Технологии анонимизации

https://www.cypherpunks.ru/

Загрязнение информацией

- Токсичность информации
- Конец эфемерности
- Телефон, email. IM, покупка, транспорт, смартфон, сайт
- RFID, WiFi, камеры, принтер, сканер
- **Сами** оповещаем о знакомствах
- **Сами** отправляем копии email, IM, SMS, разговоров

Бизнес–модель Интернета

Обмен приватности на дешёвые услуги

Загрязнение информацией

- Токсичность информации
- Конец эфемерности
- Телефон, email. IM, покупка, транспорт, смартфон, сайт
- RFID, WiFi, камеры, принтер, сканер

- **Сами** оповещаем о знакомствах
- **Сами** отправляем копии email, IM, SMS, разговоров

Бизнес–модель Интернета

Обмен приватности на дешёвые услуги

Загрязнение информацией

- Токсичность информации
- Конец эфемерности
- Телефон, email. IM, покупка, транспорт, смартфон, сайт
- RFID, WiFi, камеры, принтер, сканер

- **Сами** оповещаем о знакомствах
- **Сами** отправляем копии email, IM, SMS, разговоров

Бизнес–модель Интернета

Обмен приватности на дешёвые услуги

Загрязнение информацией

- Токсичность информации
- Конец эфемерности
- Телефон, email. IM, покупка, транспорт, смартфон, сайт
- RFID, WiFi, камеры, принтер, сканер

- **Сами** оповещаем о знакомствах
- **Сами** отправляем копии email, IM, SMS, разговоров

Бизнес–модель Интернета

Обмен приватности на дешёвые услуги

Загрязнение информацией

Конфиденциальность ⇒ приватность

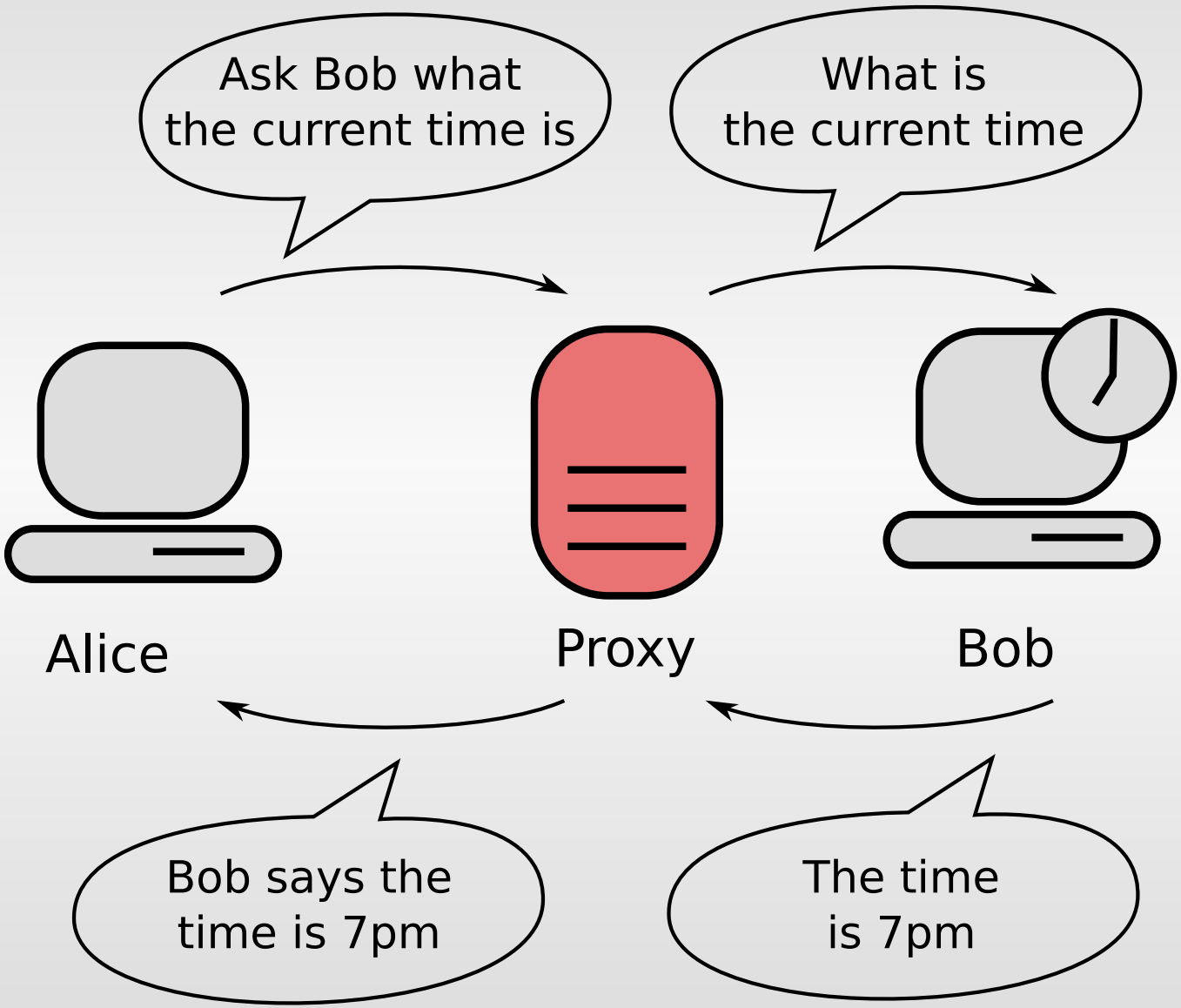
- Шифрование — полезная нагрузка сообщений
- Анонимизация — метаинформация сообщений (адреса, время, размер)

Загрязнение информацией

Конфиденциальность $\Rightarrow$ приватность

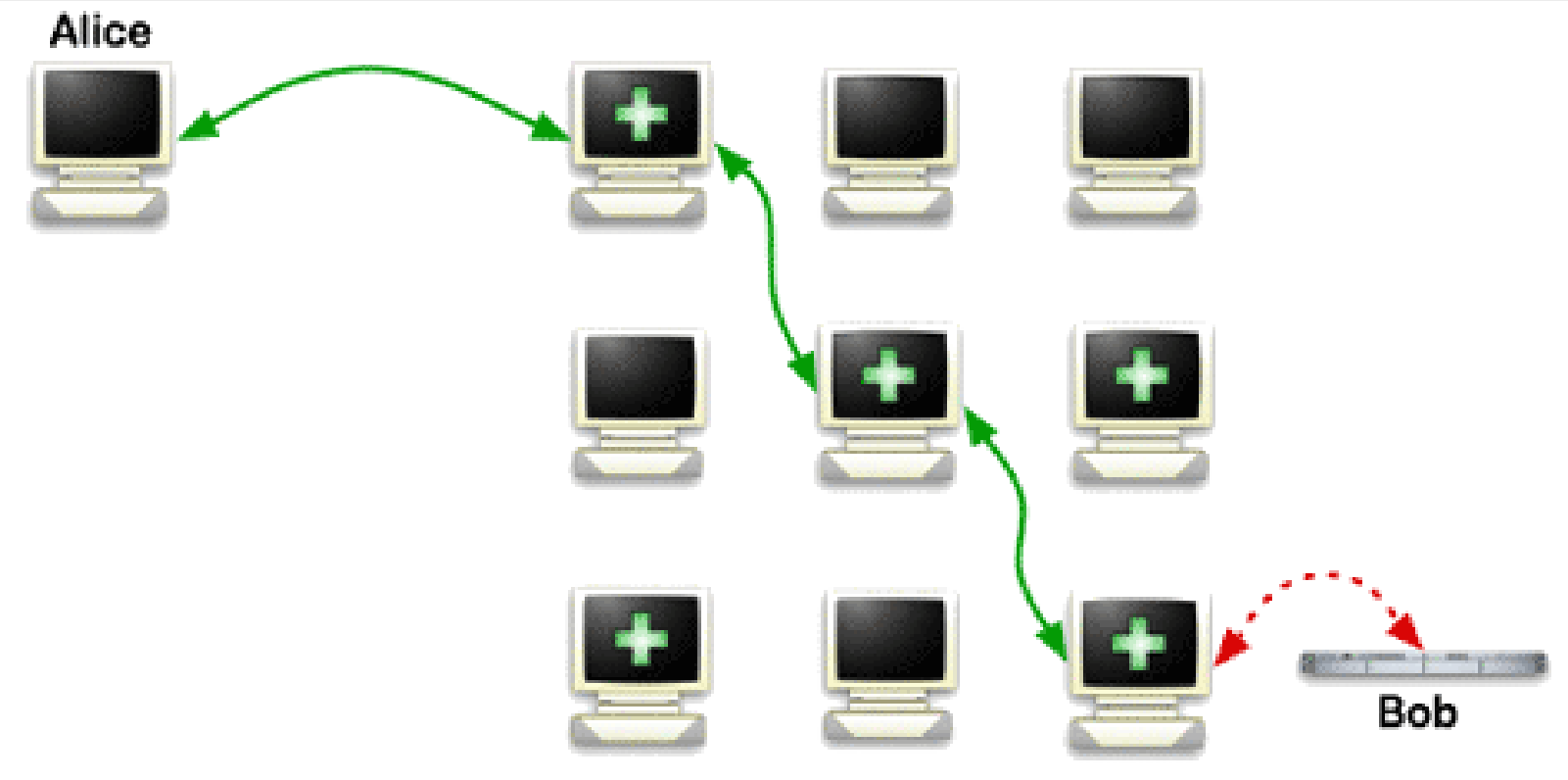
- Шифрование — полезная нагрузка сообщений
- Анонимизация — метаинформация сообщений (адреса, время, размер)

Прокси/VPN–серверы



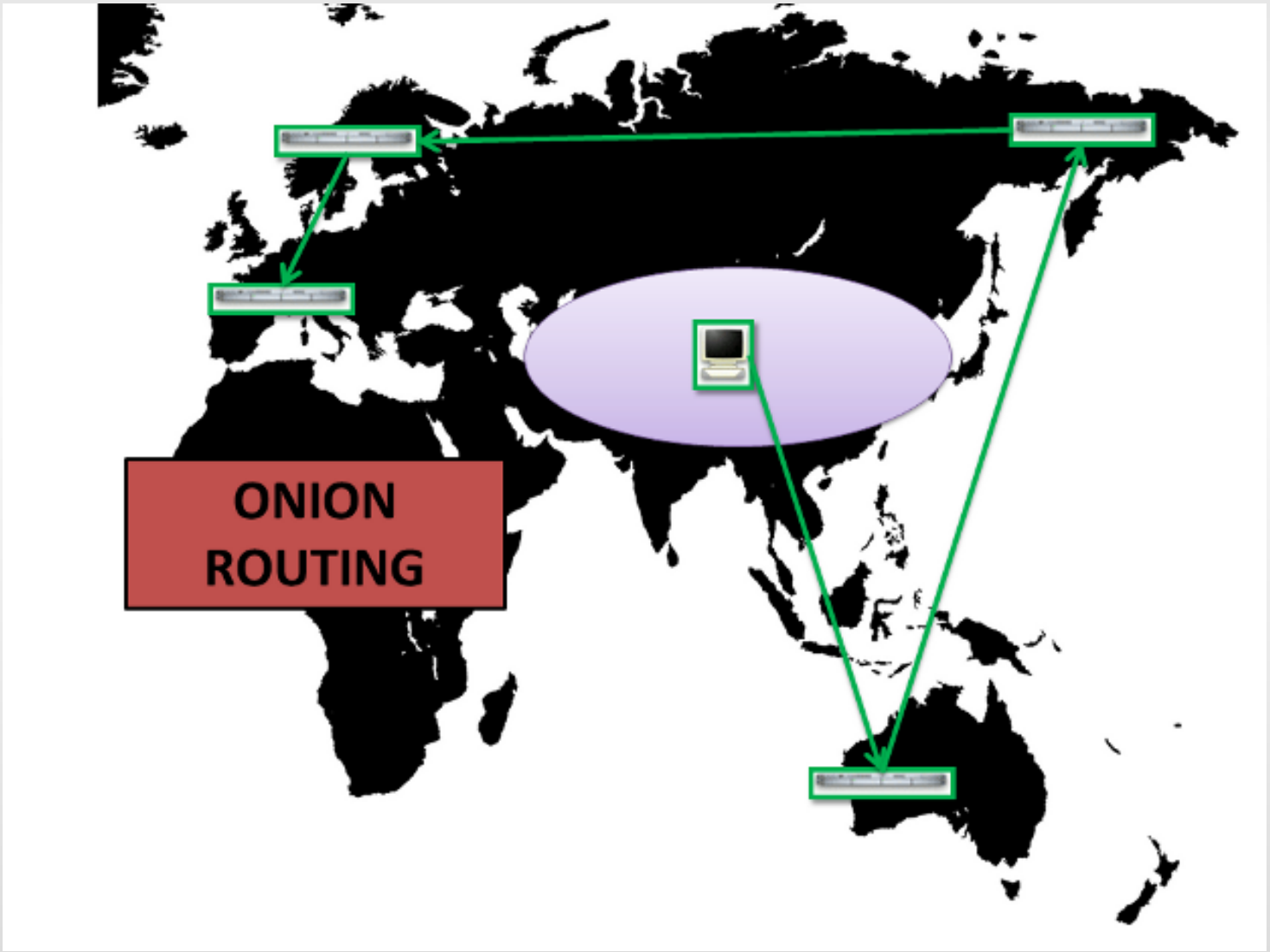
Tor

Цепочка прокси



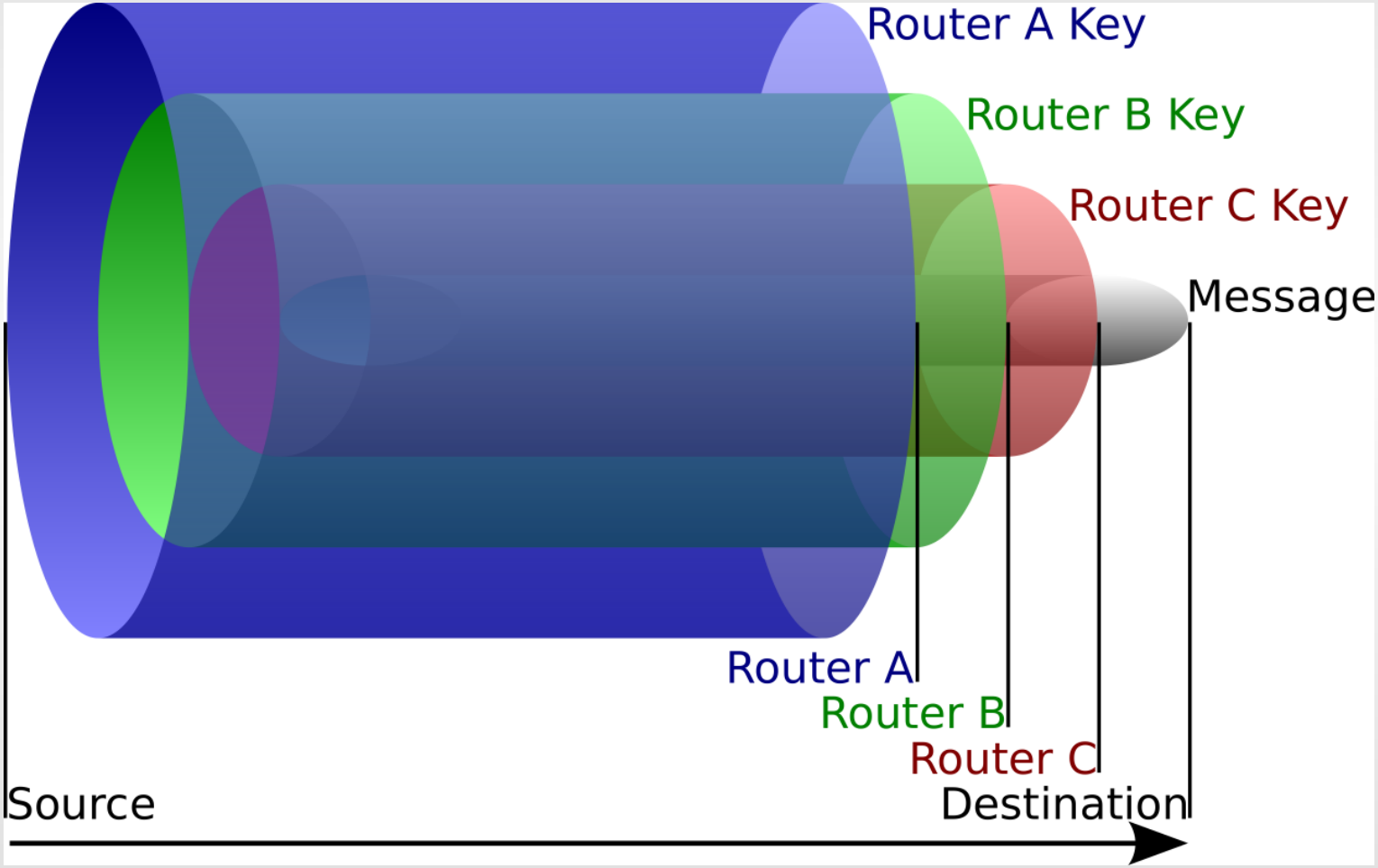
Tor

Onion routing



Tor

Луковичное шифрование



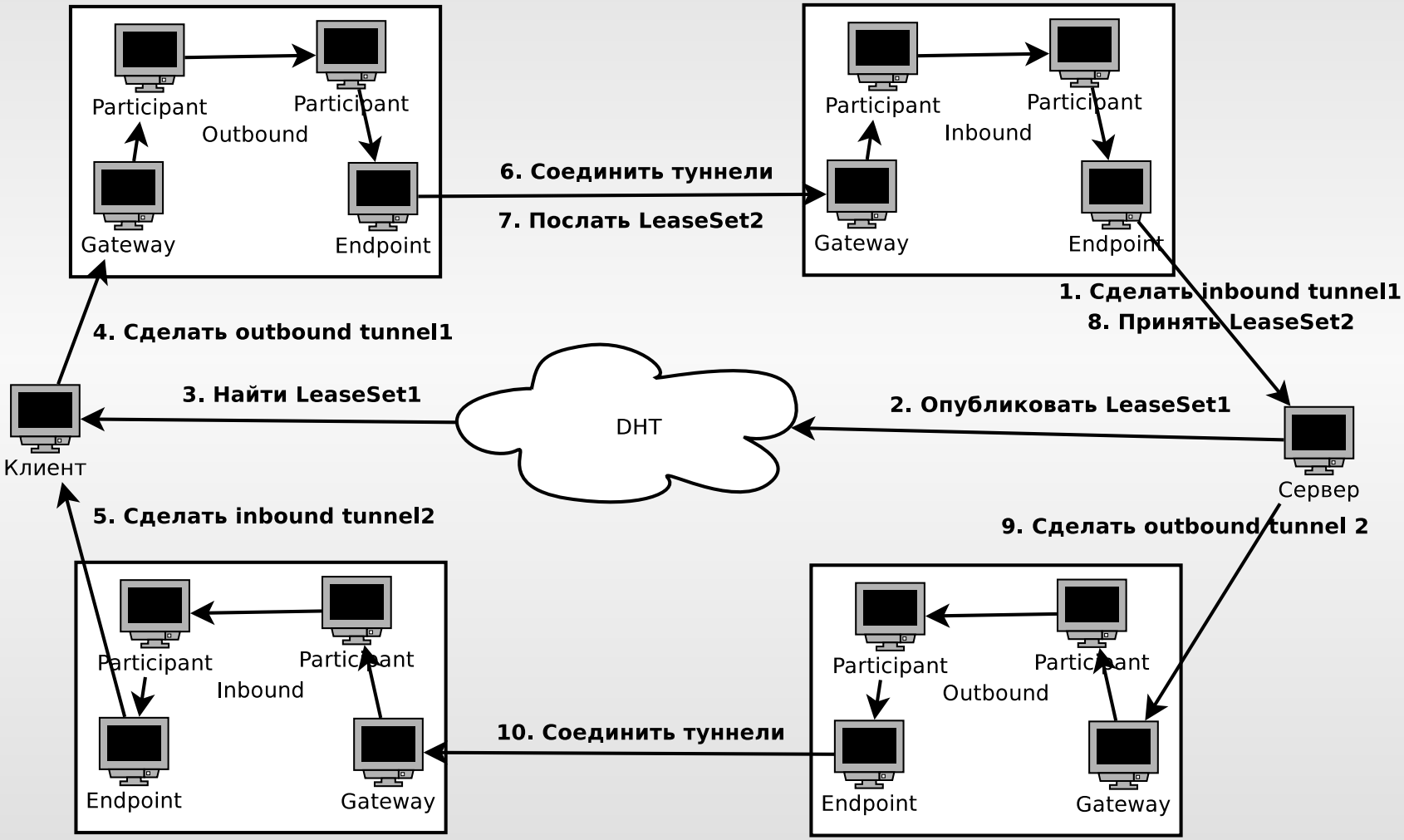
I2P

Отличия от Tor

Tor	I2P
Централизованная директория	DHT
Двунаправленные каналы	Outbound и inbound
512 байт размер сообщения	Чесночные сообщения

I2P

Рукопожатие



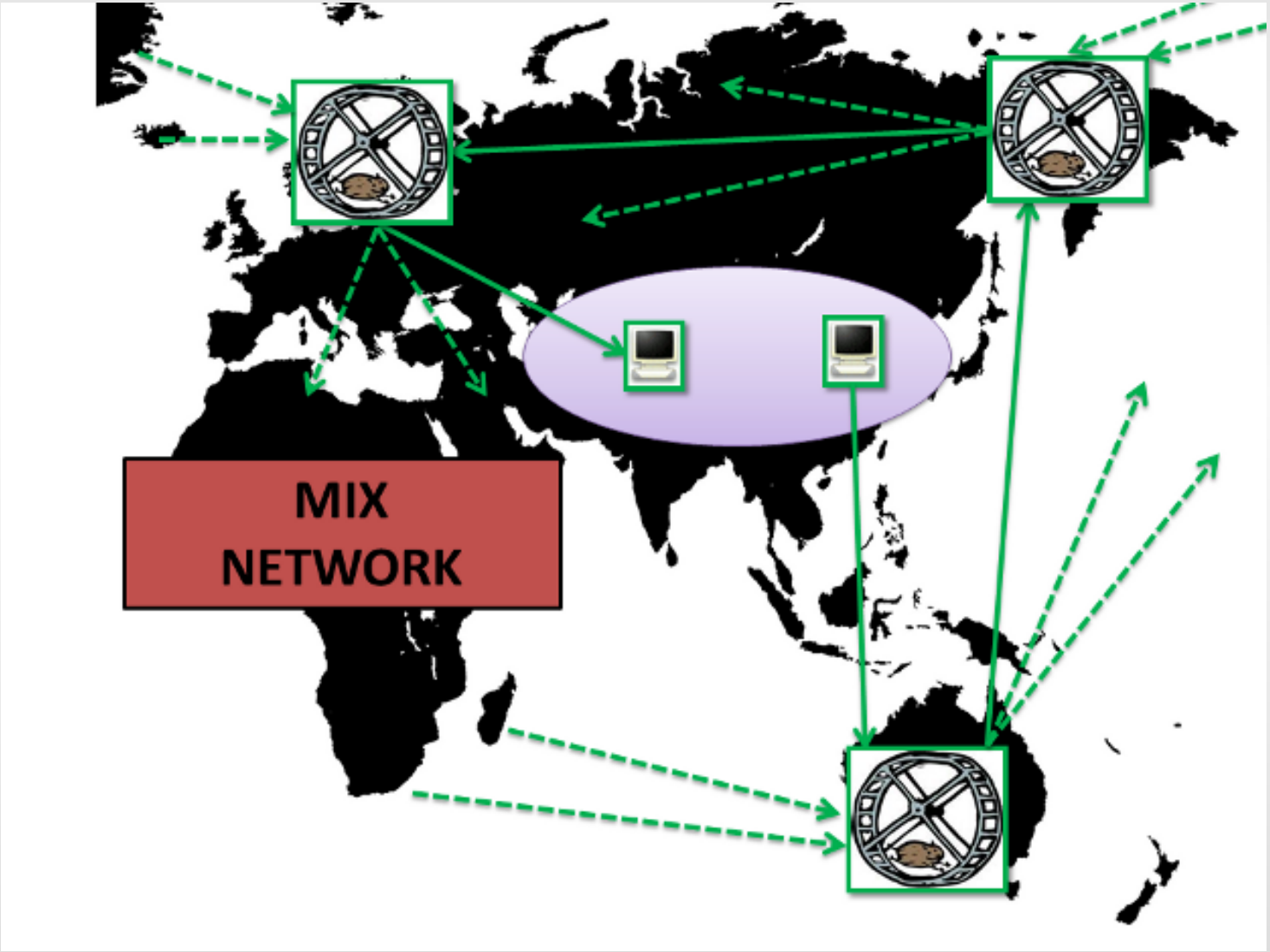
Проблемы real-time Web сервисов

Сторонние каналы

- cookie
- подгрузка изображений и JavaScript
- закрытый/обфусцированный код JavaScript/Java/Flash и перманентные хранилища
- HTTP–заголовки предпочтений и версий
- DNS запросы сайтов
- скомпрометированный PKI
- водяные знаки мультимедиа данных

Проблемы real-time Web сервисов

Mix routing



Для почты реализовано в **Mixmaster**, **Mixminion**

Freenet

- Распределённое децентрализованное хранилище *key* $\leftrightarrow$ *value* пар
- Цензуроустойчивая
- Отказоустойчивая

Freenet

- Распределённое децентрализованное хранилище *key* $\leftrightarrow$ *value* пар
- Цензуроустойчивая
- Отказоустойчивая

Freenet

- Распределённое децентрализованное хранилище *key* $\leftrightarrow$ *value* пар
- Цензуроустойчивая
- Отказоустойчивая

Freenet

Кирпичики

Content Hash Key (CHK)

ключ $hash(enc(M, K)) \parallel K$

значение $enc(M, K)$

Signed Subspace Key (SSK)

ключ $hash(K_{pub}) \parallel K$

значение $K_{pub} \parallel enc(M, K) \parallel sign(enc(M, K), K_{priv})$

Freenet

Кирпичики

Content Hash Key (CHK)

ключ $hash(enc(M, K)) \parallel K$

значение $enc(M, K)$

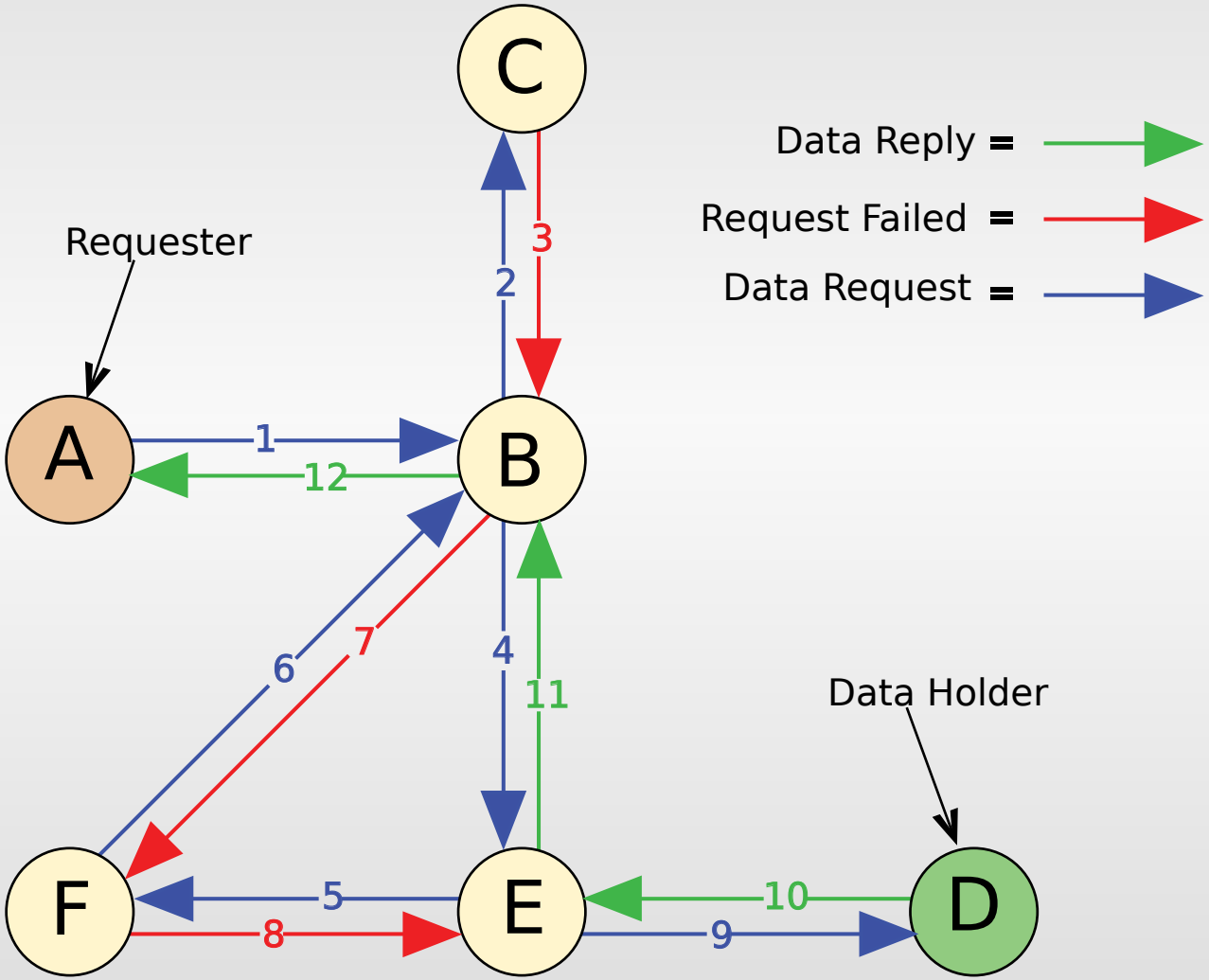
Signed Subspace Key (SSK)

ключ $hash(K_{pub}) \parallel K$

значение $K_{pub} \parallel enc(M, K) \parallel sign(enc(M, K), K_{priv})$

Freenet

Путь запроса/ответа



Opennet/P2P vs Darknet/F2F

- Уязвимый bootstrap
- DoS
- Чёрная дыра для запросов
- Блокирование известных нод

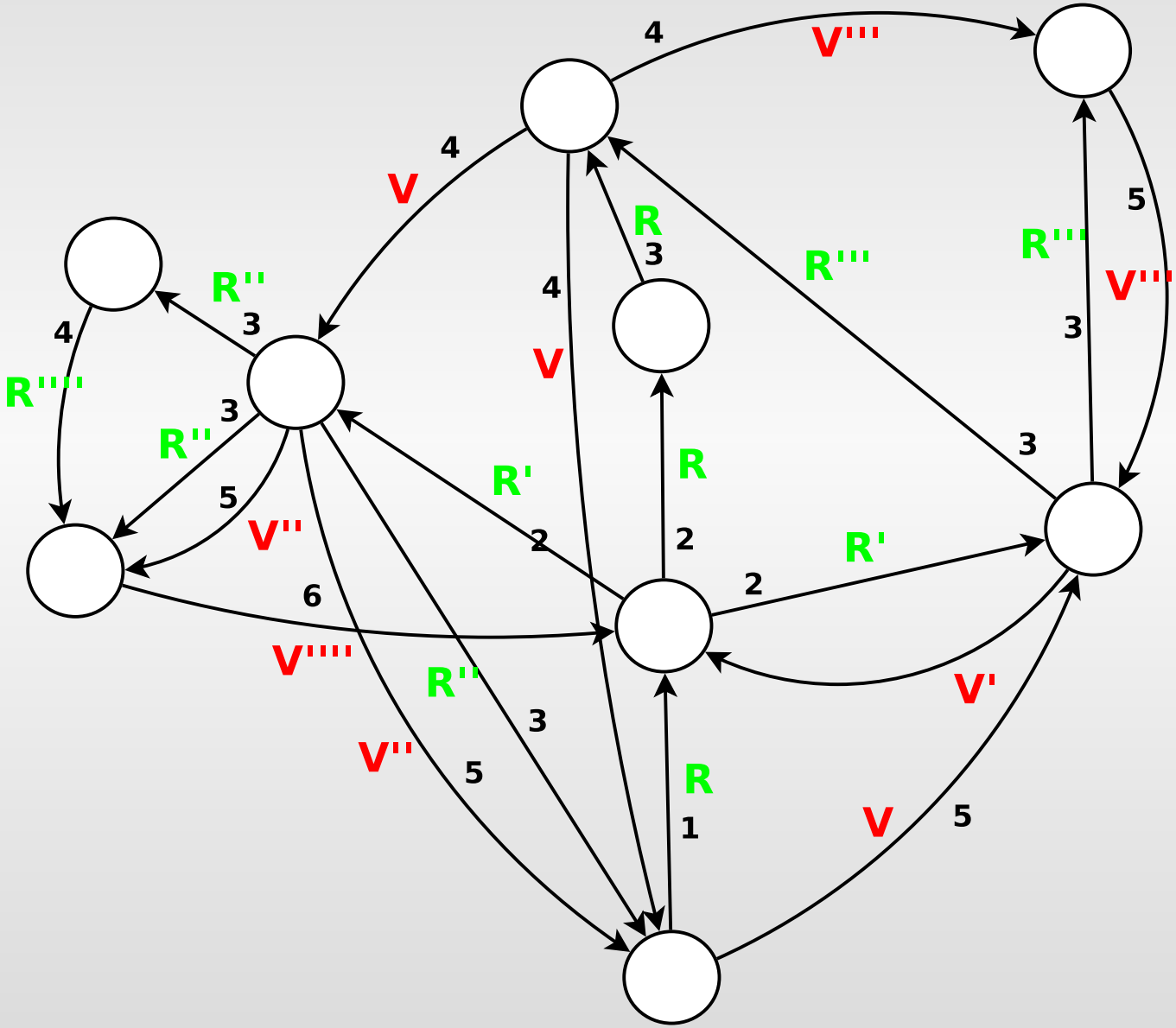
GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов

GNUnet anonymous protocol

Независимые пути следования запросов и ответов



GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов
- Случайность везде
  - Обрабатывать пакет?
  - Если есть reply (на диске), то отвечать?
  - Перенаправлять дальше?
  - Запоминать кто делал запрос?
  - Подменять return-path?
  - Кэшировать reply?
  - Перенаправлять ответ?
  - Как много, кому и с какими задержками разослать?
- Чесночные сообщения, фиксированный размер
- Шум в каналах
- Экономическая модель

GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов
- Случайность везде
  - Обрабатывать пакет?
  - Если есть reply (на диске), то отвечать?
  - Перенаправлять дальше?
  - Запоминать кто делал запрос?
  - Подменять return-path?
  - Кэшировать reply?
  - Перенаправлять ответ?
  - Как много, кому и с какими задержками разослать?
- Чесночные сообщения, фиксированный размер
- Шум в каналах
- Экономическая модель

GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов
- Случайность везде
  - Обрабатывать пакет?
  - Если есть reply (на диске), то отвечать?
  - Перенаправлять дальше?
  - Запоминать кто делал запрос?
  - Подменять return-path?
  - Кэшировать reply?
  - Перенаправлять ответ?
  - Как много, кому и с какими задержками разослать?
- Чесночные сообщения, фиксированный размер
- Шум в каналах
- Экономическая модель

GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов
- Случайность везде
  - Обрабатывать пакет?
  - Если есть reply (на диске), то отвечать?
  - Перенаправлять дальше?
  - Запоминать кто делал запрос?
  - Подменять return-path?
  - Кэшировать reply?
  - Перенаправлять ответ?
  - Как много, кому и с какими задержками разослать?
- Чесночные сообщения, фиксированный размер
- Шум в каналах
- Экономическая модель

GNUnet anonymous protocol

Отличия от Freenet

- Независимые пути следования запросов и ответов
- Случайность везде
  - Обрабатывать пакет?
  - Если есть reply (на диске), то отвечать?
  - Перенаправлять дальше?
  - Запоминать кто делал запрос?
  - Подменять return-path?
  - Кэшировать reply?
  - Перенаправлять ответ?
  - Как много, кому и с какими задержками разослать?
- Чесночные сообщения, фиксированный размер
- Шум в каналах
- Экономическая модель

Современный Интернет

Что контролируют США/правительства

- Распределение адресов (IANA)
- DNS (корневая зона)
- Корневые сертификаты DNSSEC
- X.509 CA
- Поставщиков броузеров и их CA

Таким образом

- Текущий PKI гарантирует отсутствие конфиденциальности и аутентификации
- Централизованные БД гарантируют цензуру

Современный Интернет

Что контролируют США/правительства

- Распределение адресов (IANA)
- DNS (корневая зона)
- Корневые сертификаты DNSSEC
- X.509 CA
- Поставщиков броузеров и их CA

Таким образом

- Текущий PKI гарантирует отсутствие конфиденциальности и аутентификации
- Централизованные БД гарантируют цензуру

Резюме

- Web–технологии (серверы, клиенты, протоколы) современные — не совместимы с анонимизацией $\Rightarrow$ специальные технологии для этого
- Real–time — гарантия возможности статистического анализа $\Rightarrow$ нужно ли он вам так?
- PKI в принципе не работает $\Rightarrow$ Web-of-Trust
- Централизация $\Rightarrow$ цензура, не отказоустойчивость, не анонимно
- Не будет вас $\rightarrow$ не будет промежуточных узлов $\rightarrow$ низкая скорость, надёжность, анонимность $\rightarrow$ сетью никто не пользуется $\rightarrow$ нет работающей серьёзной анонимизации $\rightarrow$ токсичность информации, нет приватности
- Закрытое проприетарное ПО — забудьте о безопасности, анонимности и конфиденциальности

Компромисы!

Шифропанки решили пойти безкомпромисным путём: **secushare.org**

- Faceboogle $\Rightarrow$ RegEx/PSYC
- DNS $\Rightarrow$ GNS
- IP/BGP $\Rightarrow$ Mesh ($ECDHE + AES$)
- Databases $\Rightarrow$ R^5N DHT
- TCP/UDP/etc $\Rightarrow$ GNUnet anonymous protocol

Компромисы!

Шифропанки решили пойти безкомпромисным путём:
secushare.org

- Faceboogle $\Rightarrow$ RegEx/PSYC
- DNS $\Rightarrow$ GNS
- IP/BGP $\Rightarrow$ Mesh ($ECDHE + AES$)
- Databases $\Rightarrow$ R^5N DHT
- TCP/UDP/etc $\Rightarrow$ GNUnet anonymous protocol

Вопросы?