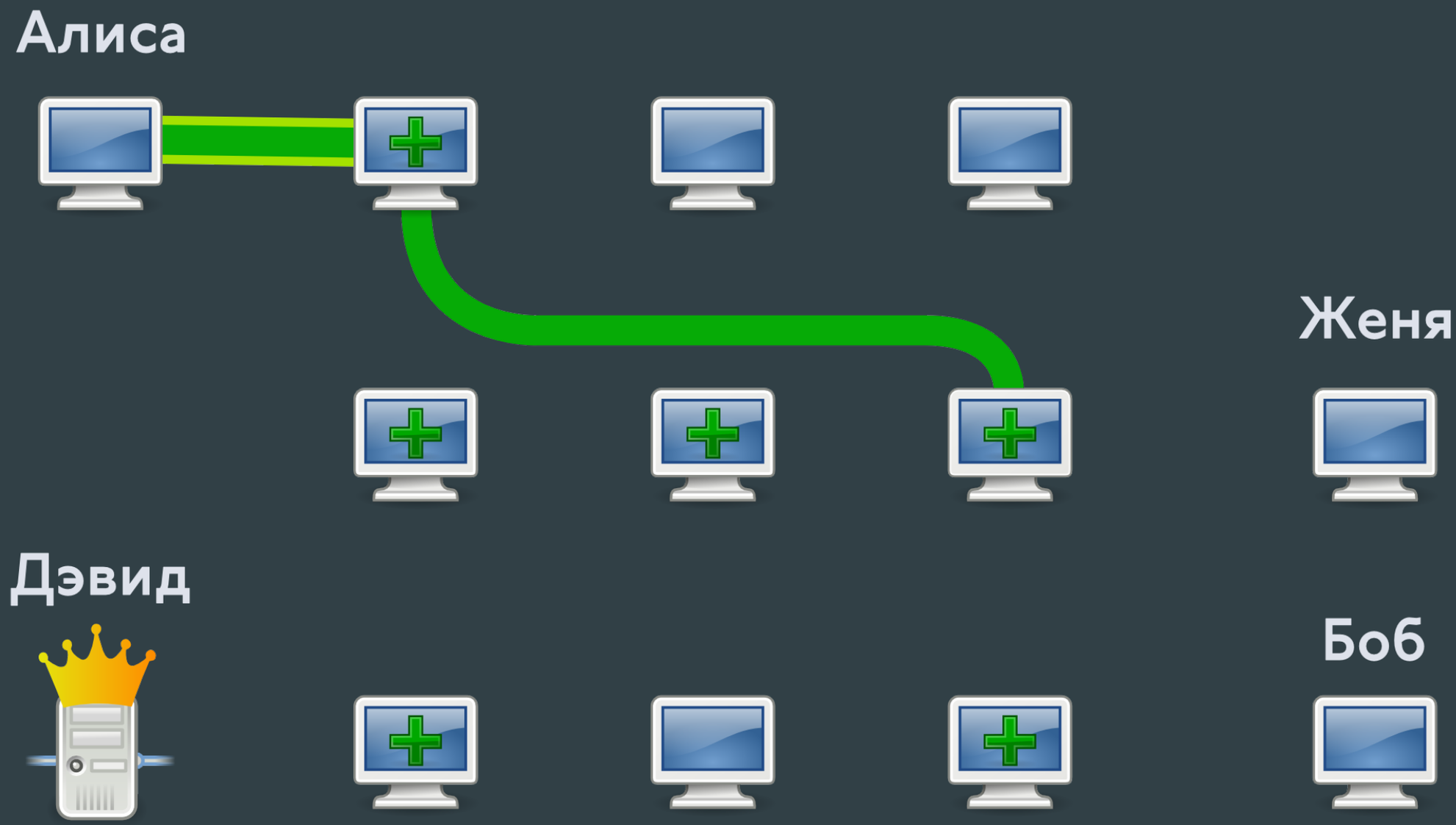

Алиса
Женя
Дэвид
Боб

Алиса

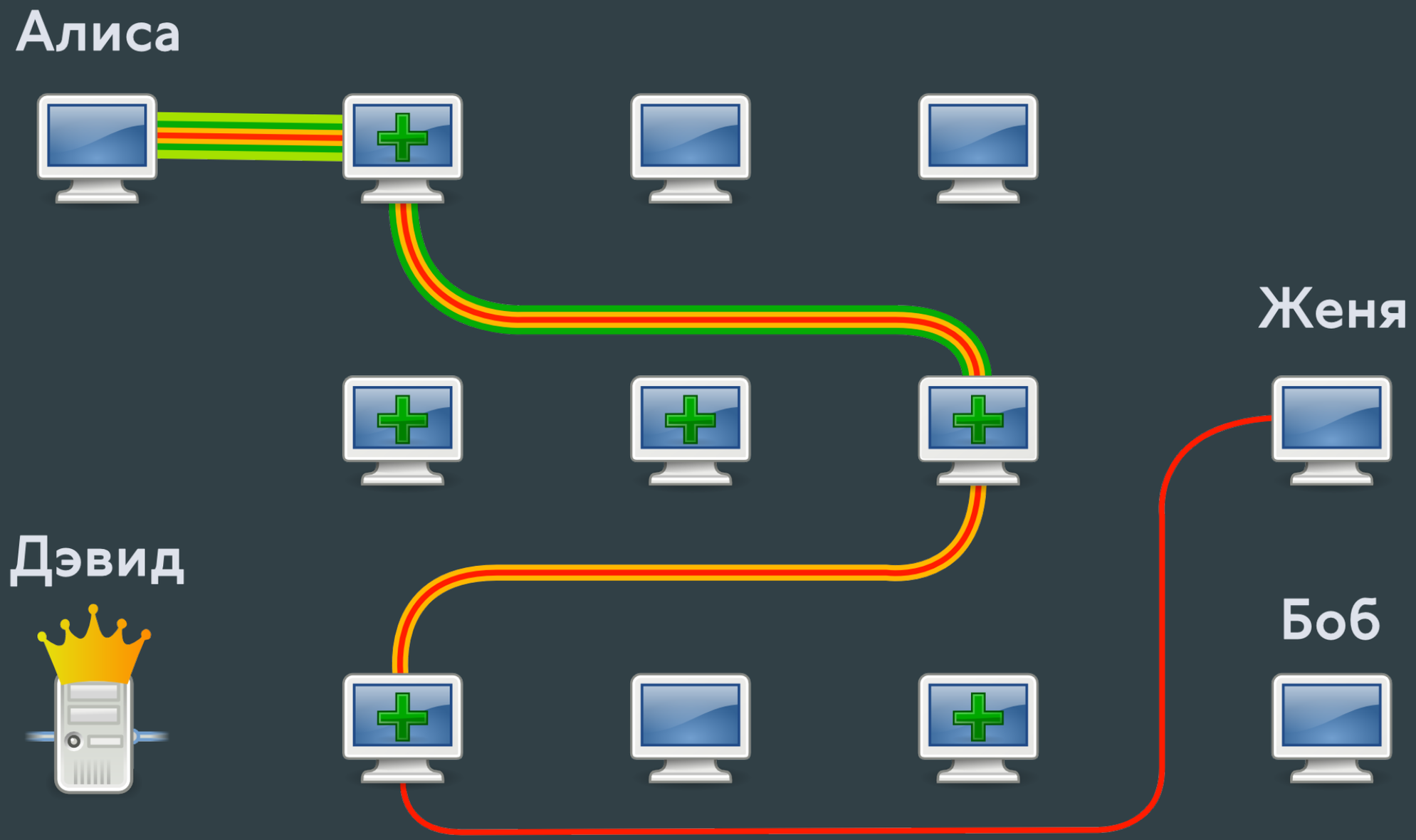
Женя

Дэвид

Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб

Кто-то говорит *с кое-кем*

Выходной релей видит передаваемые данные!

Цель:
кто-то говорит с *кем-то*

Луковичные сервисы Tor

Tor Onion Services

Анонимность как клиента, так и сервера

Публичные ключи вместо имен

Достаточно сгенерировать ключевую пару

zkym3uprkoddlxpq.onion

facebookcorewwwi.onion

Сквозное шифрование

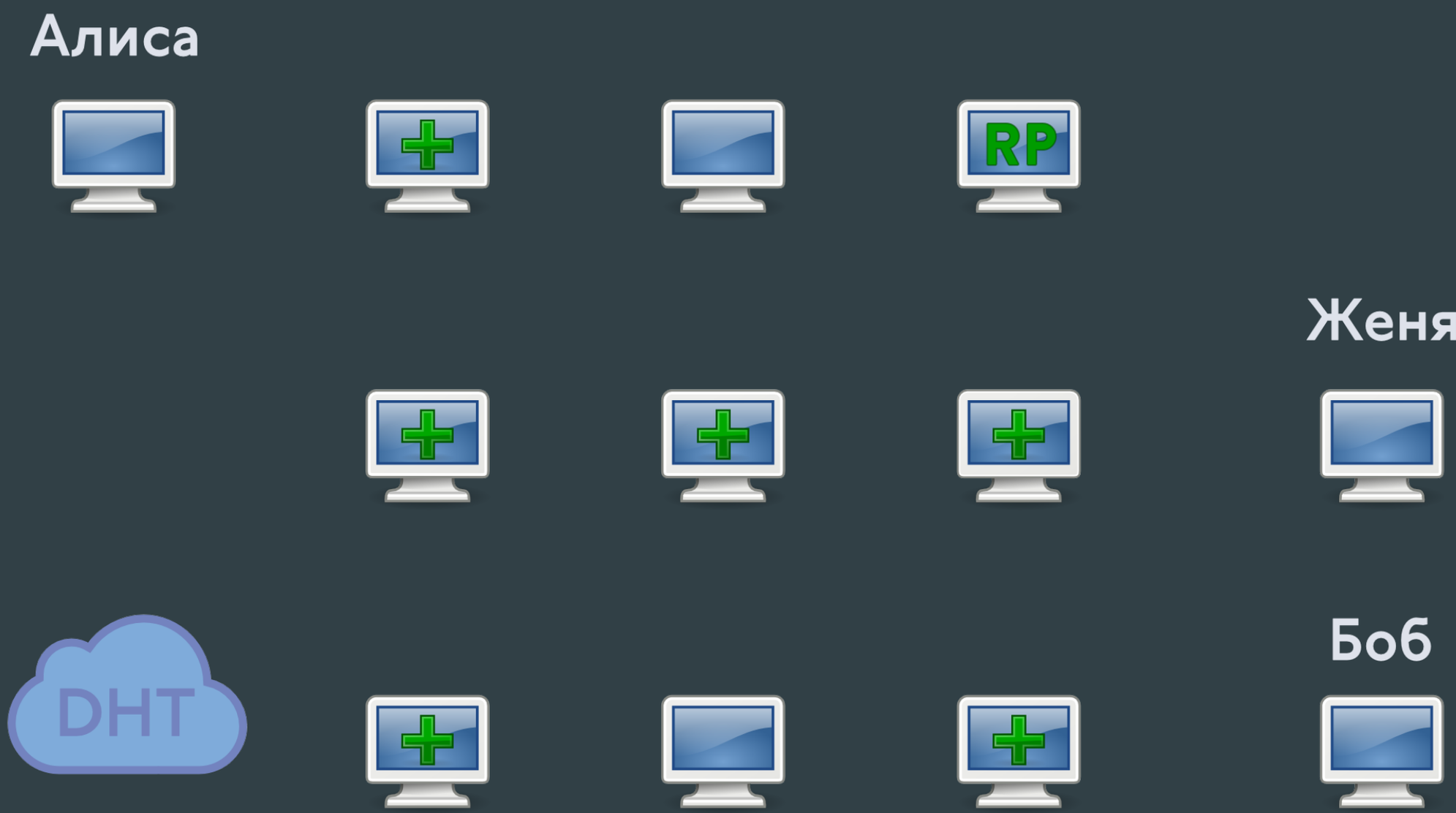
Forward Secrecy

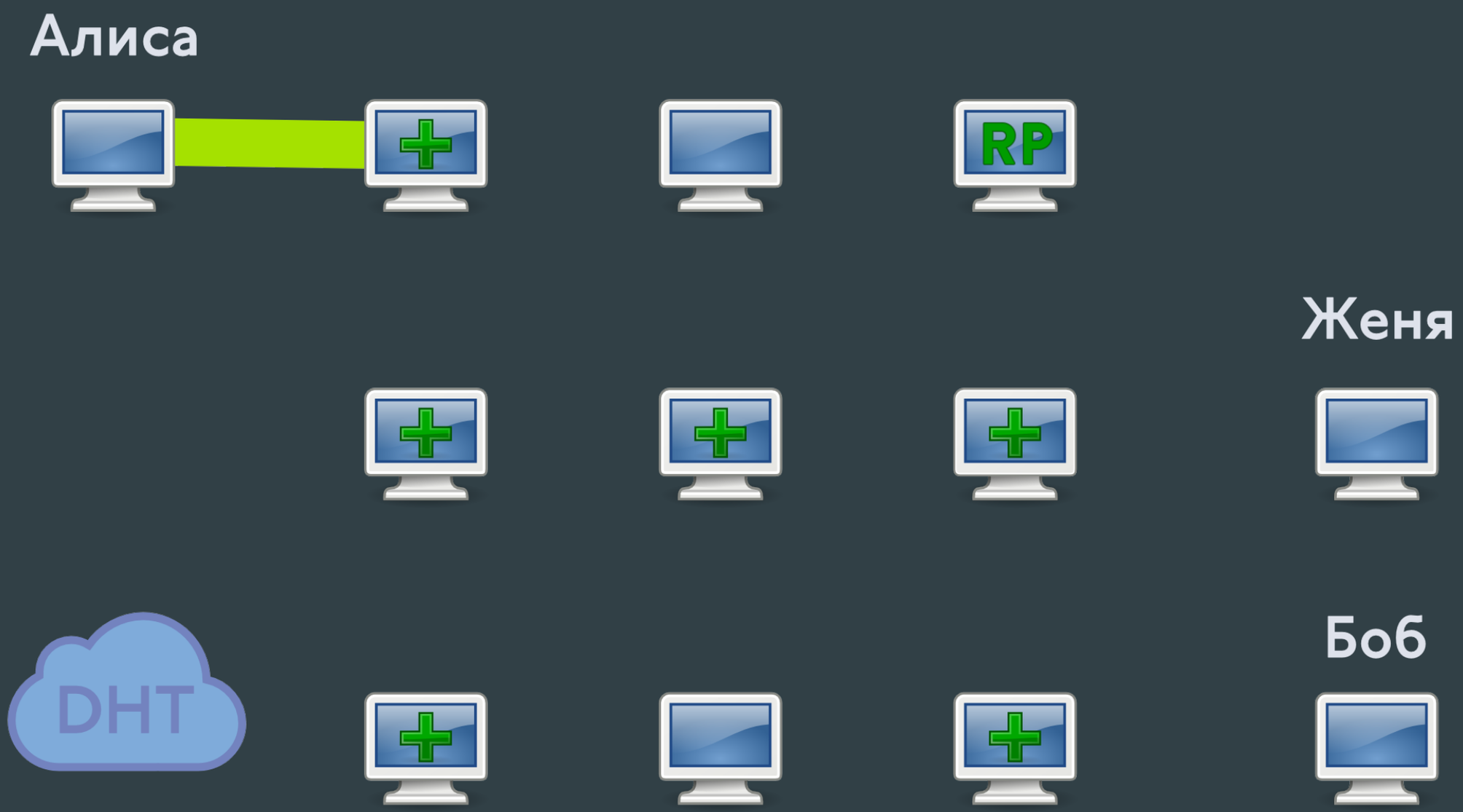
Запускаются везде

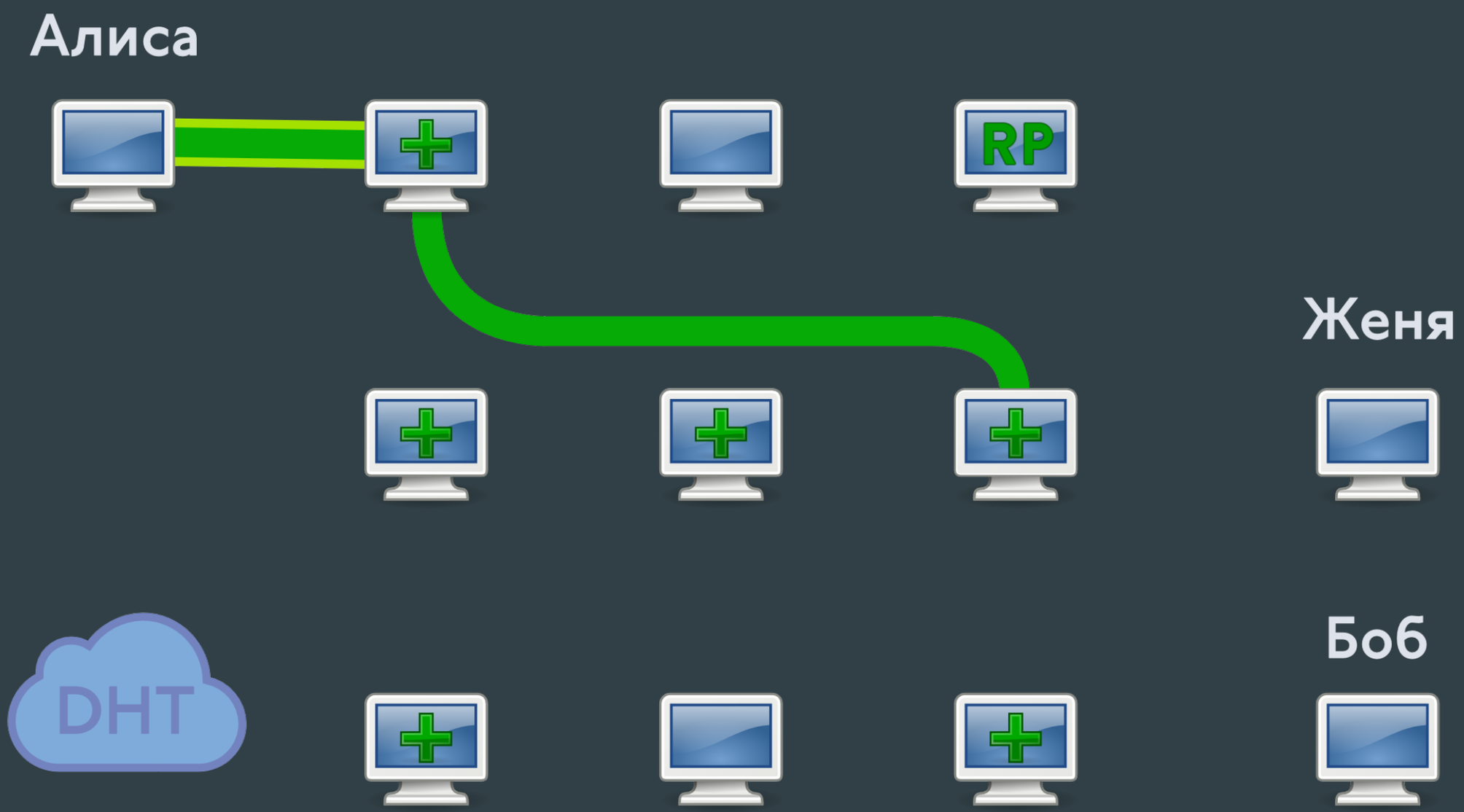

Алиса
Женя
Боб
DHT

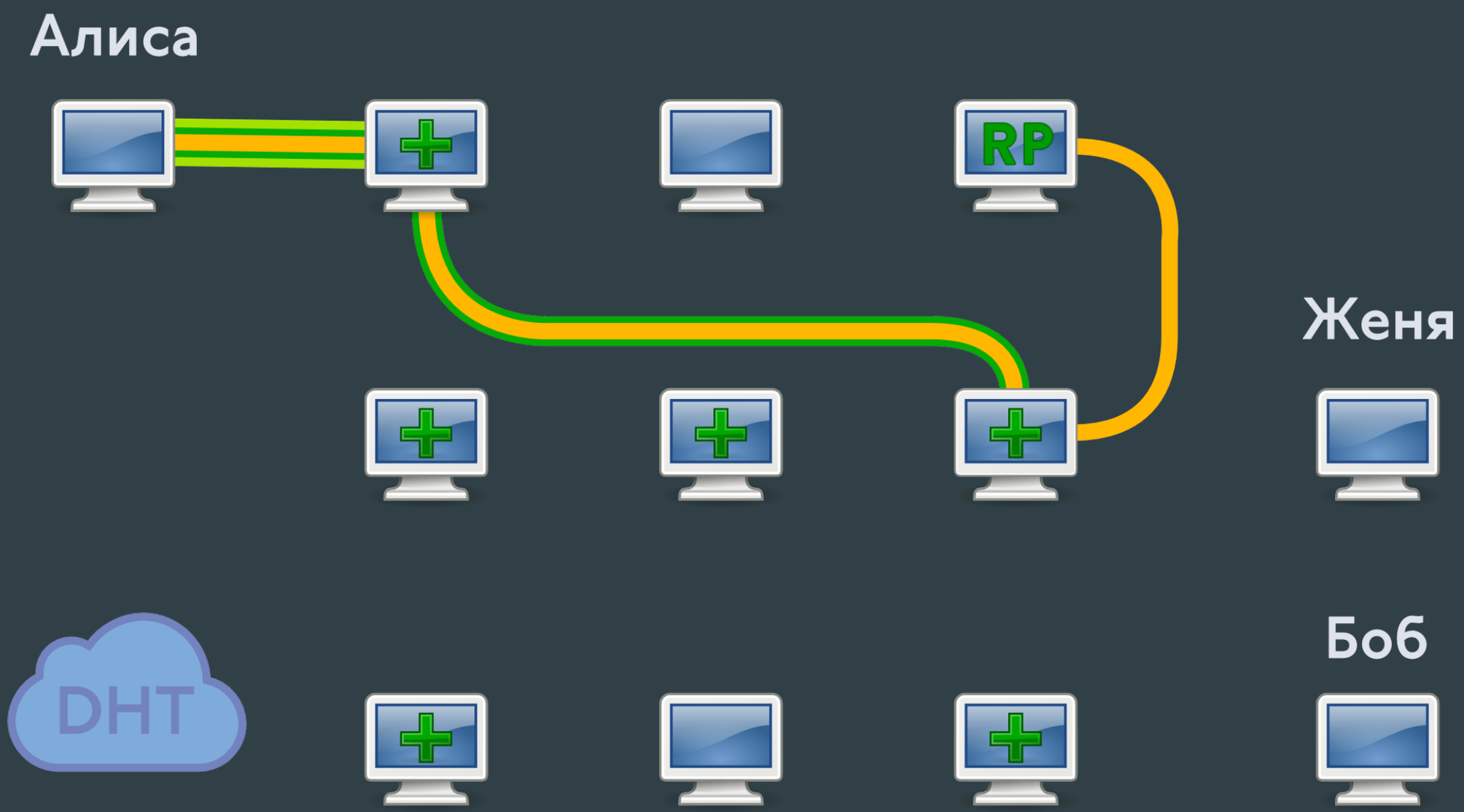

Алиса
.onion
?
Женя
DHT
Боб

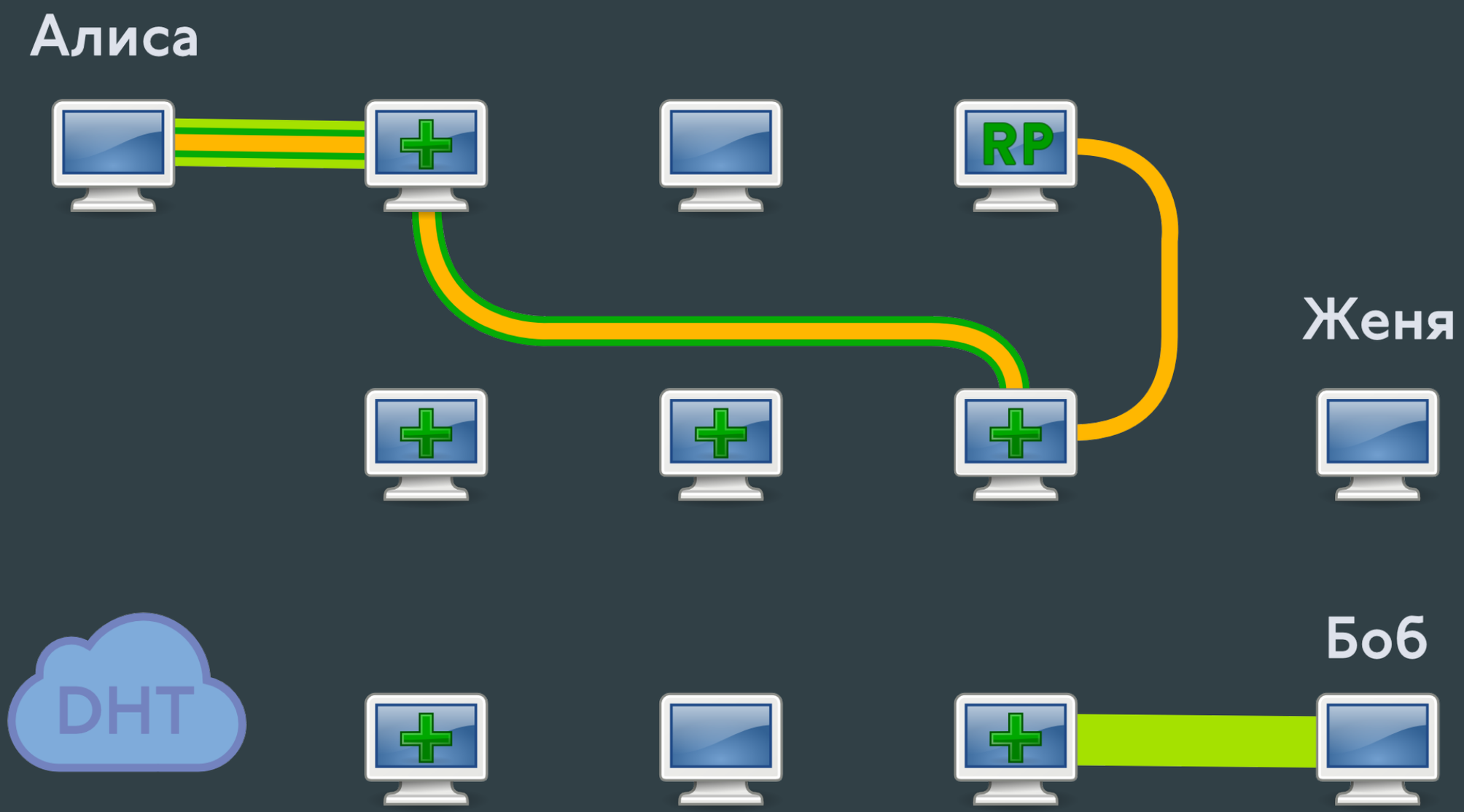

Алиса
Женя
Боб
DHT

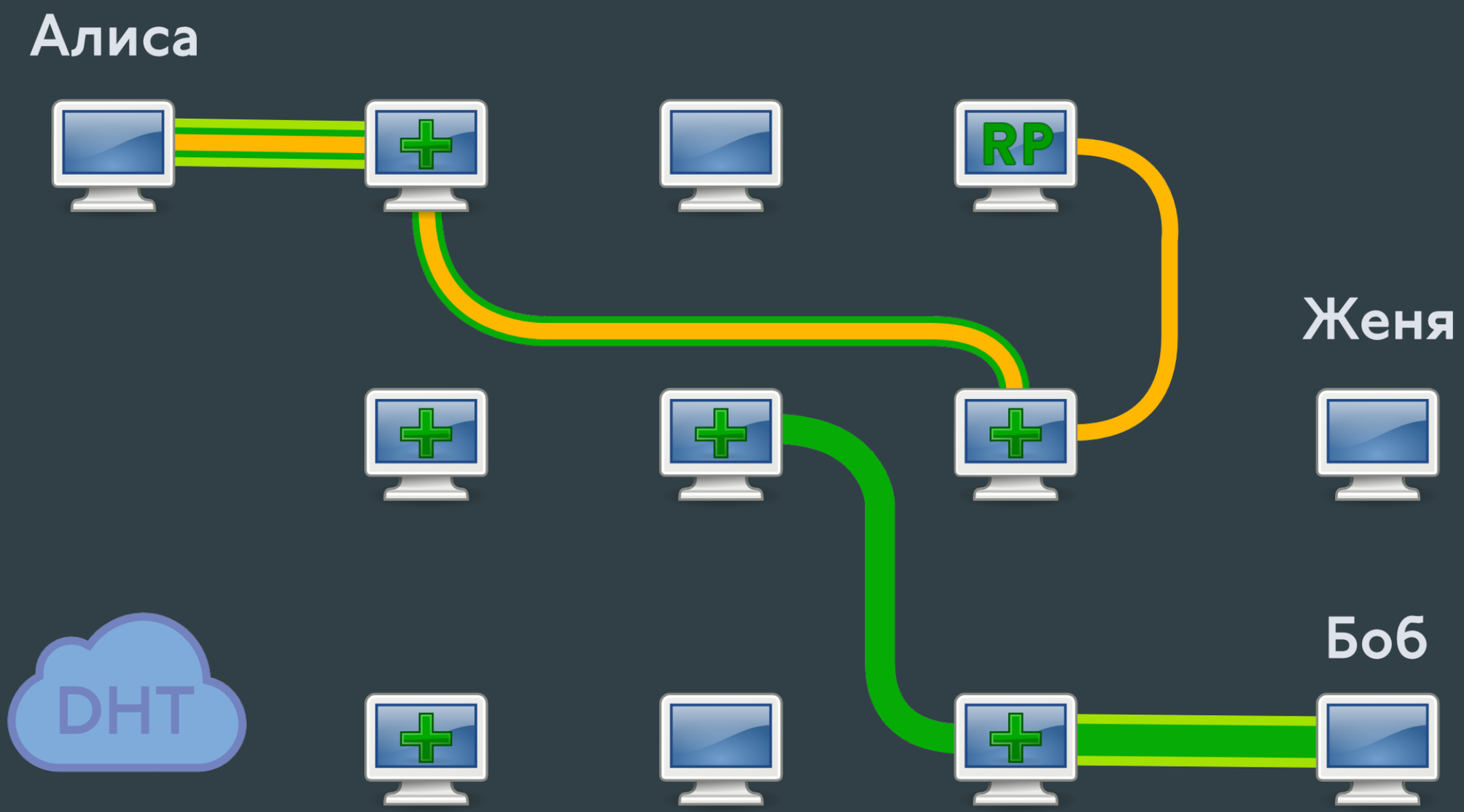

Алиса
RP
Женя
DHT
Боб

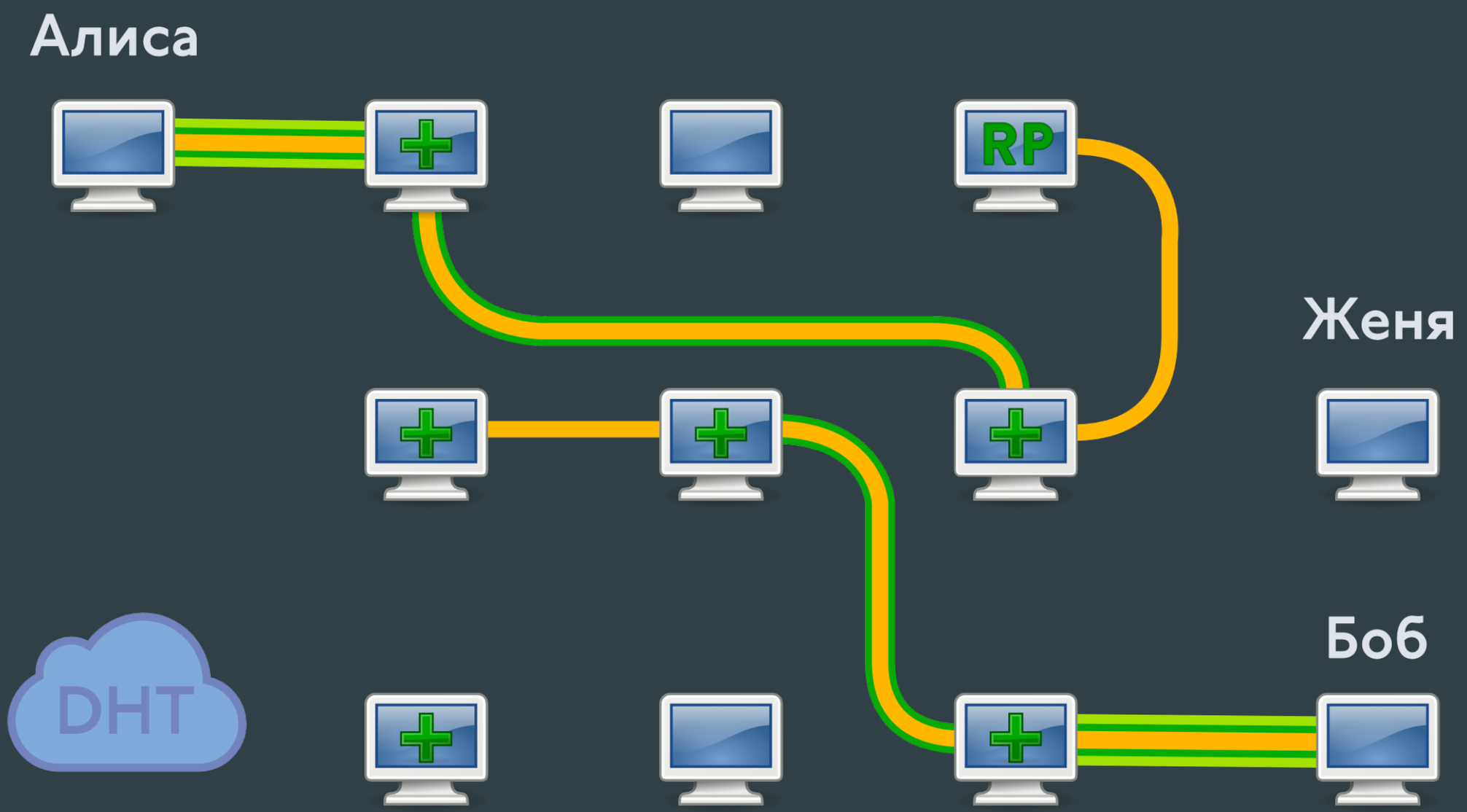

Алиса
RP
Женя
DHT
Боб

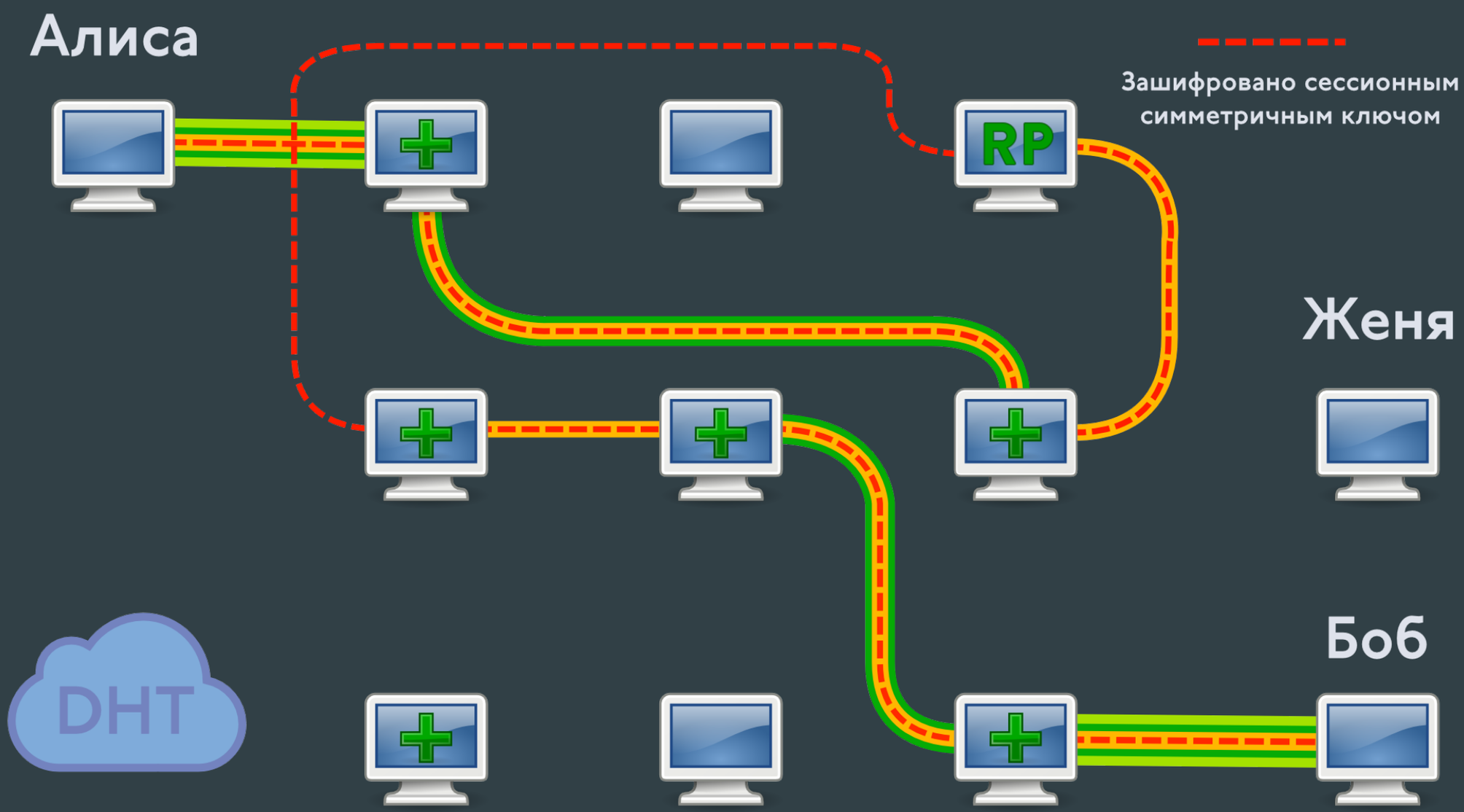

Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб

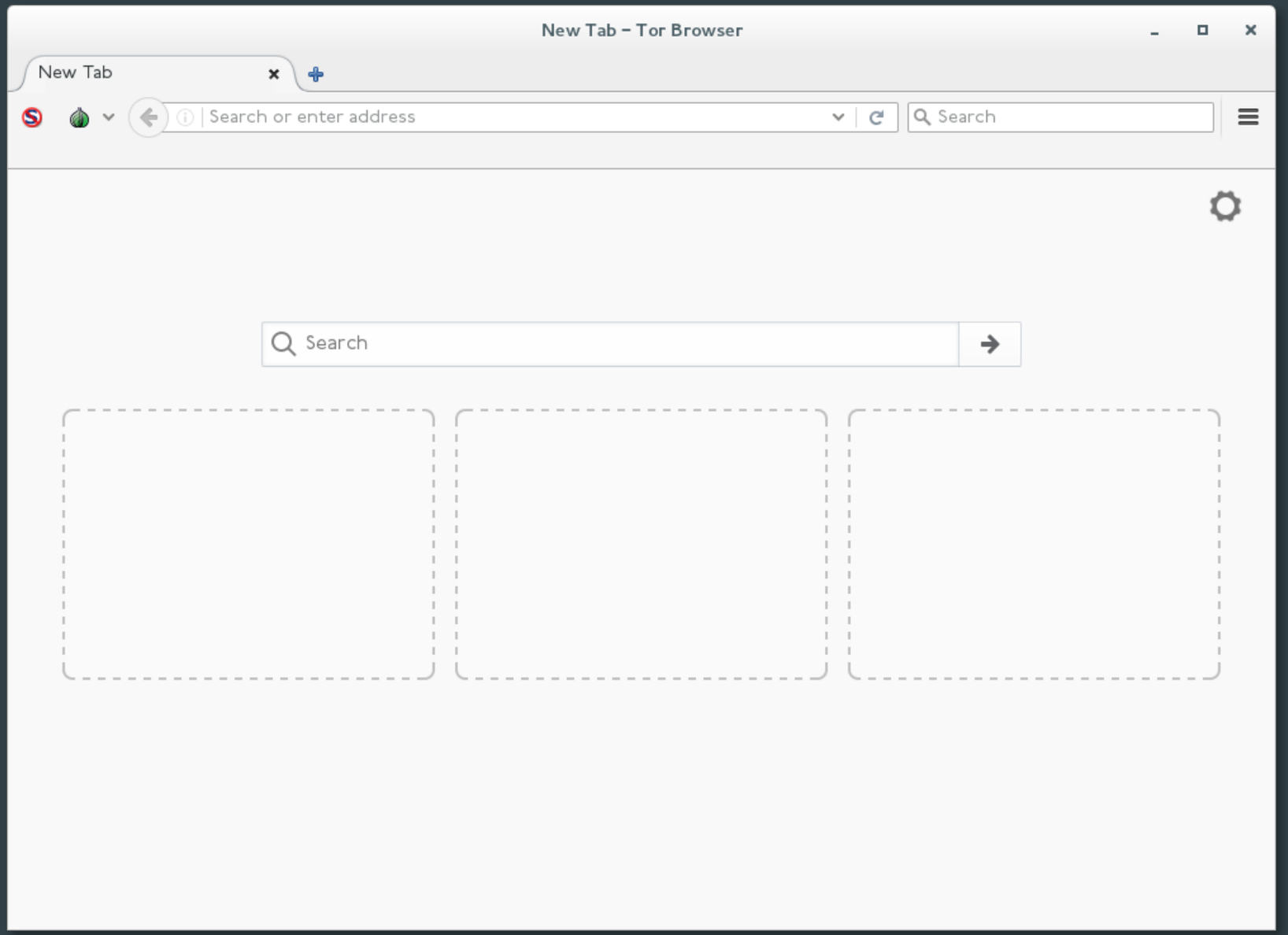

Алиса
Зашифровано сессионным симметричным ключом
RP
Женя
DHT
Боб

Tor Browser

Mozilla Firefox* + tor

* с огромным количеством исправлений для повышения приватности

Tor Browser выглядит так:


New Tab – Tor Browser
New Tab
Search or enter address
Search
Search

Мосты

Релеи Tor, которых нет в публичном состоянии сети

Используются как входные релеи в цепочках

Подключаемые Транспорты

Pluggable Transports

Алгоритмы маскировки подключений Tor

для обхода цензуры

Защита чатов

OTR

Off-The-Record Messaging

Почему OTR?

Открытый

Простой

Хорошо проанализирован

Отрицание авторства

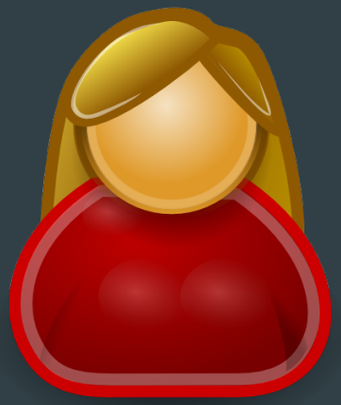
Forward Secrecy

Mar 16, 2012 13:43:55	[redacted]	[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:43:59		[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:44:20		[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:44:46		[OC: No decrypt available for this OTR encrypted message.]

***

Устанавлиается зашифрованый канал

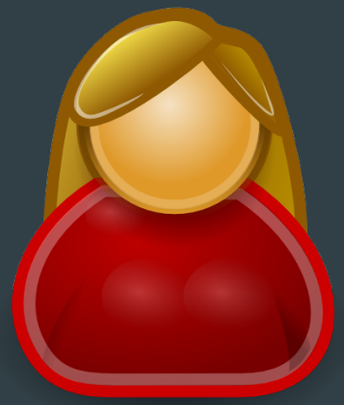
Можно сверить отпечаток, чтобы убедится в подлинности



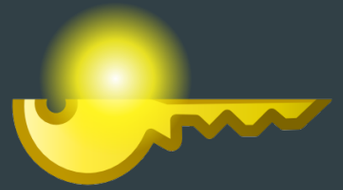
Алиса

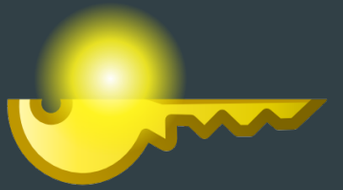
Ирина

Боб



Алиса

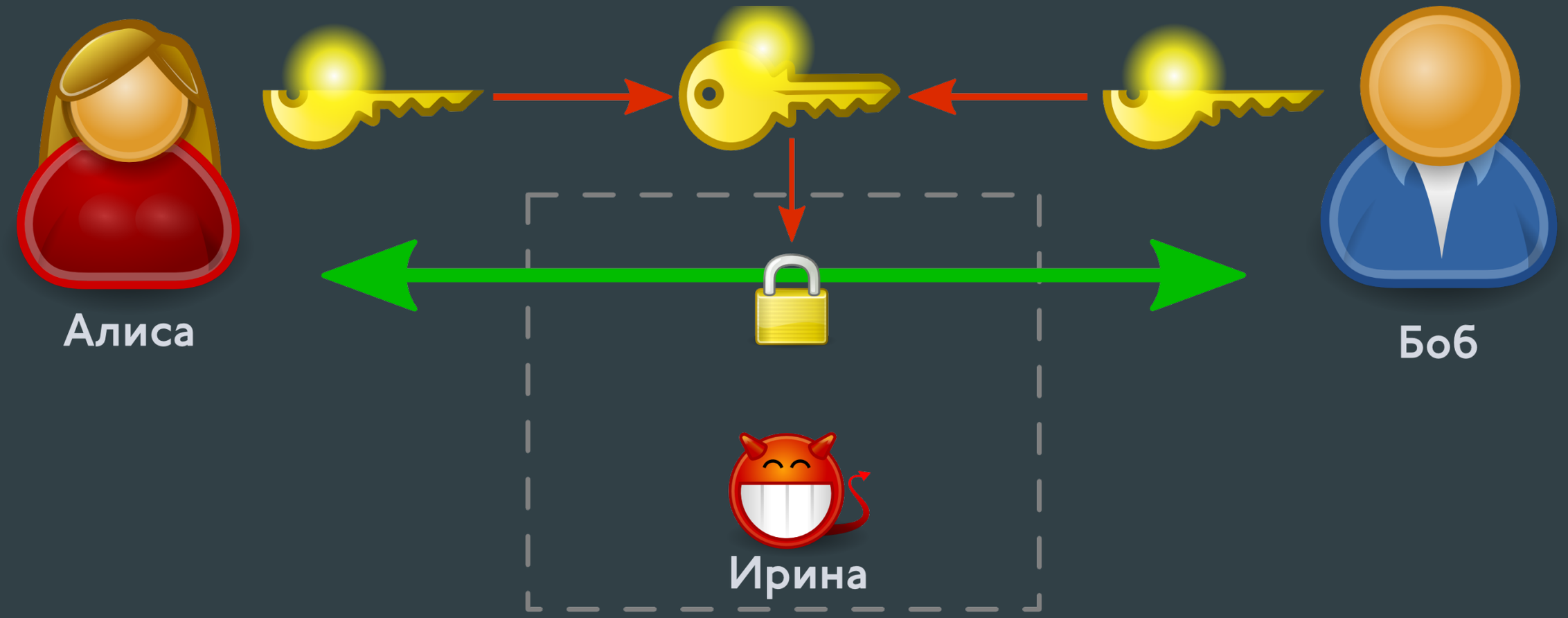


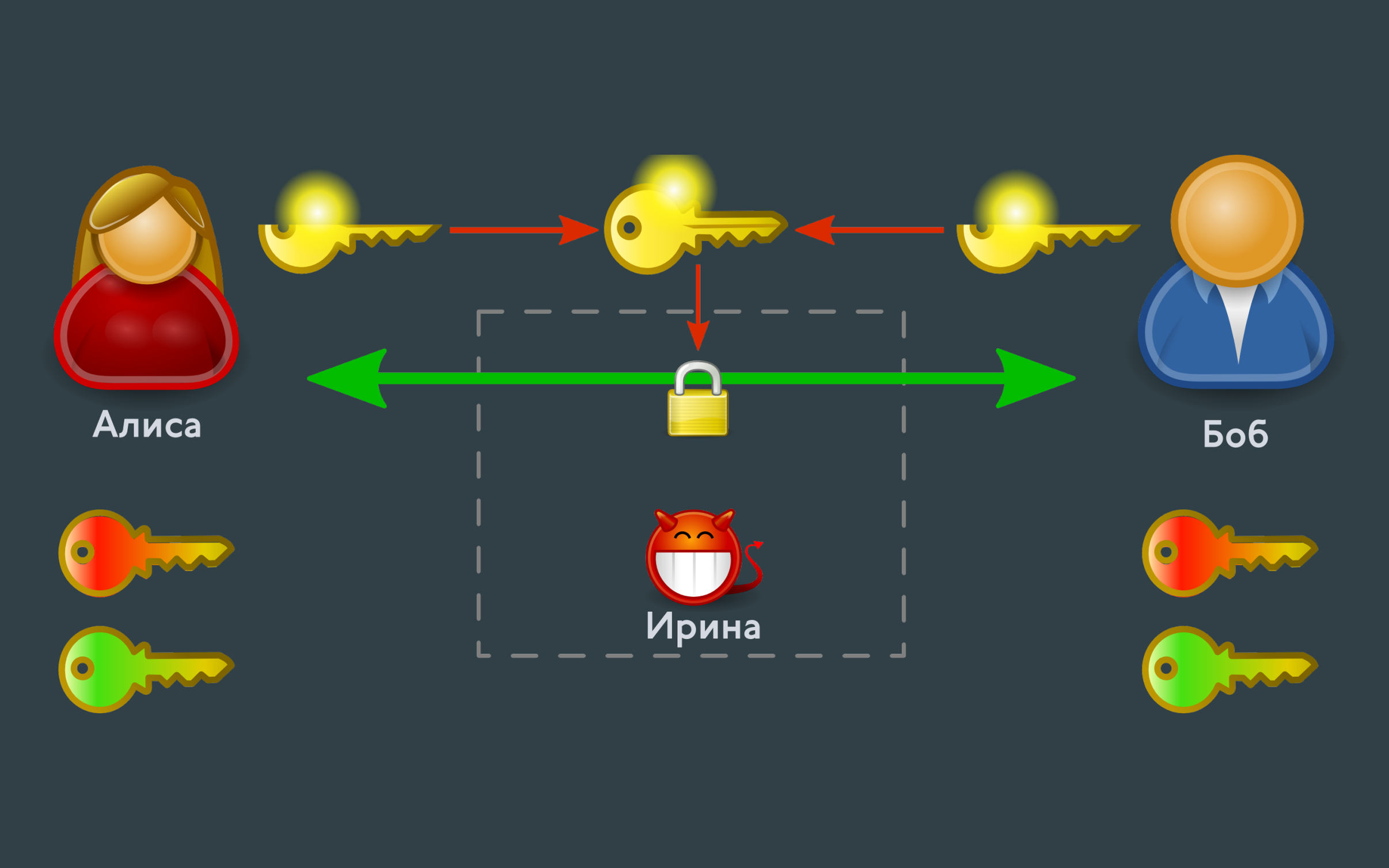


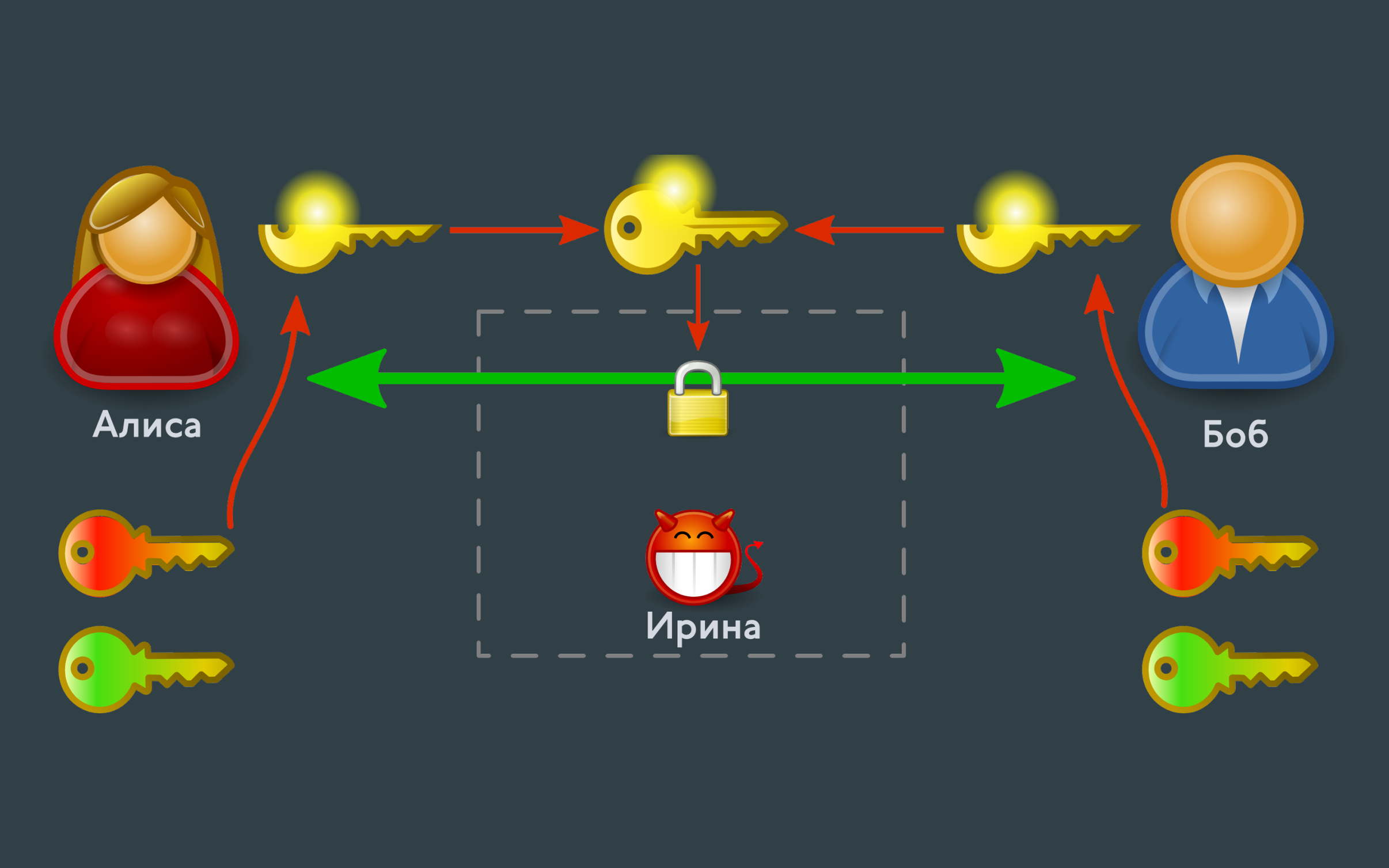
Боб

Ирина


Алиса
Боб
Ирина


Алиса
Боб
Ирина


Алиса
Боб
Ирина


Алиса
Боб
Ирина

Сообщение OTR выглядит так:

?OTRv2?Y3J5cHRvcGFydHkK

В текущей версии протокола нет передачи файлов

Используйте OpenPGP/OnionShare

Предпочтительный вариант использования OTR

Протокол XMPP

Децентрализованный

Похож на эл. почту

cryptoparty@jabber.ccc.de

Можно зарегистрироваться на любом сервере

Можно связываться с пользователями на любом сервере

Защита файлов/почты

OpenPGP

Система шифрования/подписи данных

Почему OpenPGP?

30 лет
в использовании

Многочисленные аудиты

Стандарт Интернета

[redacted]

SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0546Z12

Received from: [redacted]
Date: Mon, 30 Jan 2012 21:46:03 -0800 (PST)
From: [redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

[OC: No decrypt available for this PGP encrypted message.]

***

TOP SECRET//COMINT//REL TO USA, AUS//20320108

GnuPG

Публичный ключ выглядит так:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mI0EV+8yFwEEAOygoNBKEPl/SiNxPb3Uq5W75cX9B2TmwYagLboifZdiCxozj7XX
b39QPmjeHnoxWKYGSfshGbKGW+RpqjNJkUwyjlJp5lH70Kj3JjLy36h3fJ963vcg
Ur0UKyTn+QIs5ePogSVyHhfC45RPwkZRmd4/HPhMBuNDFUIw/AN0XRYfABEBAAG0
C0NyeXB0bIBhcnR5iLgEEwECACIFAlfvMhcCGwMGCwkIBwMCBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEIwmVKbI7KOs/UAD/IaZYs7gaEUtnhERkh05mRIH8xTDnPFdIdv9
bTiqrdtyIOLnSuI7P8XoUvxjkvlyI/NMgENS8WOYXK+iDXvikZ9MqnRjhM/NErNI
05apOJ0/JoTw+Ks0bUhUcfZSbjNOC0VakNKY74HEKffV3e+c/igIJzUAyEkM+sIM
A+d0XwZx
=3/wJ
-----END PGP PUBLIC KEY BLOCK-----

Например, зашифрованное сообщение

выглядит так:

```
-----BEGIN PGP MESSAGE-----
jA0EAwMCgIjZTeRJlkNgyVDGJu44088NxfOmvDBZovUjkgAuEsBU6CjRRpwqrVFh
T+MFmt6+FYh/yKPt8kiDtO0d0/xkvckNMU2M/iPD5uIlqM+HACmZv06HioE9mZeY
8g==
=V84U
-----END PGP MESSAGE-----
```

Защита работы на компьютере

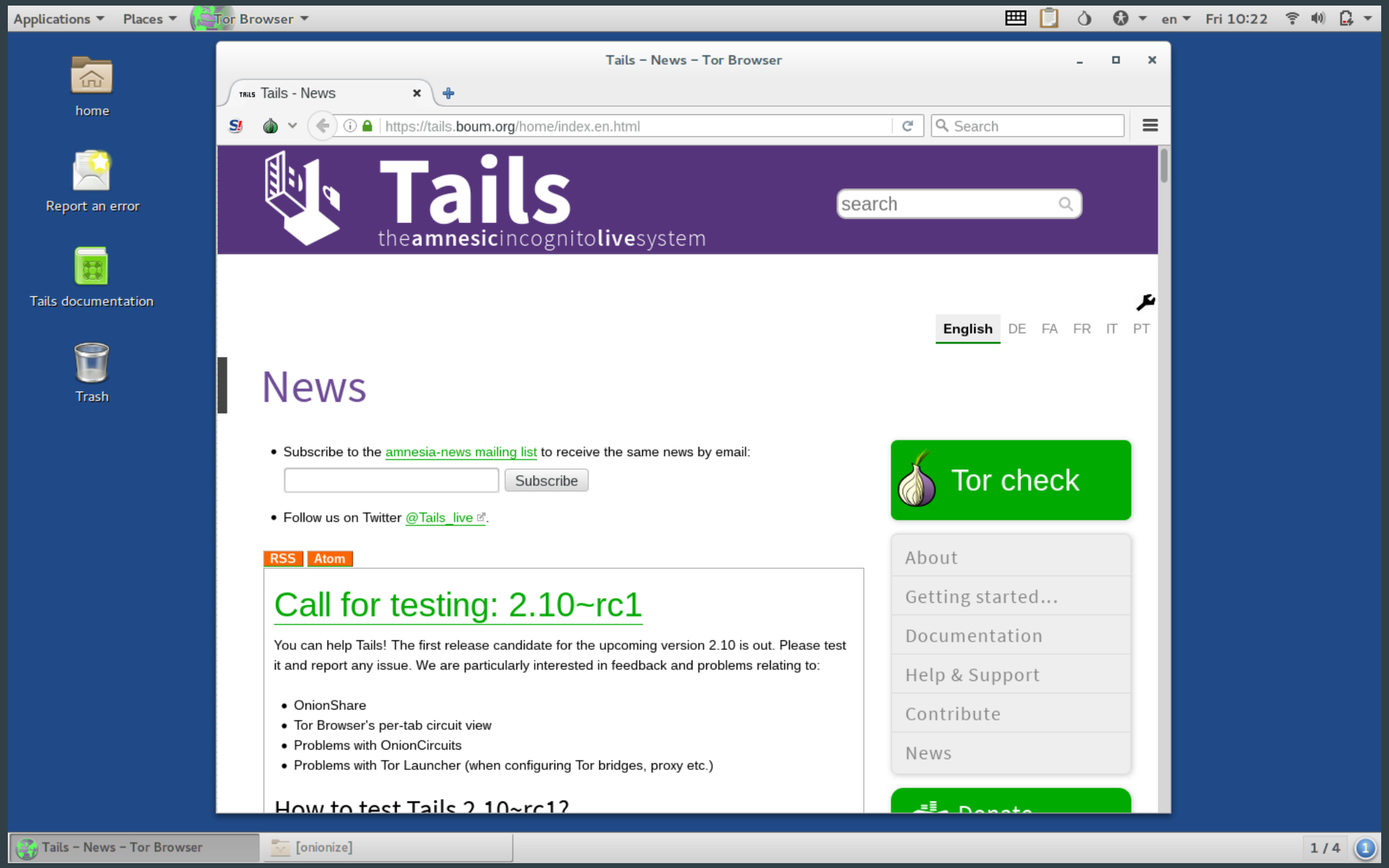
Tails

Ориентированный на приватность вариант GNU\Linux

Запускается с флешки

Все соединения через Tor или I2P

TorBrowser, OTR, GPG и все, что нужно для работы


Applications
Places
Tor Browser
en
Fri 10:22
home
Report an error
Tails documentation
Trash
Tails – News – Tor Browser
Tails - News
https://tails.boum.org/home/index.en.html
Search
Tails
theamnesicincognitolivesystem
search
English DE FA FR IT PT
News
Subscribe to the amnesia-news mailing list to receive the same news by email:
Subscribe
Follow us on Twitter @Tails_live.
RSS Atom
Call for testing: 2.10~rc1
You can help Tails! The first release candidate for the upcoming version 2.10 is out. Please test it and report any issue. We are particularly interested in feedback and problems relating to:
OnionShare
Tor Browser's per-tab circuit view
Problems with OnionCircuits
Problems with Tor Launcher (when configuring Tor bridges, proxy etc.)
How to test Tails 2.10~rc1?
Tor check
About
Getting started...
Documentation
Help & Support
Contribute
News
Tails – News – Tor Browser
[onionize]
1 / 4

Ссылки

Пароль WiFi: password

Tor
https://torproject.org/
Orbot (Android)

F-Droid

https://f-droid.org/

OTR
https://otr.cypherpunks.ca
Pidgin/Adium/CoyIM
(Linux, Windows, macOS)
Conversations (Android)
ChatSecure (iOS, Android)

GnuPG
https://gnupg.org/
GnuPG+Thunderbird+Enigmail (Desktop)
OpenKeyChain+K9-Mail (Android)

Tails
https://tails.boum.org/