

# Криптография

## Лекция 4. Цифровые подписи.

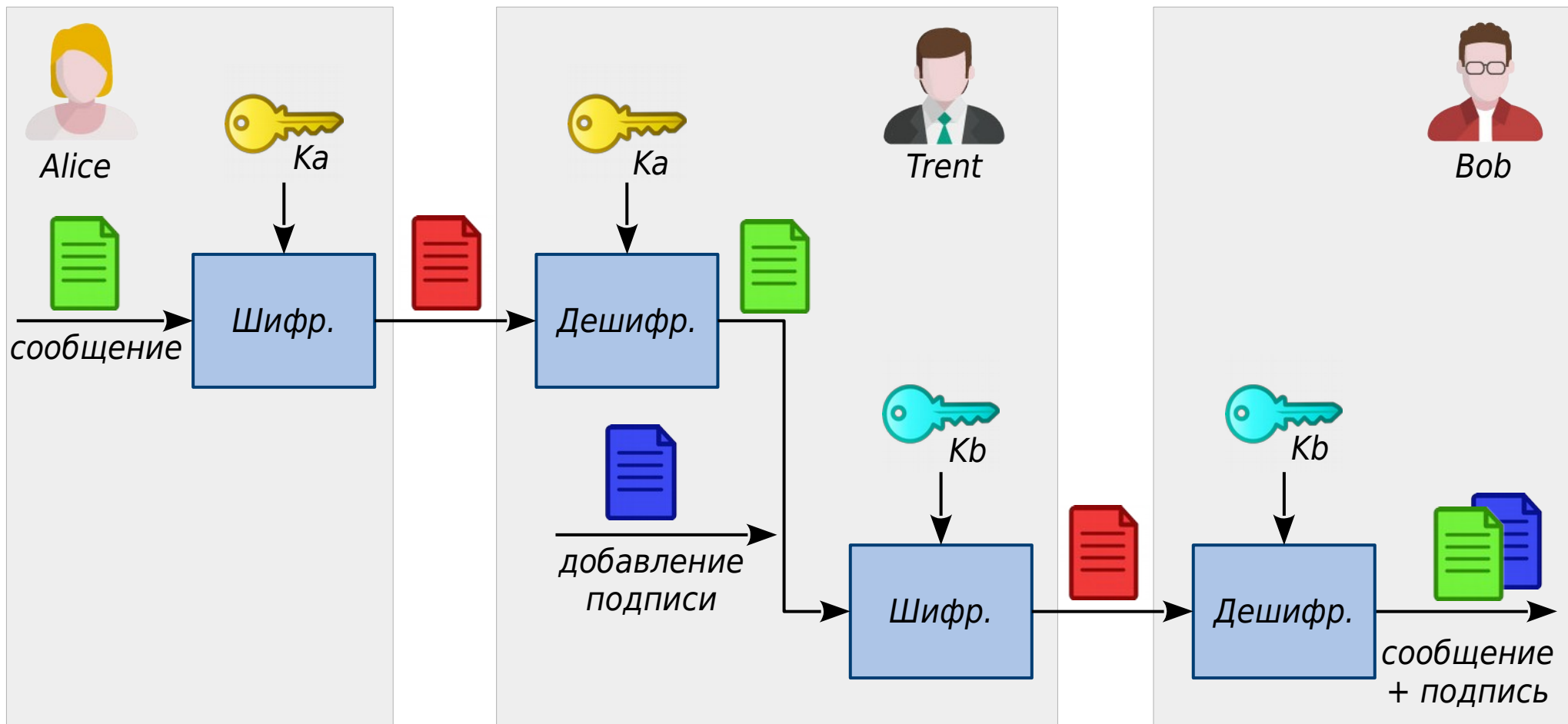
*Дмитрий Яхонтов*

*“Кочерга”, 2018*

# Требования к цифровой подписи

- Подпись удостоверяет автора сообщения именно автор подписи, и никто иной, сознательно подписал документ
- Подписанный документ нельзя изменить любое изменение документа приводит к тому, что подпись становится недействительной
- Подпись нельзя использовать повторно она является частью документа, перенести подпись на другой документ невозможно
- От подписи невозможно отречься автор не может сформировать отказ от своей подписи или утверждать, что подпись создана не им.

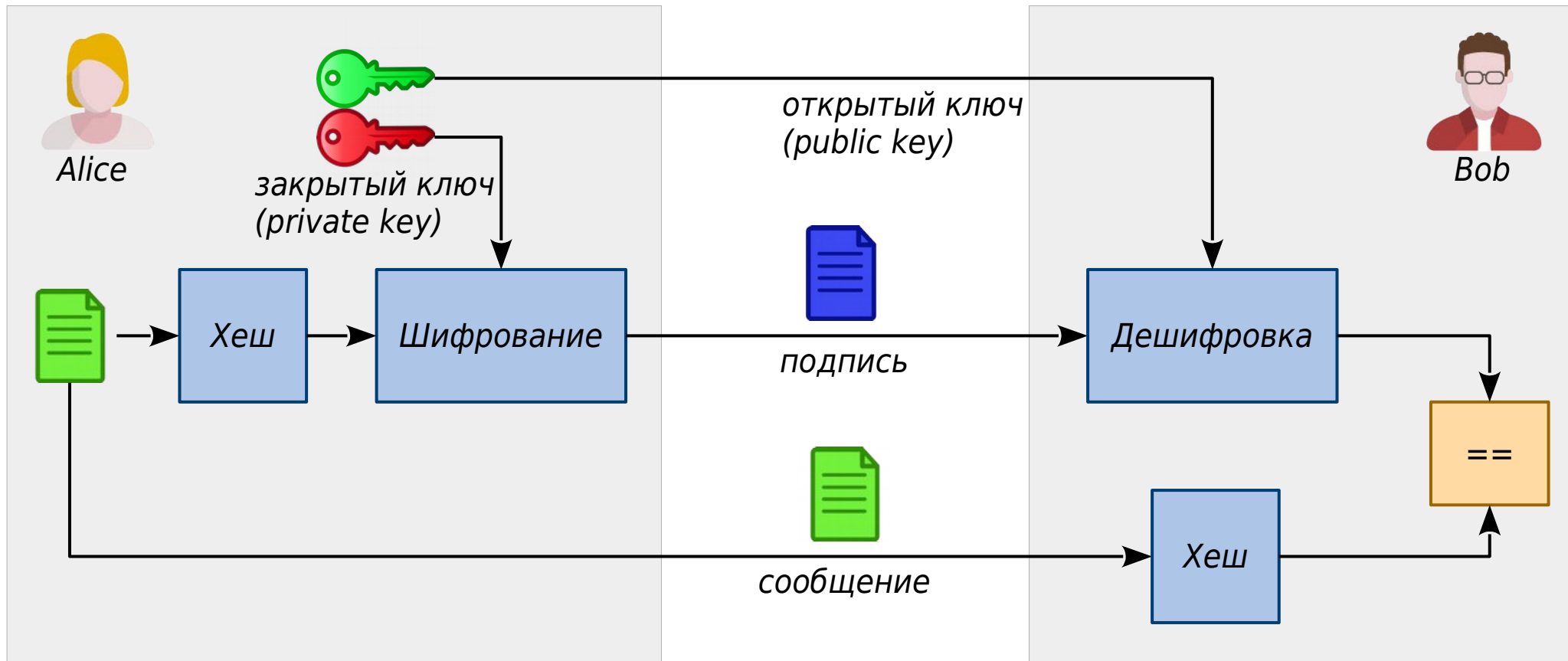
# Симметричная схема (с посредником)



# Недостатки симметричной схемы

- Нужны защищенные каналы для обмена закрытыми ключами между Трентом и каждым из остальных участников
- Если Боб получил от Алисы подписанное сообщение, он может продемонстрировать подпись кому-то еще только через Трента
- Трент должен хранить базу сообщений, либо пересылать Бобу копию зашифрованного сообщения Алисы
- Самое главное:  
необходим Трент — сторона, которой все доверяют

# Асимметричная схема



# Алгоритм DSA (Digital Signature Algorithm)



Alice

открытые простые  $p, q \longrightarrow p, q$

открытое  $g = h^{(p-1)/q} \bmod p \longrightarrow g$

закрытый ключ:  $X < q$

открытый ключ:  $Y = g^x \bmod p \longrightarrow Y$

сообщение  $\longrightarrow$  хеш  $H$

секретное случайное  $K < q$

подпись:

$R = (g^K \bmod p) \bmod q \longrightarrow$

$S = (K^{-1} (H + X \cdot R)) \bmod q \longrightarrow$



Bob

сообщение  $\longrightarrow$  хеш  $H$

проверка подписи:

$U1 = (H \cdot S^{-1}) \bmod q$

$U2 = (R \cdot S^{-1}) \bmod q$

$V = ((g^{U1} \cdot y^{U2}) \bmod p) \bmod q$

если  $V = R$ , то подпись верна

название системы	год	вычислительная задача	примечание
RSA (Rivest-Shamir-Adleman)	1977	разложение на простые множители	
ESIGN (Efficient digital SIGNature)	1985	разложение на простые множители	быстрее, чем RSA
Эль-Гамала (Elgamal)	1985	дискретный логарифм	
Шнорра (Schnorr)	1989	дискретный логарифм	модификация схемы Эль-Гамала
DSA (Digital Signature Algorithm)	1991	дискретный логарифм	
ECDSA (Elliptic Curve Digital Signature Algorithm)	1999	дискретный логарифм на эллиптич. кривых	
ГОСТ Р 34.10-2012	2012	дискретный логарифм на эллиптич. кривых	

# Подсознательный канал (на примере DSA)

- Алиса и Боб выбирают **Z** — закрытый ключ для подсознательного канала
- Алиса подписывает сообщение. Она выбирает случайное число **K** так, чтобы:
  - для передачи 1:  
параметр подписи **R** был квадратичным вычетом по модулю **Z**  
(существует **n** такое, что  $R = n^2 \bmod Z$ )
  - для передачи 0:  
**R** не был квадратичным вычетом по модулю **Z**
- Боб проверяет подпись, а затем восстанавливает переданный бит из параметра **R**, зная **Z**
- Передать несколько бит можно, используя сразу несколько модулей **Z**



# Уничтожение подсознательного канала

- Число **K** должно генерироваться совместно обеими сторонами
- Алиса не должна контролировать ни один бит числа K
- Боб не должен узнать ни один бит числа K
- Боб должен иметь возможность проверить, что для подписи использовалось именно сгенерированное K



*выбирает **k1***

$$\mathbf{u} = g^{k1} \bmod p \longrightarrow \mathbf{u}$$

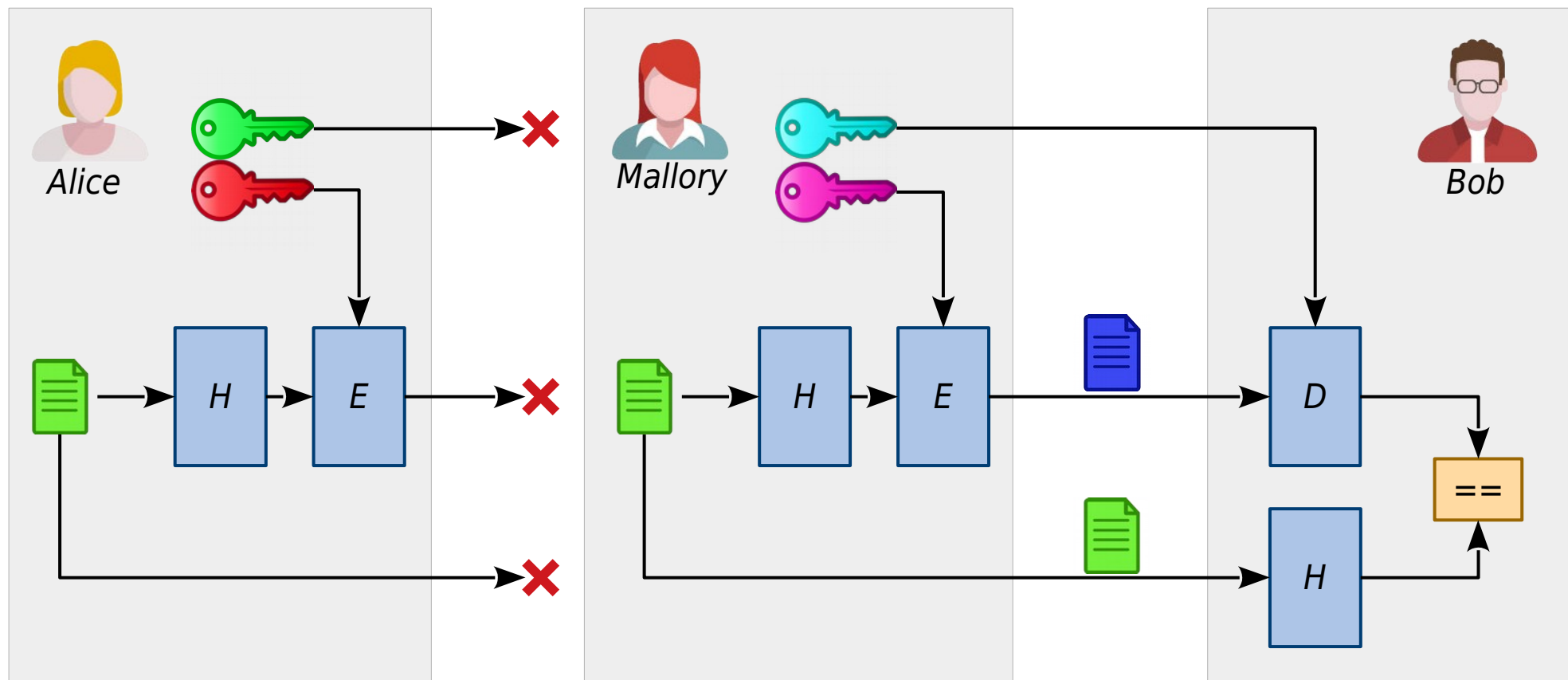
**k2**  $\longleftarrow$  *выбирает **k2***

$$\mathbf{K} = k1 * k2 \bmod (p-1)$$

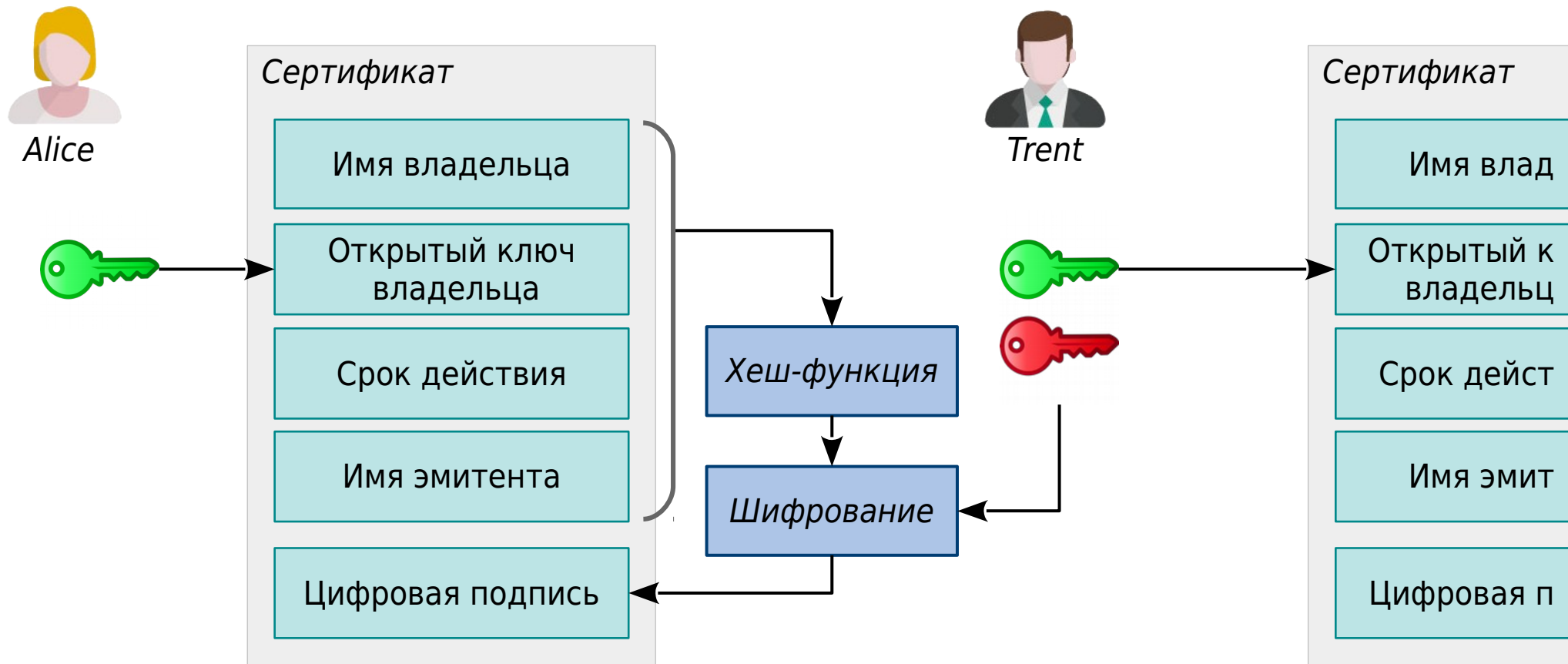


*проверяет, что*  
 $(\mathbf{u}^{k2} \bmod p) \bmod q = \mathbf{R}$

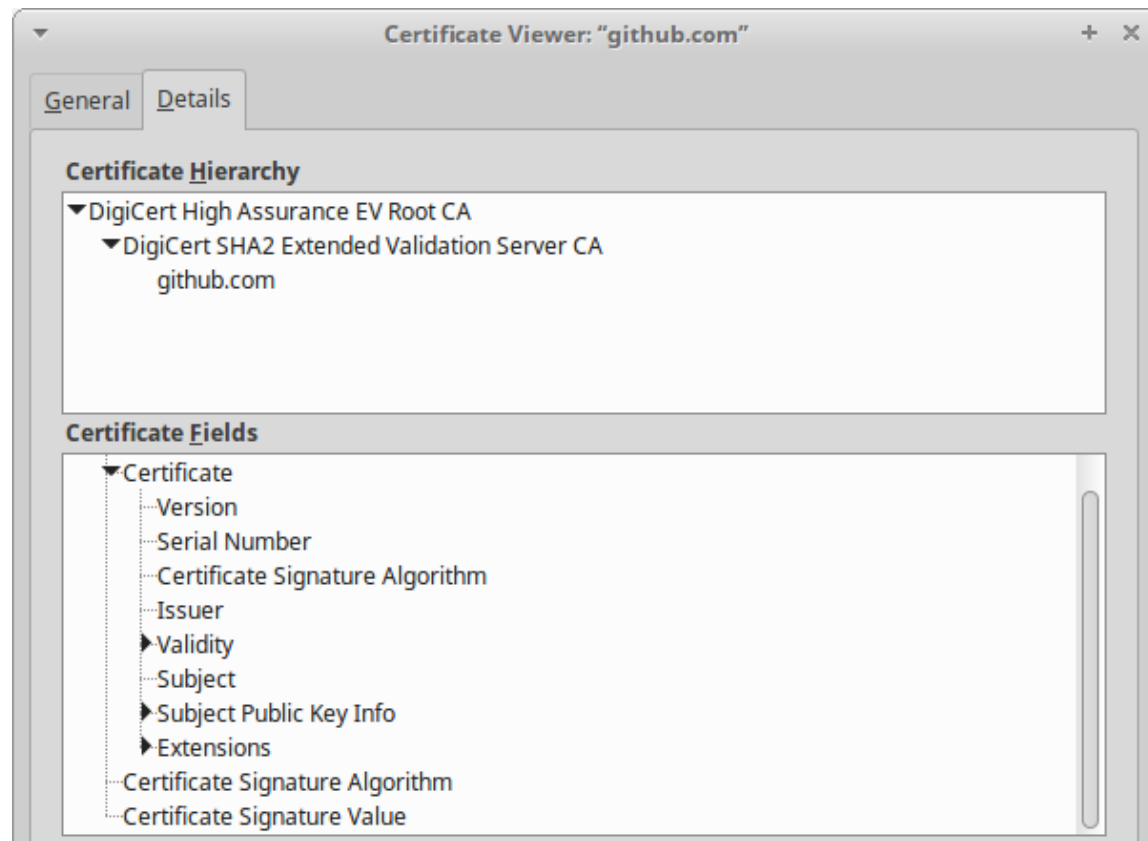
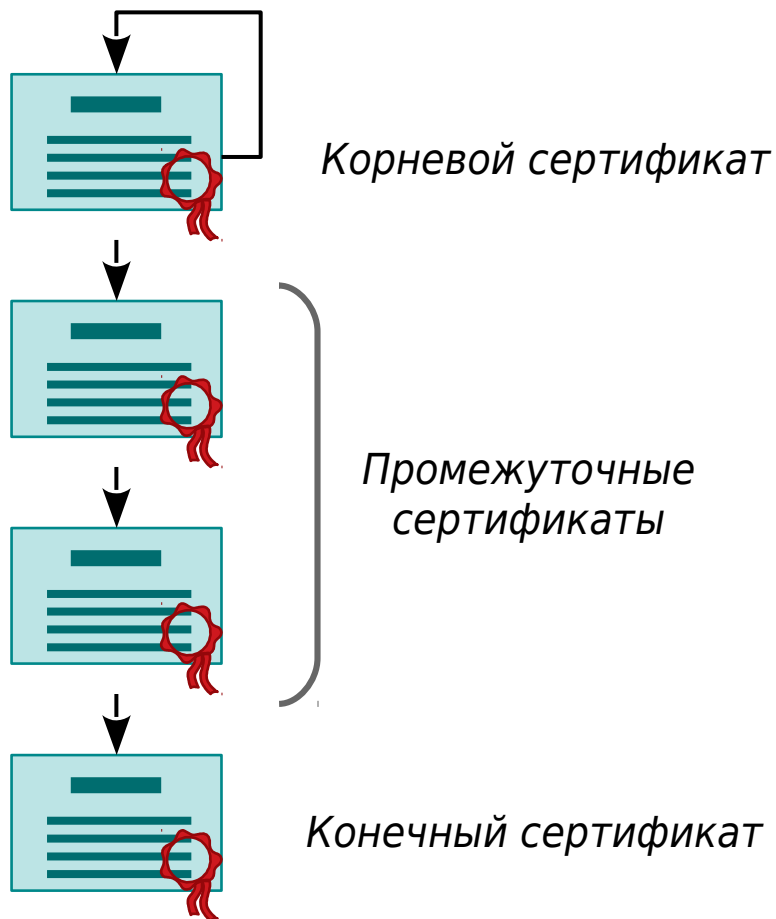
# Атака “человек посередине” (Man-in-the-Middle, MitM)



# Сертификат открытого ключа

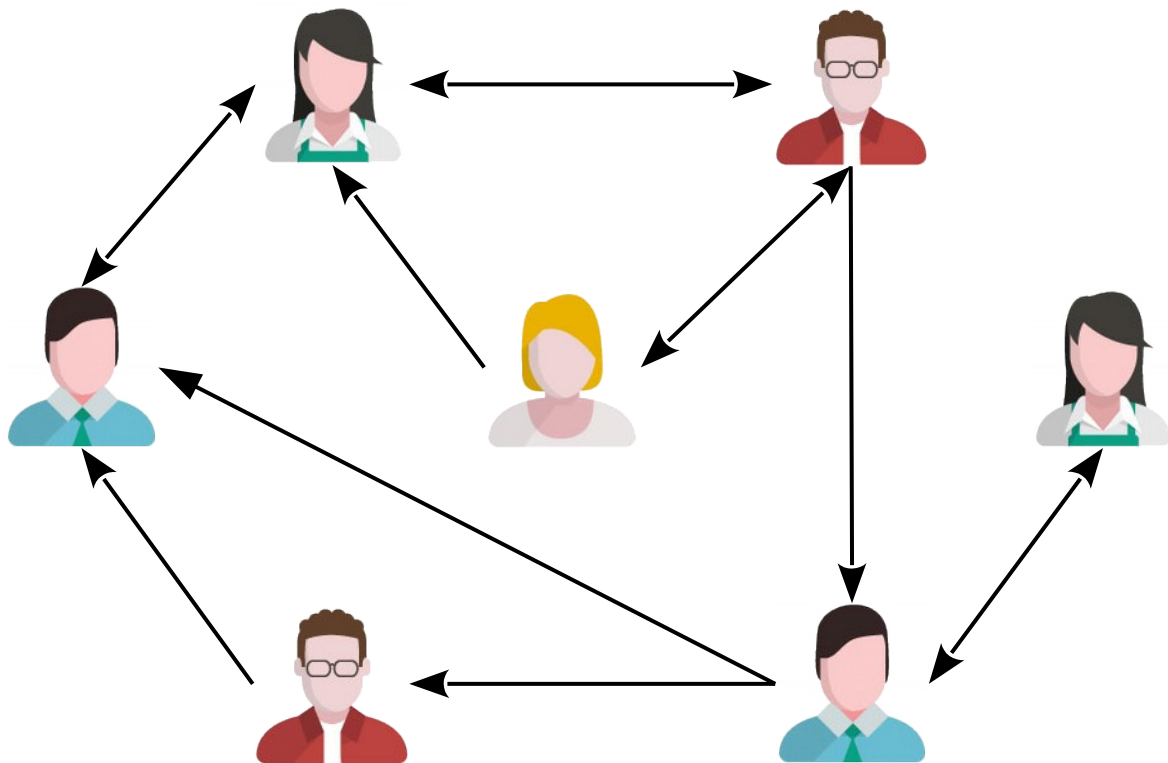


# Цепочка доверия



Пример: цепочка сертификатов в протоколе TLS

# Сеть доверия (Web of Trust, WoT)



- Принадлежность открытого ключа участнику сети удостоверяют другие участники
- Возможны различные уровни доверия:
  1. “Я его знаю”
  2. “Я знаю того, кто его знает”
  3. “Я знаю того, кто знает того, кто его знает” и так далее.



— это не оно :)

# Задача\*

Трент поручил Бобу разработать интерактивный телефонный справочник. Боб написал программу, которая на запрос {имя} отвечает парой {имя, номер\_телефона}, сопровождаемой подписью Трента. Подпись доказывает, что абонент с определенным именем действительно имеет определенный номер телефона.

Помогите Бобу модернизировать программу так, чтобы она дополнительно возвращала доказательство отсутствия в справочнике абонента с определенным именем. Доказательство должно представлять собой структуру данных, подписанную Трентом.

Трент опасается передавать Бобу личный ключ подписи, поэтому все доказательства должны быть созданы Трентом заранее, в момент формирования справочника.

# Ссылки

- Обратная связь:

 [android.ruberoi@gmail.com](mailto:android.ruberoi@gmail.com)

 [@android\\_ruberoi](https://lesswrongru.slack.com)

- Анонсы:

 [facebook.com/kocherga.club](https://facebook.com/kocherga.club)

 [vk.com/kocherga\\_club](https://vk.com/kocherga_club)

 [vk.com/kocherga\\_prog](https://vk.com/kocherga_prog)

- Материалы лекций:

 [github.com/notOcelot/Kocherga\\_crypto](https://github.com/notOcelot/Kocherga_crypto)

- Видео:

 [youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg](https://youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg)

