

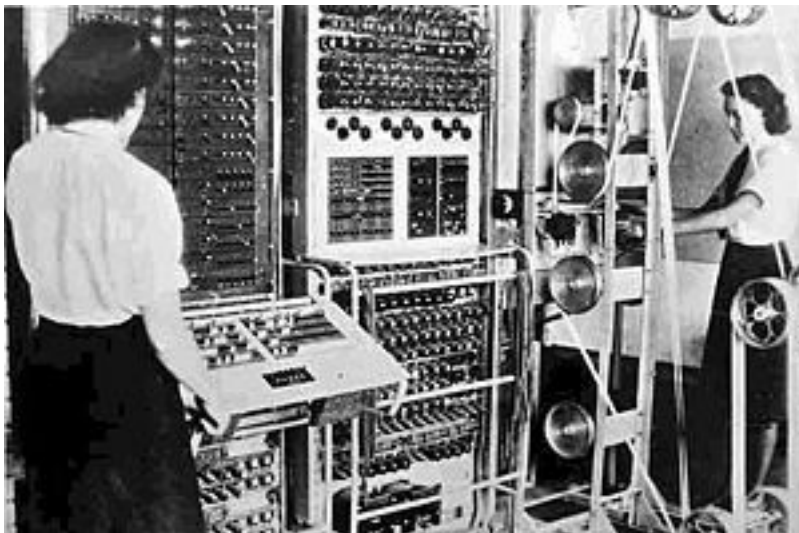
# Инфраструктура ОТКРЫТЫХ КЛЮЧЕЙ (PKI)

Антон Карпов для студентов КИТ, 6 ноября 2013 г.

Яндекс

# Криптография

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

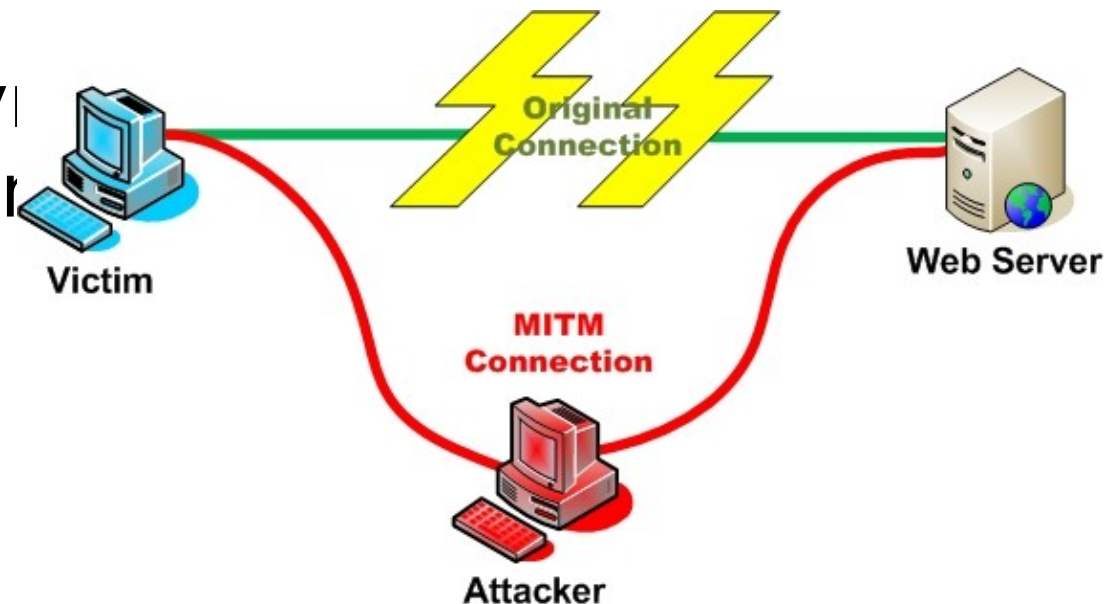


$$\begin{aligned} & (y f(x) + g(x))y_1 + e_2(x)y_2 + e_3(x)y_3 \\ & (x+1)^2 = \left(\frac{x(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right) \\ & = \left(\frac{(x-1)(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right) \\ & f(x, y) \\ & (y+6x+2)^4(y+3x+8x)^2(y+9x+6)^4(y+1) \\ & 1)(x+6)^4(x+9)^4 \quad x(x+1)(x+2)^4 \\ & -9b + \sqrt{3}\sqrt{4a^3+27b^2}(y+6x)^2(y+10x+5)^2x+1 \\ & \frac{2^{1/3}3^{2/3}}{x(x+6)^2} \frac{(y+8x)^2}{(y+9x+)} \\ & \frac{(1-i\sqrt{3})(-9b+\sqrt{3}\sqrt{4a^3+27b^2})^{1/3}}{2^{1/3}3^{2/3}} \frac{(y+8x+)}{(y+8x)^2(y+7x+4)^4(y+)} \end{aligned}$$

# Прикладная криптография в интернете

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

- Защита от прослушивания сообщений “Man in the Middle”



# 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

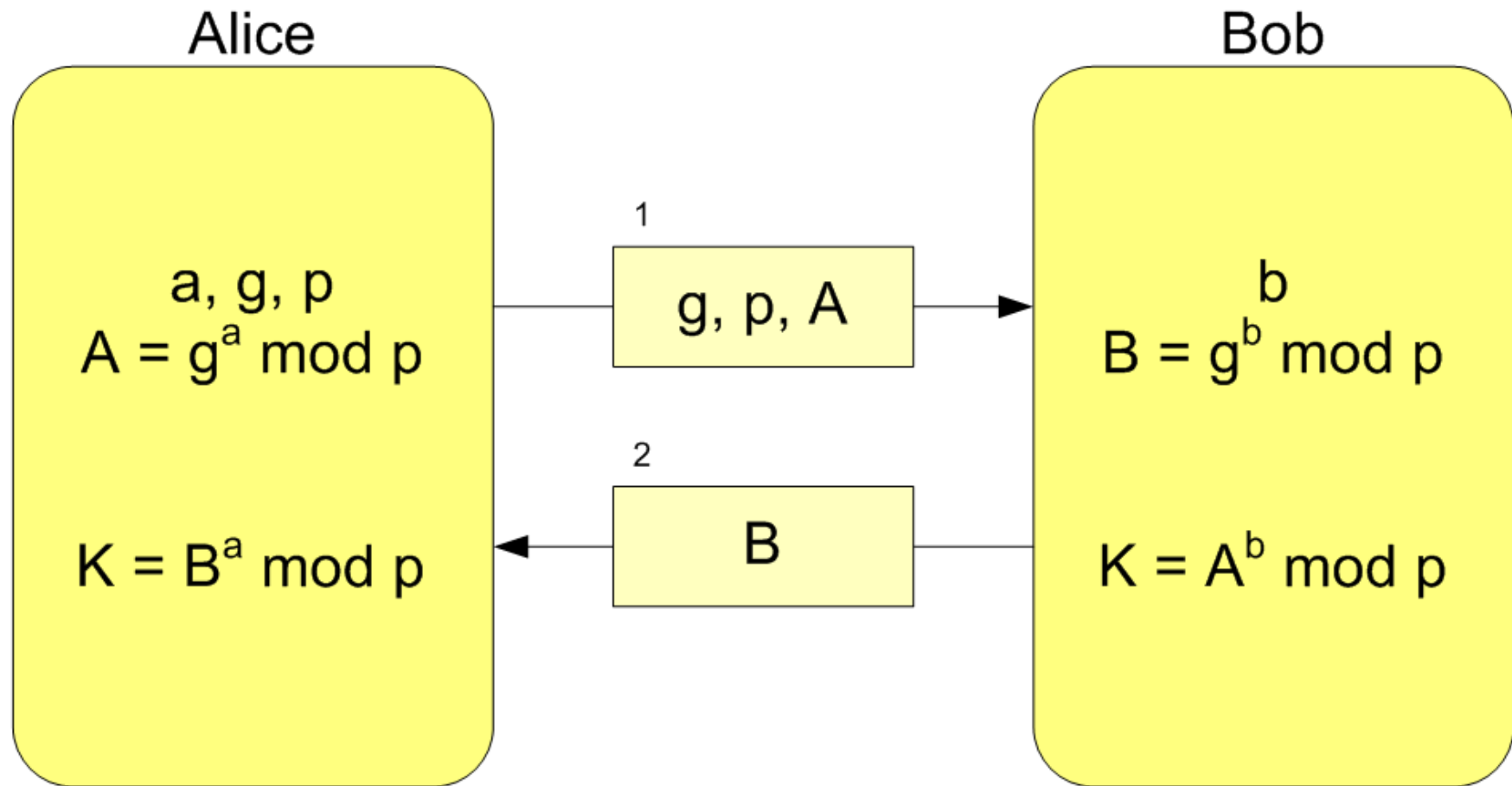




# Криптография с открытым ключом

- 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  $\phi(n) = (q-1)(p-1)$
4. Выбираем  $e$  – взаимно простое с  $\phi(n)$
5. Вычисляем  $d$ :  $ed = 1 \pmod{\phi(n)}$

# RSA

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

# RSA, шифрование

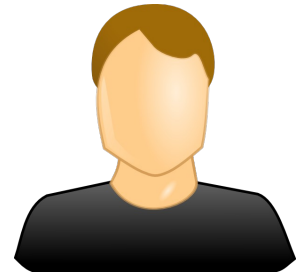
Шифрование на открытом ключе  
( $e, n$ )

- Открытый текст  $M$
- Шифротекст  $C = M^e \bmod n$

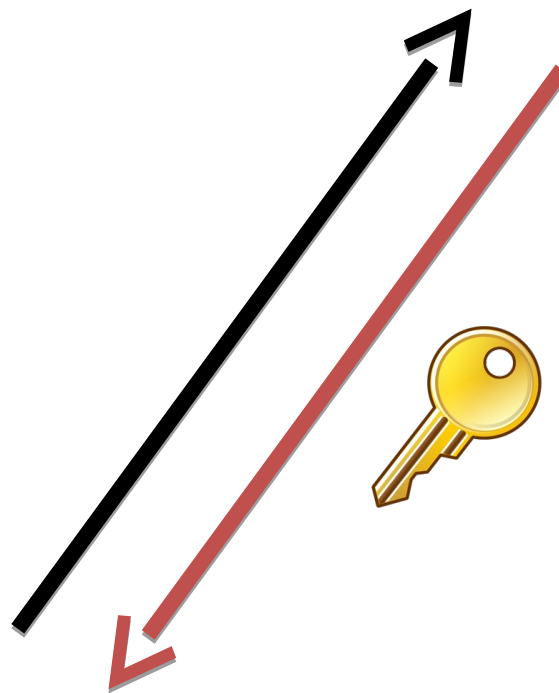
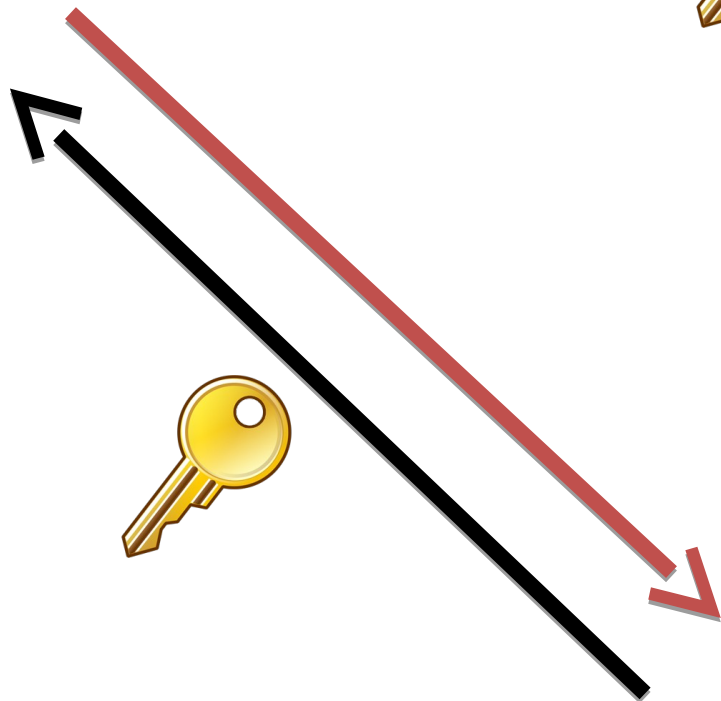
# RSA, дешифрование

Дешифрование за закрытом ключе  
(d, n)

$$C d \bmod n = (M e \bmod n) d \bmod n =$$
$$M e d \bmod n = M \bmod n$$



- Алиса генерирует закрытый ключ (privkey)
- Алиса генерирует открытый ключ (pubkey)
- Алиса отправляет открытый ключ Бобу по открытому 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?

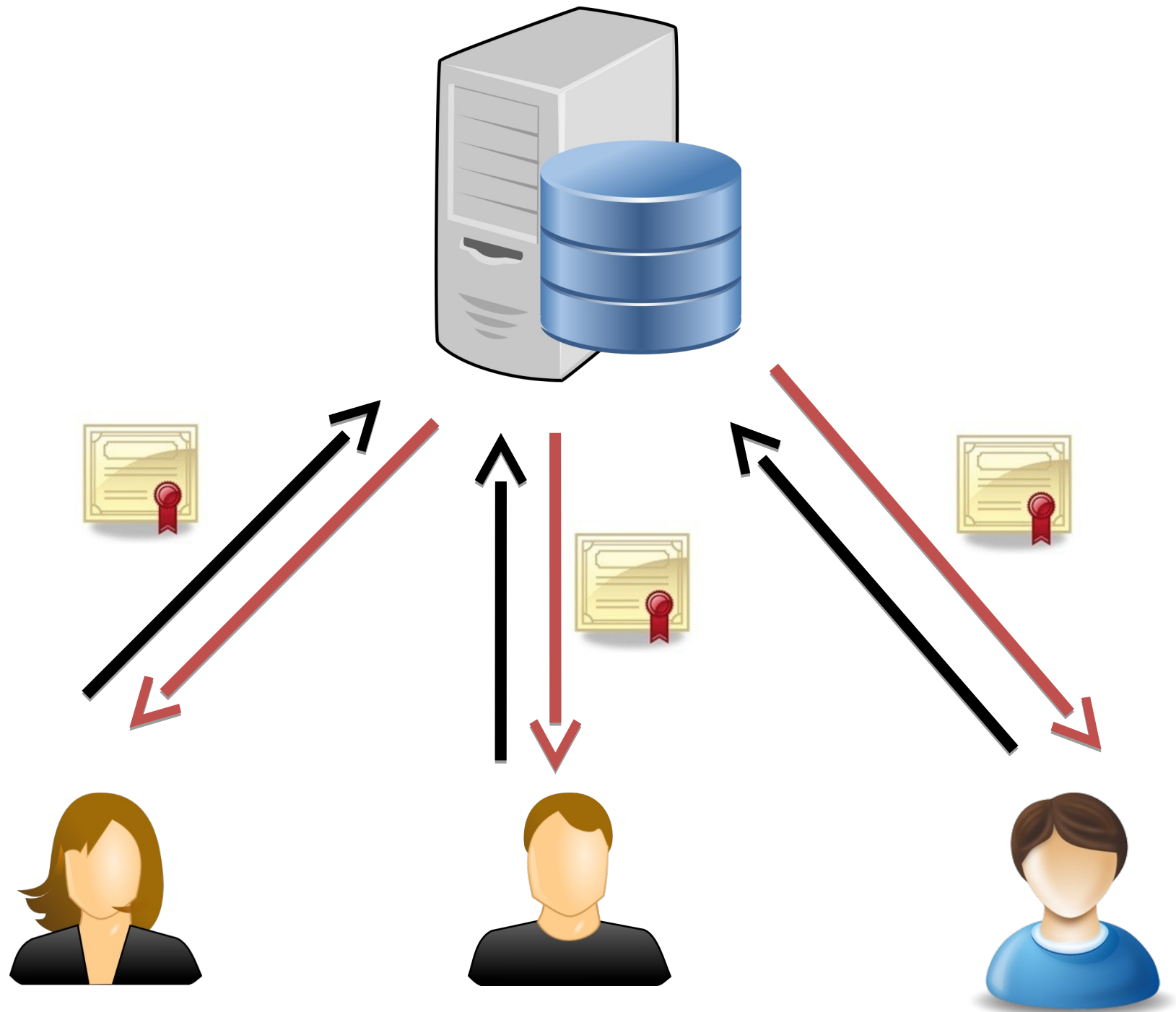


# Public Key Infrastructure

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

# Цифровой сертификат

- Открытый ключ субъекта, подписанный закрытым ключом СА
- 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

Keychain Access

Click to unlock the System Roots keychain.

Keychains

login

Micr...ertificates

Local Items

System

System Roots

Category

All Items

Passwords

Secure Notes

My Certificates

Keys

Certificates

Certificate

Root

**A-Trust-nQual-01**  
Root certificate authority  
Expires: Monday, 1 December 2014 03:00:00 Moscow Standard Time  
✔ This certificate is valid

Name	Kind	Expires	Keychain
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3	certificate	21 Aug 2017 15:37:07	System Roots
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	22 Mar 2015 14:27:17	System Roots
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	16 Sep 2015 14:07:57	System Roots
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	22 Dec 2017 22:37:19	System Roots
TWCA Root Certification Authority	certificate	31 Dec 2030 19:59:59	System Roots
UCA Global Root	certificate	31 Dec 2037 04:00:00	System Roots
UCA Root	certificate	31 Dec 2029 04:00:00	System Roots
UTN - DATACorp SGC	certificate	24 Jun 2019 23:06:30	System Roots
UTN-USERFirst-Client Authentication and Email	certificate	9 Jul 2019 21:36:58	System Roots
UTN-USERFirst-Hardware	certificate	9 Jul 2019 22:19:22	System Roots
UTN-USERFirst-Network Applications	certificate	9 Jul 2019 22:57:49	System Roots
UTN-USERFirst-Object	certificate	9 Jul 2019 22:40:36	System Roots
VAS Latvijas Pasts SSL(RCA)	certificate	13 Sep 2024 13:27:57	System Roots
VeriSign Class 1 Public Primary Certification Authority - G3	certificate	17 Jul 2036 03:59:59	System Roots
VeriSign Class 2 Public Primary Certification Authority - G3	certificate	17 Jul 2036 03:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G3	certificate	17 Jul 2036 03:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G4	certificate	19 Jan 2038 03:59:59	System Roots
VeriSign Class 3 Public Primary Certification Authority - G5	certificate	17 Jul 2036 03:59:59	System Roots
VeriSign Class 4 Public Primary Certification Authority - G3	certificate	17 Jul 2036 03:59:59	System Roots
VeriSign Universal Root Certification Authority	certificate	2 Dec 2037 03:59:59	System Roots
Visa eCommerce Root	certificate	24 Jun 2022 04:16:12	System Roots
Visa Information Delivery Root CA	certificate	29 Jun 2025 21:42:42	System Roots
VRK Gov. Root CA	certificate	18 Dec 2023 17:51:08	System Roots
Wells Fargo Root Certificate Authority	certificate	14 Jan 2021 20:41:28	System Roots
WellsSecure Public Root Certificate Authority	certificate	14 Dec 2022 04:07:54	System Roots
XRamp Global Certification Authority	certificate	1 Jan 2035 09:37:19	System Roots

i

Copy

209 items

# 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 СА 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

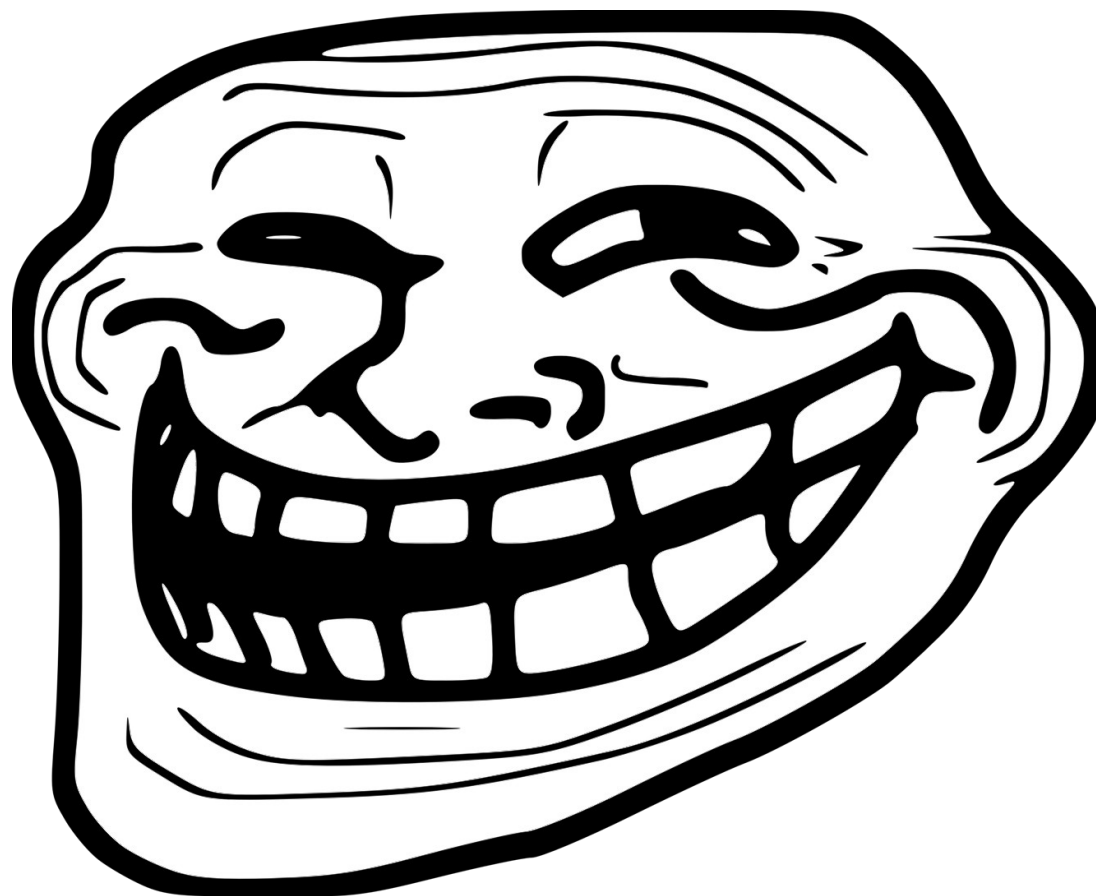
- Нет возможности ограничить Subordinate CA в выдаче сертификатов
- Что делать при недоступности CRL или OCSP?

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 СА?



## **X.509 PKI: проблемы**

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

# Extended Validation Certificates

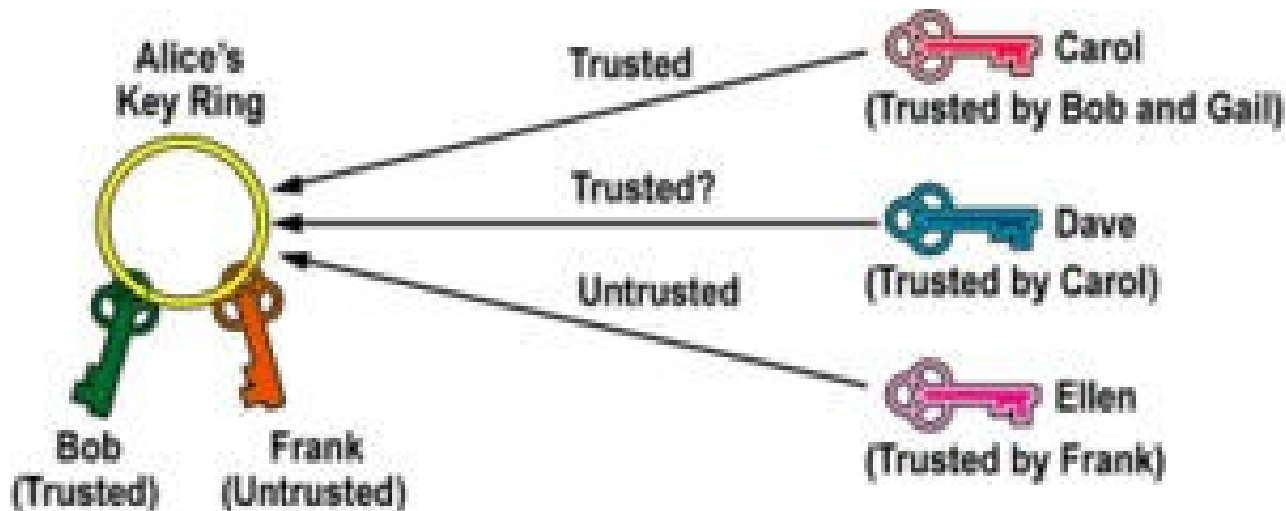




# Pretty Good Privacy (PGP)

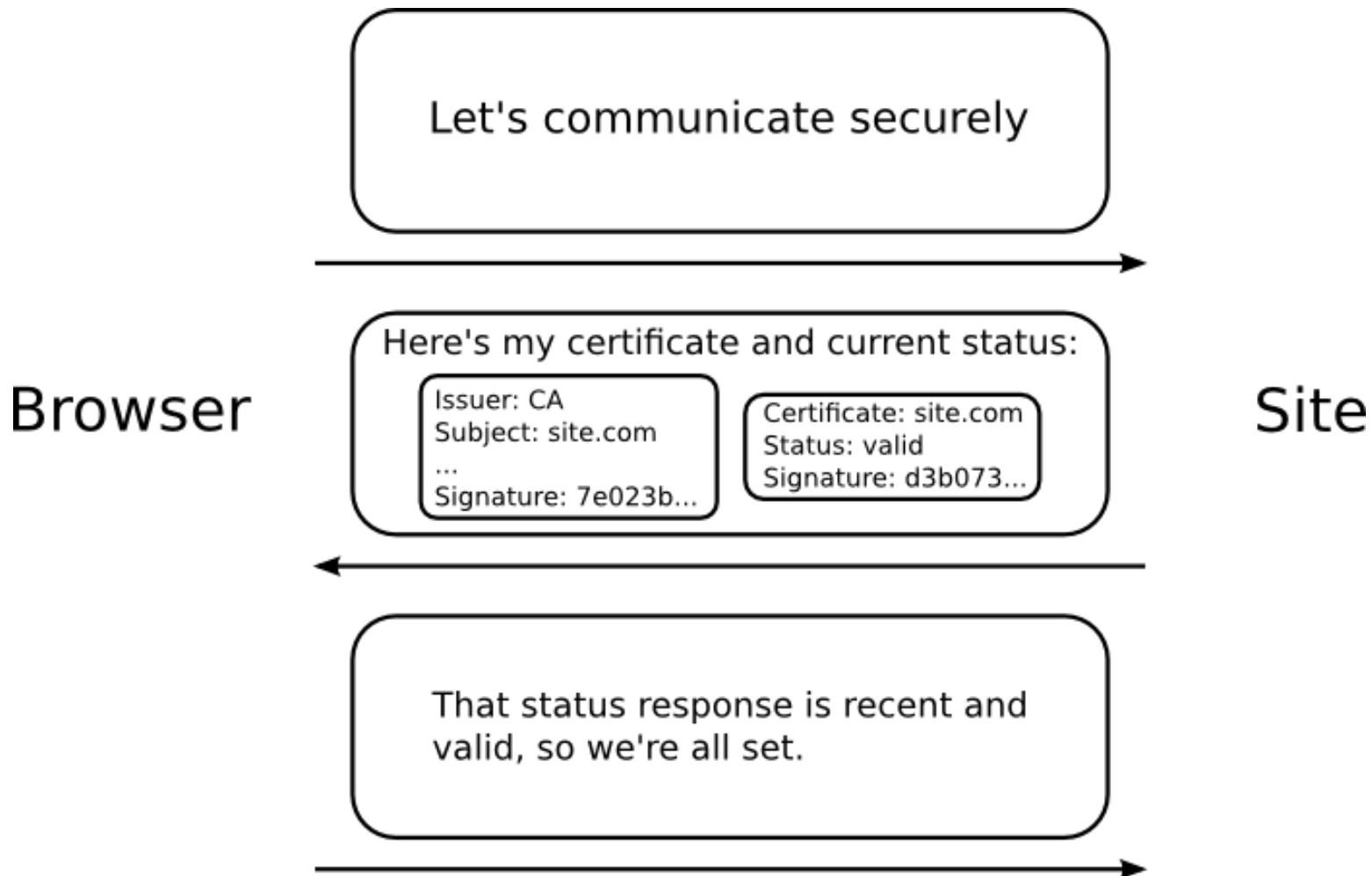
- Филл Циммерман, 1991
- Web of Trust

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



# Расширения PKI

## OCSP stapling



# Расширения PKI

Certificate pinning

Доверие СА, 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/>