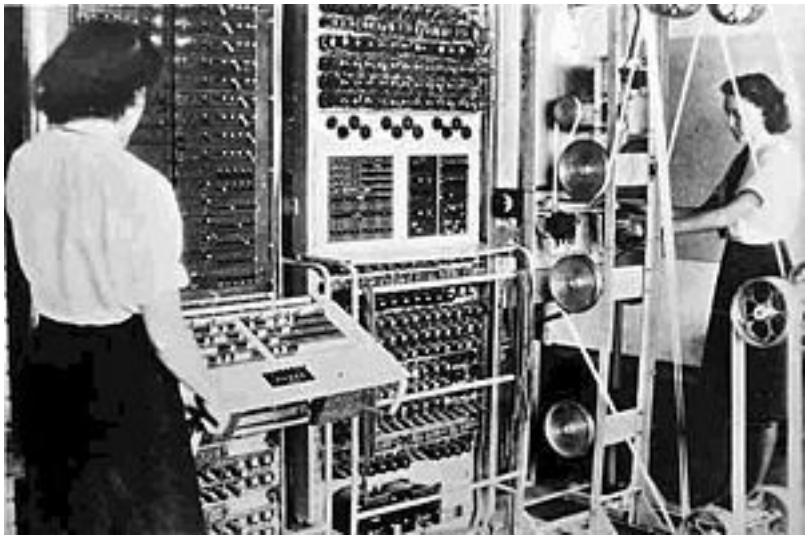
Инфраструктура открытых ключей (PKI)

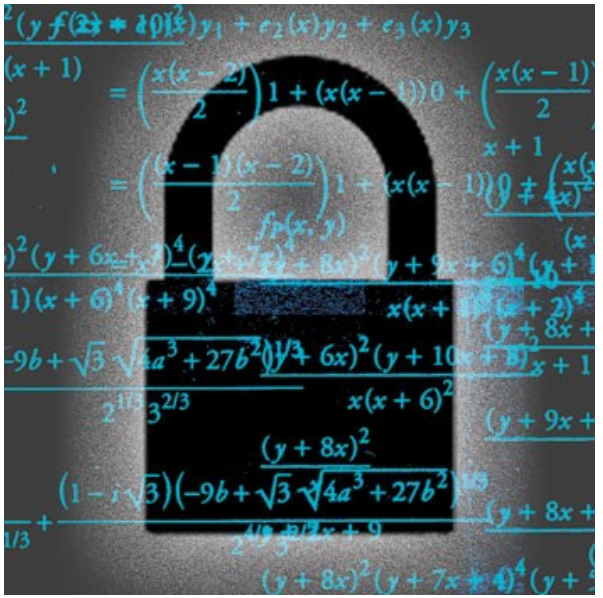
Антон Карпов для студентов КИТ, 6 ноября 2013 г.

Яндекс

Криптография

- Конфиденциальность (шифрование)
- Целостность (подпись)
- Аутентификация
- Невозможность отказа от авторства

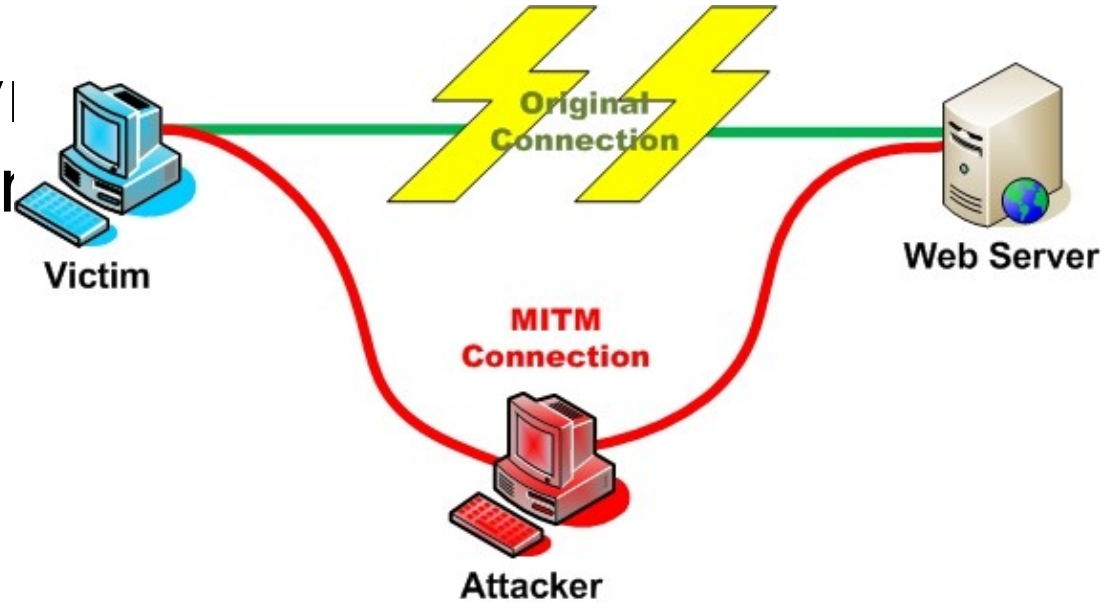




Прикладная криптография в интернете

- Удаленное управление (SSH, RDP)
- Безопасные транзакции на веб-сайтах (HTTPS)
- Конфиденциальность переписки (PGP, S/MIME)

- Защита от прослу
сообщений “Man i



Криптосистема

- Отправитель
- Получатель
- Сообщение
- Алгоритм шифрования
- Ключ шифрования
- (Ключ для дешифрования)

Виды шифрования

Симметричное

- Общие ключи шифрования и дешифрования
- Типичные длины ключей 128-256 бит

Ассиметричное

- Различные ключи для шифрования и дешифрования
- Типичные длины ключей: 1024-4096 для операций в конечном поле, 256 бит для операций на эллиптической кривой

Симметричные шифры

- Начиная от древнейших времен и до наших дней
- Предполагают передачу секрета (ключа) по доверенному (защищенному) каналу

Симметричные шифры: преимущества

- Быстрые
- Простые и хорошо изученные

Симметричные шифры: проблемы

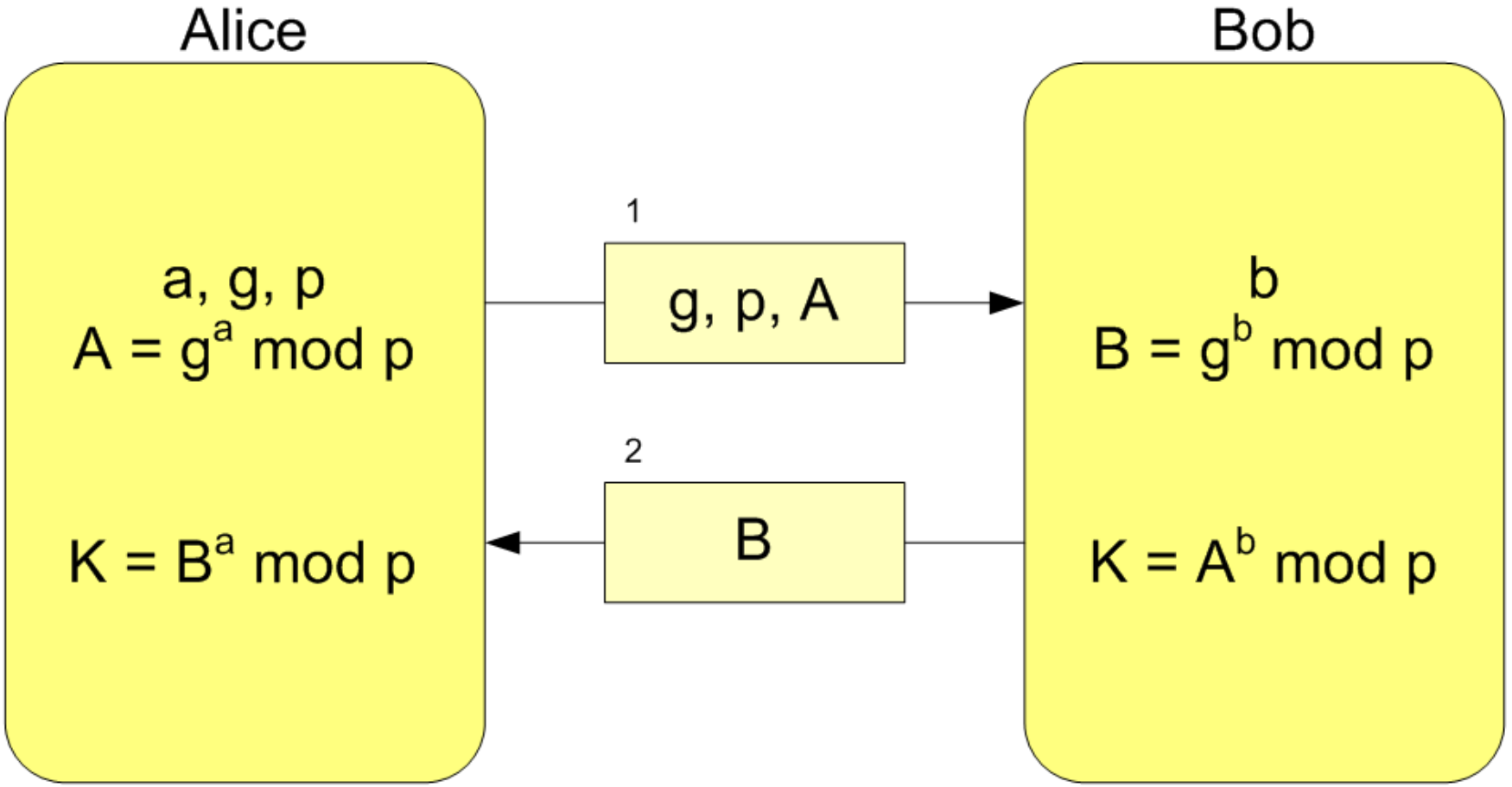
- Распределение ключей
- Безопасная передача ключей

Криптография с открытым ключом

- 1976, Diffie-Hellman. Выработка и распространение секретного ключа по недоверенному каналу.
- 1977, RSA. Обмен ключами, шифрование и цифровая подпись.

- На практике используется для передачи сессионного симметричного ключа

Diffie-Hellman



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

RSA

1. Выбираем простые числа p, q (1024-4096 бит)
2. Вычисляем $n = pq$
3. Вычисляем $\varphi(n)=(q-1)(p-1)$
4. Выбираем e – взаимно простое с $\varphi(n)$
5. Вычисляем d: $ed=1(\mathrm{mod}\varphi(n))$

RSA

- Пара P = (e,n) публикуется в качестве открытого ключа
- Пара S = (d,n) играет роль секретного ключа

RSA, шифрование

Шифрование на открытом ключе (e, n)

- Открытый текст M
- Шифротекст C = Me mod n

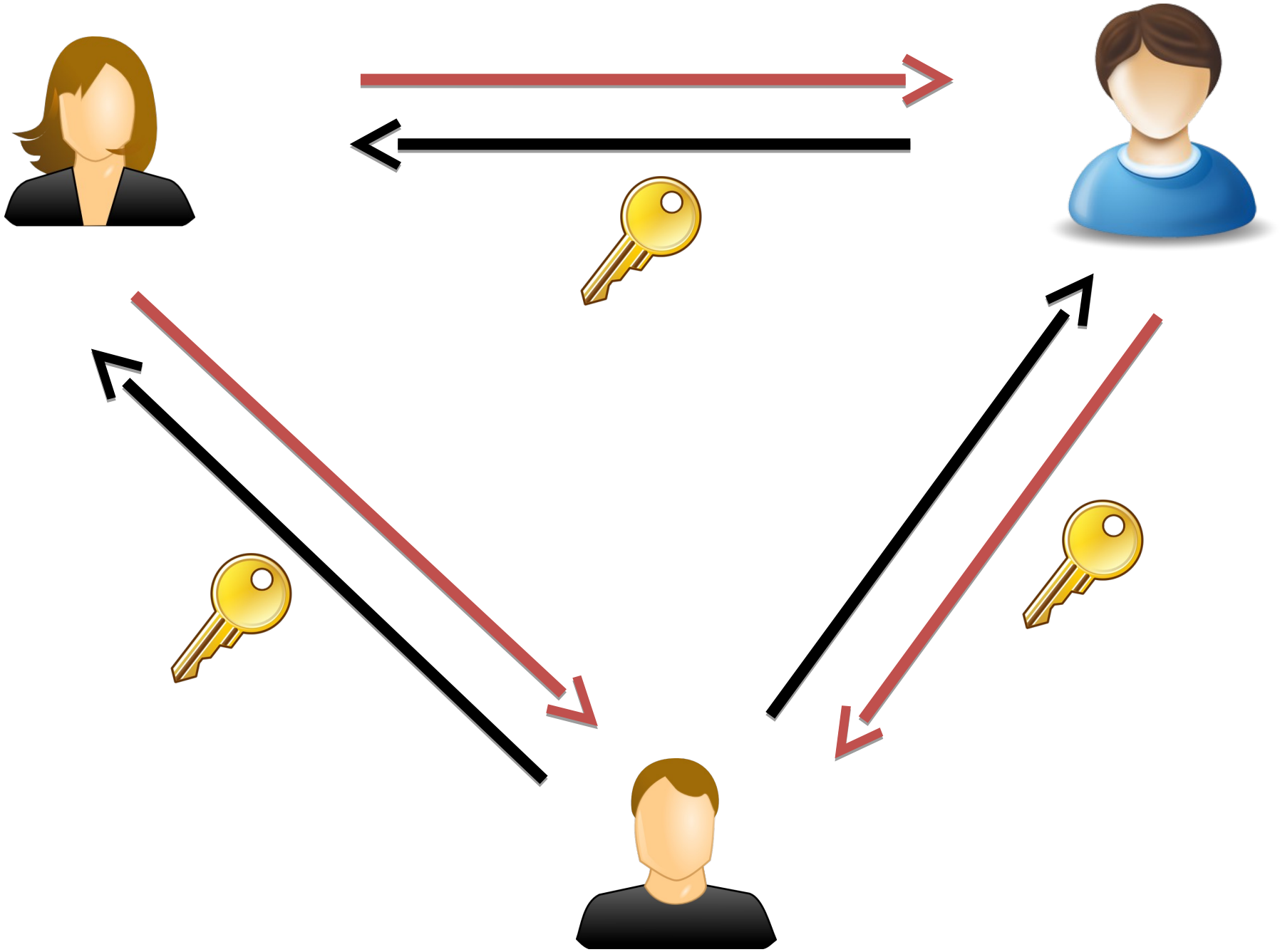
RSA, дешифрование

Дешифрование за закрытом ключе (d, n)

$C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M \bmod n$

- Алиса генерирует закрытый ключ (privkey)
- Алиса генерирует открытый ключ (pubkey)
- Алиса отправляет открытый ключ Бобу по открытом каналу

- Боб **шифрует сообщение на открытом ключе** Алисы и отправляет его Алисе по открытому каналу
- Алиса **расшифровывает сообщение, используя свой закрытый ключ**



Криптография с открытым ключом: проблемы

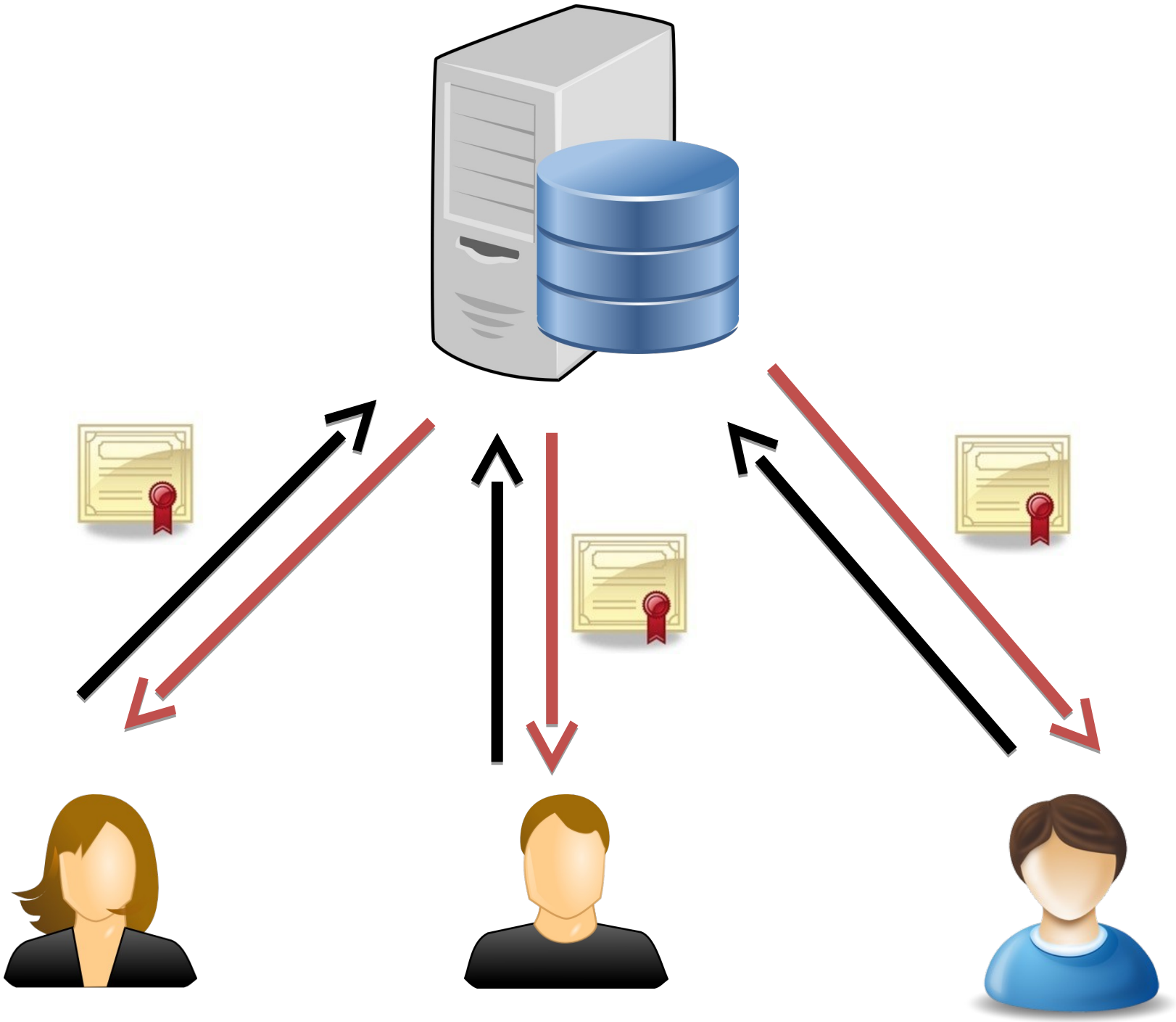
- Как подтвердить подлинность открытого ключа?

Public Key Infrastructure

- Certificate Authority – сущность, которой все доверяют
- Иерархическая система доверия
- CA выдает цифровые сертификаты
- Возможность делегирования (subordinate CA)

Цифровой сертификат

- Открытый ключ субъекта, подписанный закрытым ключом CA
- Сертификаты могут использоваться для подписи, шифрования, аутентификации клиента или сервера



Инфраструктура PKI

- Root CA
- Subordinate (intermediate) CAs
- Защищенное хранилище для ключа (HSM)
- Набор политик и регламентов
- Каталог выданных сертификатов
- Каталог отозванных сертификатов

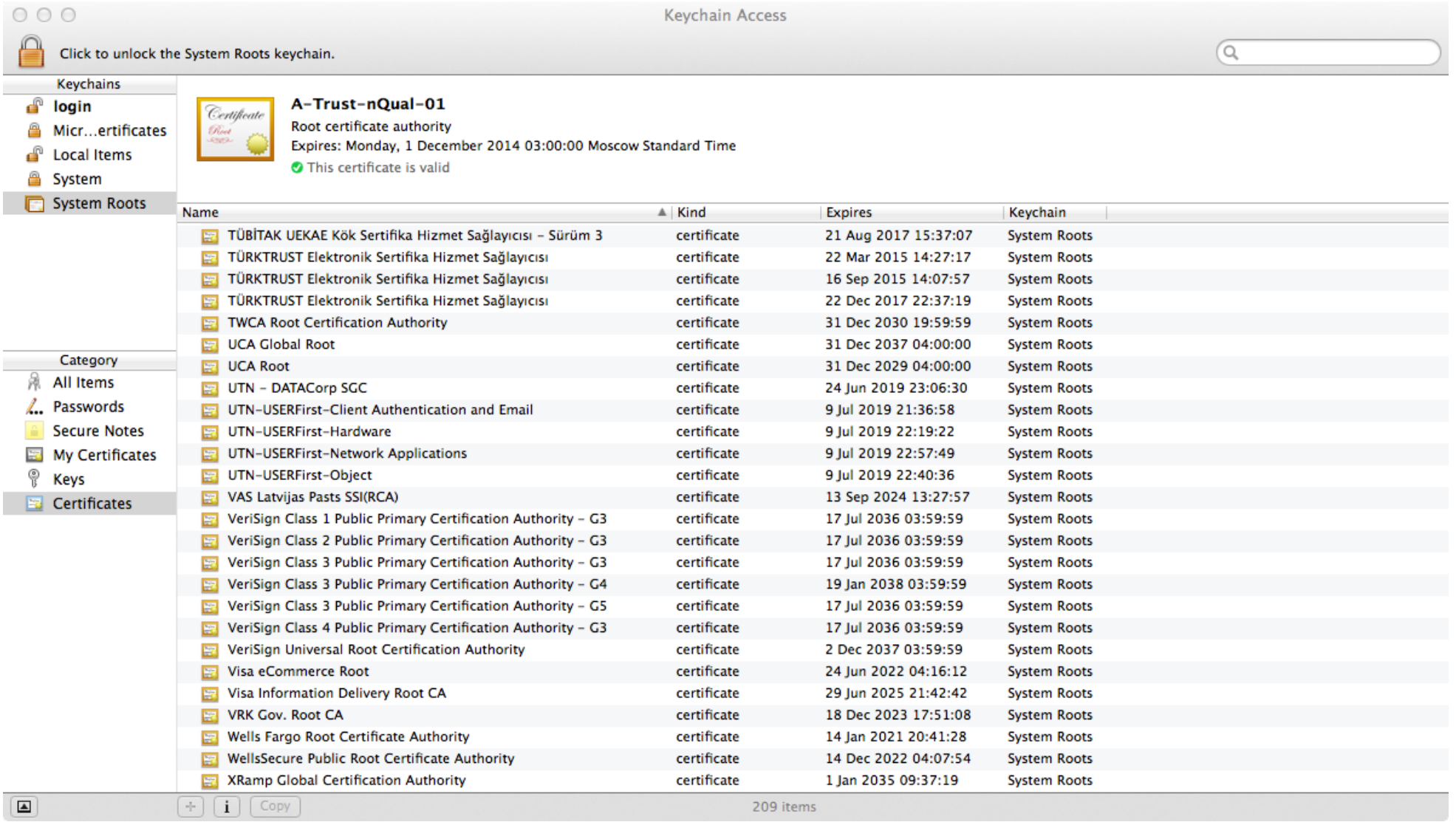
Mesh

- Алиса генерирует закрытый ключ
- Алиса генерирует открытый ключ
- Алиса передает открытый ключ Бобу
- Боб верит Алисе и шифрует сообщения на полученном открытом ключе

PKI

- Алиса генерирует закрытый ключ
- Алиса генерирует CSR
- Алиса отправляет CSR в УЦ
- УЦ подписывает CSR своим закрытым ключом, выпуская сертификат (CER)
- Боб получает CER Алисы из публичного каталога
- Боб проверяет валидность CER и шифрует сообщения на нем

Модель доверия



Модель доверия

Webtrust program for certificate authorities

http://www.webtrust.org/homepage-documents/item27839.aspx

Baseline requirements and guidelines

https://www.cabforum.org/documents.html

Стандарт X.509

- Разработан в 1988 году в RSA

- Стандартная структура сертификата
- Стандартные механизмы получения и отзыва
- Стандарты на проверку валидности

Структура сертификата

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity (Not Before, Not After)
- Subject
- Subject Public Key Info (Algorithm, Key)
- Extensions (Certificate Usage, etc)
- Certificate Signature Algorithm
- Certificate Signature

Стандартные форматы файла

- PEM (Base64)
- DER (binary)
- PKCS#12 (контейнер)

CRL

- Список, публикуемый CA на регулярной основе
- Имеет время жизни
- Содержит причину отзыва сертификата
- Revoked или Hold

OCSP

- Проверка статуса в реальном времени
- Недоступность?
- Нарушение приватности?

X.509 PKI: проблемы

- Нет возможности ограничить Subordinate CA в выдаче сертификатов
- Что делать при недоступности CRL или OCSP?

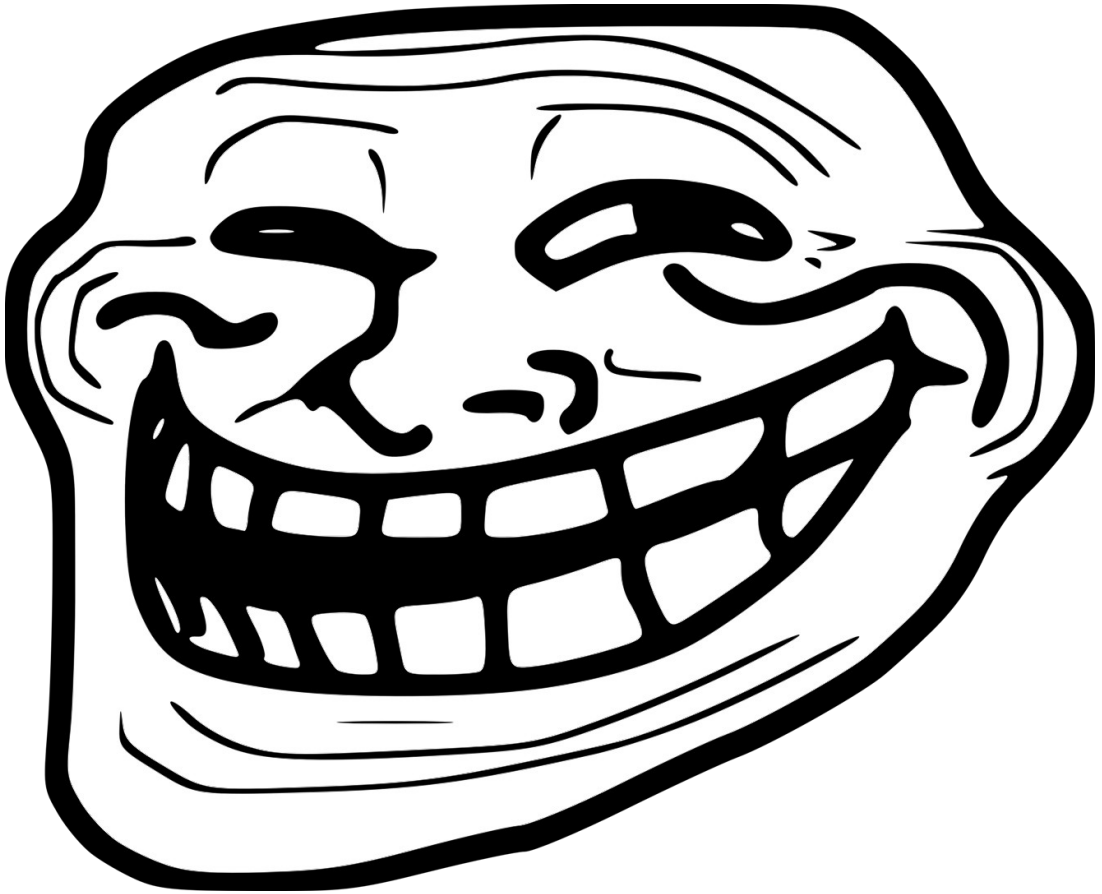
Что делать при компрометации Root CA?

Что делать при компрометации Root CA?

- В мире около 1500 CA, которым доверяют популярные браузеры, от 650 организаций

- Весна 2011: взлом Comodo
- Лето 2011: взлом Diginotar
- Весна 2012: взлом Verisign
- Зима 2012: Trsutwave и сертификат для MITM

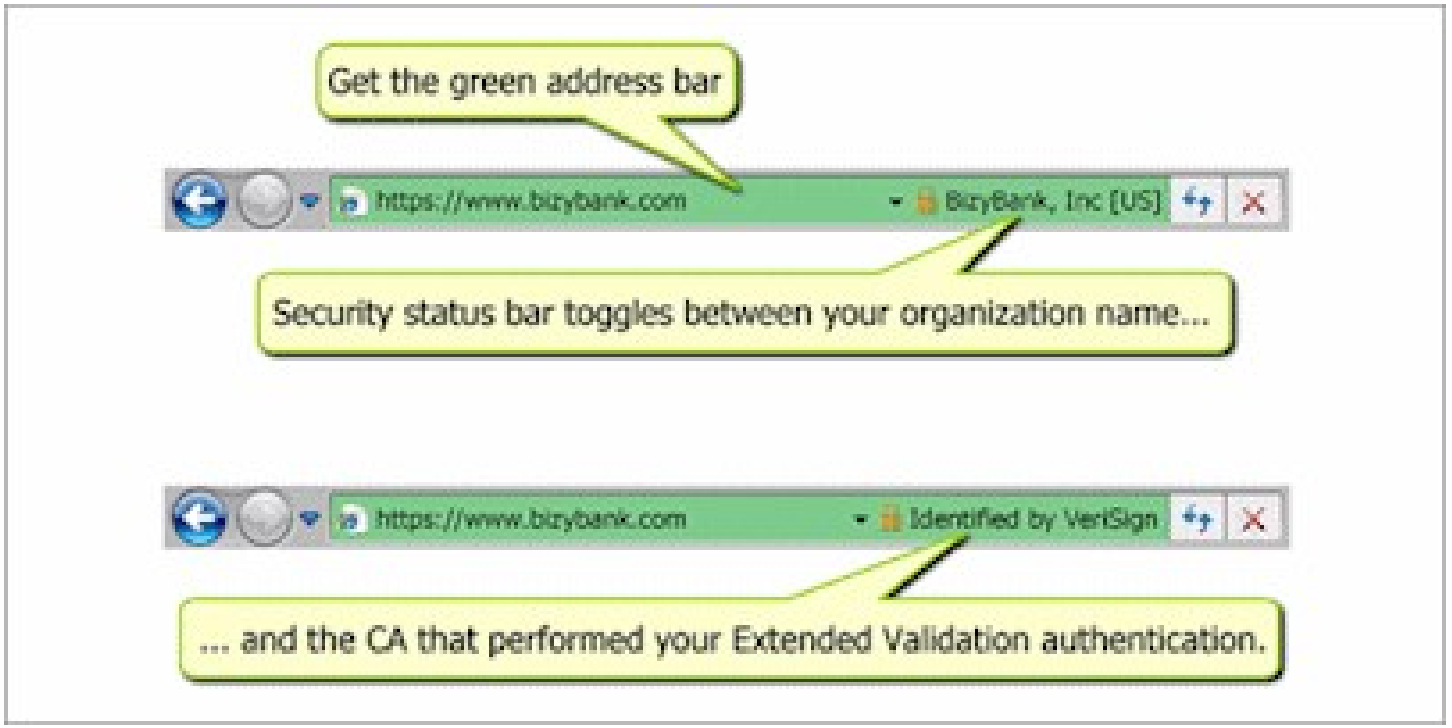
Отозвать сертификат скомпрометированного CA?



X.509 PKI: проблемы

Все потому, что PKI превратился в бизнес. Удостоверяющие центры – торговцы воздухом

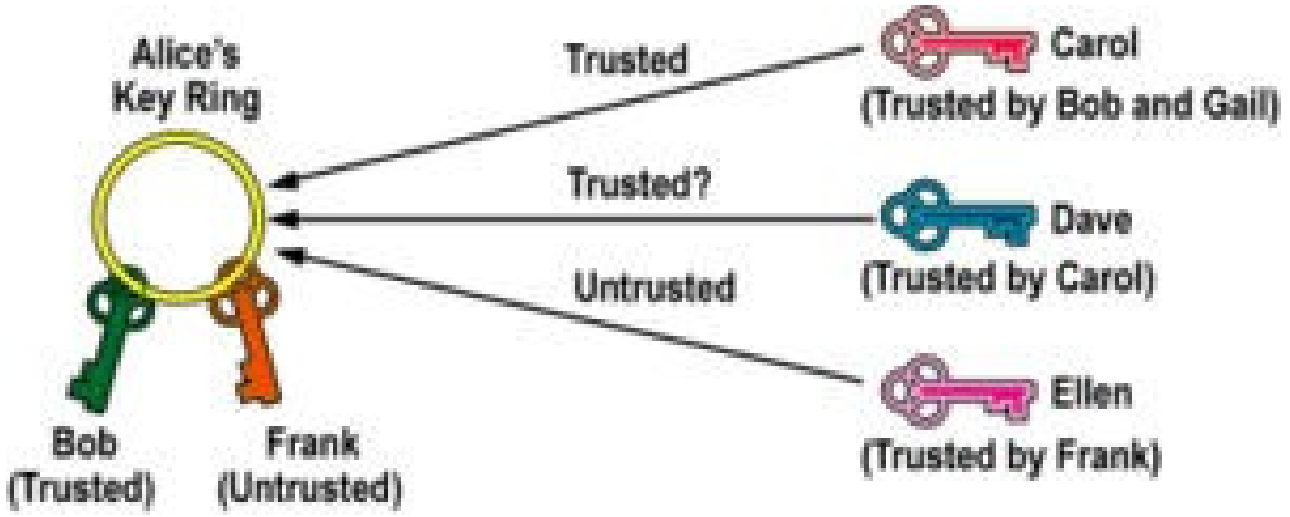
Extended Validation Certificates



Pretty Good Privacy (PGP)

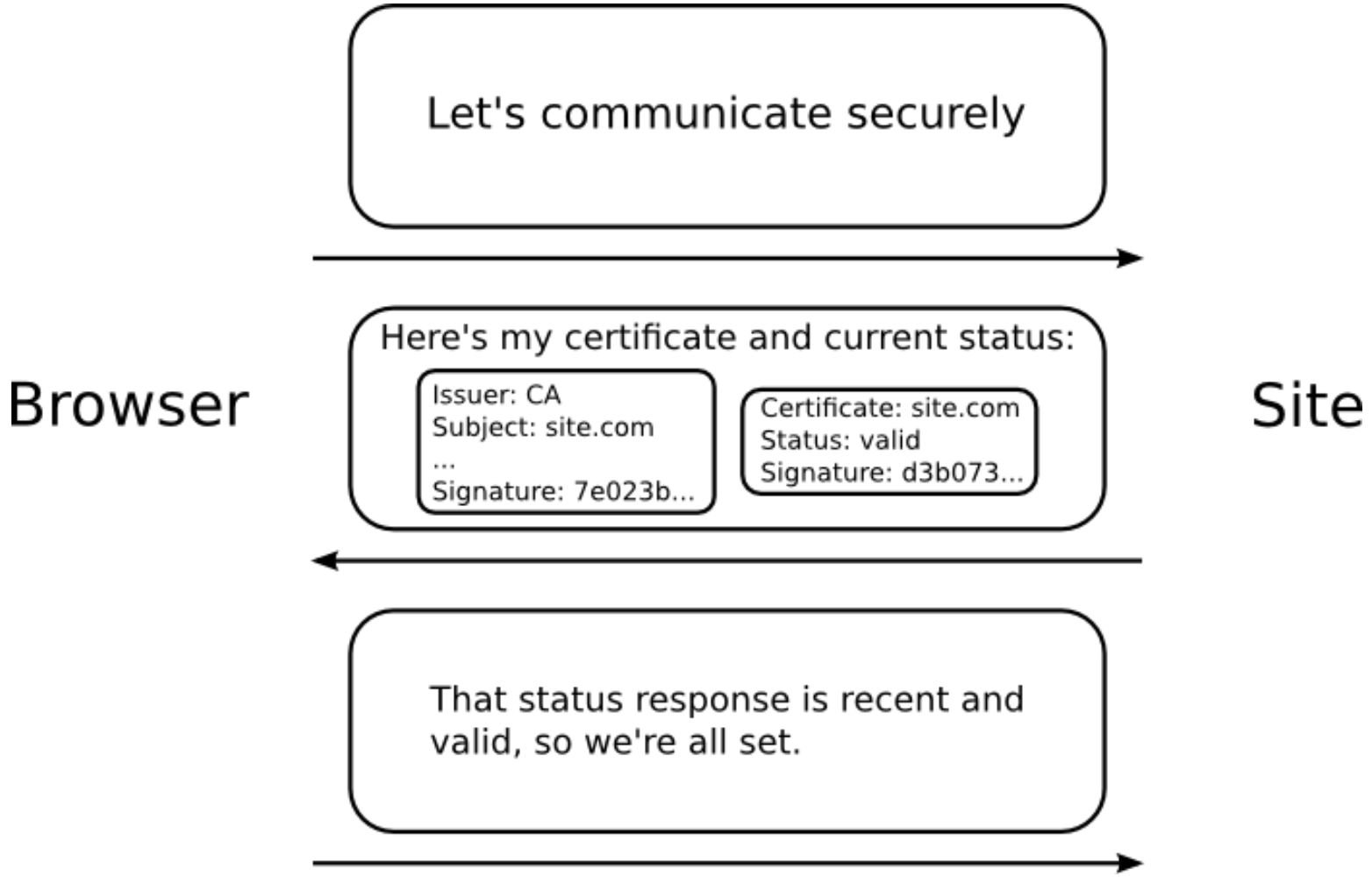
- Филл Циммерман, 1991
- Web of Trust

http://malpaso.ru/gpg-keysigning-party/



Расширения PKI

OCSP stapling



Расширения PKI

Certificate pinning

Доверие CA, а не закрытому ключу ;-(

Альтернативы PKI

Convergence (http://convergence.io)

- Гибкость доверия (trust agility)
- Распределенная система доверия
- Проверка сертификата третьими сторонами (нотариусами)

Альтернативы PKI

TACK (http://tack.io)

- Расширение TLS
- Передача ключа в рамках TLS handshake
  - Клиент передает TLS extension “tack” в ClientHello
  - Сервер отвечает TackExtension с ключом сервера
- Подпись сертификата сервера ключом TSK
- TACK-ключи имеют время жизни и механизм перевыдачи

- Не защищает от MITM при первоначальном подключении

Альтернативы PKI

Google Key Pinning

- Расширение HTTP
- Пиннинг ключей сервера
- Backup key. Backup backup key


That's all Folks!

Домашнее задание: OpenSSL

http://www.madboa.com/geek/openssl/

Задания: http://intern.contest.yandex.ru/