### Security and privacy in networks

Damien Saucez Inria Sophia Antipolis

Université d'Avignon et des Pays de Vaucluse, CERI - Securité dans les réseaux - November 2017

#### Contact information

- Damien Saucez
  - Email: damien.saucez@inria.fr
  - Mobile: +33 6 95.06.46.11
  - Phone: +33 4 89.73.24.18

#### Table of Content

- 1. Reminders
- 2. Threats by the example
- 3. The basics of security
- 4. Securing communications
- 5. Blockchains
- 6. Privacy
- 7. Overlay networking

#### References

- O. Bonaventure. Computer Networking: Principles, Protocols and Practice. http://inl.info.ucl.ac.be/CNP3.
  - some network slides inspired from this book
- J. Kurose and K. Ross. Computer Networking: A Top-Down Approach, Addison-Wesley, 6th Edition.
- L. Peterson and B. Davie.
   Computer Networks: A Systems Approach.
   Morgan Kaufmann Publishers, 4th Edition.
- A. Tanenbaum, D. Wetherall, Computer Networks, Prentice Hall, 4th Edition
- A. Legout, Peer-to-Peer Applications From BitTorrent to Privacy, Inria
  - some privacy and peer-to-peer slides inspired from this course
- J. Kehrli, The Blockchain The Technology behind Bitcoin, https://www.slideshare.net/ JrmeKehrli/the-blockchain-the-technology-behind-bitcoin, November 2017
  - some blockchain slides inspired from this presentation

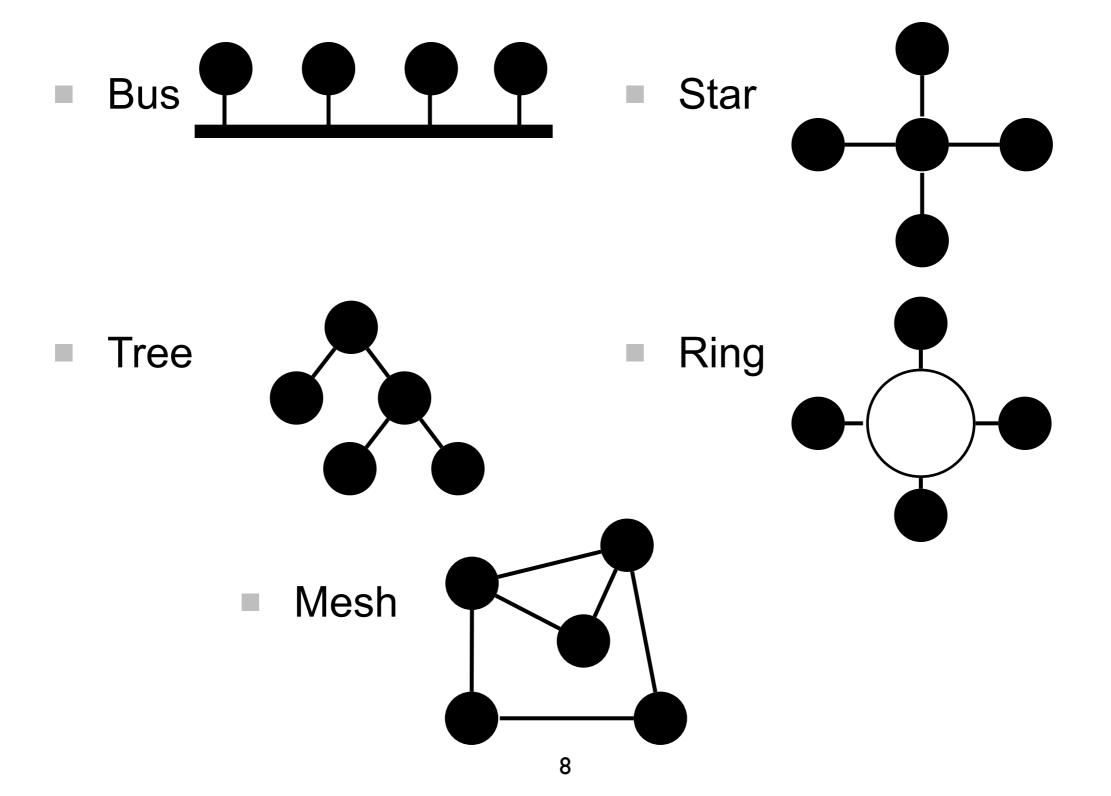
#### Reminders

#### Generalities

#### Network

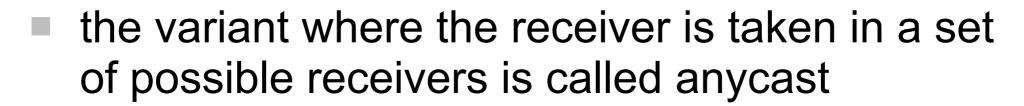
- Network:
  - set of nodes (e.g., hosts, routers) exchanging information and interconnected with links
- Communication rules in a network are specified by a set of protocols (e.g., IEEE 802.3, IP, OSPF, BGP)
- Example of networks:
  - Telephone System
  - Mobile network
  - Television, radio
  - Internet, LAN

### Network topologies

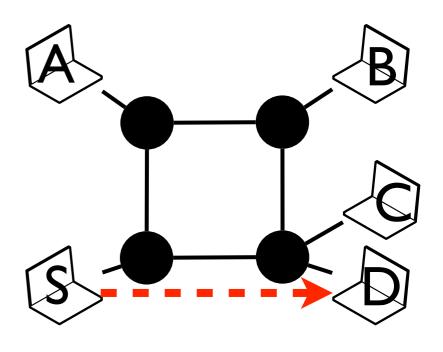


#### Transmission modes

- Unicast (Point-to-Point)
  - one sender
  - one receiver
  - example: telephone



anycast helps scalability



# Transmission modes (cont.)

- Multicast (Point-to-Multipoint)
  - one sender
  - a group of receivers
  - every member of the group receives the same information
  - example: videoconference
  - when the information is sent to every node, the term broadcast is used (e.g., Terrestrial television)

### Digital networking communications modes

- Circuit switching
  - before transmitting information, a dedicated circuit is established from the source to the destination nodes
  - the information is transmitted through its dedicated circuit that guarantees the bandwidth during the whole communication
  - each intermediate node knows how to forward information received on circuits crossing itself
  - example: 19<sup>th</sup> century telephone system

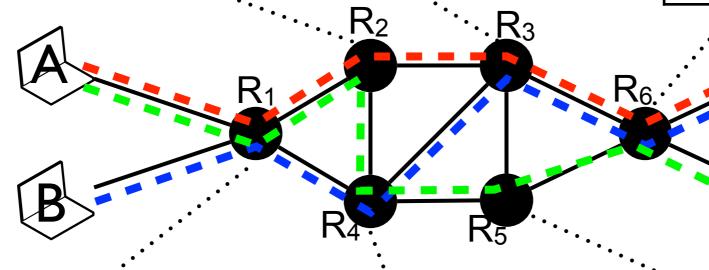


## Circuit switching example

Send to
E
S

Circuit	Send to
Red	SE
Blue	SE

Circuit	Send to
Red	NE
Green	SE
Blue	NE



Circuit	Send to
Red	NE
Green	NE
Blue	SE

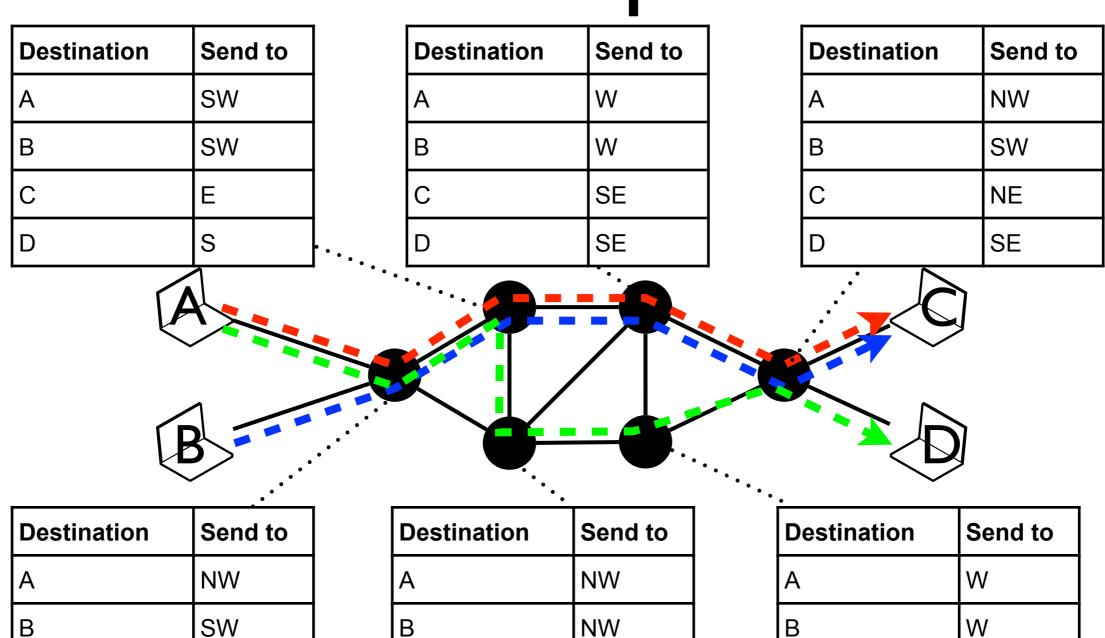
Circuit	Send to
Green	E
Blue	NE

Circuit	Send to
Green	NE

### Digital networking communications modes (cont.)

- Packet switching
  - data is divided in packets of information containing
    - a piece of data
    - the address of the source node
    - the address of the destination node
  - packets are transmitted on the network independently of each others
  - each intermediate node knows how to forward information to each destination
  - example: IP, Internet

### Packet switching example



Ε

Ε

C

D

NE

NE

NE

NE

D

### Layered model

- Network systems are complex
  - dividing the functionality helps reasoning on them
- Divide network functionalities into layers
  - Layer i provides services to layer i+1
  - Layer i relies on services provided by layer i-1

### Layers

**Application** 

Exchange of useful information (Service Data Unit) between applications relying on the transport layer hiding the network complexity (e.g., HTTP)

**Transport** 

Provide a service to (reliably) exchange data between hosts with segments (e.g., TCP, UDP)

**Network** 

Provide a service to exchange packets of information between hosts that can be arbitrarily distant (e.g., IP)

**Datalink** 

Provide a service to exchange structured group of bits called frames (e.g., Ethernet)

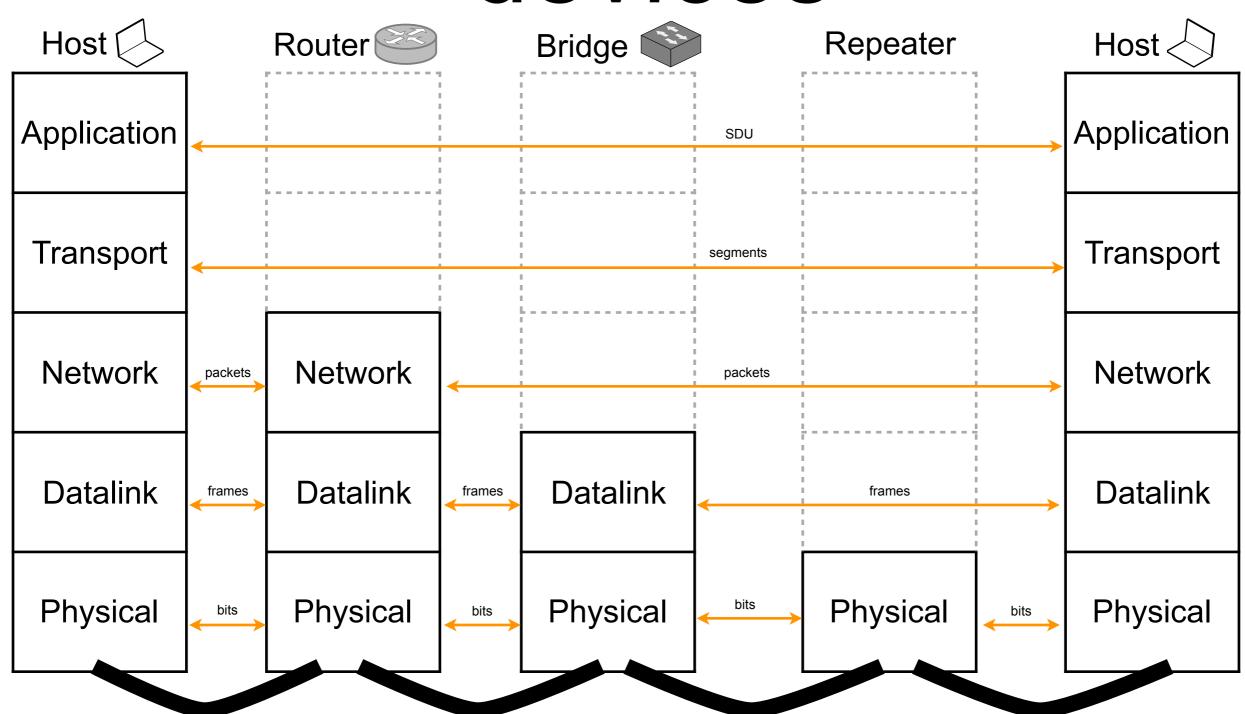
Physical

Transmit bits between two physically connected devices (e.g., Manchester)

Physical

transmission medium (e.g., UTP)

### Layer of networking devices



#### Middleboxes

- The original TCP/IP architecture is only composed of hosts and routers
- Modern networks contain devices that
  - process (e.g., proxies)
  - analyze (e.g., firewall)
  - modify (e.g., NAT)
- Middleboxes can work at any layer or even be cross layer

### Middleboxes are everywhere

In enterprise networks [SHC+12]

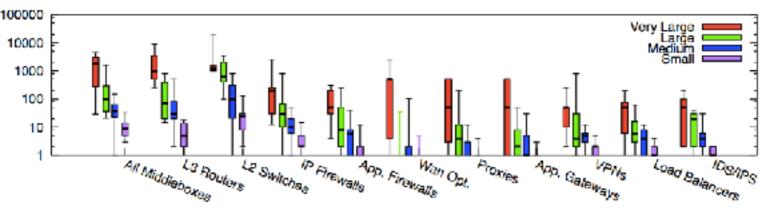


Figure 1: Box plot of middlebox deployments for small (fewer than 1k hosts), medium (1k-10k hosts), large (10k-100k hosts), and very large (more than 100k hosts) enterprise networks. Y-axis is in log scale.

- In ISP networks [HRN+11]
  - very likely that your packet will be touched by a middlebox before reaching its destination
- Middleboxes limit deployment of new protocols in the Internet
- Middleboxes can be used against user interests

# Naming and addressing

### Name and addresses in the Internet

- DNS Names identify hosts
- IP addresses uniquely identify host interfaces

```
nslookup example.com
Server: 138.96.0.10
Address: 138.96.0.10#53

Non-authoritative answer:
Name: example.com
Address: 192.0.43.10
```

Ethernet address identifies network adapters in a collision domain

```
arp -na
? (138.96.192.3) at 0:50:56:88:0:0 on en1 ifscope [ethernet]
? (138.96.192.250) at 0:1e:4a:e0:9e:0 on en1 ifscope [ethernet]
? (138.96.193.164) at 0:23:df:aa:cc:4c on en1 ifscope
[ethernet]
...
```

Names and addresses may be hierarchically organized

## Hierarchical naming/addressing

- Objectives: ensure uniqueness of names/addresses and provide naming/addressing scalability
- Flat: probe all the other naming/addressing authorities before choosing a name/address
  - doesn't scale
  - not robust to network partition
- Hierarchy: carve up set of possible names/address (i.e., the name/address space) into mutually exclusive portions

#### Addressing in Ethernet

- Objective: determine the origin and destination of a frame within a collision domain
- Every Ethernet network adapter is assigned a unique datalink layer address encoded on 48 bits
- Every frame is transmitted to all network adapters of the collision domain
  - but only the network adapter with the address corresponding to the destination address of the frame accepts it

### Addressing in IP

- Objective: determine the origin and destination of a packet in the Internet
- Every host interface has its own IP address
  - routers have multiple interfaces, each with its own IP address
  - the IP address determines the topological position of the interface
- Current version of IP is version 4 (IPv4)
  - addresses are encoded on 32 bits, fixed length
- 4 billions addresses were a lot... in 1981, but today it becomes too short for 1 billion hosts [ISC]
- IP version 6 (IPv6) starts to be deployed
  - addresses are encoded on 128 bits, fixed length\*

#### IP address structure

- Addresses are separated in two parts
  - network number: identifies the network the address belongs to
  - local address: identifies the interface of the host in the network
    - all bits = 0: network address
    - all bits = 1: broadcast address
- Addresses are aggregated according to the network number
  - routing and packet forwarding are based on the network number only, the local address is ignored

### IP address example

- IP: 192.0.2.1
  - I 10000000 00000000 00000010 00000001
- Subnet: 255.255.255.0

### IP address example

IP: 192.0.2.1

What part is for hosts? what part is for the network?

IP: 11000000 00000000 00000010 00000001

IP: 11000000 00000000 00000010 00000001

IP: 11000000 00000000 00000010 00000001

11000000 00000000 0000010 00000000

network hosts

## Classless InterDomain Routing (CIDR)

- No predetermined separation position between network number and local address with CIDR
  - number of bits allocated for the network number may vary from 0 to 32 bits
  - the address contains no information about the separation position
  - Routers determine the network number by using longestprefix matching
- Notation a.b.c.d/n
  - a.b.c.d is the address
  - n is the number of bits assigned to the network number

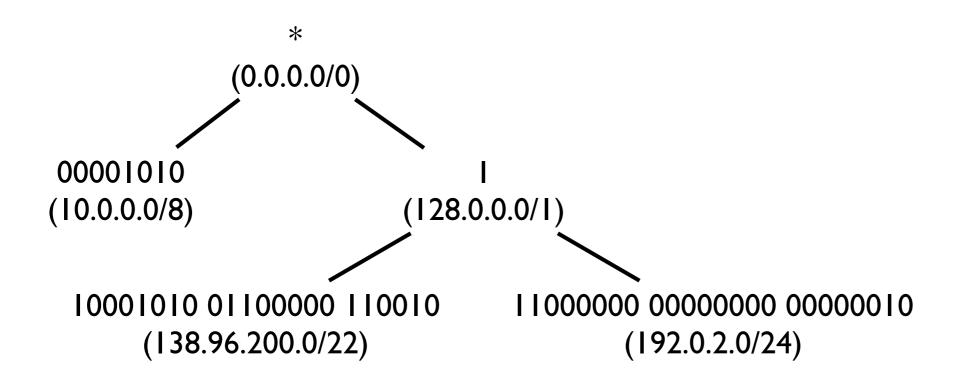
### CIDR (cont.)

- An address matches a route if both share the same prefix
  - 0.0.0.0/0 is the default route matched by every addresses
- With CIDR, an address can match several routes
  - 192.0.2.1 matches 128.0.0.0/1, but also 192.0.2.0/24 or 0.0.0.0/0
- Longest prefix matching is used to determine the route that has the longest prefix in common with the address
- Typically implemented with a trie

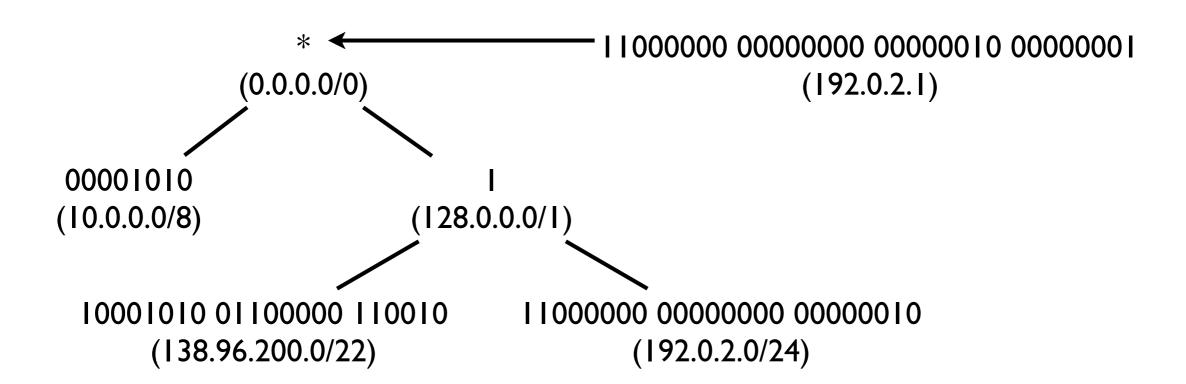
### Longest prefix matching with a trie

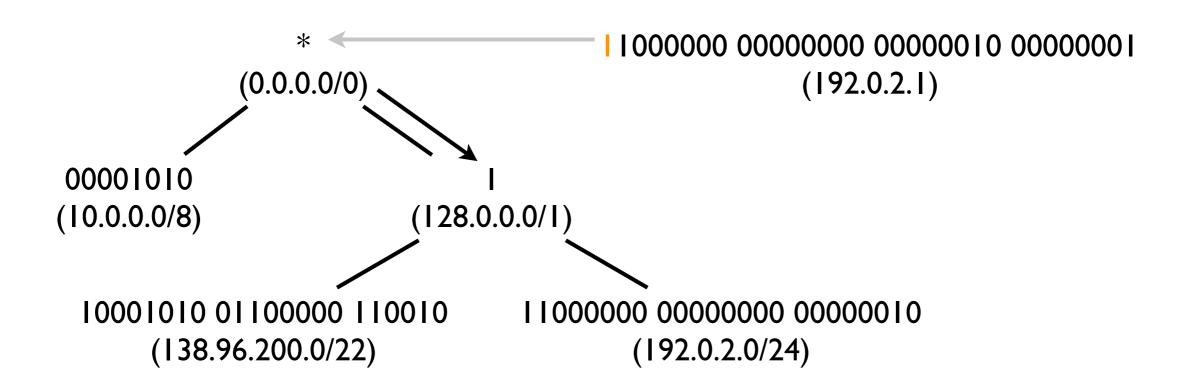
- Routes are inserted in a trie, route prefixes being node keys
- The key of a node is a prefix of the key of all of its children, recursively;
  - siblings cannot be prefixes
- The binary tree is descended, starting from the root, following the children with the key that is a prefix of the address to match
- The descend ends when no children has a key prefixing the address to match
  - the route corresponding to the node where the descent stopped it the best matching route

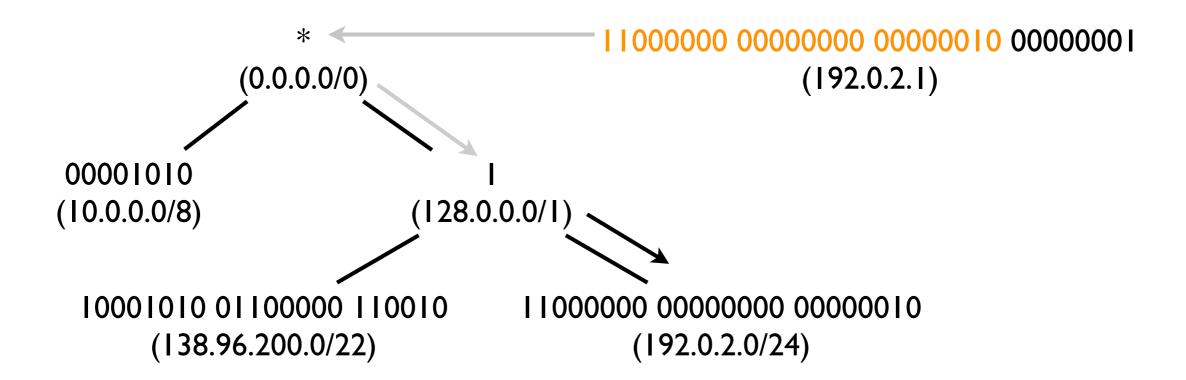
### Longest prefix matching with a trie (examples)

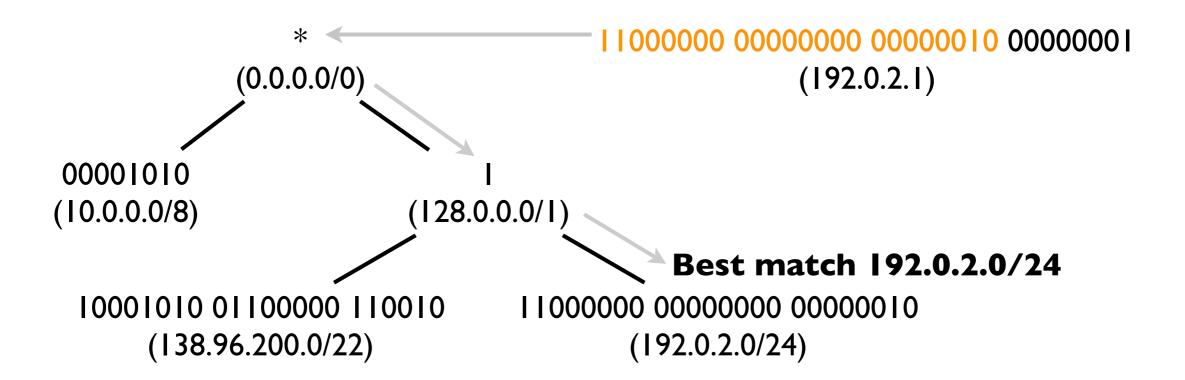


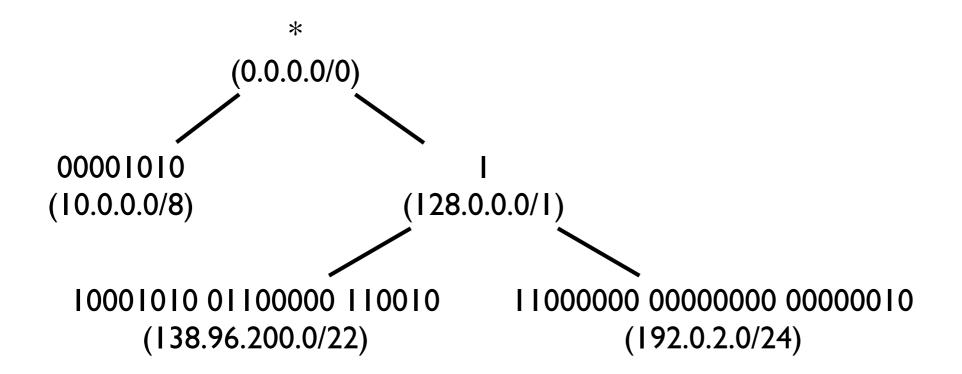
### Longest prefix matching with a trie (examples)

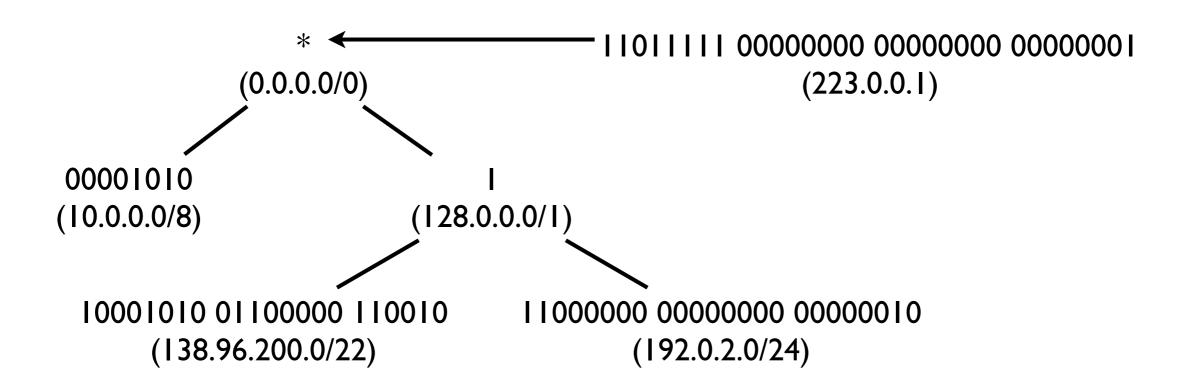


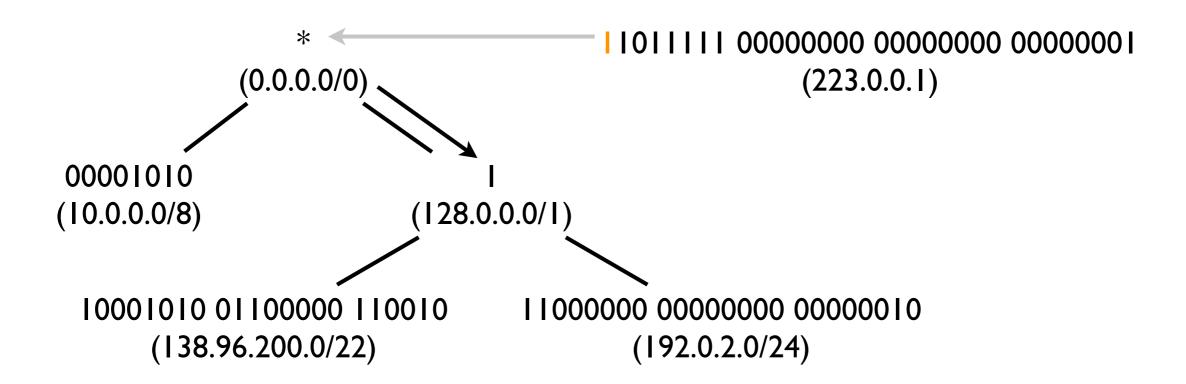


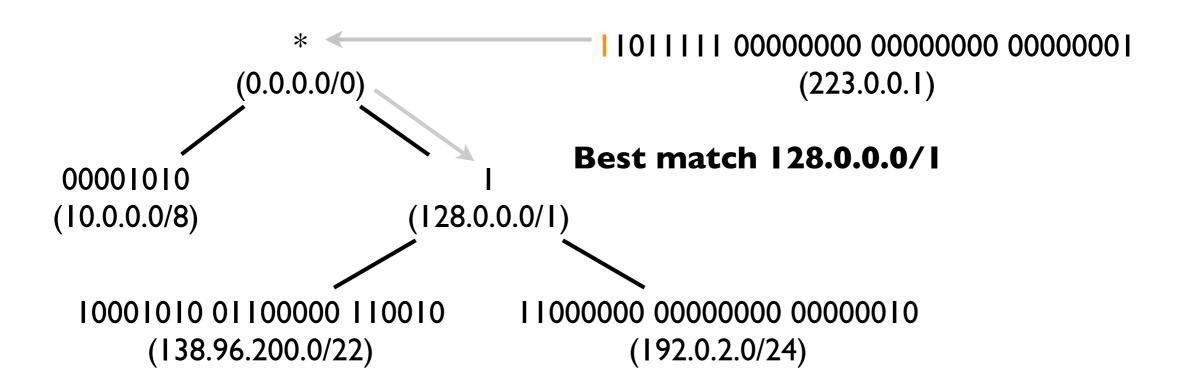












#### IP to Ethernet Address

- To put an IP packet over an Ethernet frame, its IP addresses must be resolved into Ethernet addresses
- Protocol used:
  - Address Resolution Protocol (ARP) in IPv4
  - Neighbor Discovery Protocol (NDP) in IPv6

#### ARP

- ARP is used to get datalink layer address of a machine on the local subnet
- Broadcast an ARP request frame on the local subnet for the IP address to resolve
  - destination address: FF:FF:FF:FF:FF (broadcast)
  - source address: Ethernet address of the network adapter that issued the ARP request
- The host (or a proxy) that owns the address replies with an ARP response frame
  - destination address: Ethernet address of the requester's network adapter
  - source address: Ethernet address of the address's owner's (or proxy) network adapter
- Every network device is required to listen for ARP requests and replies on its network adapters
- Optimizations
  - replies are stored in an ARP cache to avoid that every single packet results in ARP request/ response
    - cached for a limited duration as host can change their IP address
  - ARP request message contains the IP address of the origin of the frame
    - destination (or any hosts in the local subnet) can learn the IP/Ethernet mapping for free

IP: 192.0.2.5

Ethernet: a

IP: 192.0.2.2

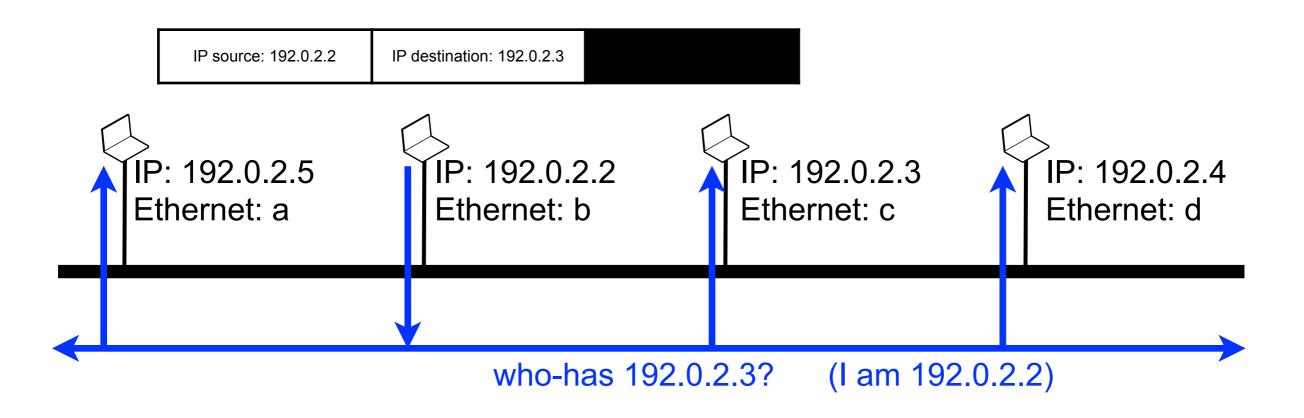
Ethernet: b

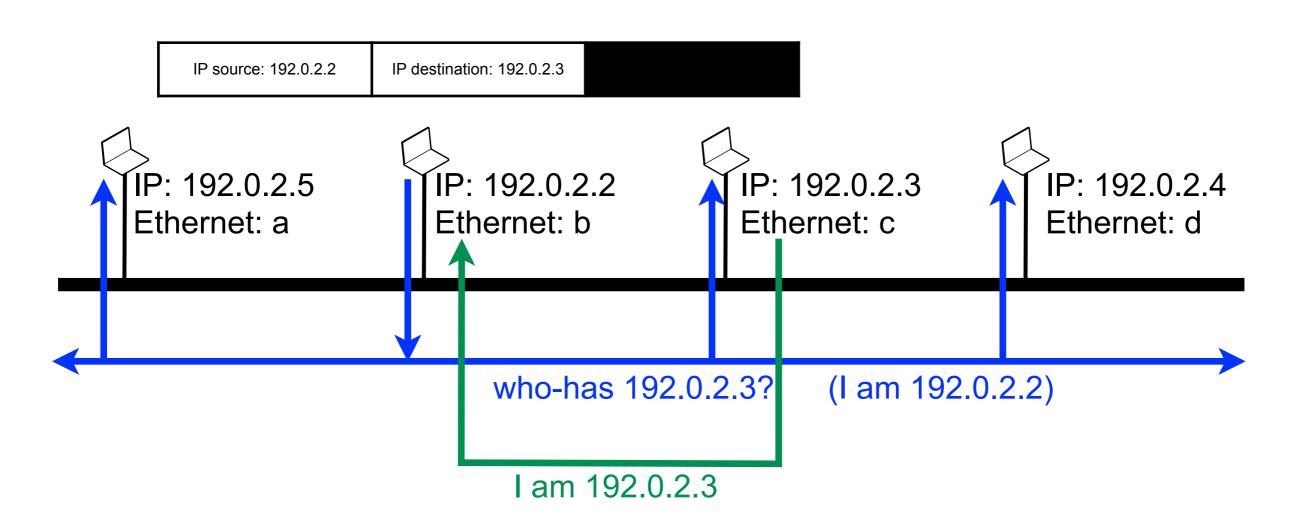
IP: 192.0.2.3

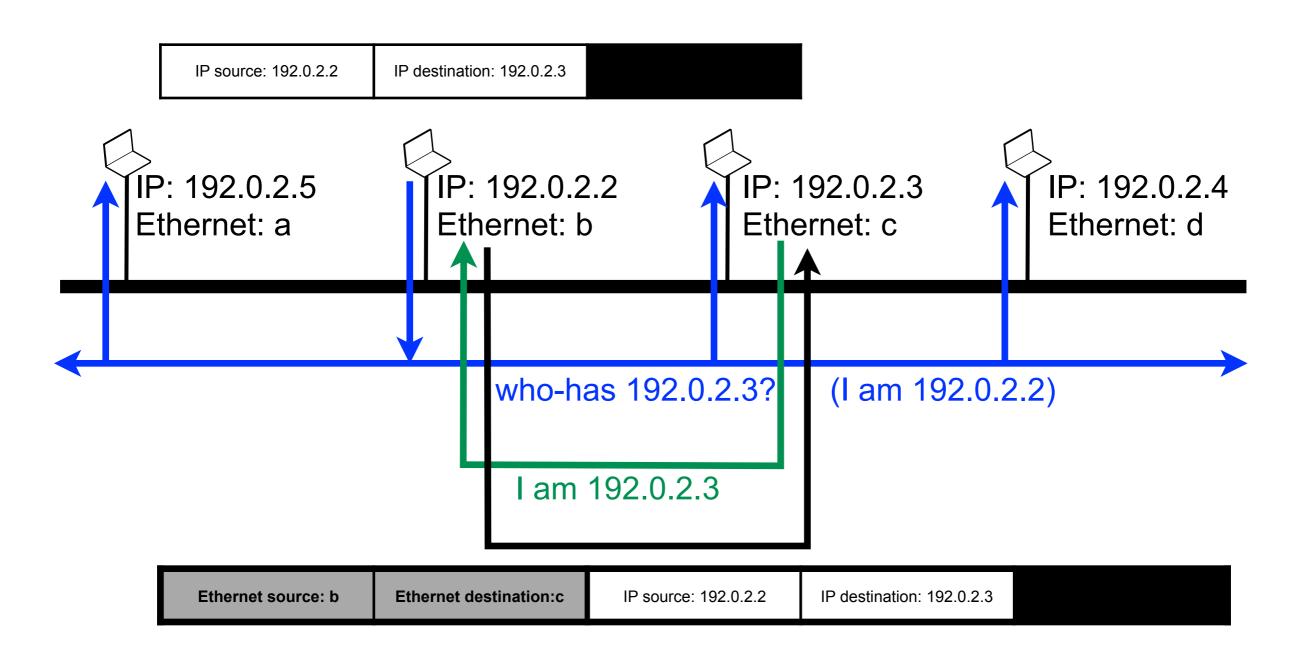
Ethernet: c

IP: 192.0.2.4

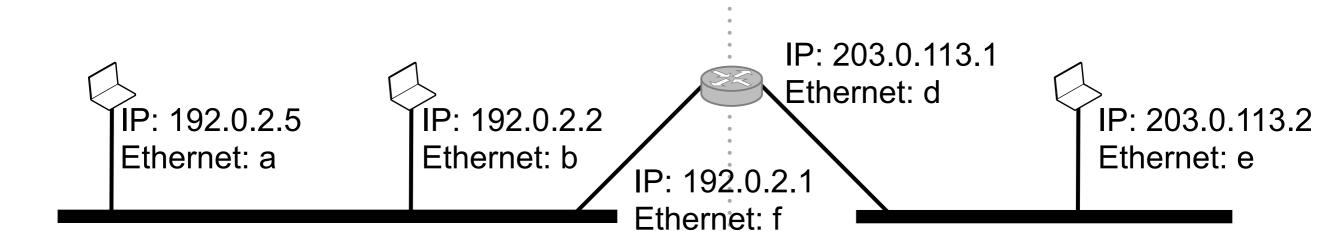
Ethernet: d





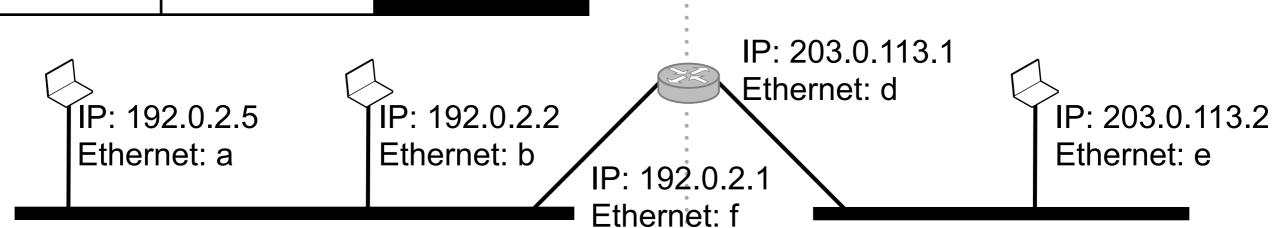


gateway: 192.0.2.1/24 gateway: 203.0.113.1/24



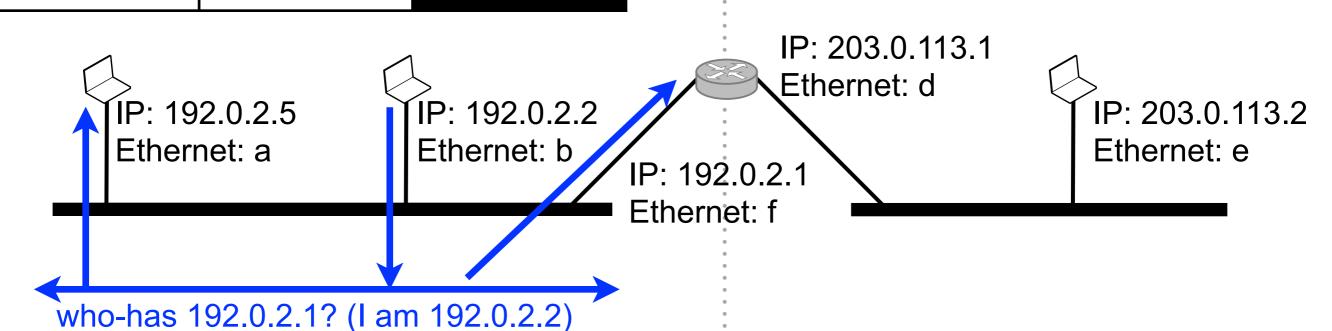
gateway: 192.0.2.1/24 gateway: 203.0.113.1/24

IP source: 192.0.2.2



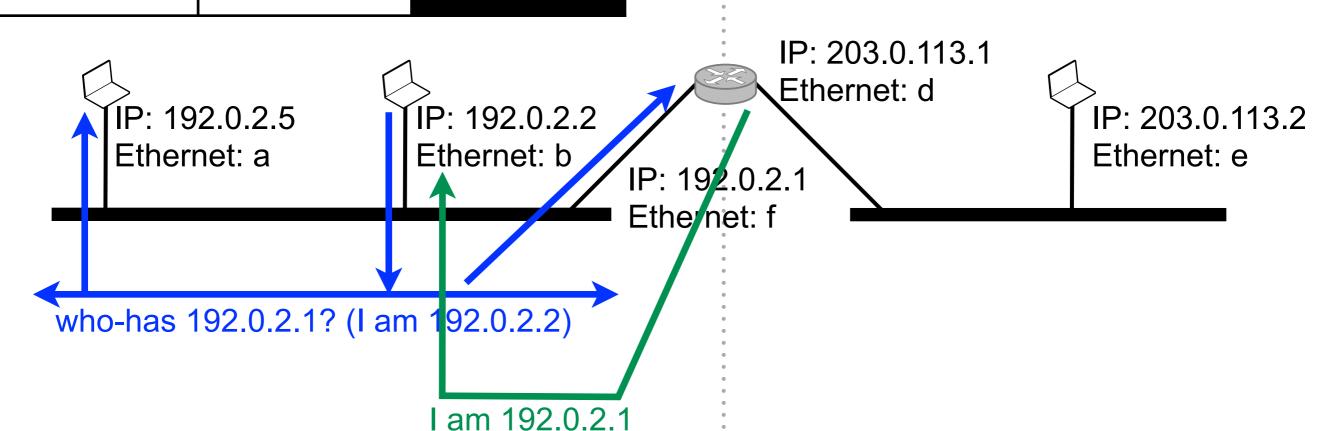
gateway: 192.0.2.1/24 gateway: 203.0.113.1/24

IP source: 192.0.2.2



gateway: 192.0.2.1/24 gateway: 203.0.113.1/24

IP source: 192.0.2.2



gateway: 203.0.113.1/24 gateway: 192.0.2.1/24 IP source: 192.0.2.2 IP destination: 203.0.113.2 IP: 203.0.113.1 Ethernet: d ÎP: 192.0.2.2 ÎP: 192.0.2.5 IP: 203.0.113.2 Ethernet: a Ethernet: b Ethernet: e Ethernet: f who-has 192.0.2.1? (I am 192.0.2.2) am 192.0.2

**Ethernet source: b** 

Ethernet destination:f

IP source: 192.0.2.2

gateway: 203.0.113.1/24

who-has 203.0.113.2? (I am 203.0.113.1)

IP: 192.0.2.5
Ethernet: a

IP: 203.0.113.1
Ethernet: d
IP: 203.0.113.2
Ethernet: b
IP: 192.0.2.1
Ethernet: f

Ethernet source: b

**Ethernet destination:f** 

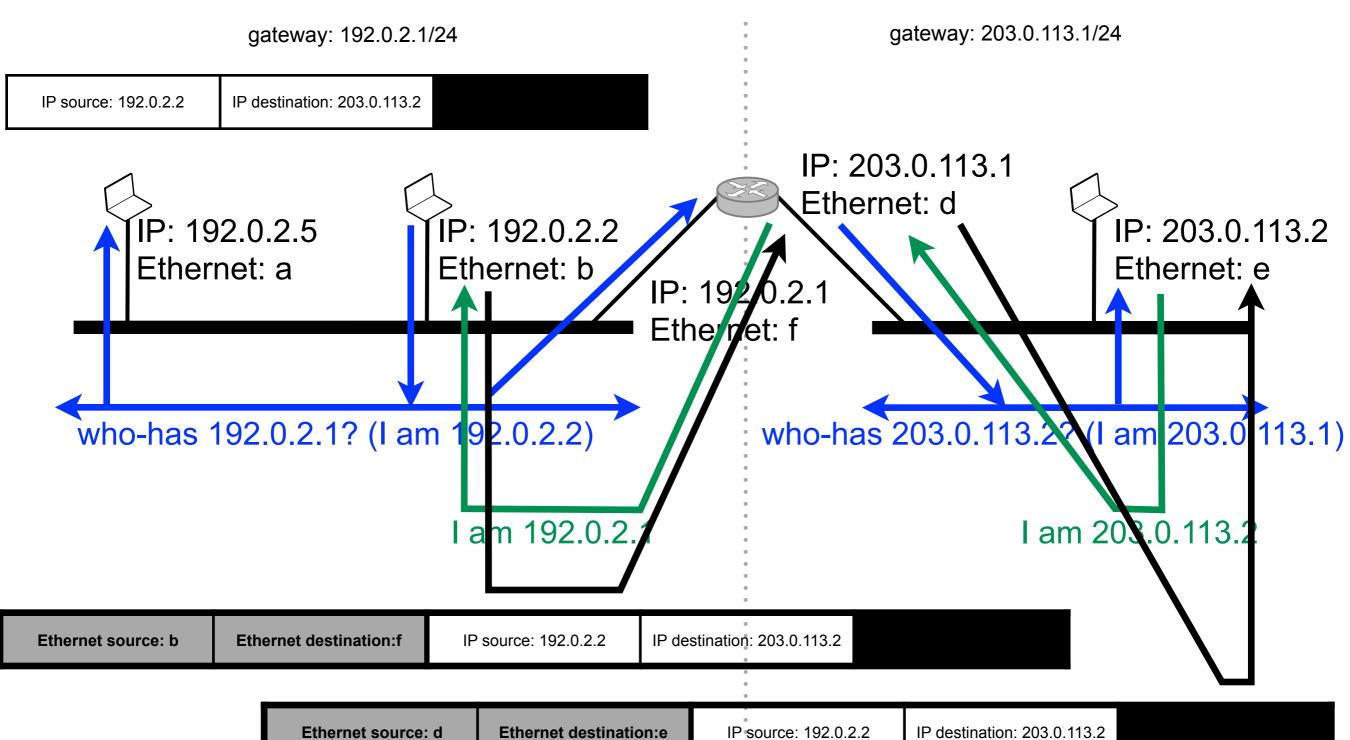
who-has 192.0.2.1? (I am 192.0.2.2)

gateway: 192.0.2.1/24

IP source: 192.0.2.2

am 192.0.2

gateway: 203.0.113.1/24 gateway: 192.0.2.1/24 IP source: 192.0.2.2 IP destination: 203.0.113.2 IP: 203.0.113.1 Ethernet: d ÎP: 192.0.2.2 IP: 192.0.2.5 IP: 203.0.113.2 Ethernet: a Ethernet: b Ethernet: e Ethe net: f who-has 203.0.113.27 (I am 203.0.113.1) who-has 192.0.2.1? (I am 192.0.2.2) am 192.0.2 I am 203.0.113.2 IP destination: 203.0.113.2 Ethernet source: b Ethernet destination:f IP source: 192.0.2.2



35

# Dynamic address configuration

- Allow a set of hosts to share a pool of IP address
- Two approaches
  - stateless auto-configuration
    - no infrastructure necessary
  - Dynamic Host Configuration Protocol (DHCP)
    - hosts query a DHCP server to obtain their configuration
- Advantages
  - less address wastage: a host can use the address of another hosts when it is not connected
  - improves flexibility and reduces the risk of configuration error as no manual operation is necessary

## Stateless autoconfiguration

- When a host connects to the network:
- 1. The host choses an address randomly in 169.254/16 (not globally routable)
- 2. Sends an ARP request for the chosen address
- 3. If an ARP reply is received (another host already uses the address
  - restart from point 1
- 4. Otherwise, the address the address is not used by another host and the host can use it safely
- Auto-configuration is used only for communications within the same network
  - In IPv6, hosts can auto-configure their globally routable addresses and discover network services (e.g., routers, DNS...)

#### Dynamic Host Configuration Protocol (DHCP)

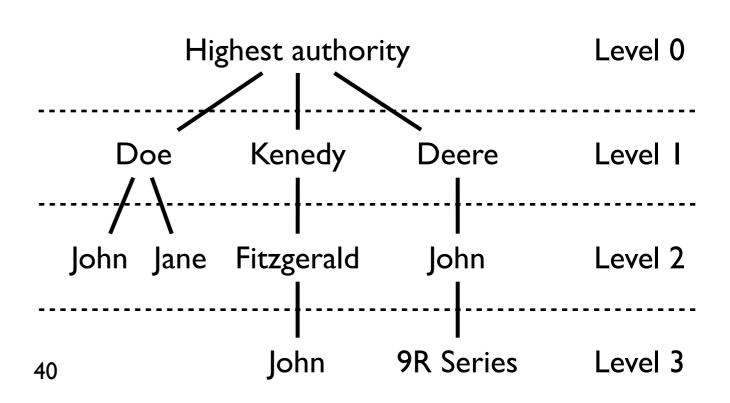
- When a host connects to the network, it broadcasts a DHCP discovery datagram
- Any DHCP server that receives such a message replies with a DHCP offer datagram that contains an offer of IP address
- The host picks one offer and broadcasts a DHCP request message to announce the offers it selected
- The selected DHCP server assigns the address to the host and sends it back a DHCP acknowledgment that confirms the lease of the address and give additional parameters such as the lease time, the IP address of the default gateway, or the IP address of the DNS servers
  - when the lease time is elapsed, the address is released and made available for other hosts
- The other DHCP servers withdraw their offers

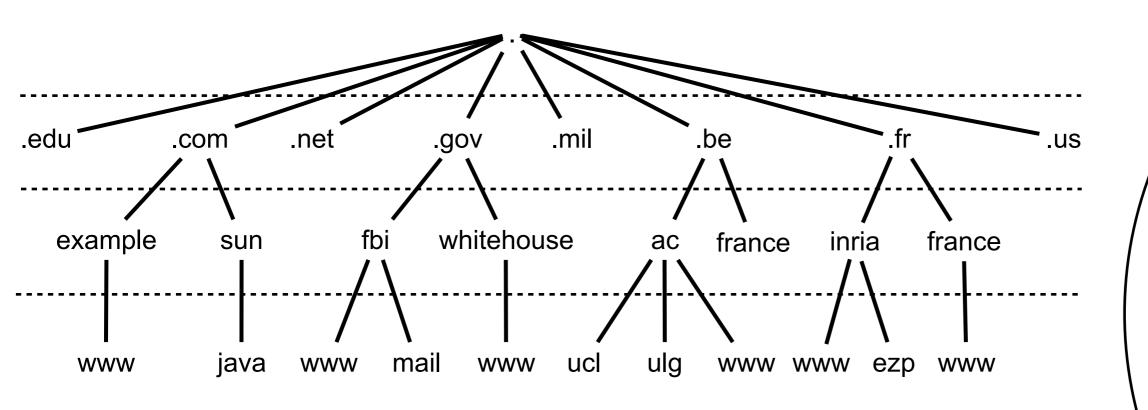
### Naming

- Objective: provide a mean for human to easily identify (and remember) hosts
- Hosts receive textual names easy to remember but long and of variable size (e.g., goo.gl, www.example.org, 3.14159265358979323846264338327950288419716939937510582 0974944592.com...)
  - wastes space to carry them in packet headers
  - hard to parse
- Address are shorter and easy to process by hosts
- Indirection
  - multiple names may point to the same address
  - upon address change, only the resolution table has to be updated

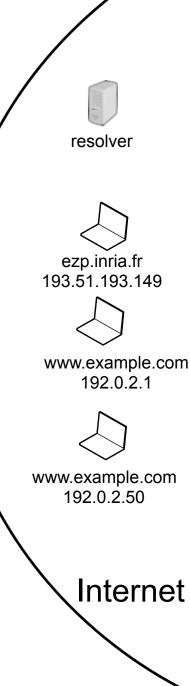
#### Hierarchical naming

- Simplifies distributed naming/addressing
  - level i deals only with level i+1
- Global uniqueness is guaranteed
  - level i ensures uniqueness at level i+1
- Scales arbitrarily
  - level i+1 does not influence level i-1

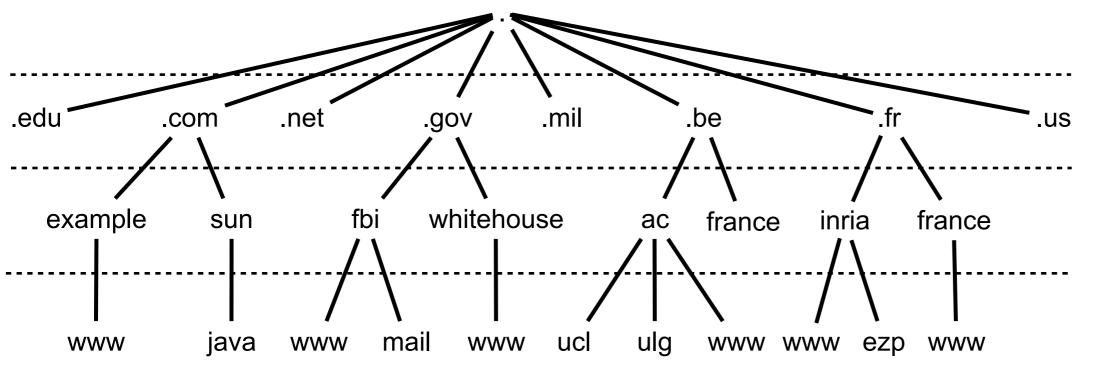




- The resolver learns the hierarchy
  - responses can be cached to avoid querying twice the same server



Query: ezp.inria.fr



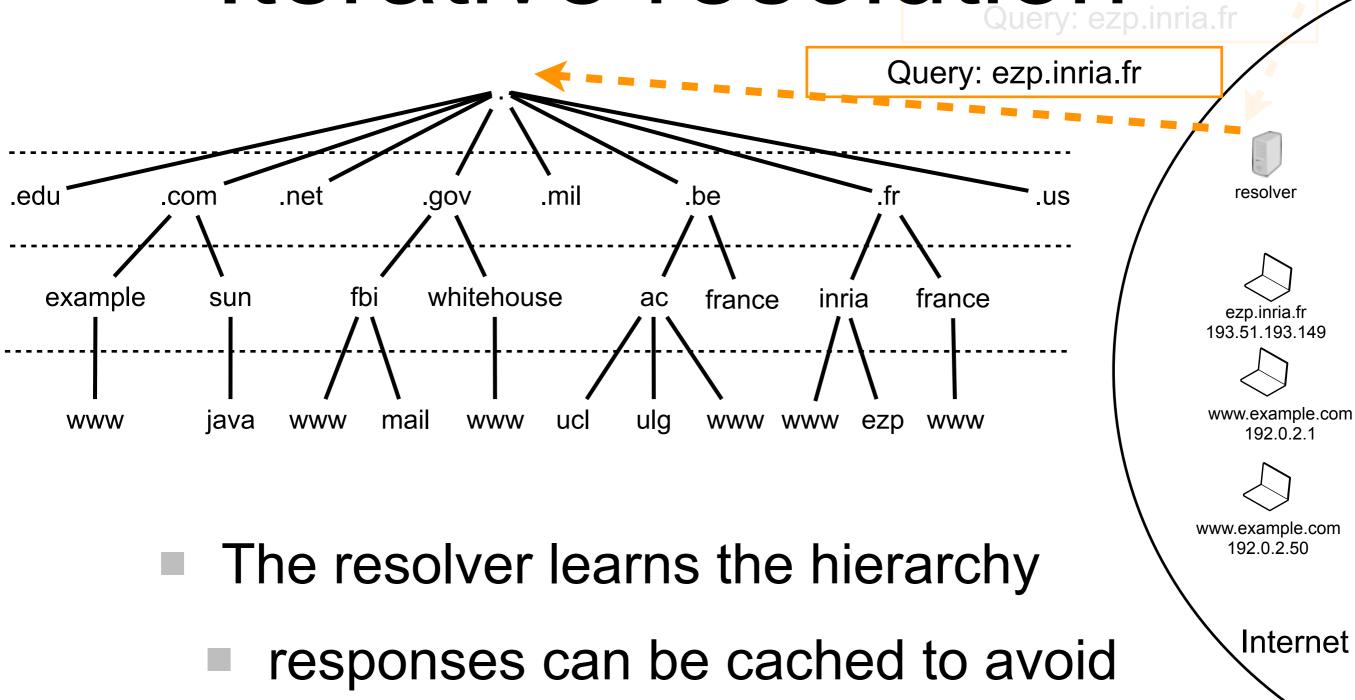
- The resolver learns the hierarchy
  - responses can be cached to avoid querying twice the same server



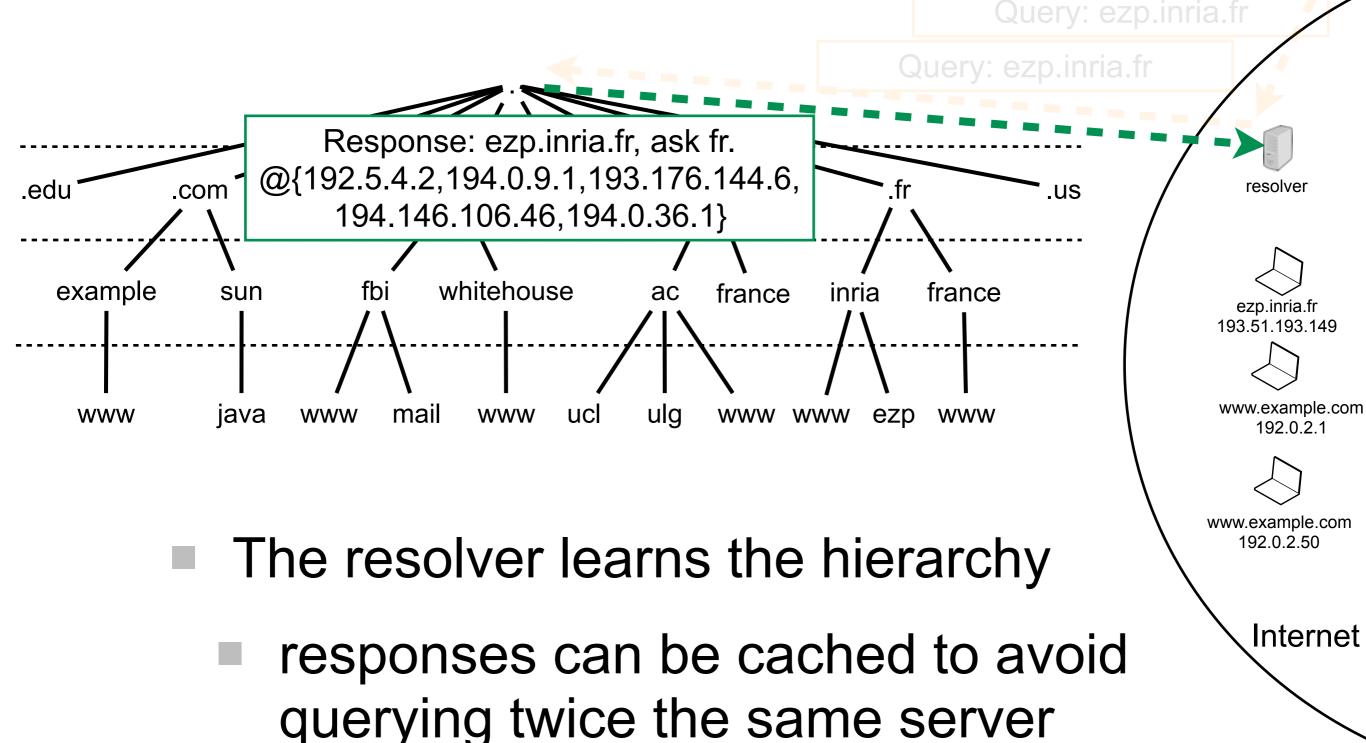
www.example.com

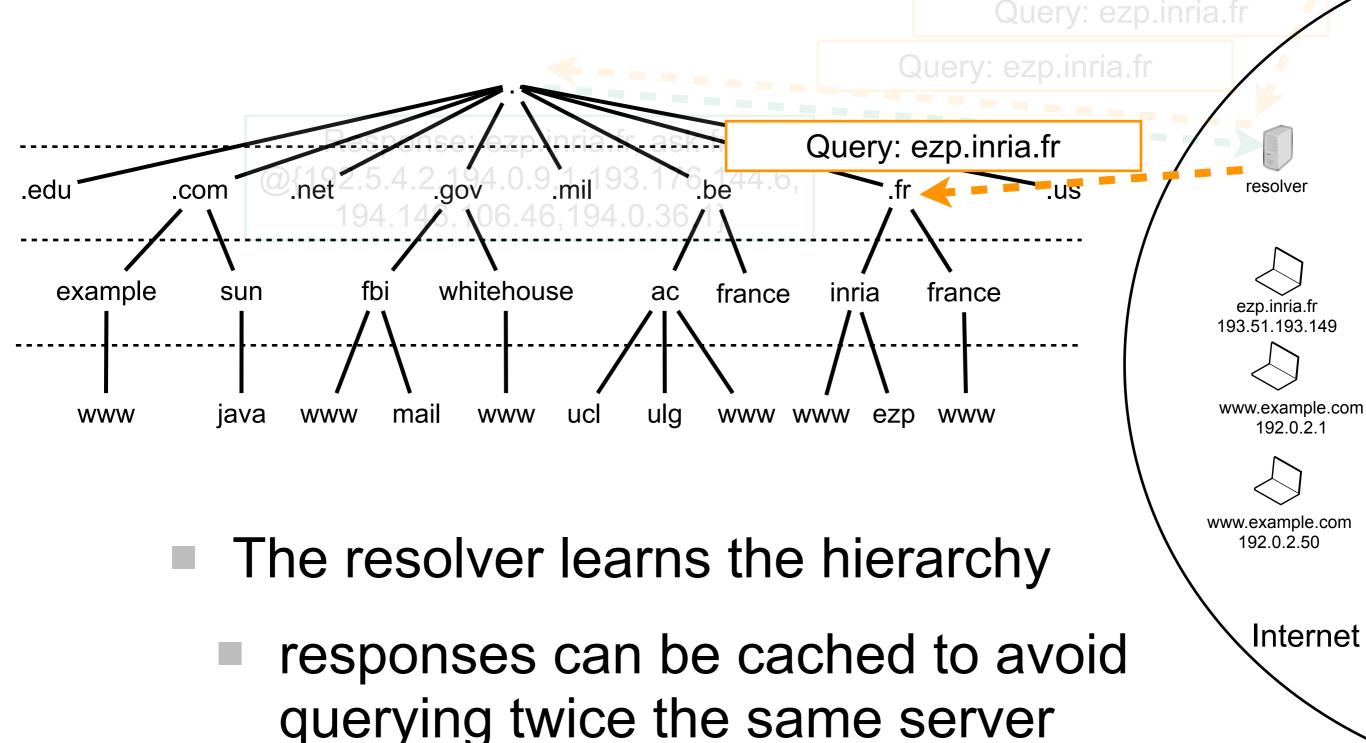
192.0.2.50

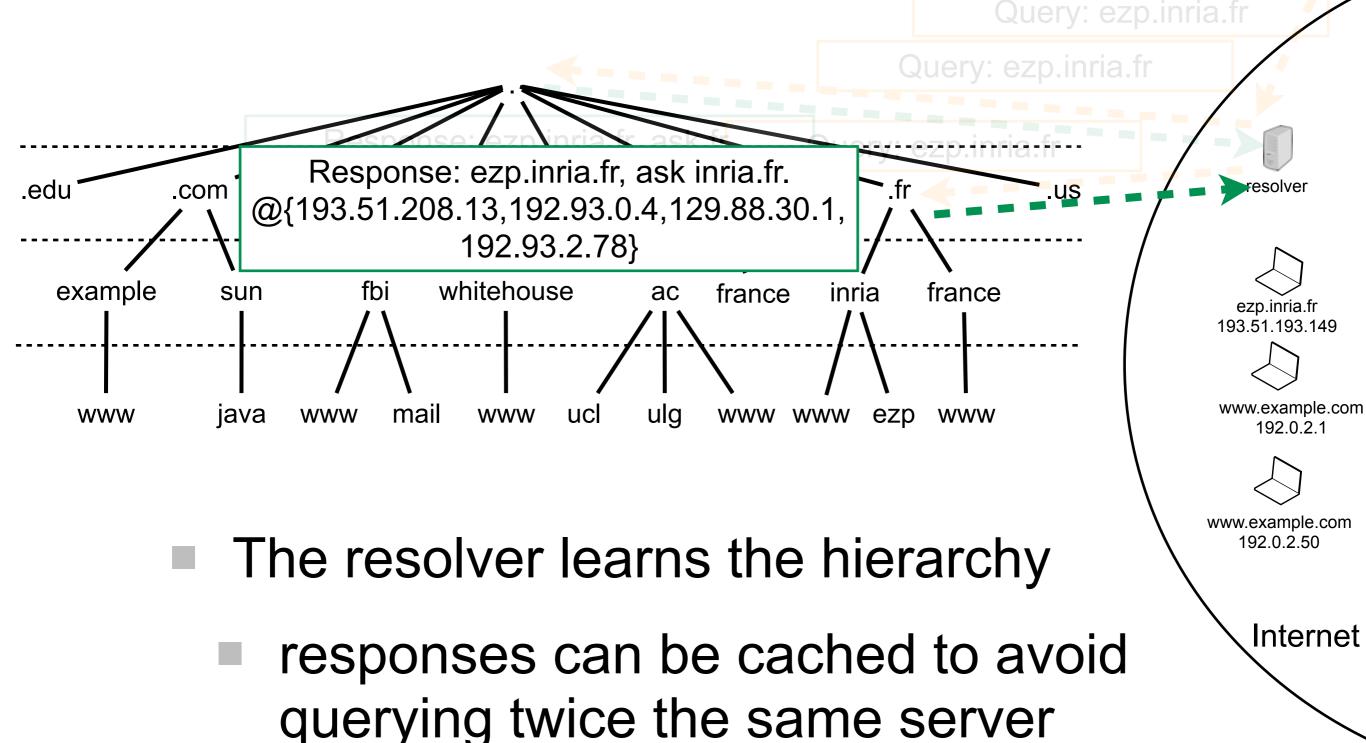
Internet

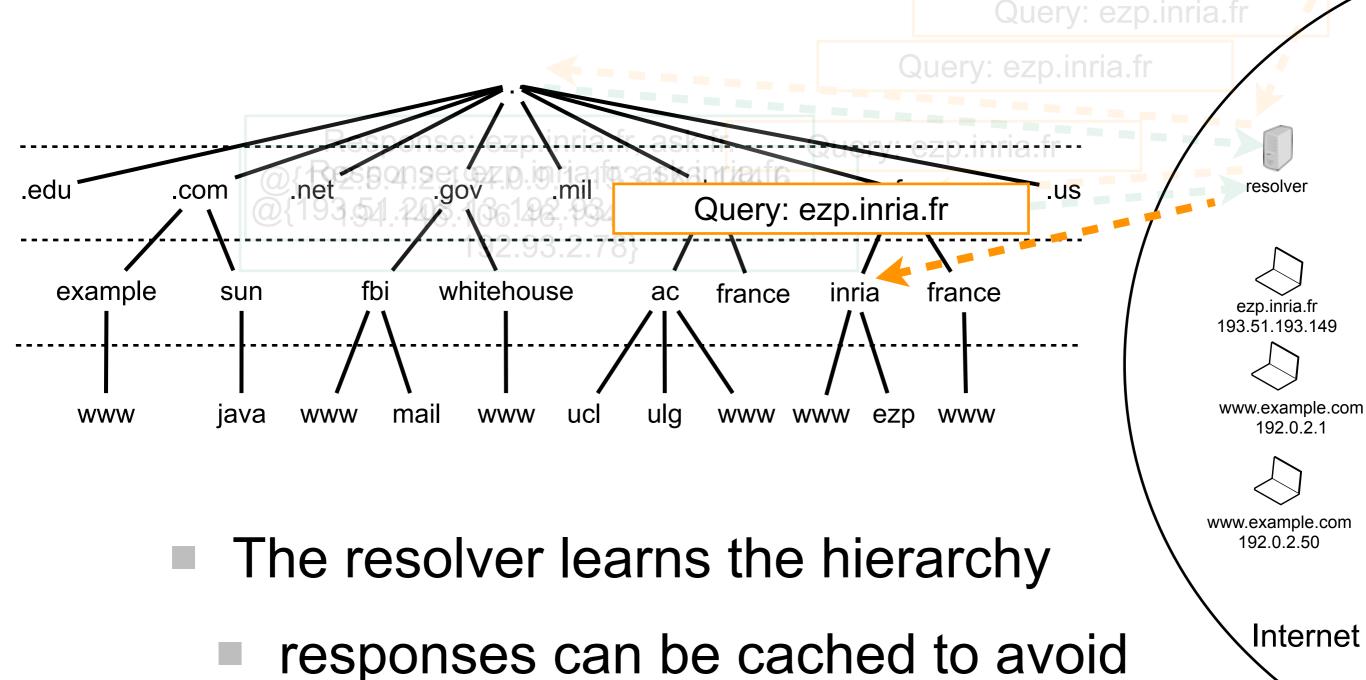


querying twice the same server

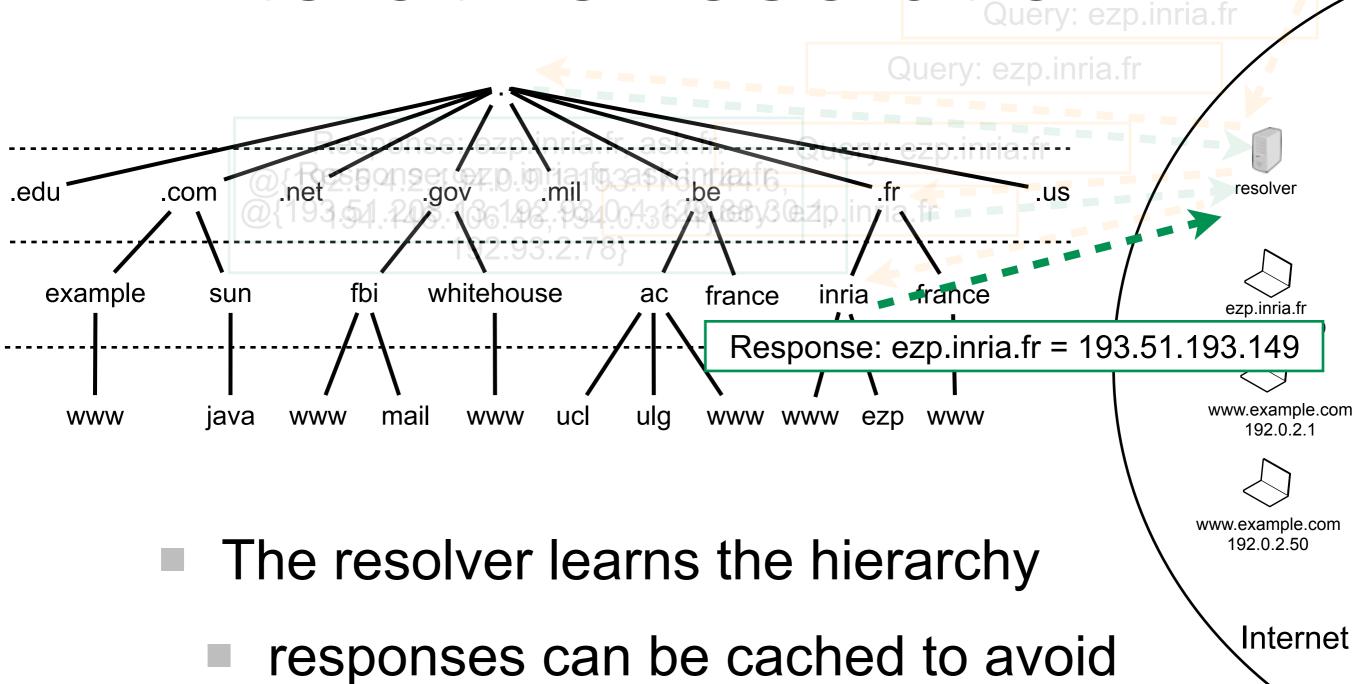








querying twice the same server



querying twice the same server

## Iterative resolution Response: ezp.inria.fr = 193.51.193.149

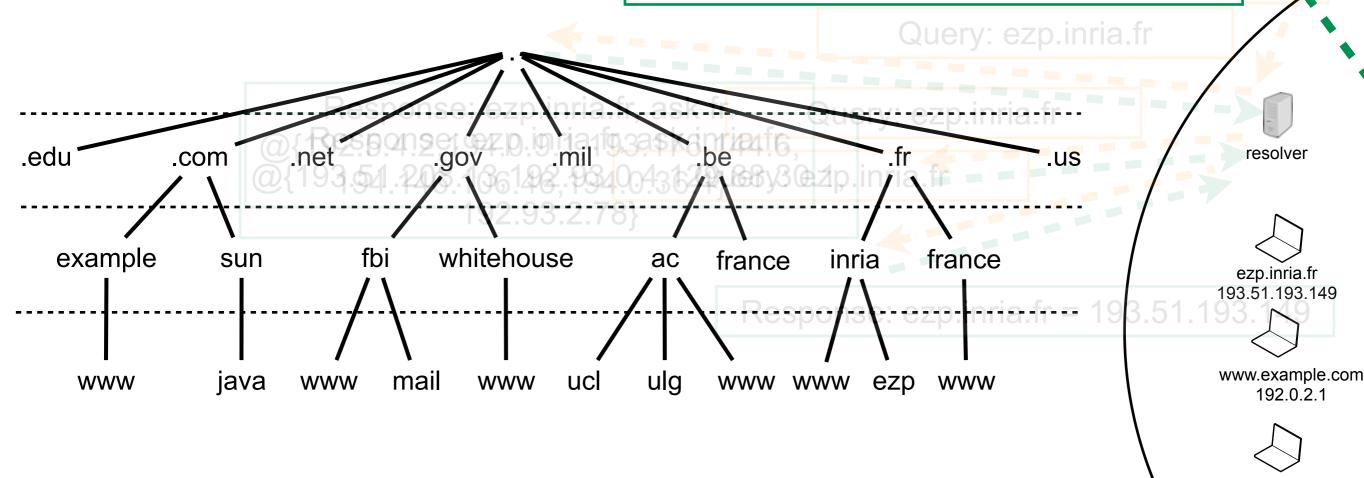
resolver

192.0.2.1

www.example.com

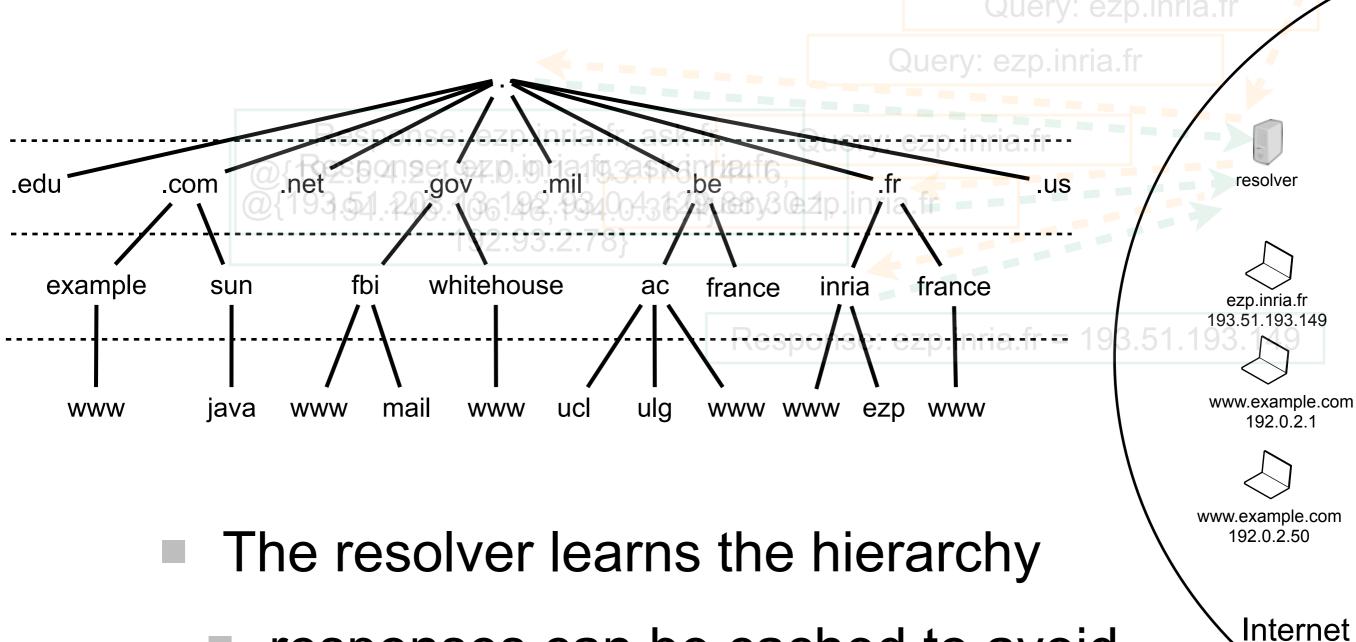
192.0.2.50

Internet



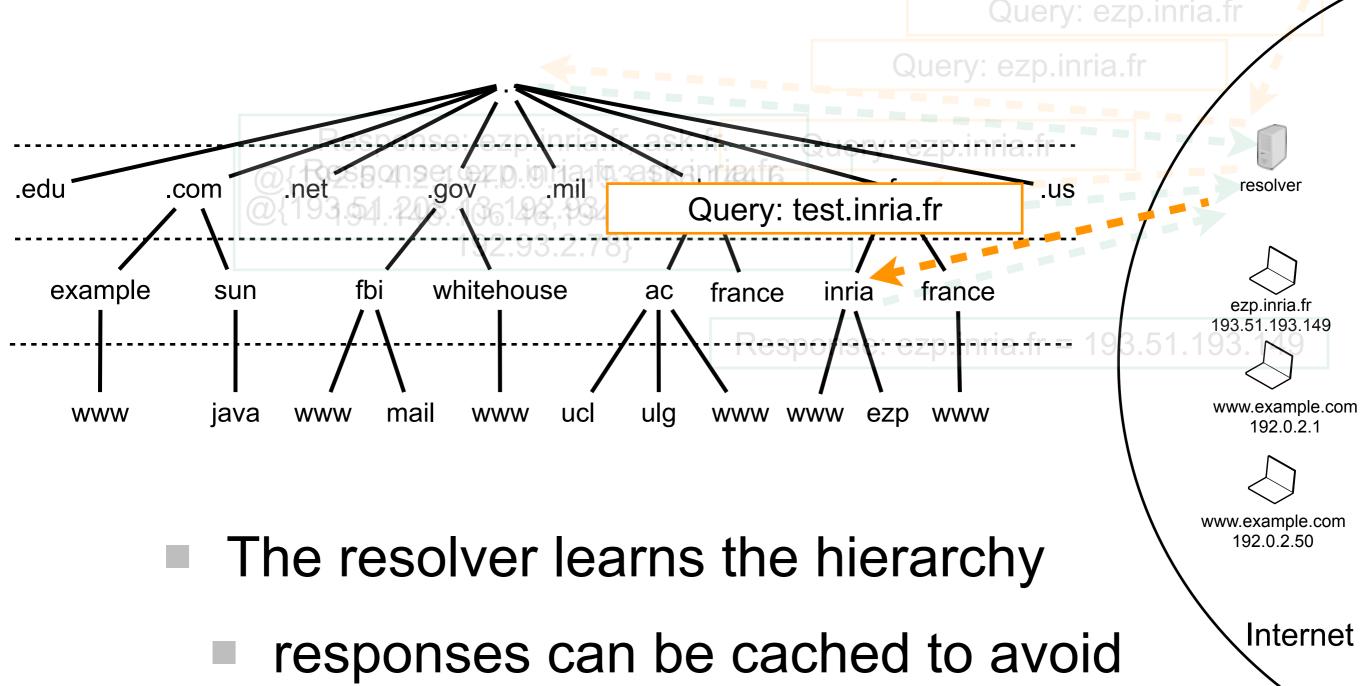
- The resolver learns the hierarchy
  - responses can be cached to avoid querying twice the same server

#### Iterative resolution



responses can be cached to avoid querying twice the same server

#### Iterative resolution

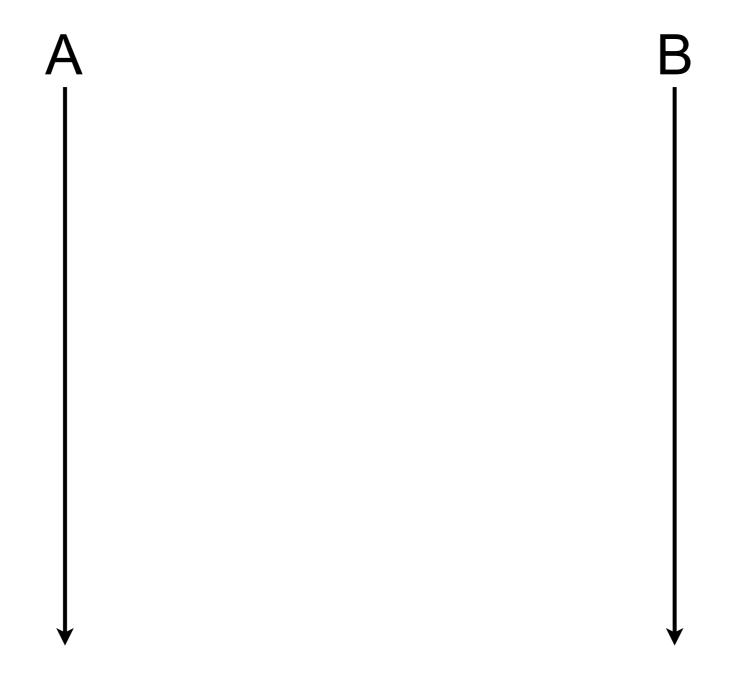


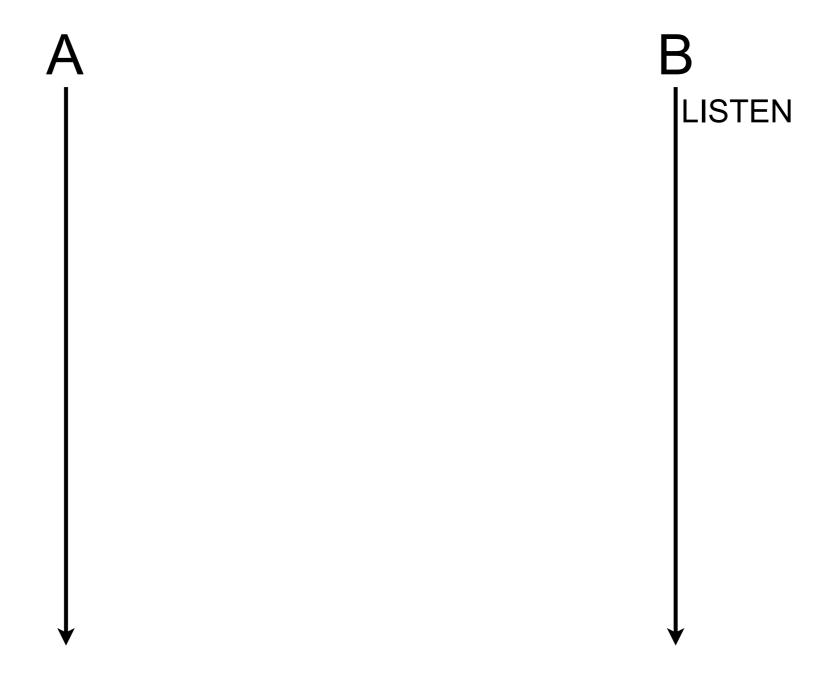
querying twice the same server

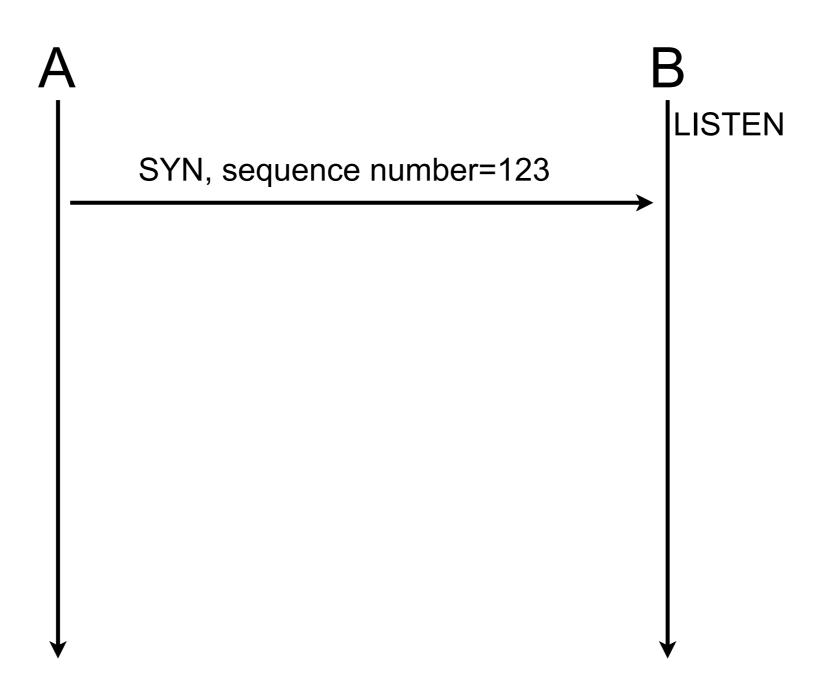
#### Transport

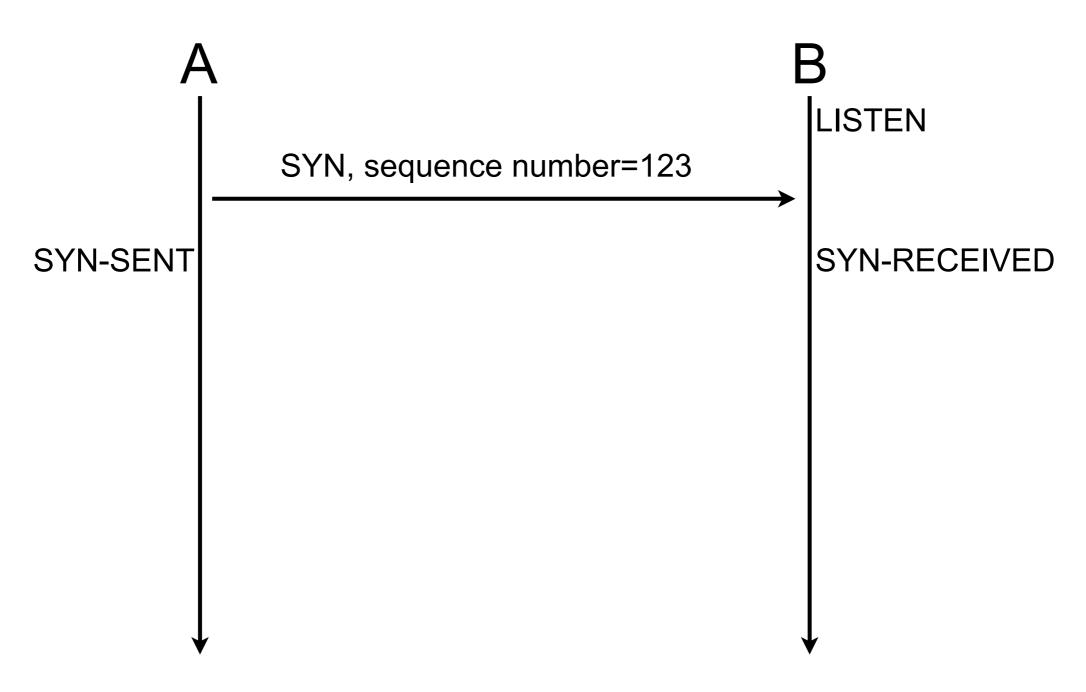
#### Transport of data between hosts

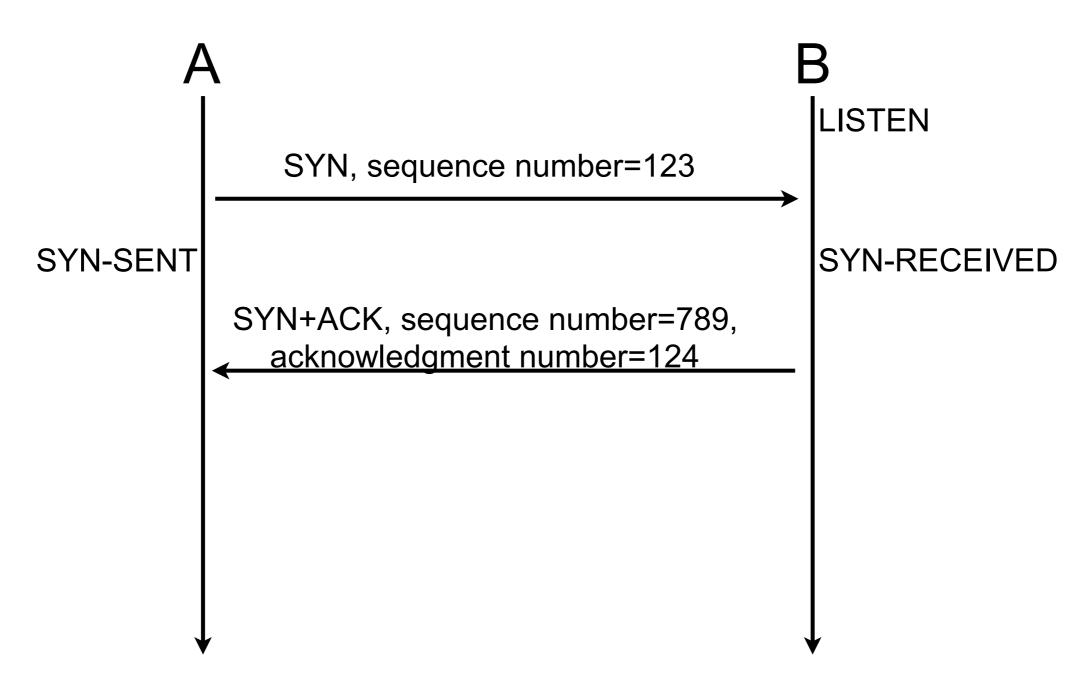
- Transport layer provides an end-to-end communication service
  - applications just deal with stream of bytes
- Most popular protocols:
  - UDP: connection-less, non reliable
  - TCP: connection-full, reliable

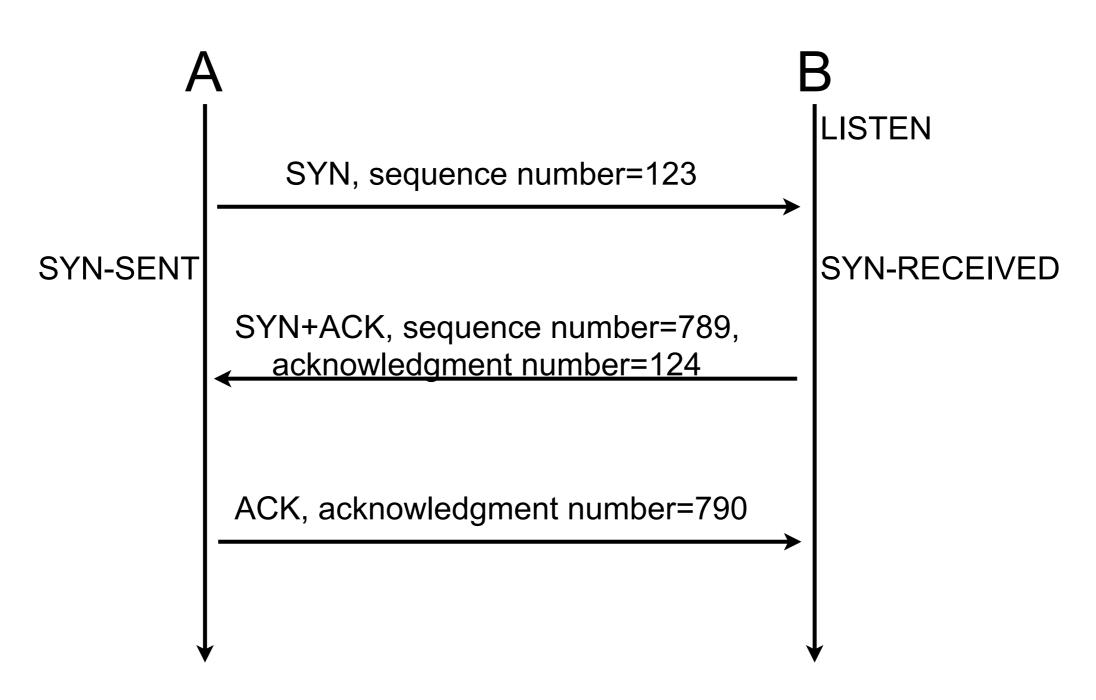


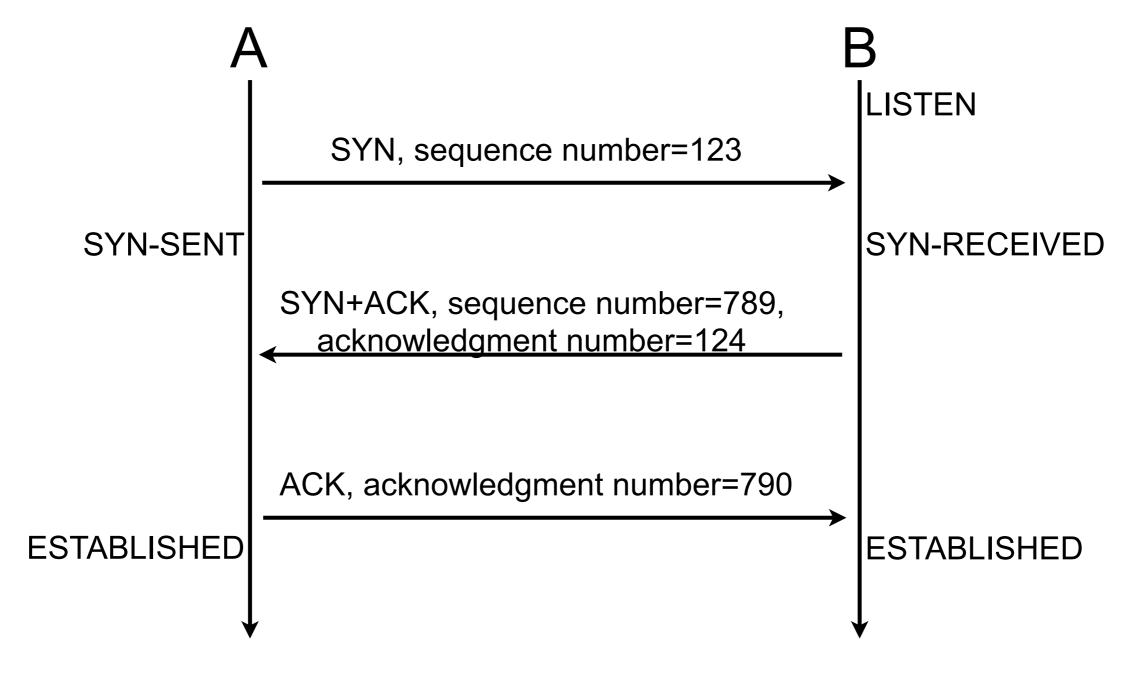




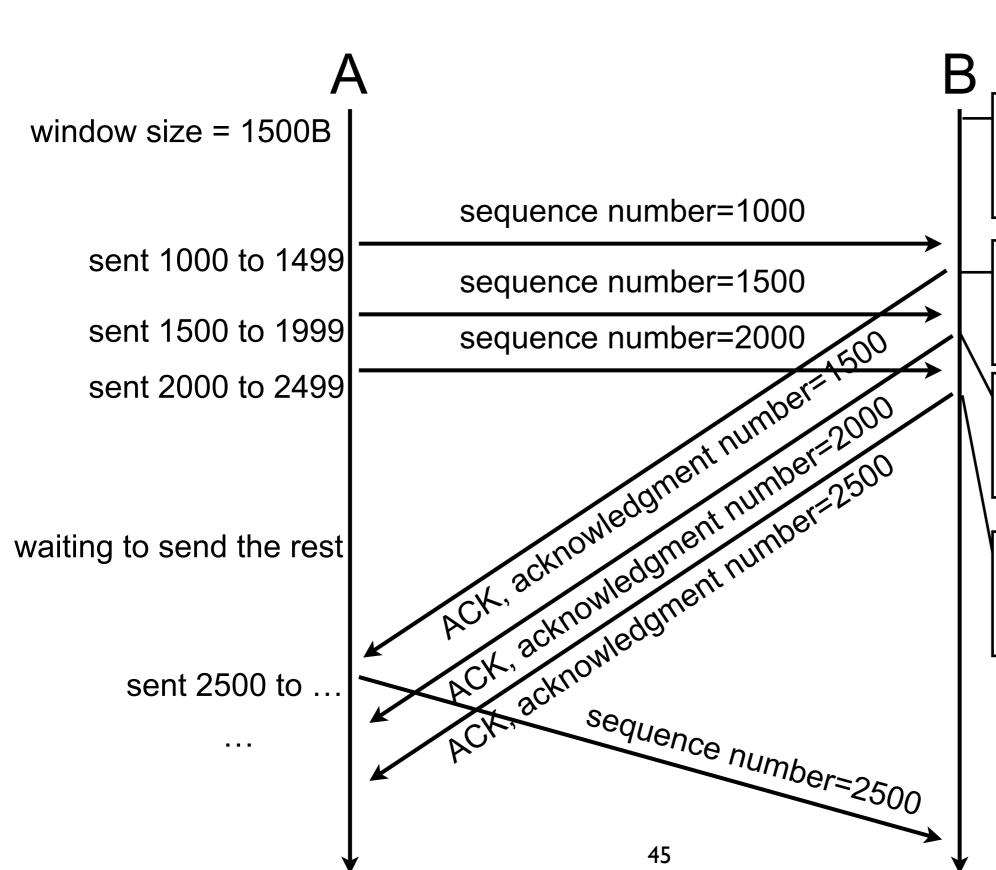








#### TCP data transfer

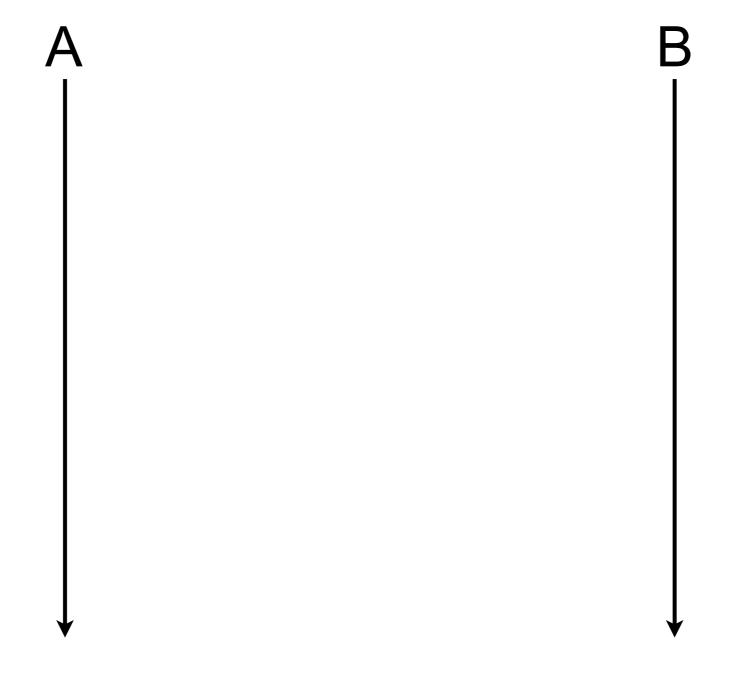


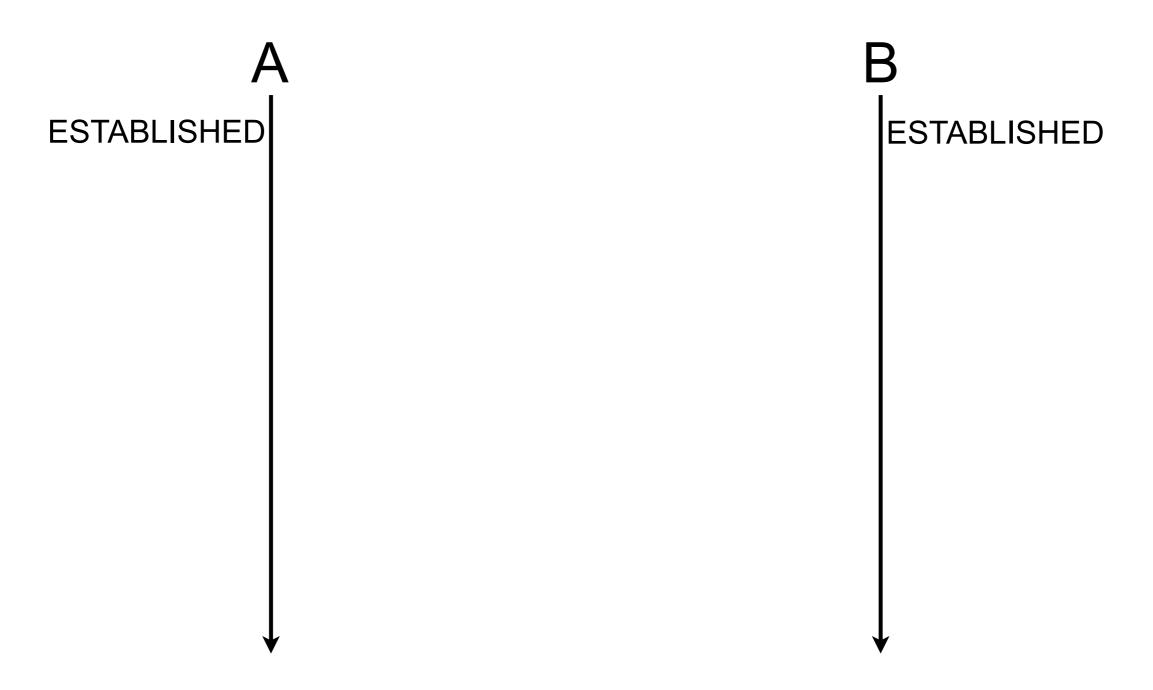
ready to receive data sequenced between 1000 and 2499

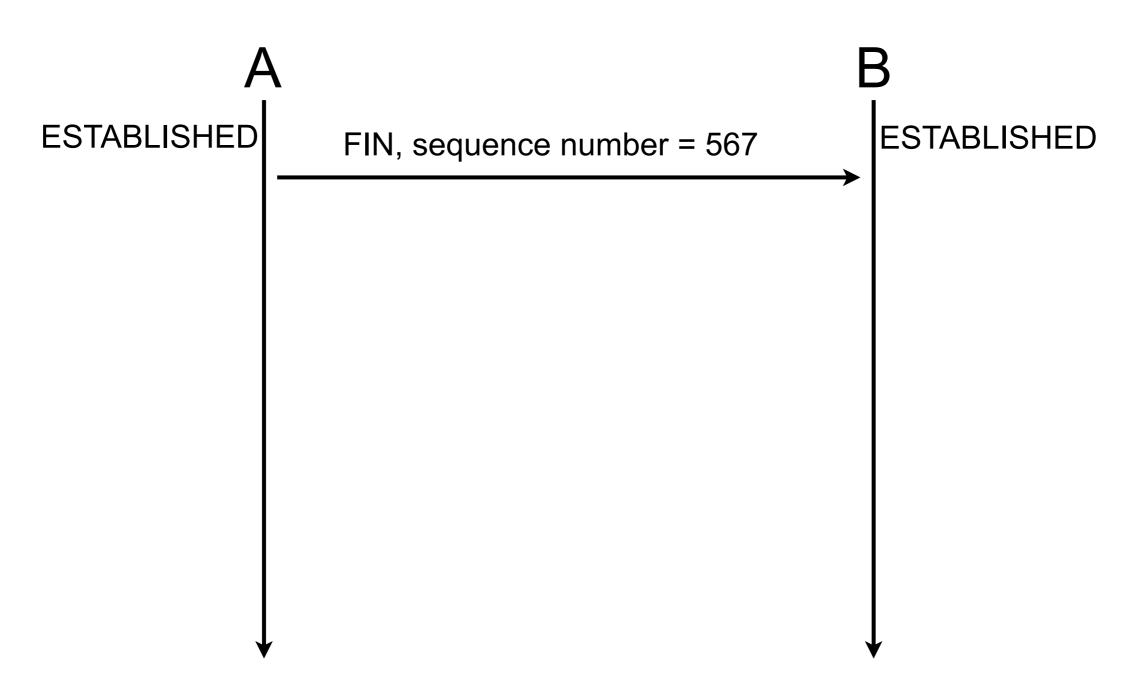
ready to receive data sequenced between 1500 to 2999

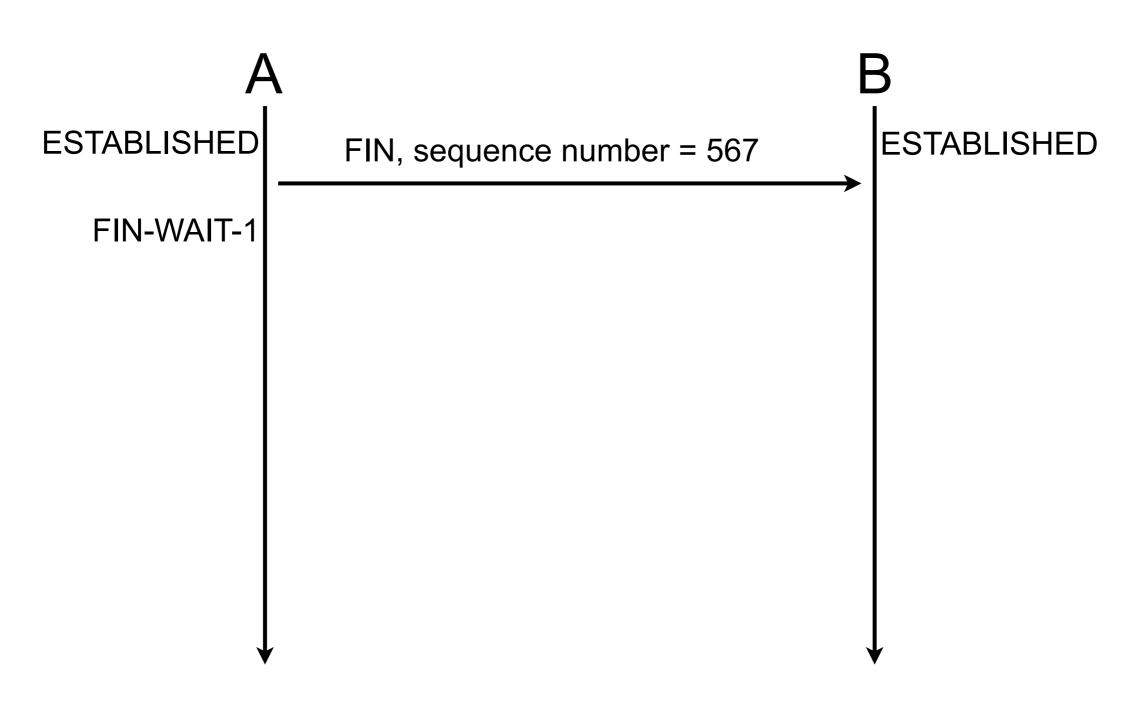
ready to receive data sequenced between 2000 to 3499

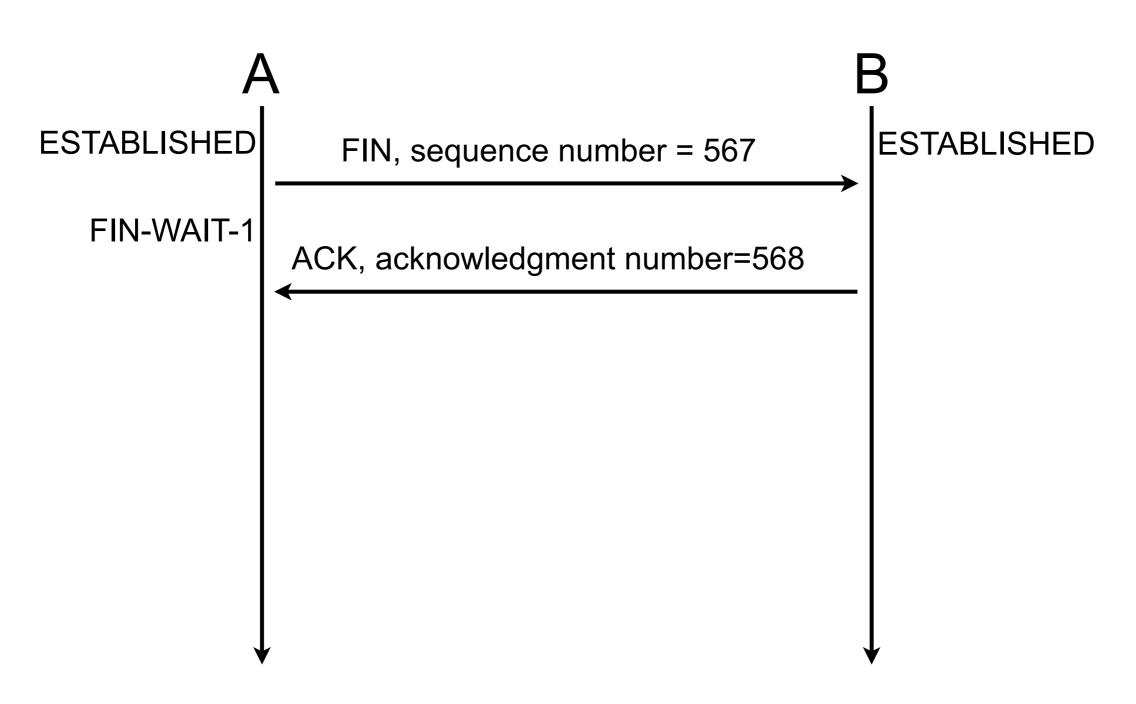
ready to receive data sequenced between 2500 to 3999

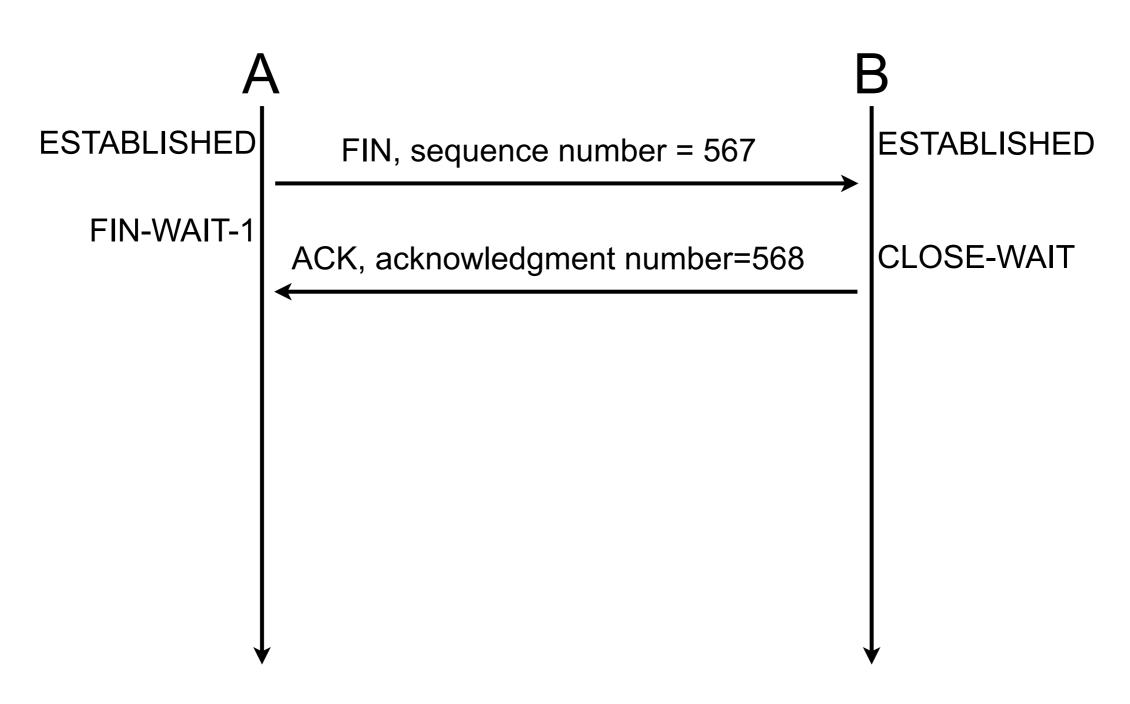


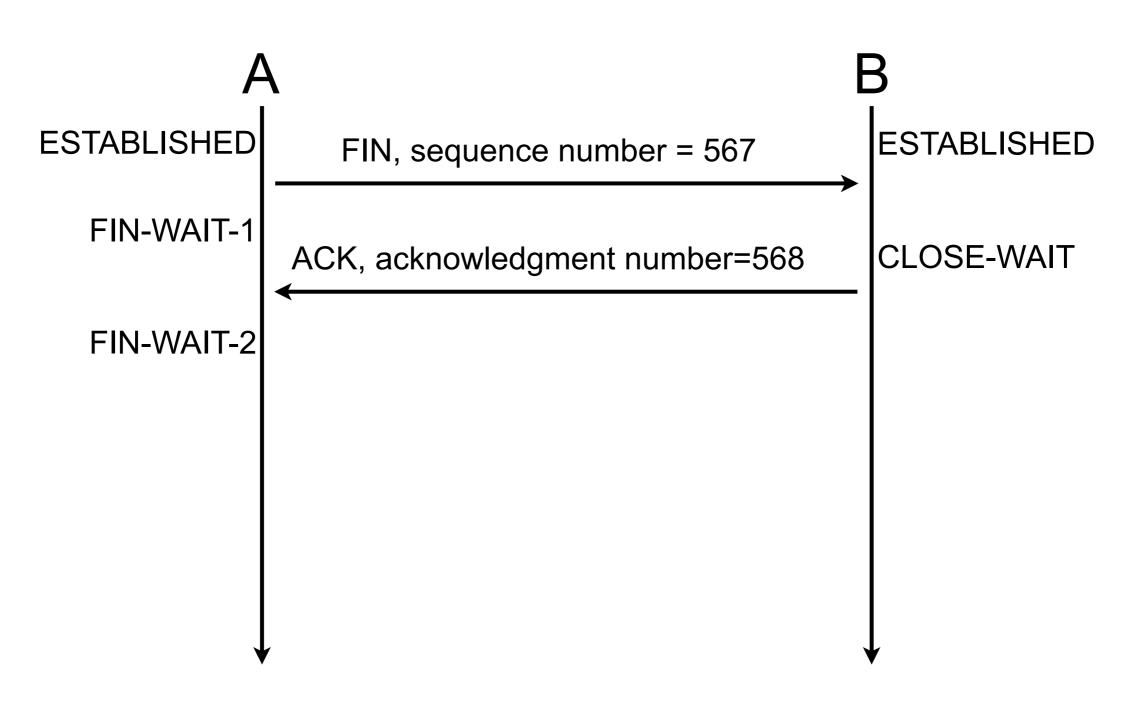


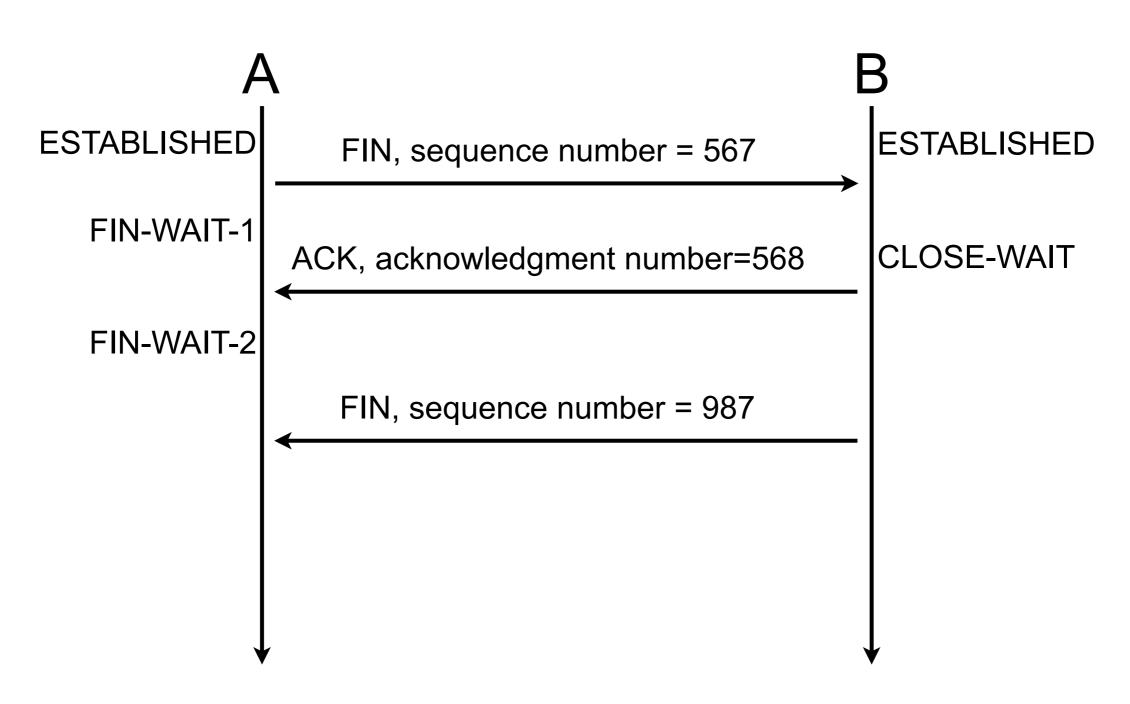


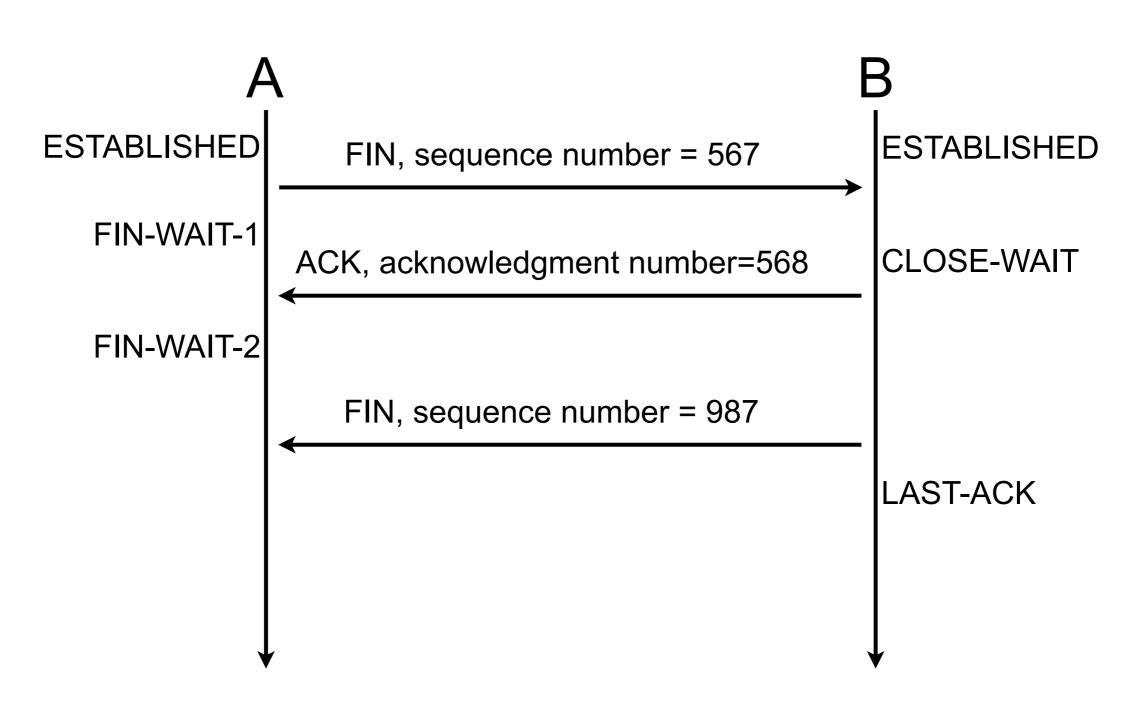


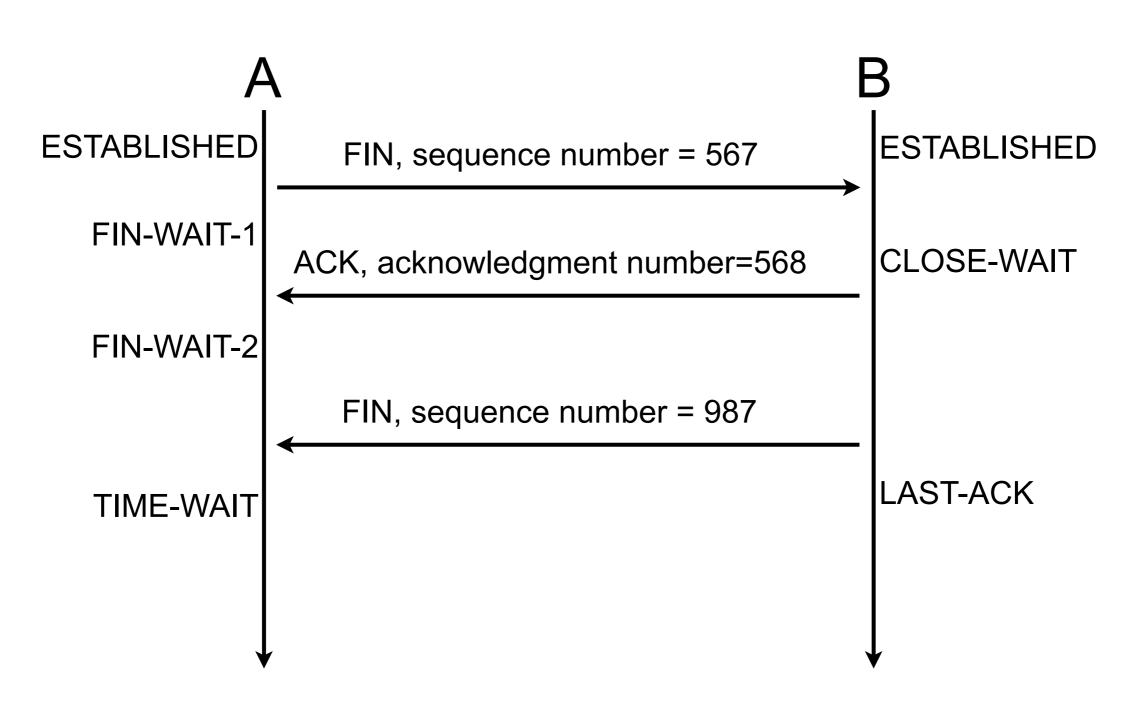


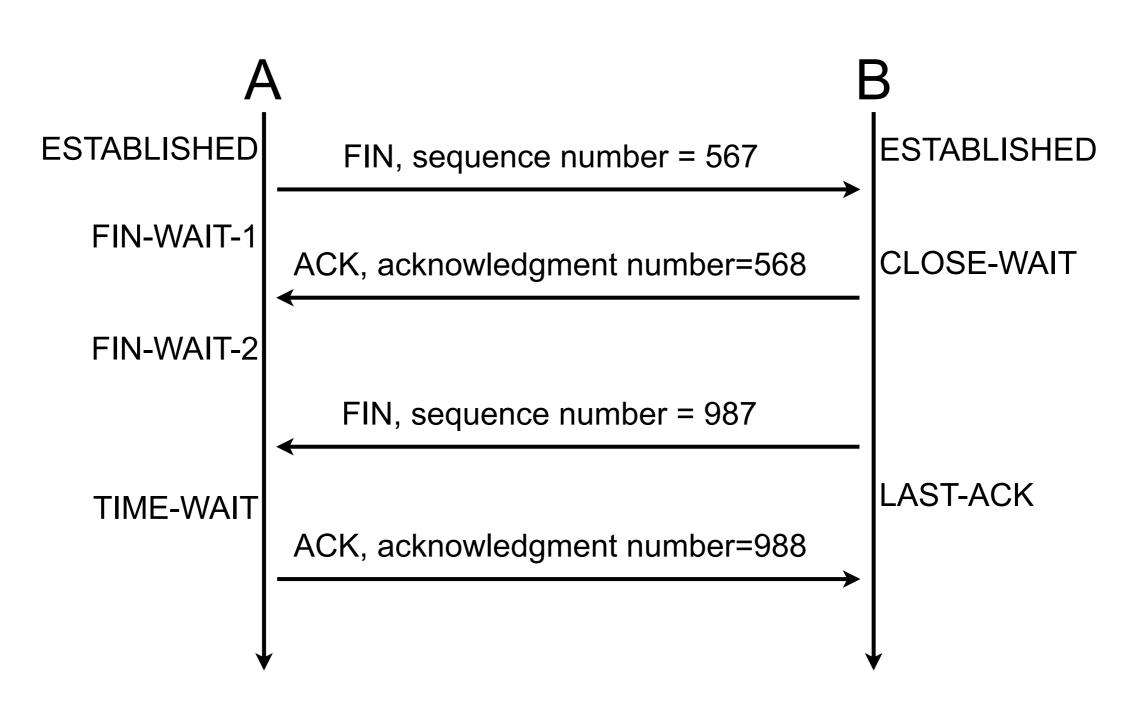


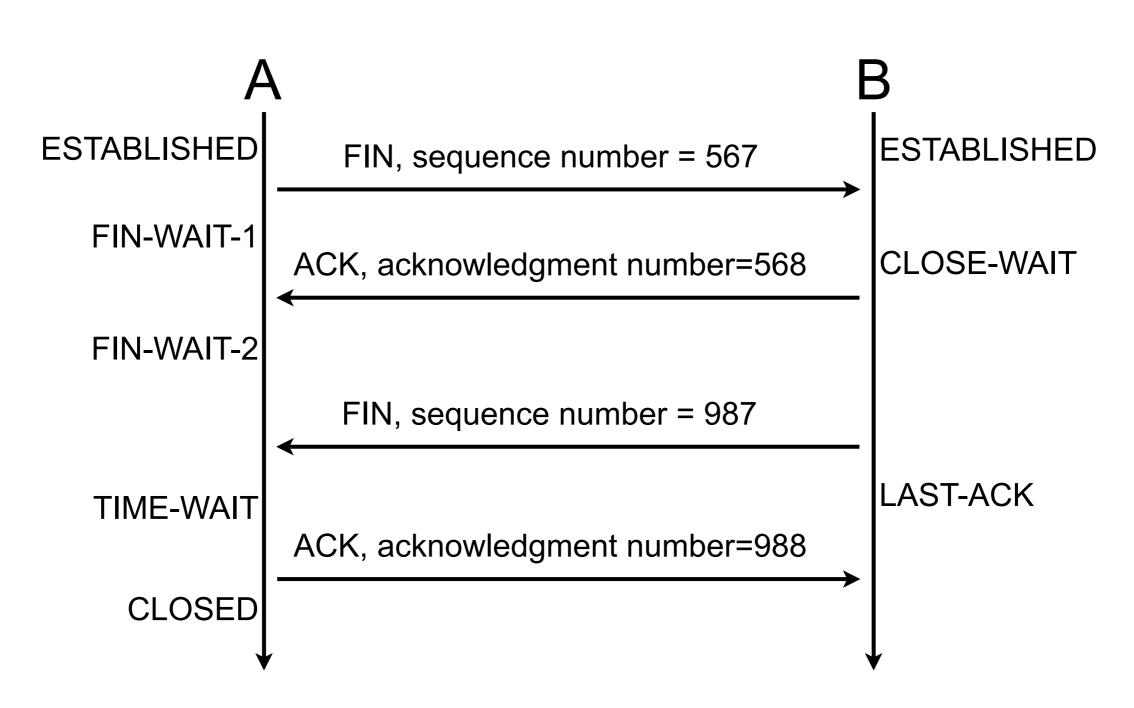


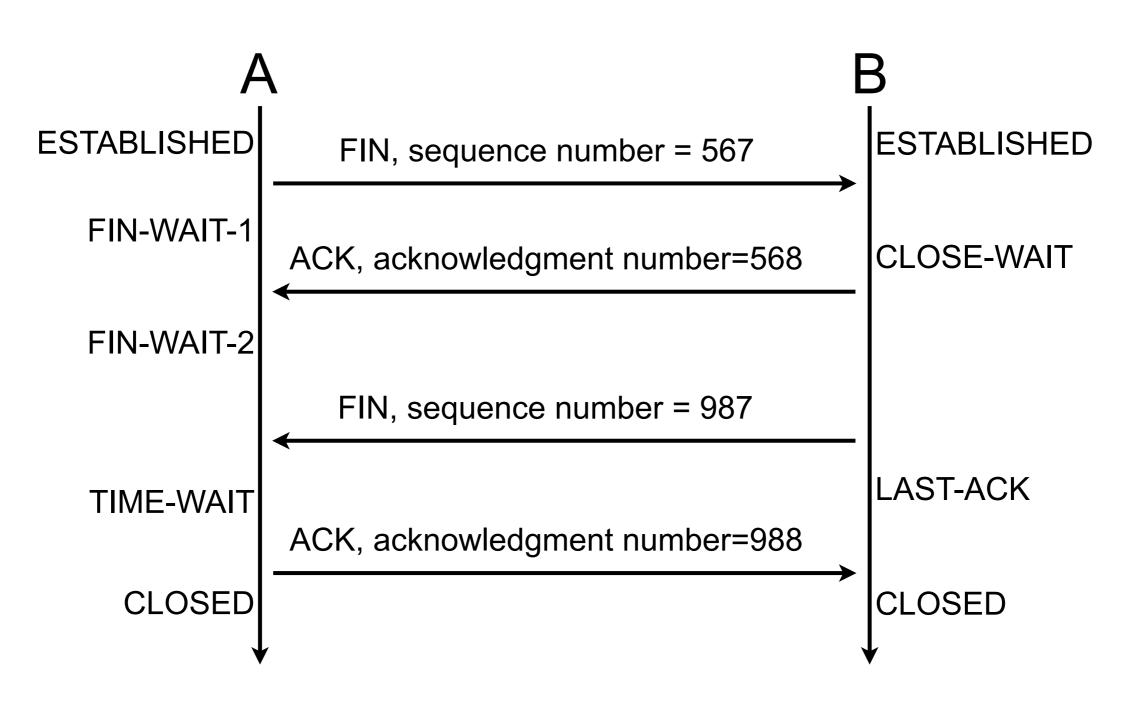






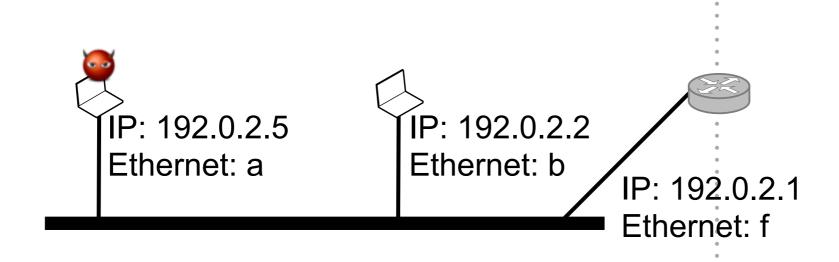




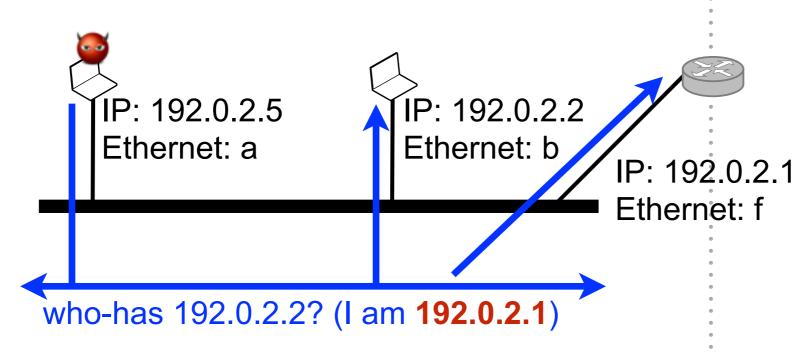


# Threats by the example

0.0.0.0/0 via 192.0.2.1 192.0.2.1 is f

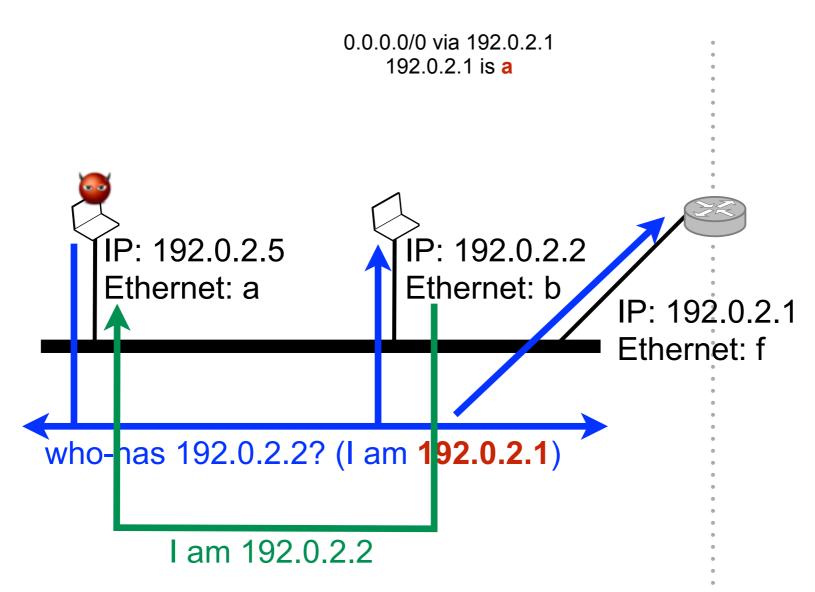


0.0.0.0/0 via 192.0.2.1 192.0.2.1 is f



0.0.0.0/0 via 192.0.2.1 192.0.2.1 is a IP: 192.0.2.5 Ethernet: a IP: 192.0.2.2 Ethernet: b IP: 192.0.2.1 Ethernet: f

who-has 192.0.2.2? (I am 192.0.2.1)



0.0.0.0/0 via 192.0.2.1 192.0.2.1 is a IP source: 192.0.2.2 IP destination: 203.0.113.2 ÍP: 192.0.2.2 IP: 192.0.2.5 Ethernet: a Ethernet: b IP: 192.0.2.1 Ethernet: f who-has 192.0.2.2? (I am **192.0.2.1**) I am 192.0.2.2

0.0.0.0/0 via 192.0.2.1 192.0.2.1 is a IP source: 192.0.2.2 IP destination: 203.0.113.2 ÍP: 192.0.2.2 IP: 192.0.2.5 Ethernet: a Ethernet: b IP: 192.0.2.1 Ethernet: f who-has 192.0.2.2? (I am 192.0.2.1) 192.0.2.2 IP destination: 203.0.113.2 Ethernet source: b Ethernet destination:a IP source: 192.0.2.2

#### Why does it work?

#### Why does it work?

- Conceptual vulnerability
  - using non-requested information as ground truth is dangerous
  - using non-authenticated information is dangerous

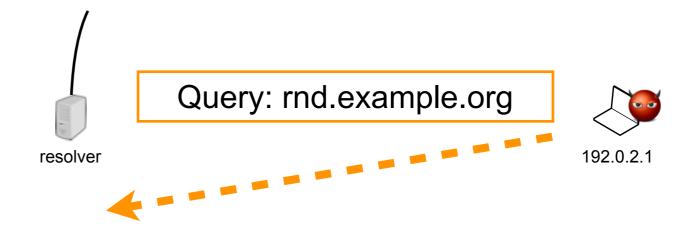
#### DNS cache poisoning



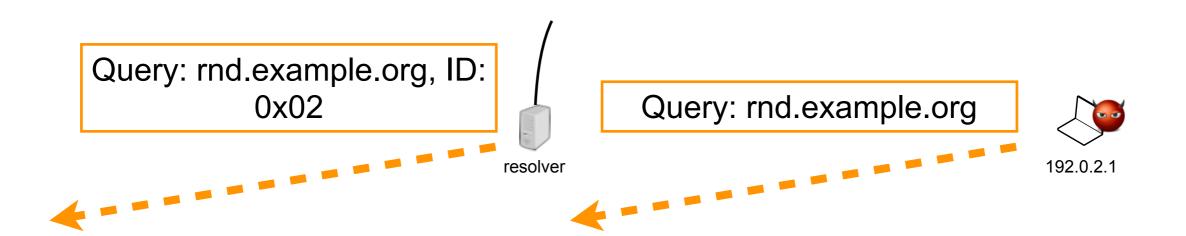




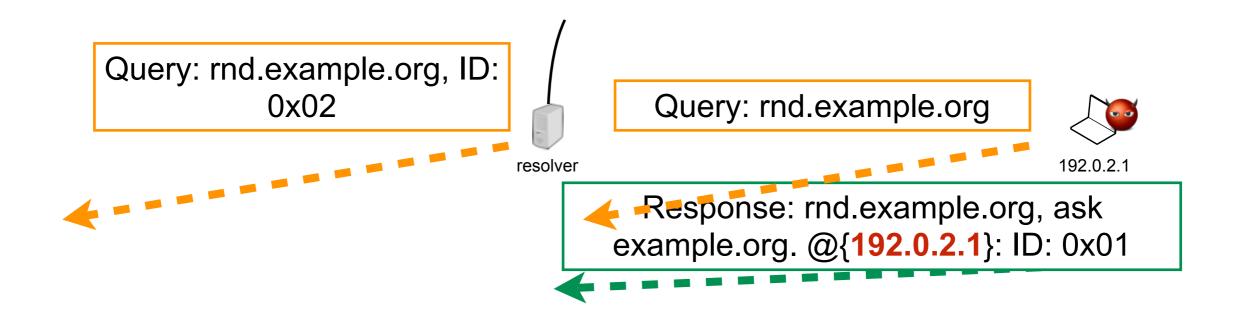
#### DNS cache poisoning



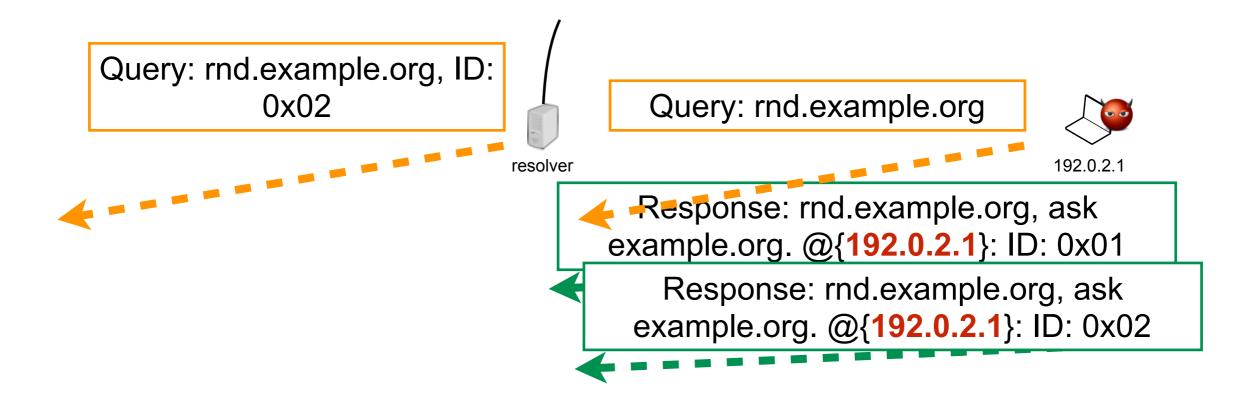




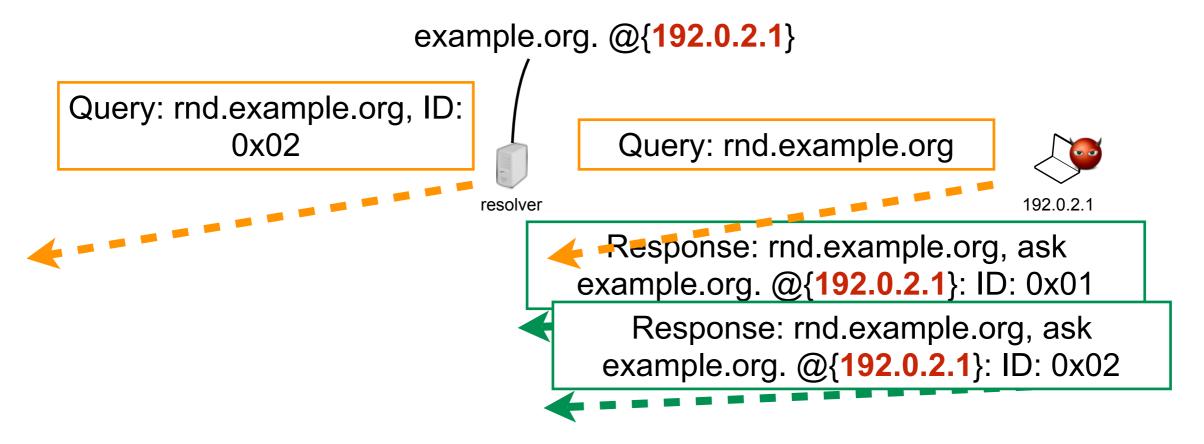




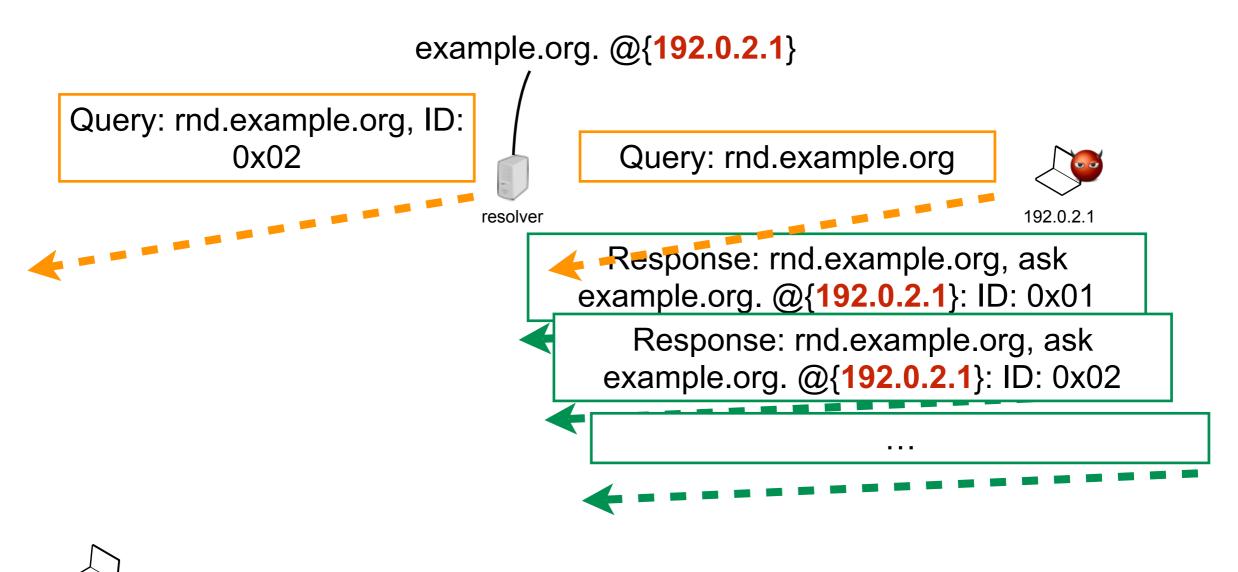


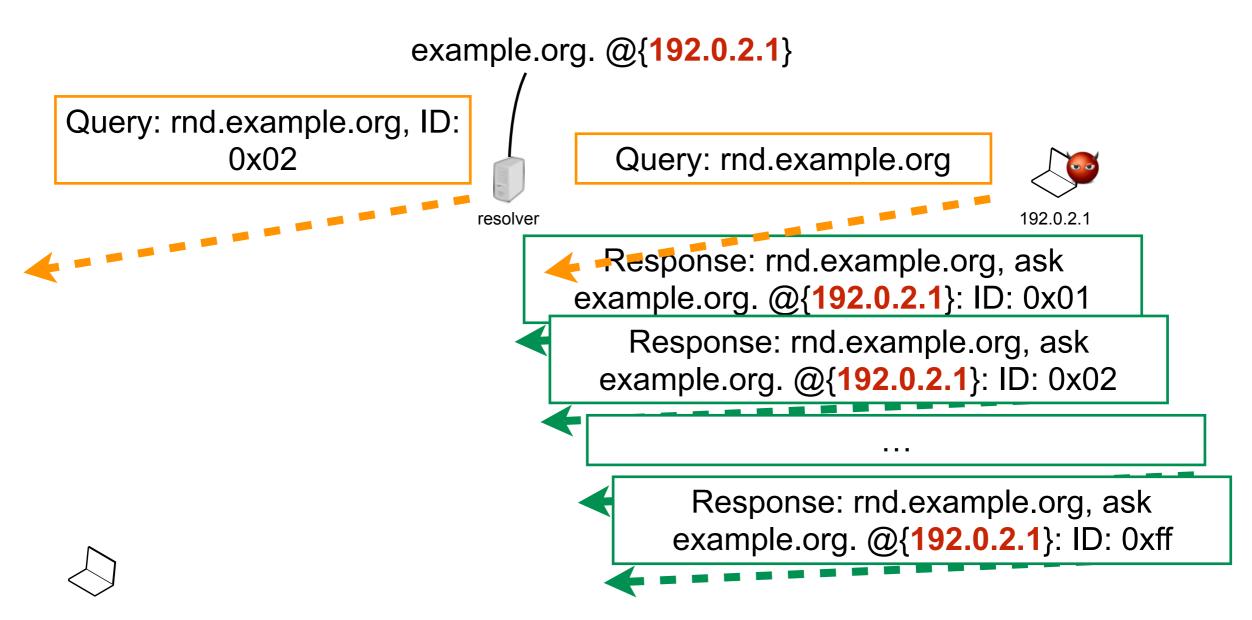






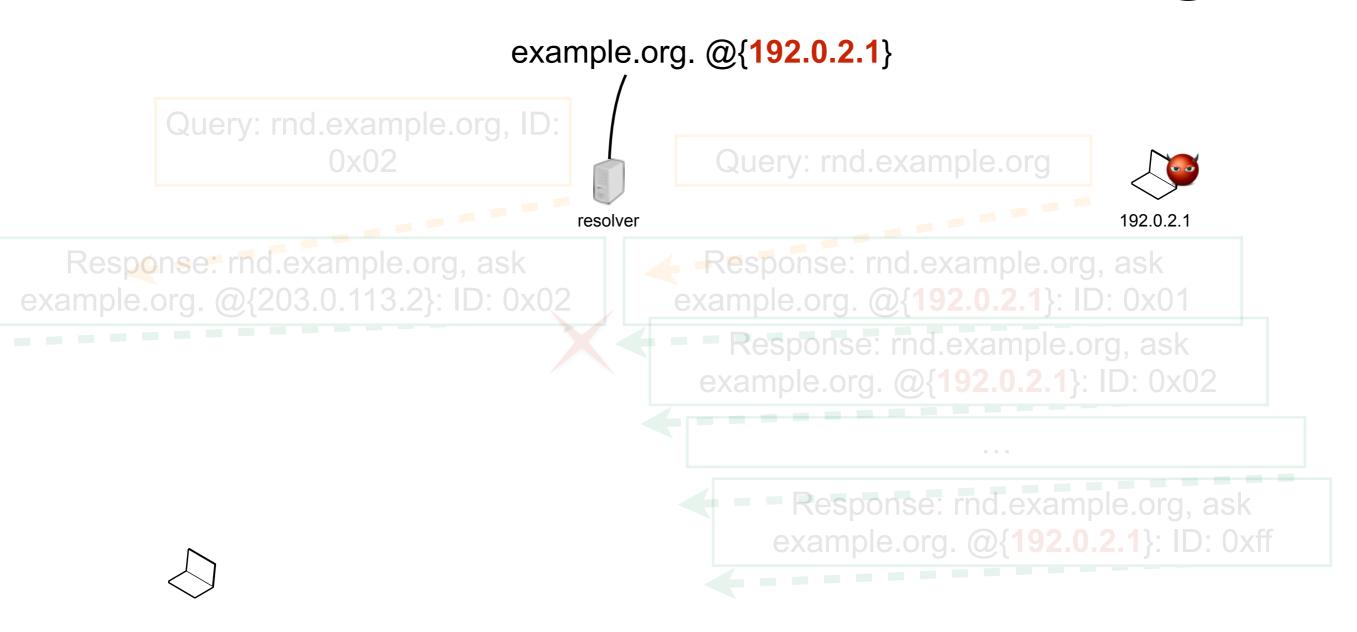


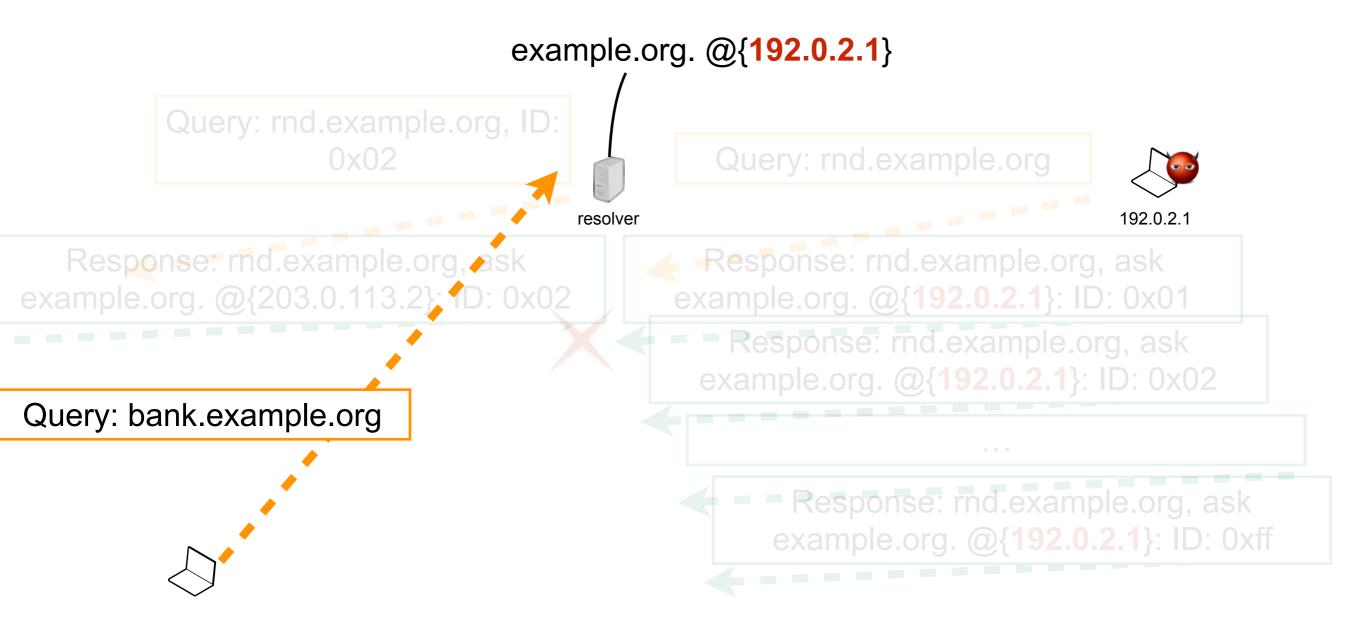


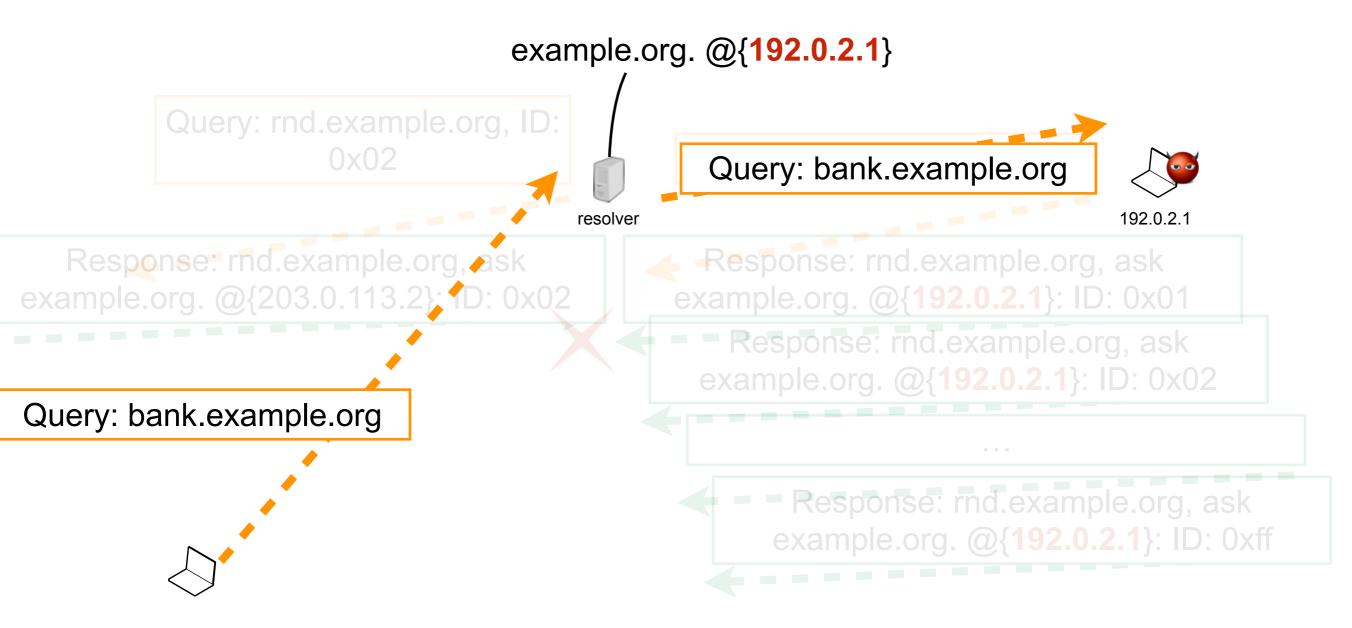


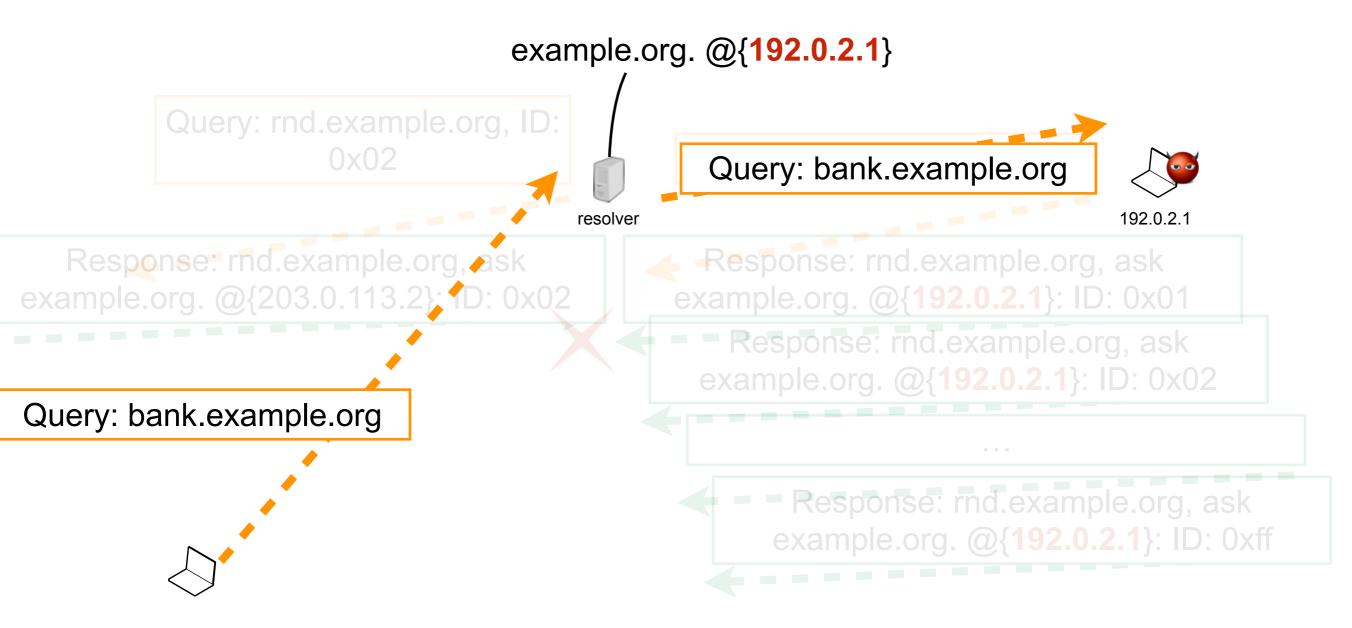
example.org. @{192.0.2.1} Query: rnd.example.org, ID: Query: rnd.example.org 0x02 resolver 192.0.2.1 Response: rnd.example.org, ask Response: rnd.example.org, ask example.org. @{203.0.113.2}: ID: 0x02 example.org. @{192.0.2.1}: ID: 0x01 Response: rnd.example.org, ask example.org. @{192.0.2.1}: ID: 0x02 Response: rnd.example.org, ask example.org. @{192.0.2.1}: ID: 0xff

example.org. @{192.0.2.1} Query: rnd.example.org, ID: Query: rnd.example.org 0x02 resolver 192.0.2.1 Response: rnd.example.org, ask Response: rnd.example.org, ask example.org. @{203.0.113.2}: ID: 0x02 example.org. @{192.0.2.1}: ID: 0x01 Response: rnd.example.org, ask example.org. @{192.0.2.1}: ID: 0x02 Response: rnd.example.org, ask example.org. @{192.0.2.1}: ID: 0xff









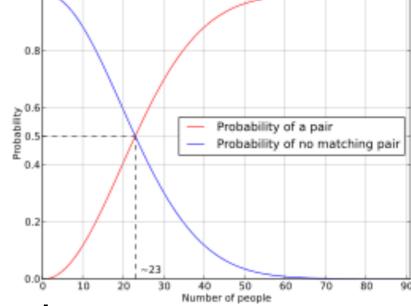
### Why does it work?

### Why does it work?

- Birthday paradox
  - probability that n elements uniformly picked

from the finite set T is

$$p(n) = 1 - \frac{|T|!}{(|T| - n)} \cdot \frac{1}{|T|^n}$$



- Relying solely on transaction ID is dangerous
  - particularly when IDs are small (16 bits in DNS)

### DNS Distributed Denial of Service (DDoS)

- Attacks against Dyn DNS infrastructure
- Two bursts: 2016-10-21 11:10 UTC -13:20 UTC; 15:50 UTC - 20:30 UTC
- Not usual DDoS
  - many more addresses than usual, non spoofed (between 40k and 100k addresses)

#### Why does it work?

- Attacks performed via a Mirai-based botnet
  - IoT devices
- End-to-End principle
  - maximizes the intelligence at the edge
  - network avoids making decisions
- What if the edge is "bad"?

### YouTube Hijacking

- BBC Breaking news: A router problem made YouTube inaccessible for many
- RIPE NIS: "On Sunday, 24 February 2008, Pakistan Telecom (AS17557) started an unauthorised announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global (AS3491) forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale"

http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

■ Before, during and after Sunday, 24 February 2008: AS36561 (YouTube) announces 208.65.152.0/22.

- Before, during and after Sunday, 24 February 2008: AS36561 (YouTube) announces 208.65.152.0/22.
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.

- Before, during and after Sunday, 24 February 2008: AS36561 (YouTube) announces 208.65.152.0/22.
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- Sunday, 24 February 2008, 20:07 (UTC): AS36561 (YouTube) starts announcing 208.65.153.0/24. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.

- **Before, during and after Sunday, 24 February 2008**: AS36561 (YouTube) announces **208.65.152.0/22**.
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- Sunday, 24 February 2008, 20:07 (UTC): AS36561 (YouTube) starts announcing 208.65.153.0/24. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- Sunday, 24 February 2008, 20:18 (UTC): AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.

- **Before, during and after Sunday, 24 February 2008**: AS36561 (YouTube) announces **208.65.152.0/22**.
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- Sunday, 24 February 2008, 20:07 (UTC): AS36561 (YouTube) starts announcing 208.65.153.0/24. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- Sunday, 24 February 2008, 20:18 (UTC): AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
- Sunday, 24 February 2008, 20:51 (UTC): All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen prepended by another 17557. The longer AS path means that more routers prefer the announcement originated by YouTube.

- **Before, during and after Sunday, 24 February 2008**: AS36561 (YouTube) announces **208.65.152.0/22**.
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- Sunday, 24 February 2008, 20:07 (UTC): AS36561 (YouTube) starts announcing 208.65.153.0/24. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- Sunday, 24 February 2008, 20:18 (UTC): AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
- Sunday, 24 February 2008, 20:51 (UTC): All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen prepended by another 17557. The longer AS path means that more routers prefer the announcement originated by YouTube.
- Sunday, 24 February 2008, 21:01 (UTC): AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24. Note that AS17557 was not completely disconnected by AS3491.
  Prefixes originated by other Pakistani ASs were still announced by AS17557 through AS3491.

http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

### Why does it work?

#### Why does it work?

- Any AS can claim to be the originator of a prefix (i.e., she hijacks the prefix)
- To protect against that, only the import filters can be used
  - rely on databases that are not so accurate
- A not secure global routing system is a major threat against freedom

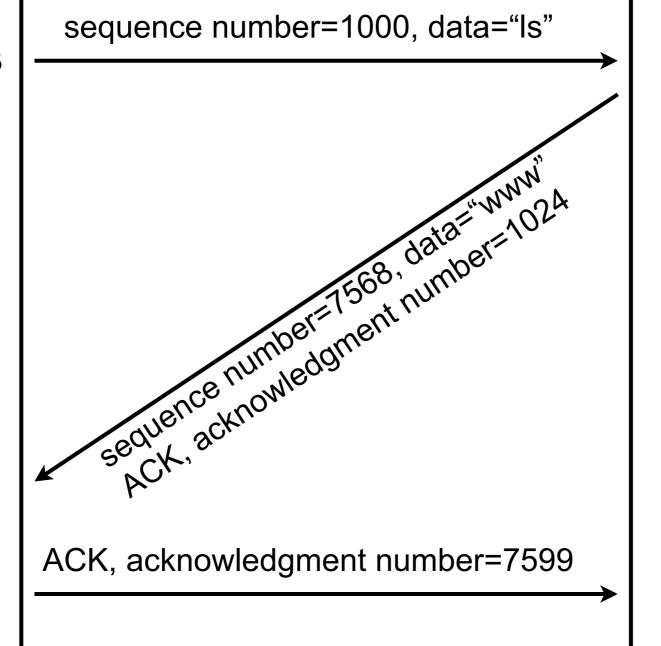
### TCP session hijacking

window size = 1500B Client

Telnet server

server

sent 1000 to 1023



### TCP session hijacking

window size = 1500B Client Telnet server

sequence number=1000, data="ls" sent 1000 to 1023 sequence number=1024, data="rm -rf /" sequence number 7000, data in 1000 ACK, acknowledgment number ACK, acknowledgment number ACK, acknowledgment number 2000, data in 1000 acknowledgment number 2000, acknowledgmen 57

### Why does it work?

#### Why does it work?

- If the attacker can
  - guess the initial sequence number
  - guess actions from the sender
- then easy to guess a sequence number that will be accepted by the receiver

### The basics of security

### Security threats

#### Intrusion

- an attacker gains remote access to some resources that are normally denied to her
  - e.g., steal processing power, botnets

#### Eavesdropping

- an attacker collects traffic of a target in order to gain access to restricted sensitive information
  - e.g., steal passwords by sniffing wireless traffic
- Denial of Service (DoS)
  - an attacker disrupts a specific targeted service
    - e.g., block the youtube website

#### The attackers

- Hackers
  - look for challenge, notoriety, and fun
    - e.g., hackers, script kiddies, students :-D
- Spies
  - look for political/business gains
    - e.g., intelligence, police, industrial spies
- Criminals
  - look for financial gains, religious/political visibility, or just to break something
  - e.g., criminals, terrorists, vandals

#### Definitions

- Key
  - input of cryptographic functions to determine its output
- Authentication
  - proof that the message is coming from the one claiming to be at the origin of the message
- Integrity
  - proof that the message has not been altered since its creation
- Non-repudiation of origin
  - an entity that generated a message cannot deny have generated the message
- Encryption
  - action of encoding of a message such that an eavesdropper can't read the message but legitimate destination can
- Decryption
  - action of decoding an encrypted message
- Signature
  - a mathematically constructed proof of authenticity of a message

#### Hall of fame

- Alice and Bob
  - are legitimate users, Alice and Bob exchange messages
- Chuck
  - is a malicious user that is not between Alice and Bob
- Eve
  - is a malicious user that can eavesdrop
- Trudy
  - is a malicious user that can perform (wo)man-in-the-middle attacks
- Trent
  - is a legitimate user that plays the role of a trusted arbitrator

### Why is good security level so hard to obtain?

- The security level of a system equals the security level of the weakest part of the system
  - e.g., encrypting your HDD to avoid information leak if the laptop is stollen is useless if the password is written on a postit attached on the laptop
- Digital system are complexes
  - interactions with many components, distribution, easily bugged...

### Security is a tradeoff

- Compare cost and probability of an attack and cost of securing the system against this attack
  - e.g., is that necessary to make data unbreakable for 20 years if they are outdated after 1 hour?
- Explain the security systems and their reasons
  - if a user does not understand why he must follow a procedure, he will not follow it
    - e.g., how many of you already give their password to someone else?
- Never "over-secure" a system
  - if the system is too hard to use, people will find countermeasure
    - e.g., too hard to use corporate mails? Then use gmail to send corporate mails...

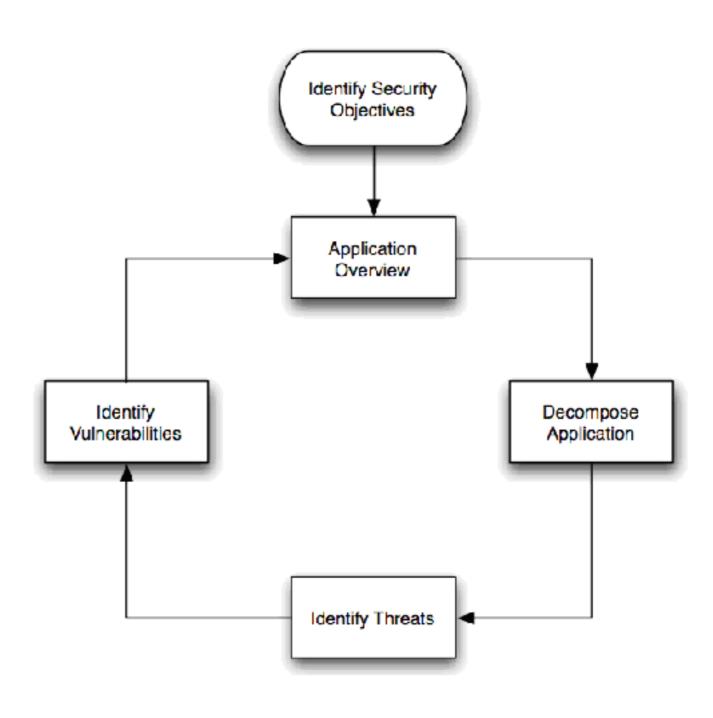
# Security is a tradeoff (contd.)

- Protection system
  - lifetime = 10 years
  - cost = 10,000 EUR
- Attack
  - yearly probability = 10%
  - cost of restoring the system = 1,000 EUR
- Do I invest?

#### Procedures!

- Protection will never be perfect
- Prepare procedures
  - what to do BEFORE an attack?
    - what to do to limit the risk (e.g., passwords) of attack and to be ready if an attack happens (e.g., backup)
  - what to do DURING an attack?
    - the attack is on going, how to stop it
  - what to do AFTER an attack?
    - the attack succeeded, how to recover from it

### Threat Risk Modelling\*



#### DREAD\*

- Damage Reproducibility Exploitability Affected users Discoverability (DREAD) is a classification scheme to assess and compare the risk presented by each evaluated threat.
- Risk\_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5
- Damage Potential (how much damage can it cause?)
  - $\blacksquare$  e.g., 0 = nothing, 5 = some, 10 = complete
- Reproducibility (how easy is it to reproduce the threat?)
  - e.g., 0 = impossible, 5 = few steps, need authentication, 10 = simple, no authentication needed.
- Exploitability (what is needed to exploit this threat?)
  - e.g., 0 = advanced tools and knowledge, 4 = using public attack tools, 10 = just a web browser
- Affected users (how many users will be affected?)
  - e.g., 0 = none, 5 = some, 10 = all users
- Discoverability (how easy is it to discover this threat?)
  - e.g., 0 = very hard, 5 = need monitoring, 9 = documented publicly, 10 = visible in the address bar.

## Securing communications

### Objective

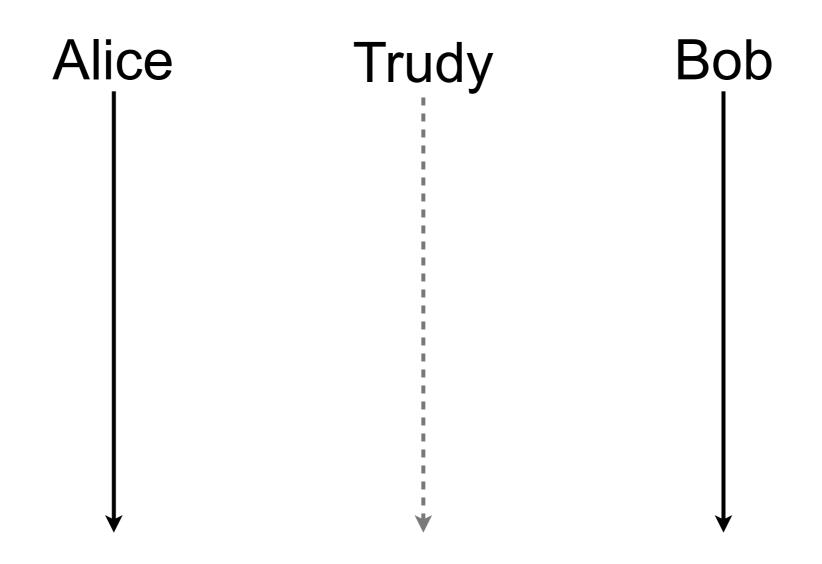
- Construct a communication mechanism where Alice and Bob can exchange messages such that
  - only Alice and Bob can generate messages
  - nobody else than Alice or Bob can read messages
  - nobody can alter messages

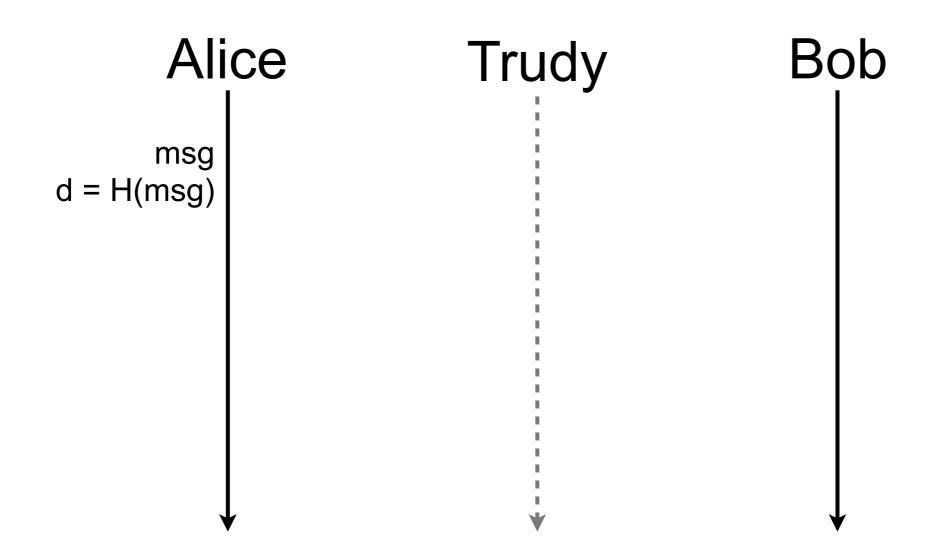
## Steps

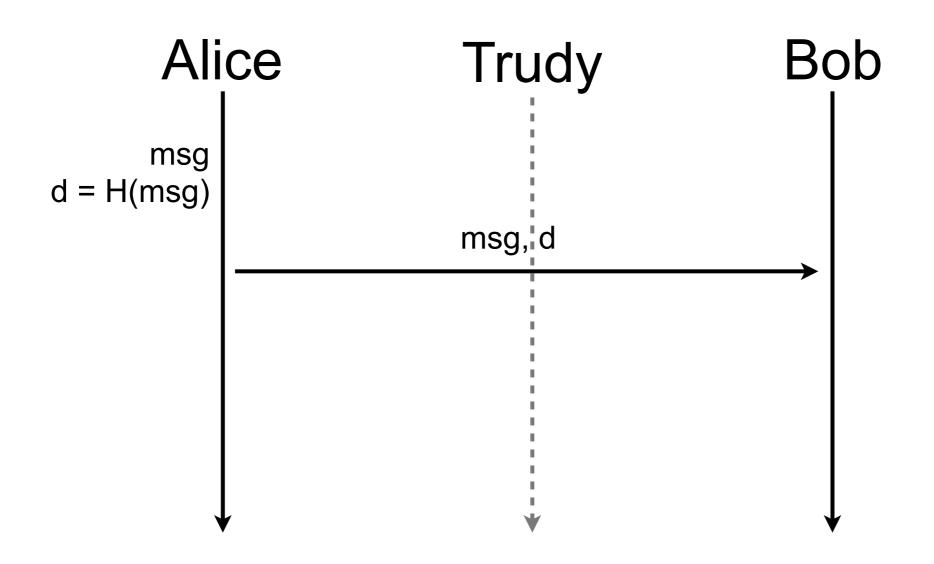
- fill me
- fill me
- fill me

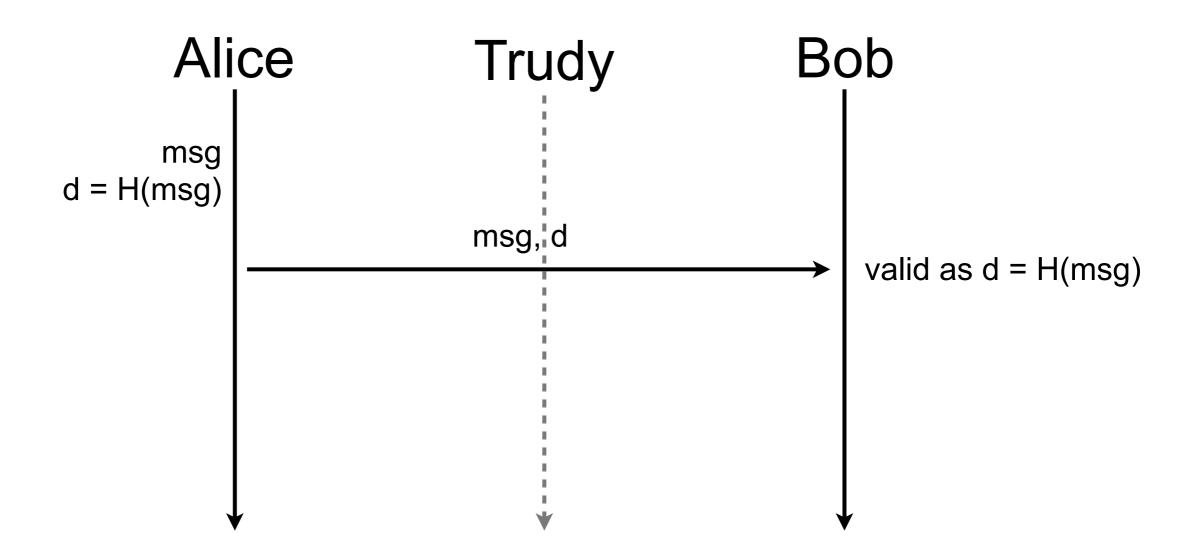
#### Hash function

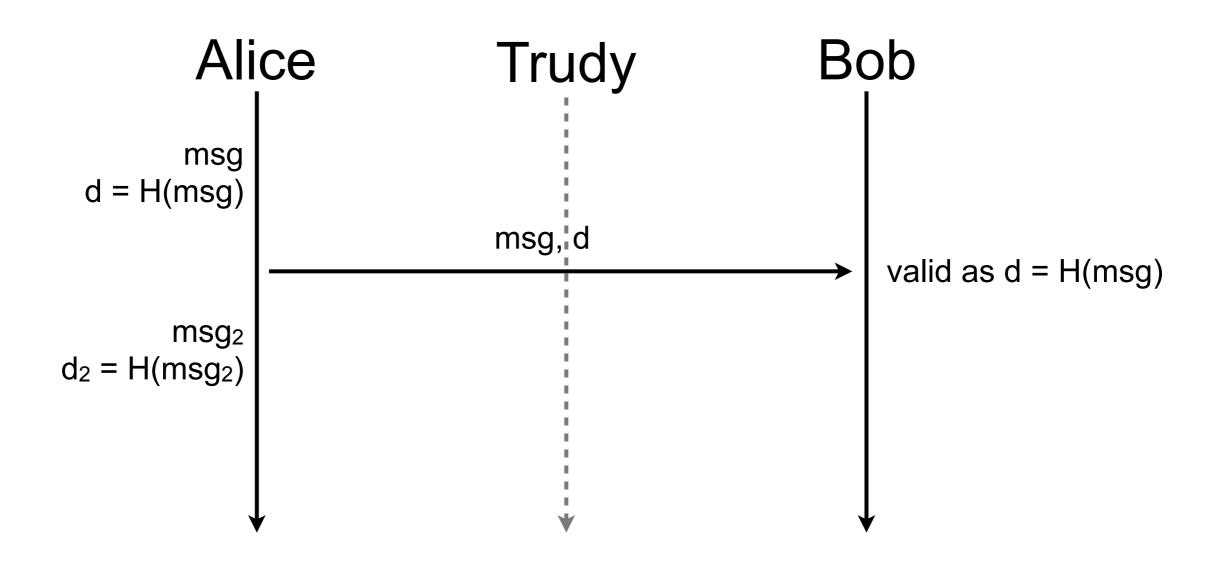
- Validate that a message has not been altered on its way between Alice and Bob
- Hash functions map arbitrary large numbers of variable length to fixed-length numbers
  - h = H(m), h is called hash or digest
  - e.g., MD5, SHA-1, SHA-256
- Good hash functions for cryptography must be such that
  - H(m) is not complex to compute
  - but finding a m<sub>2</sub> such that H(m<sub>2</sub>) = H(m) is complex,
  - H(m) is deterministic,
  - H output must be evenly distributed over the output set
- Example
  - SHA-1 maps messages its input space on a 160-bits output
    - SHA-1(Message to validate) = 5e06ee754bda0d33cf65ec305ffc779404e66029
    - SHA-1(Message t**Q** validate) = b1c306f8cb792fa14d4d1fdcf6f37d86c2fe6bb9

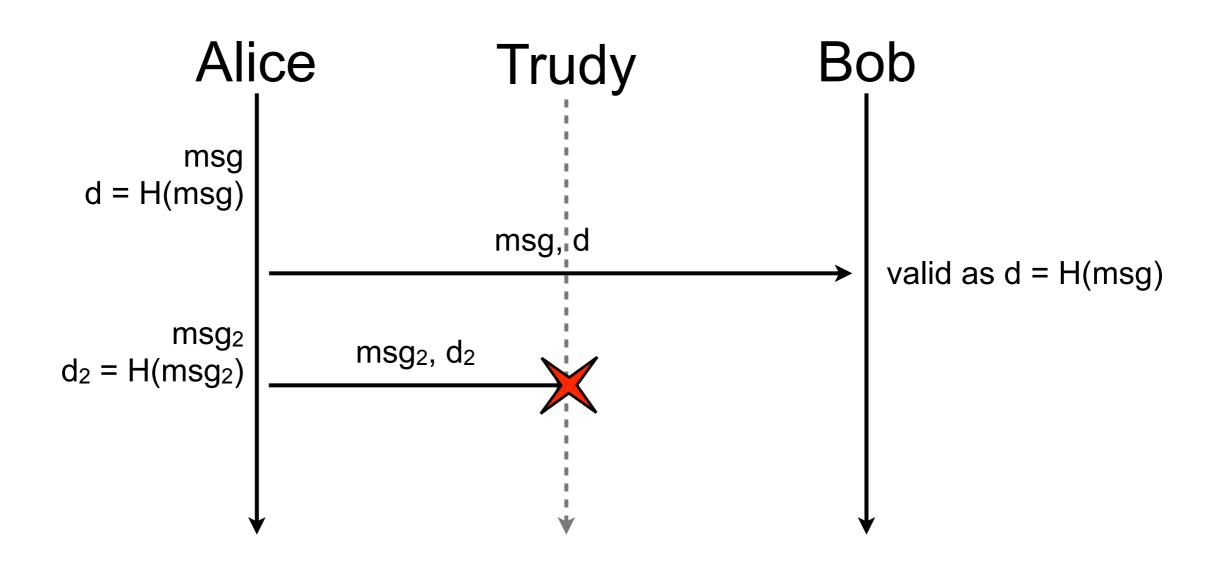


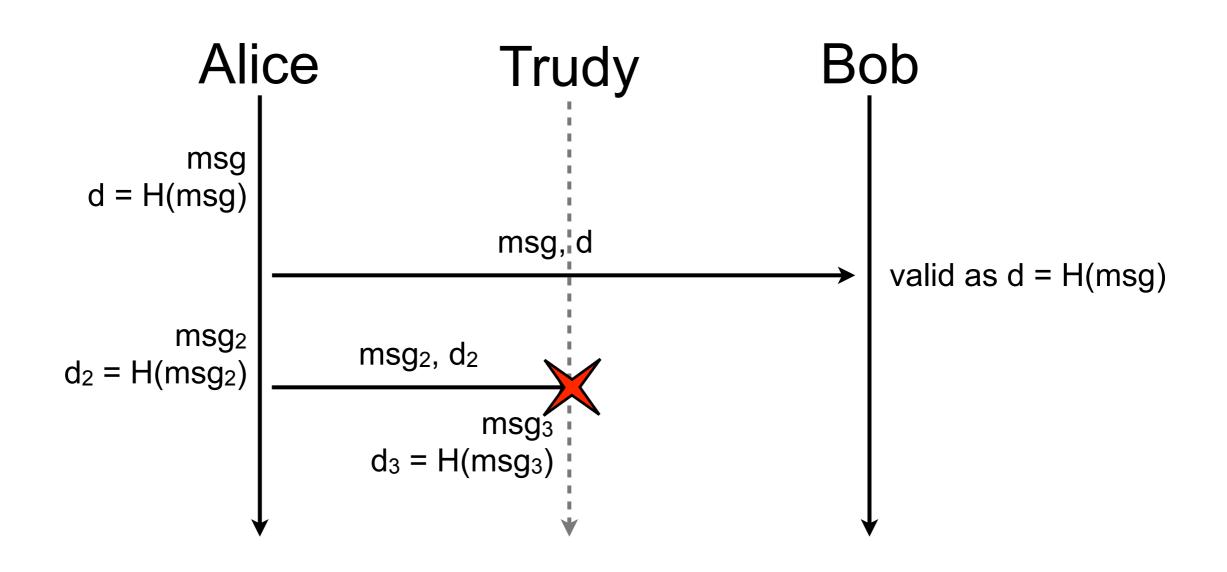


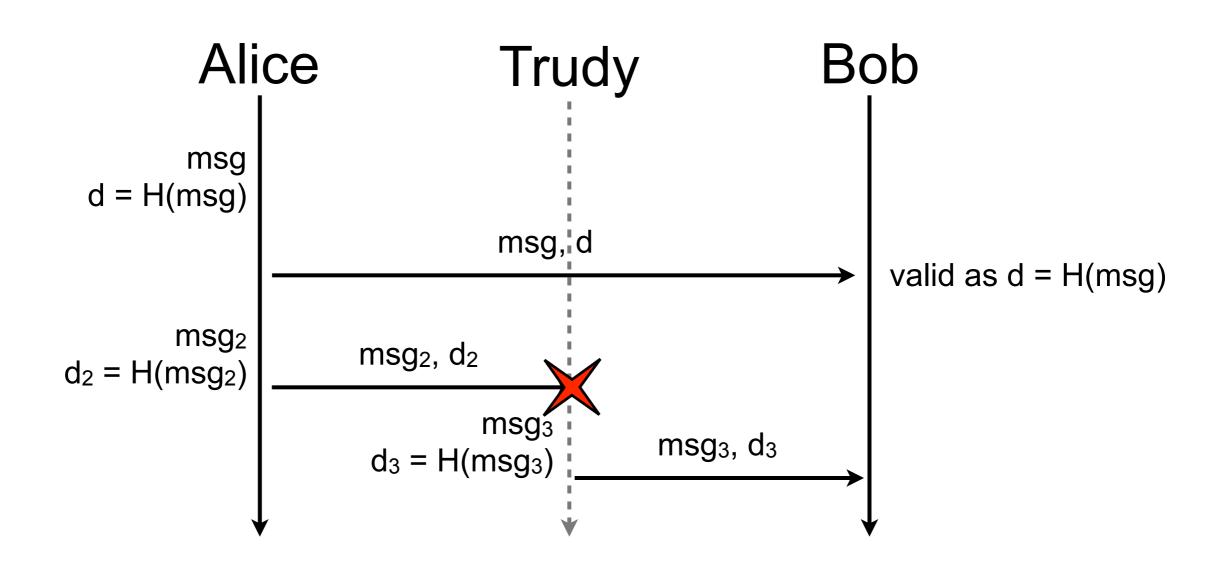


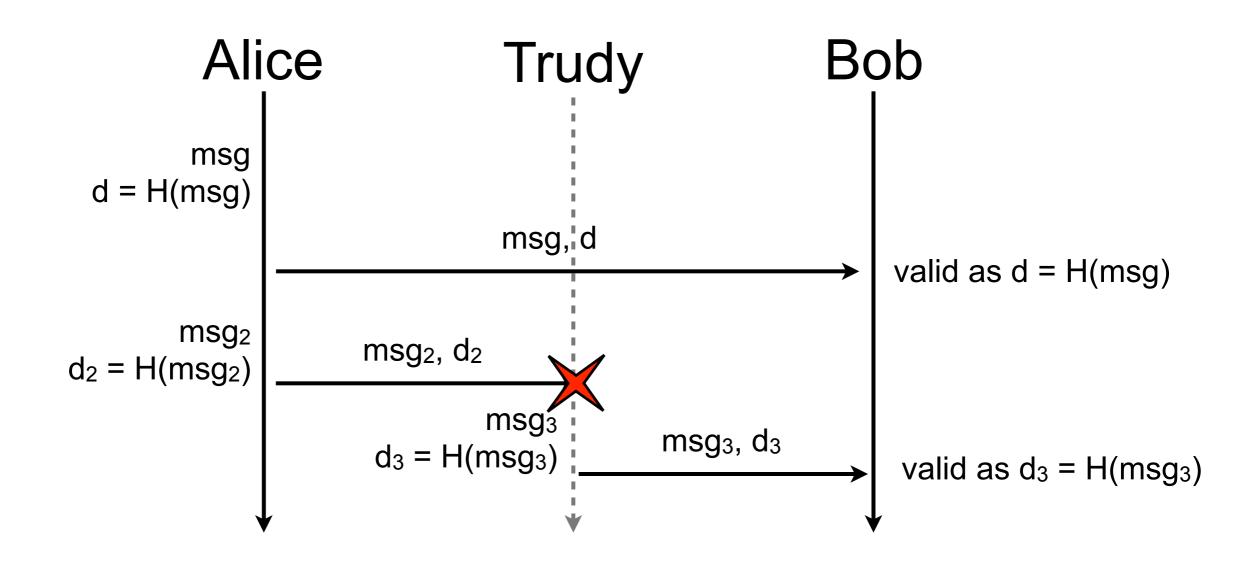






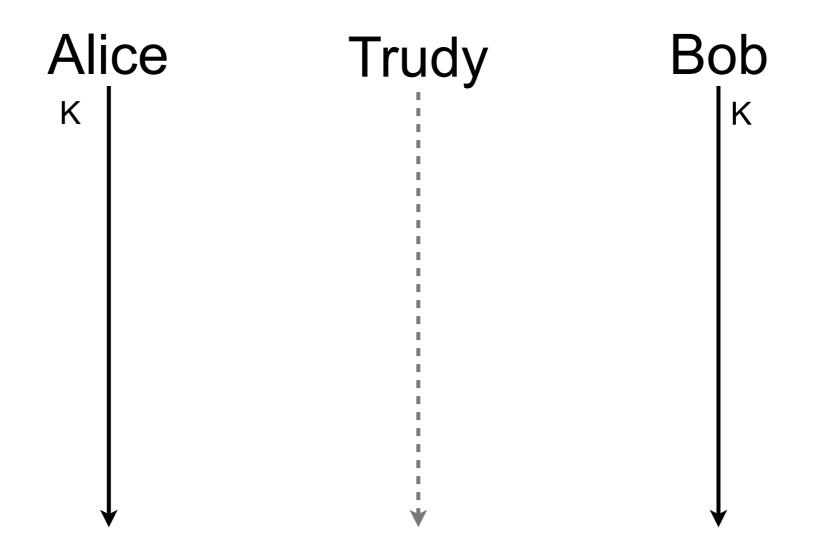


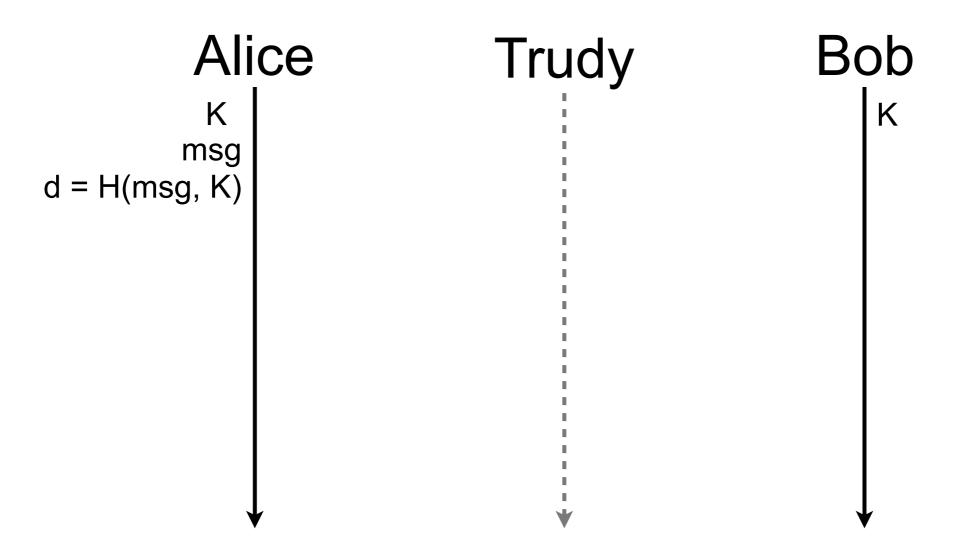


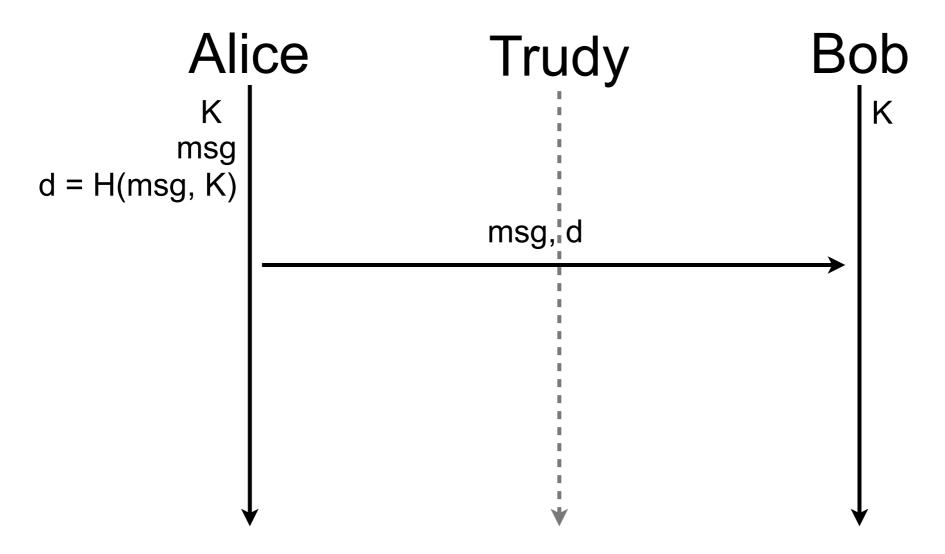


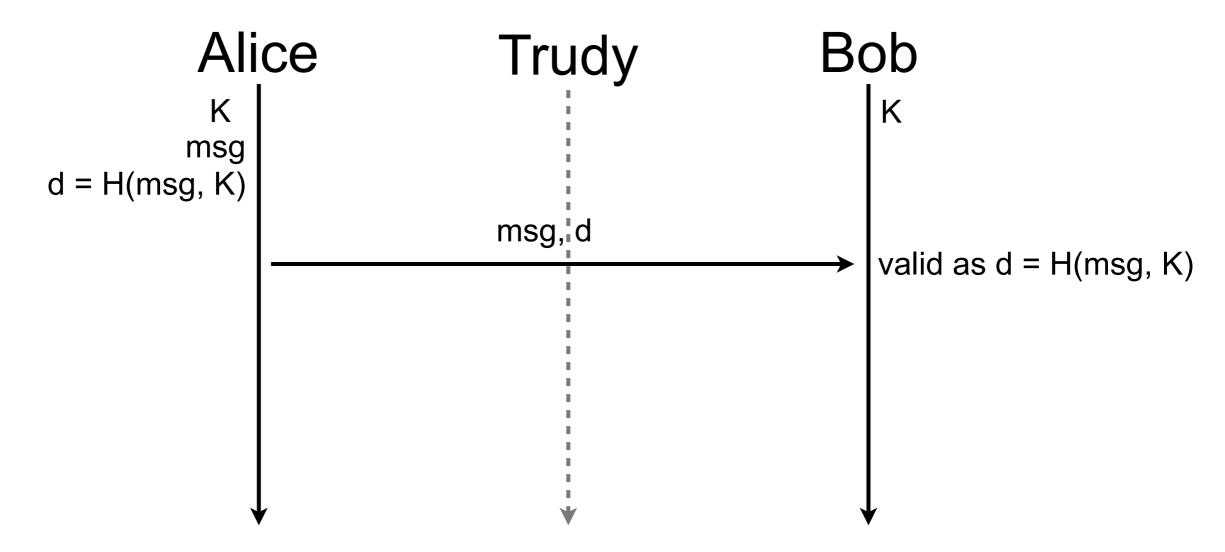
#### Hash function with salt

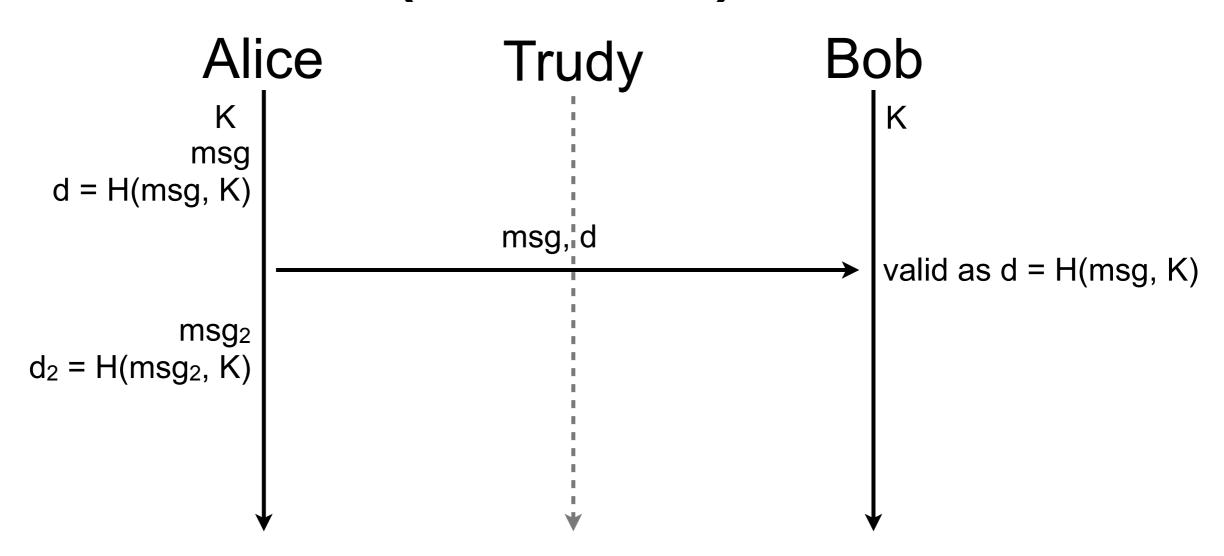
- Hash functions are deterministic
- Add a salt such that the output of the hash function is a function of the message and the salt
  - h = H(m, K) where K is the salt or key of the hash function
- As long as Trudy does not know the salt, she can't forge a valid digest

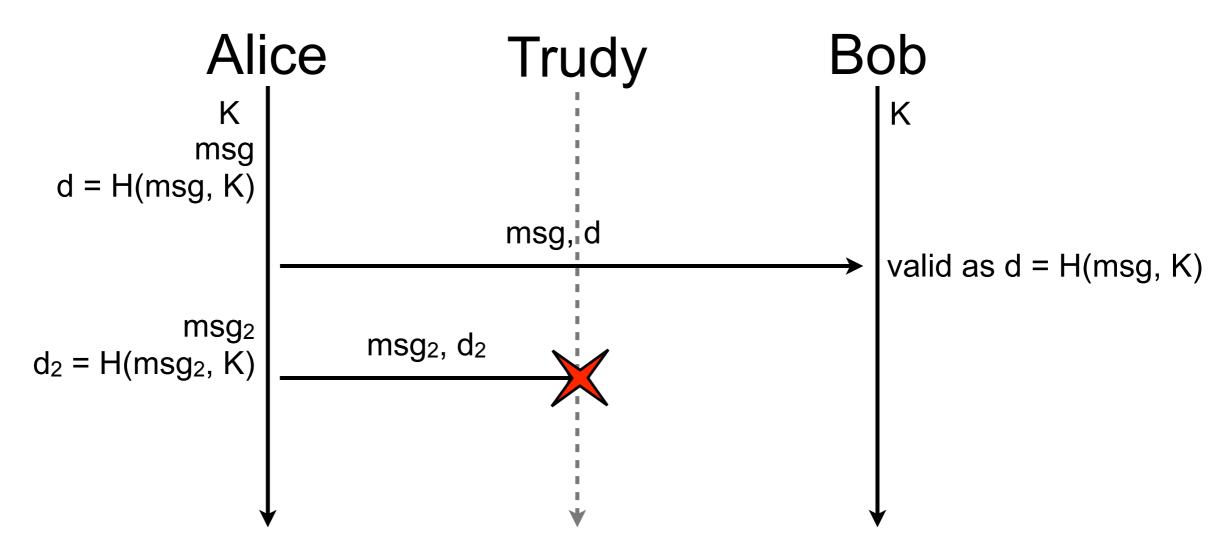


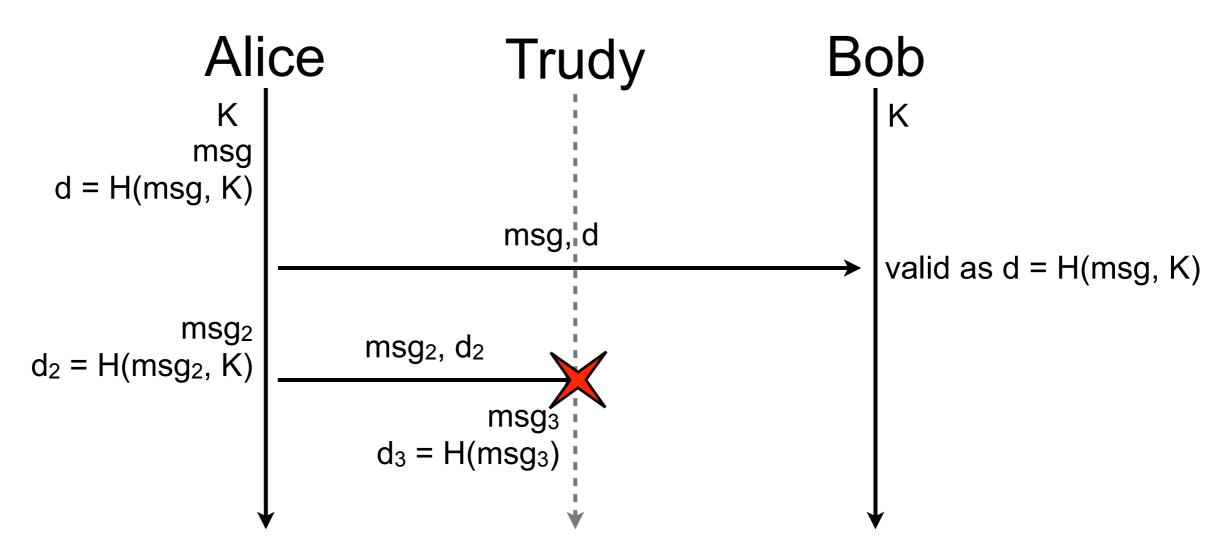


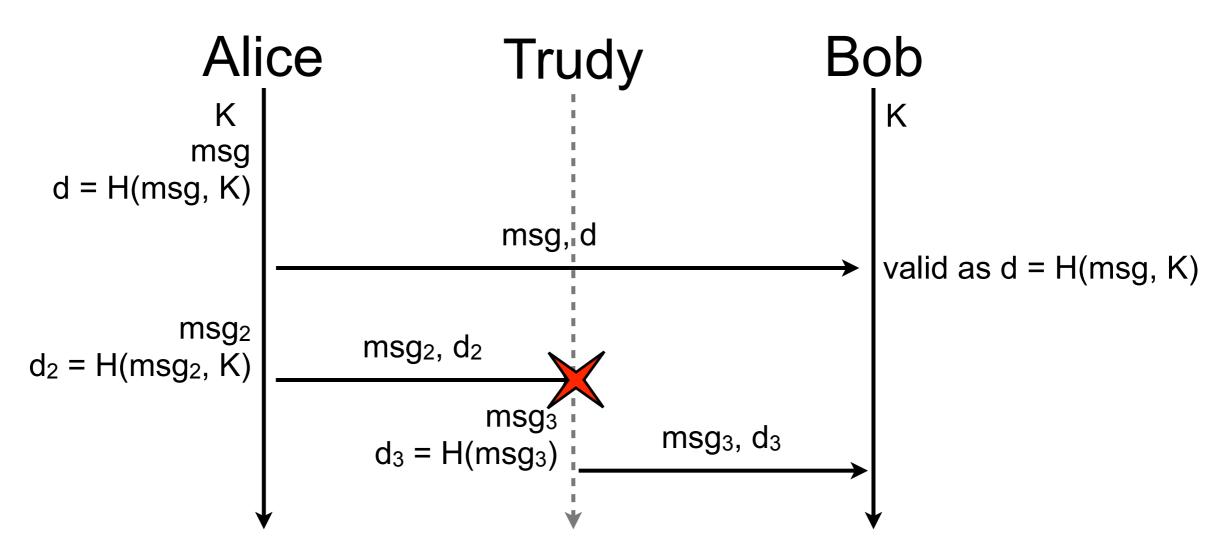


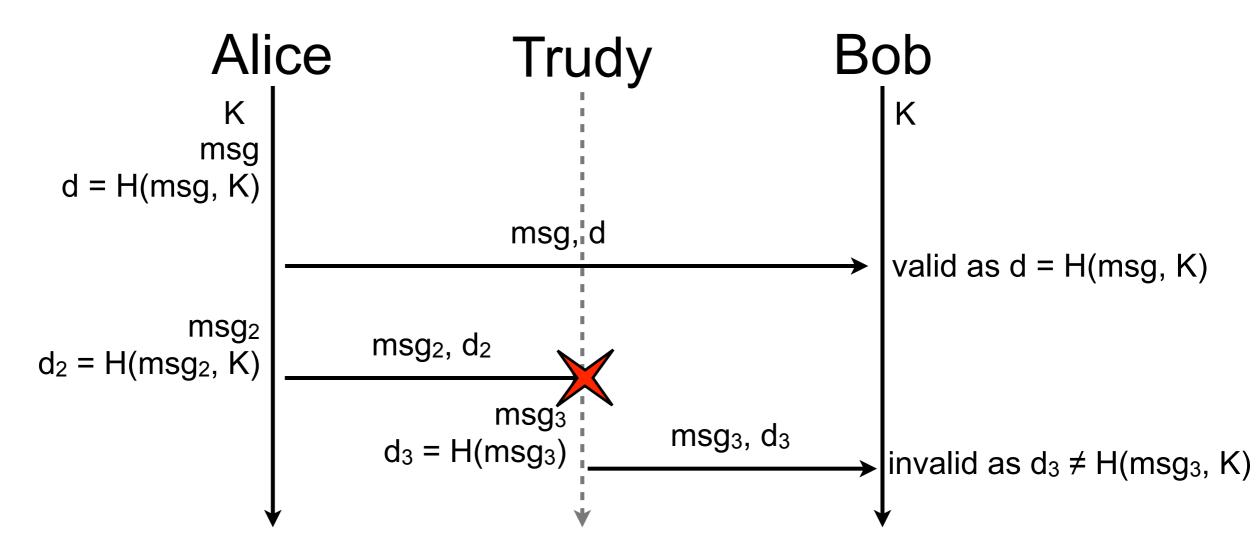












### Problem solved?

- fill me
- fill me
- fill me

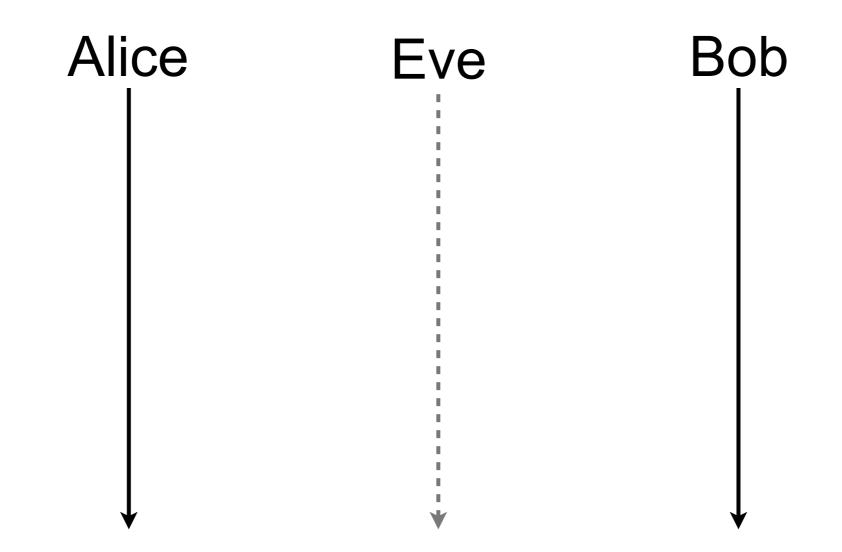
### Problem solved?

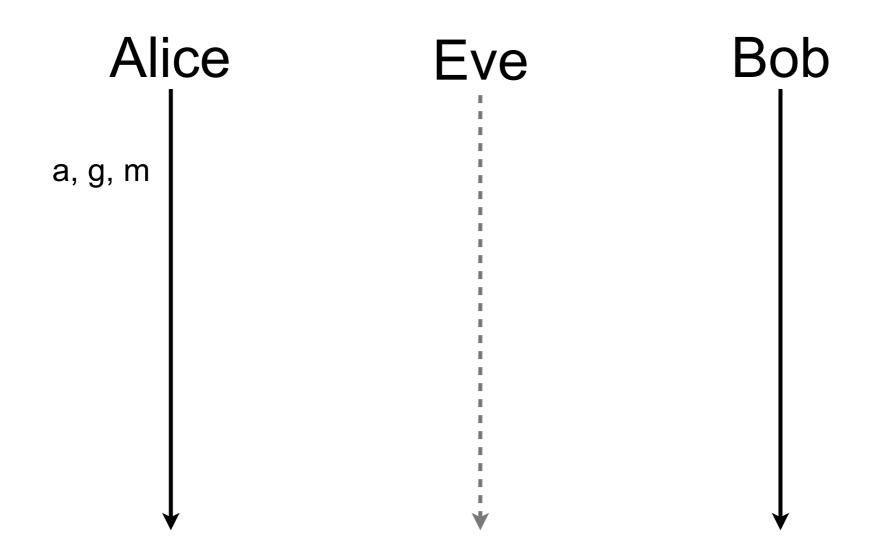
- fill me
- fill me
- fill me

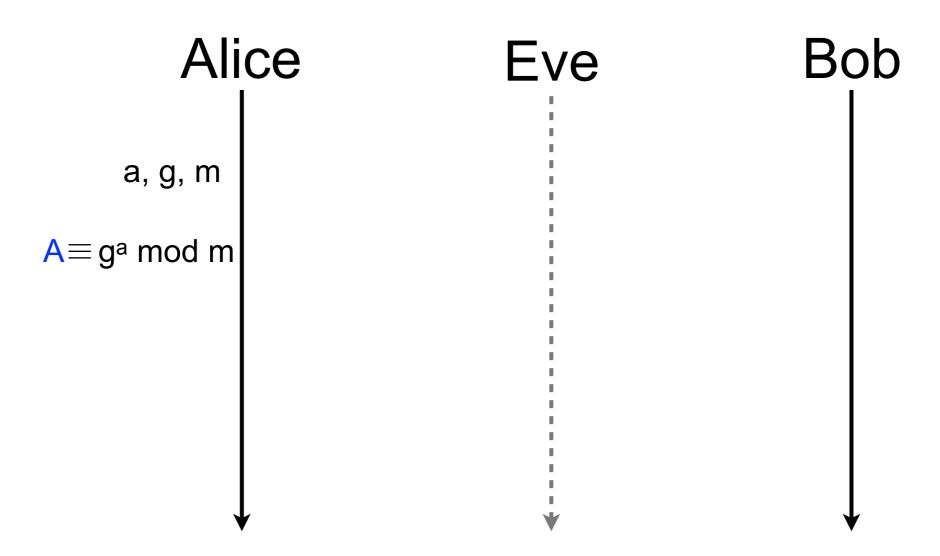
How can Alice and Bob agree on K?

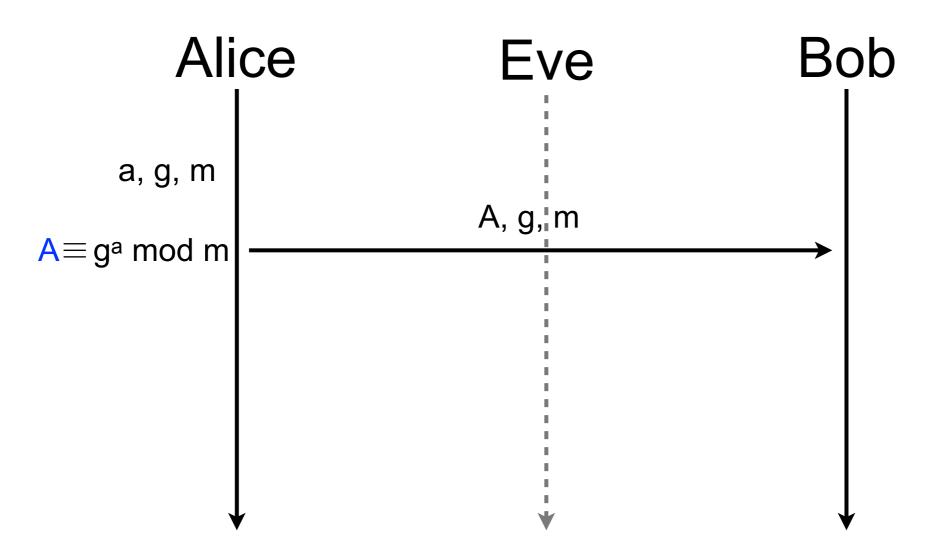
# Diffie-Hellman key exchange

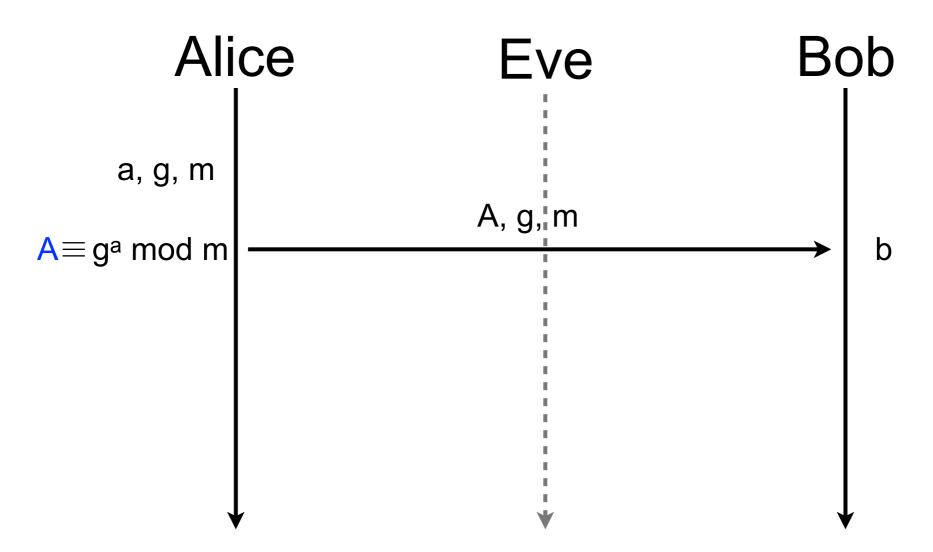
- How can Alice and Bob agree on a secret number and be sure that Eve will not discover it?
- Principle
  - do not exchange the secret number but other numbers that are use to build up the secret

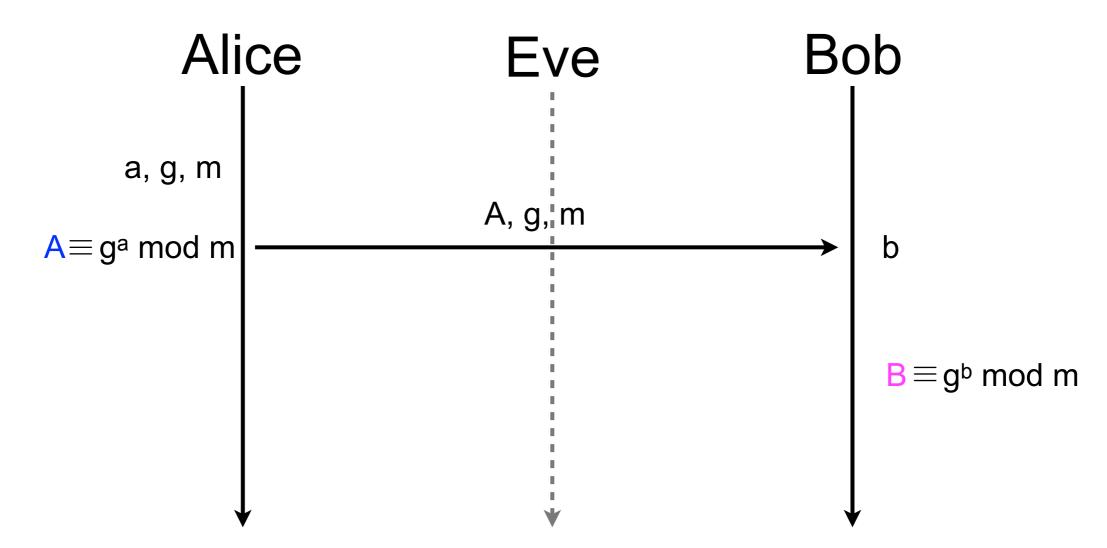


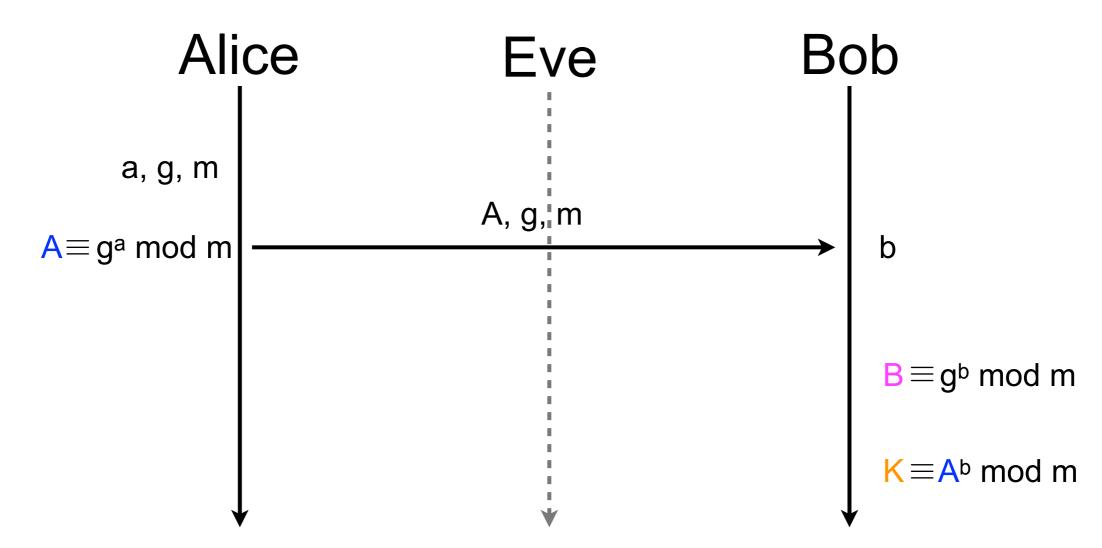


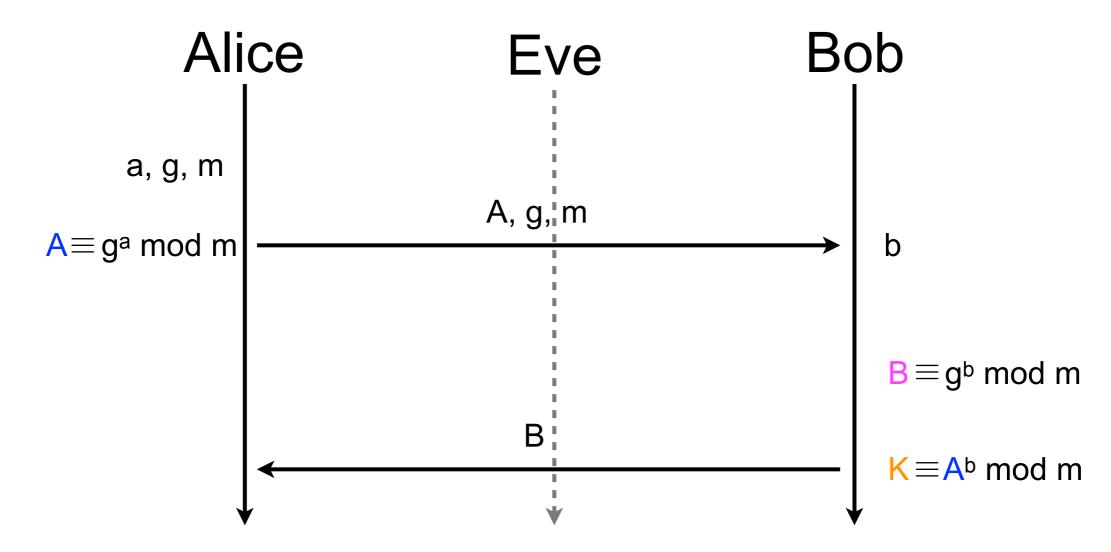


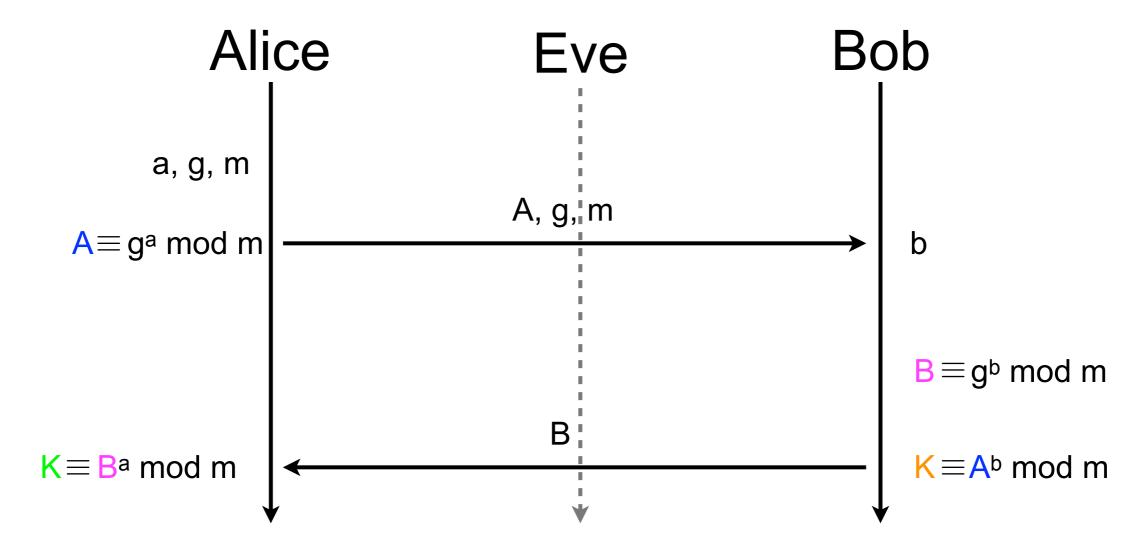




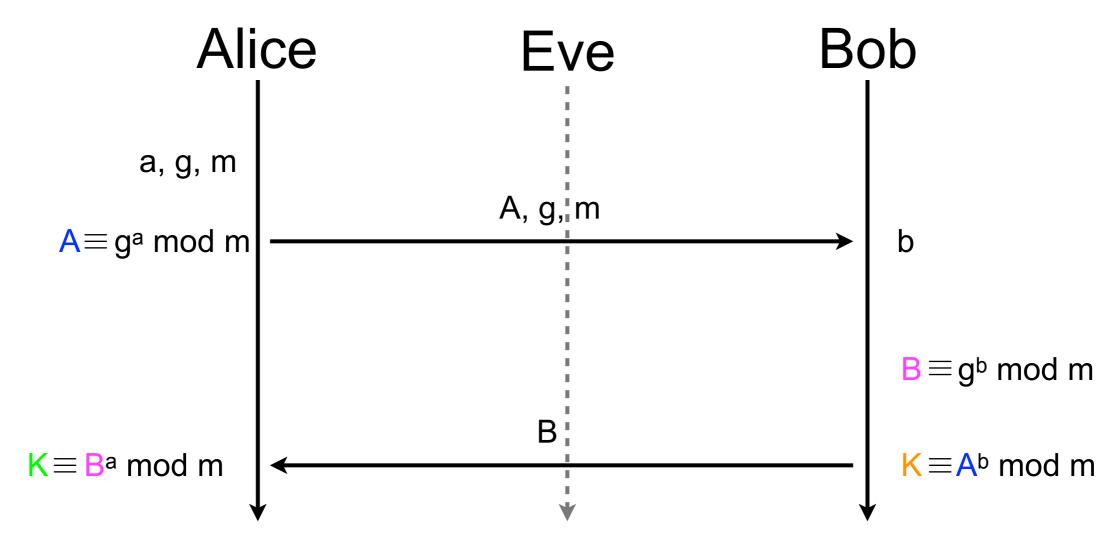








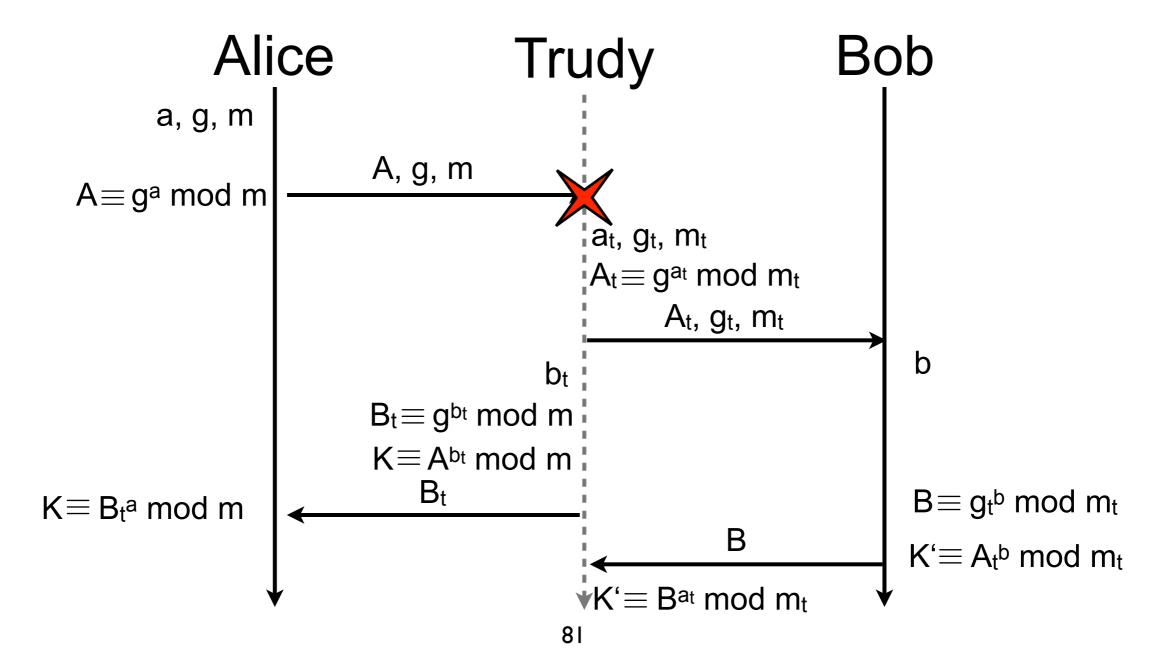
Working on finite group and positive integers



 $K \equiv A^b \mod m \equiv (g^a \mod m)^b \mod m \equiv g^{ba} \mod m \equiv (g^b \mod m)^a \mod m \equiv B^a \mod m \equiv K$ 

- Why can't Eve guess K if she knows A, B, g, and m?
  - discrete exponentiation is linear with the size of the argument
    - easy to compute  $x \equiv y^z \mod p$
  - but for some discrete groups, no efficient algorithm is known to compute discrete logarithm
    - hard to determine natural z that ensures  $x \equiv y^z \mod p$
  - Eve knows A, B, g, and m but can't determine neither a nor b that are absolutely necessary to compute K
    - $K \equiv A^b \mod m \equiv (g^a \mod m)^b \mod p \equiv g^{ba} \mod m$  $\equiv (g^b \mod m)^a \mod m \equiv B^a \mod m$

Trudy can break Diffie-Hellman



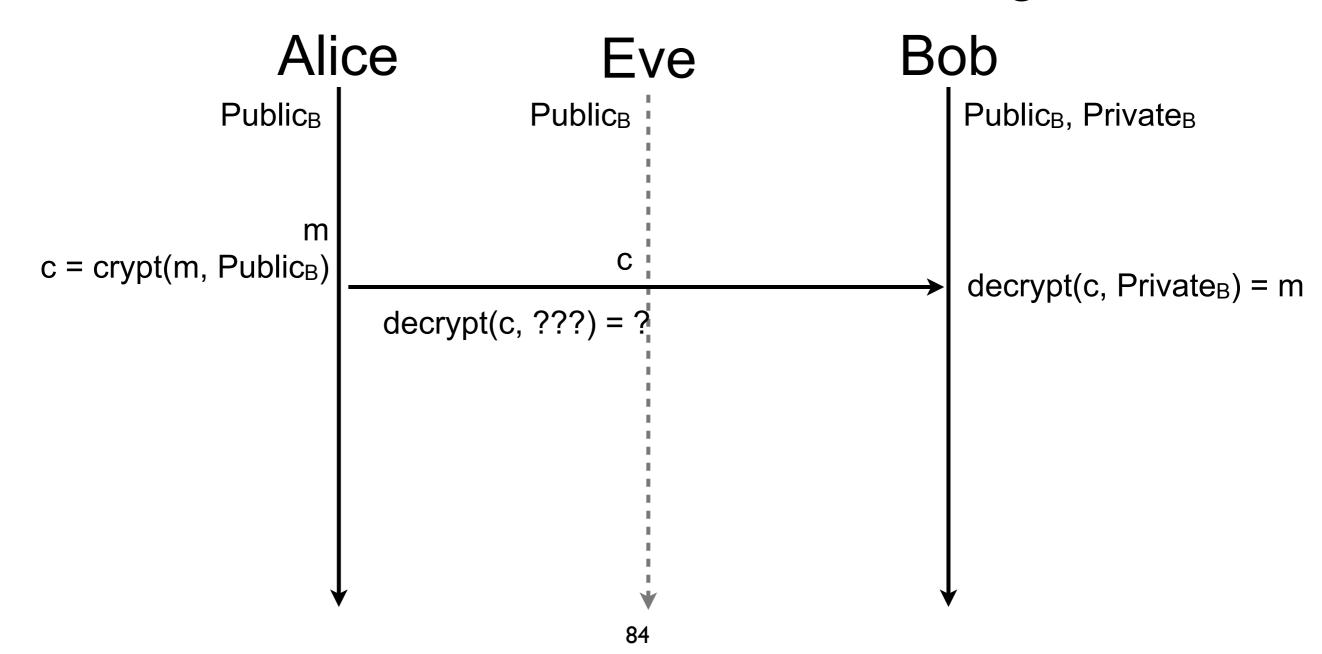
- How can we protect Diffie-Hellman from Trudy?
- Principle
  - Alice and Bob sign the messages exchanged in Diffie-Hellman (?!)

# Asymmetric cryptography

- In asymmetric cryptography (aka public-key cryptography), two keys are used
  - public key
    - publicly available to anybody (even attackers)
    - used to encrypt a message
  - private key
    - known only by the legitimate owner of the public key
    - used to decrypt a message
- e.g., RSA, PGP, Diffie-Hellman
- Public-key cryptography is 10 to 100 times slower than symmetric-key cryptography
  - seldom (never?) used to encrypt communications

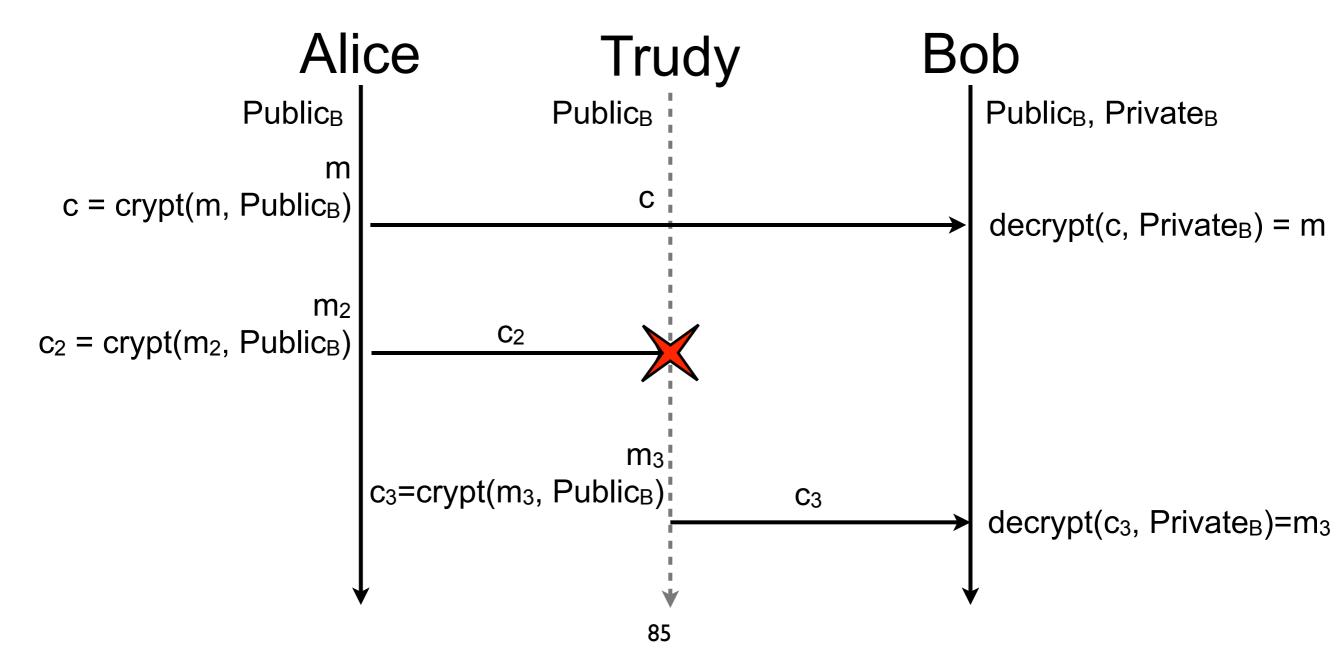
# Asymmetric cryptography (contd.)

Eve cannot determine the message



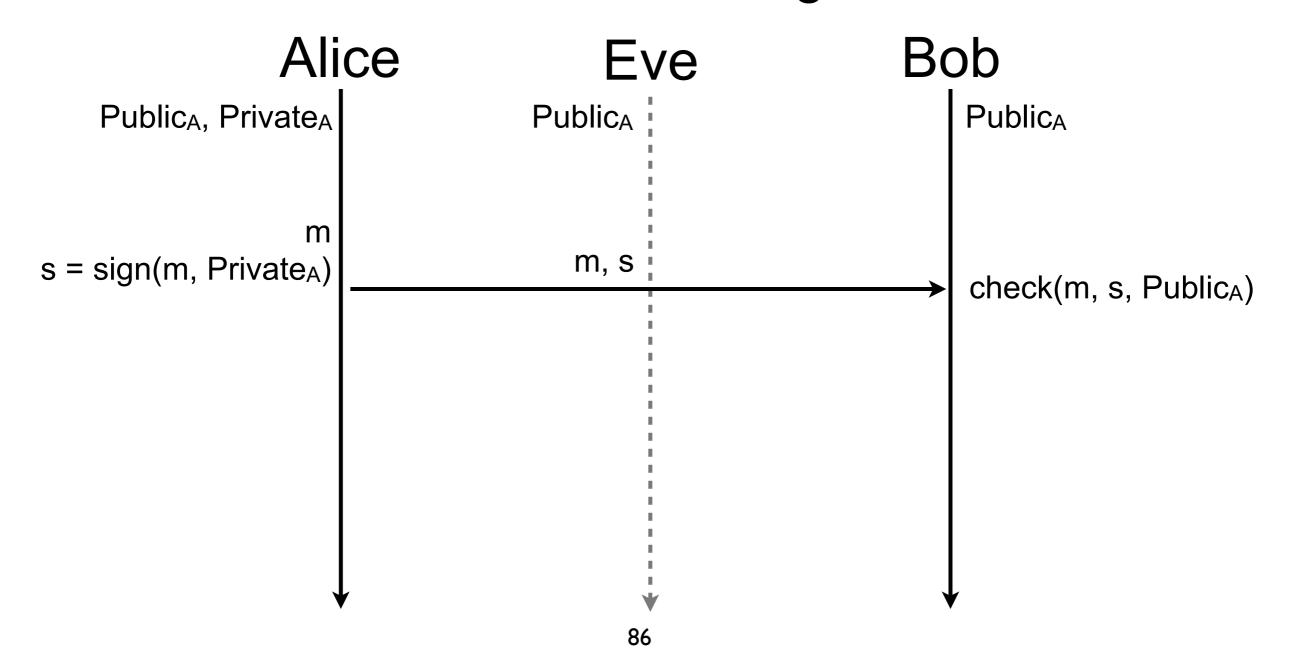
# Asymmetric cryptography (contd.)

Trudy can send a forged message



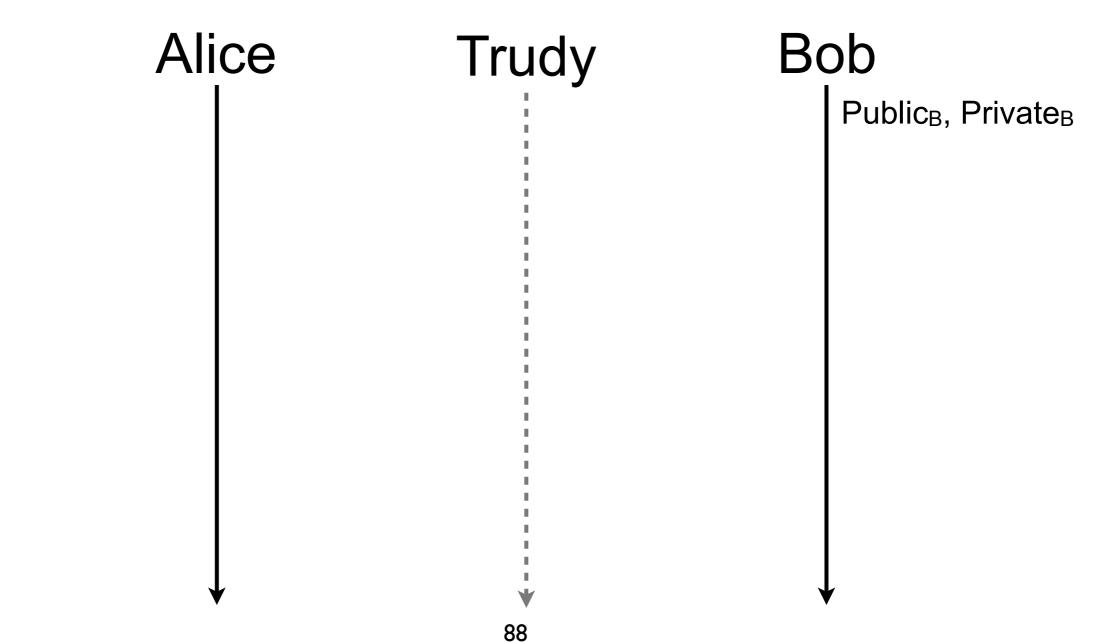
## Asymmetric cryptography (contd.)

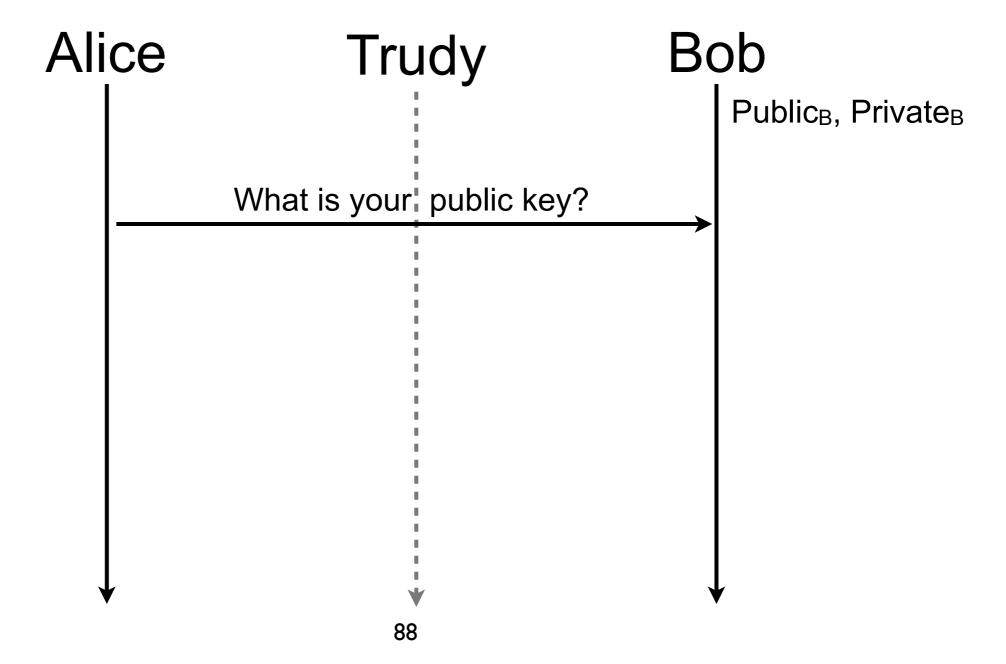
Eve can read the message

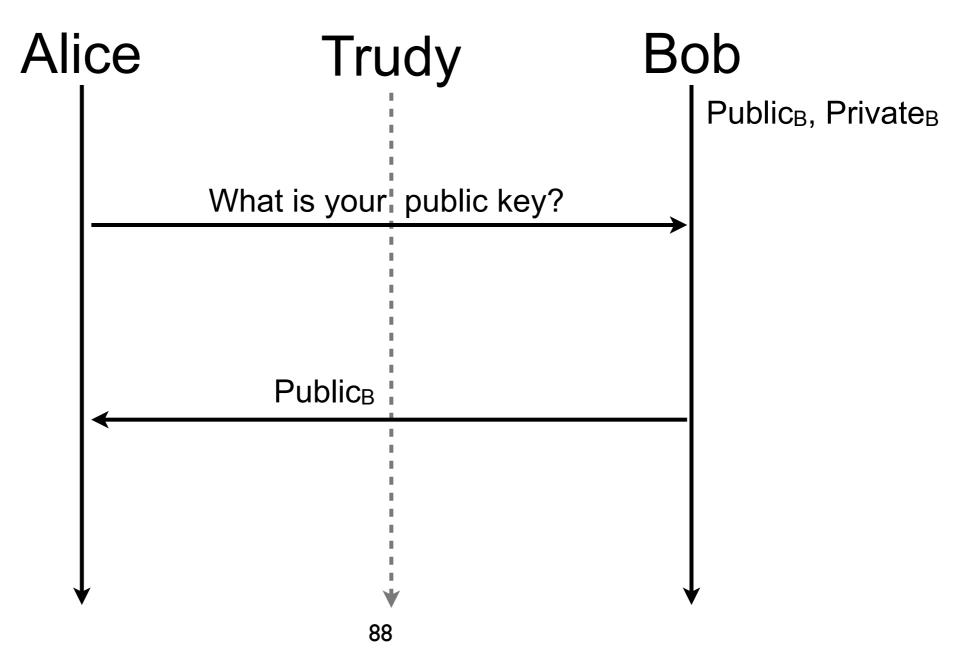


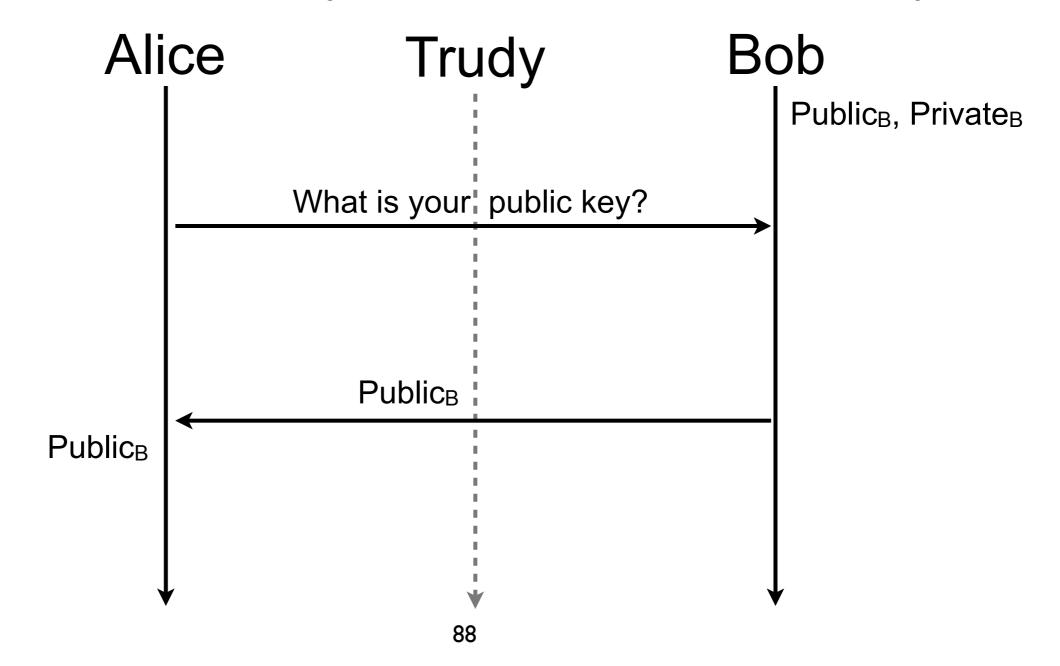
### How to build sign and check?

- $\blacksquare$  s = sign(H(m), k) = crypt(H(m), k)
- check(m, s, K) = (H(m)==decrypt(s, K))
  - where k is the private key of the signer and K is the public key
- Asymmetric cryptography is slow and m can be large
  - encrypting m would be too costly
  - solution: consider the digest of m while signing

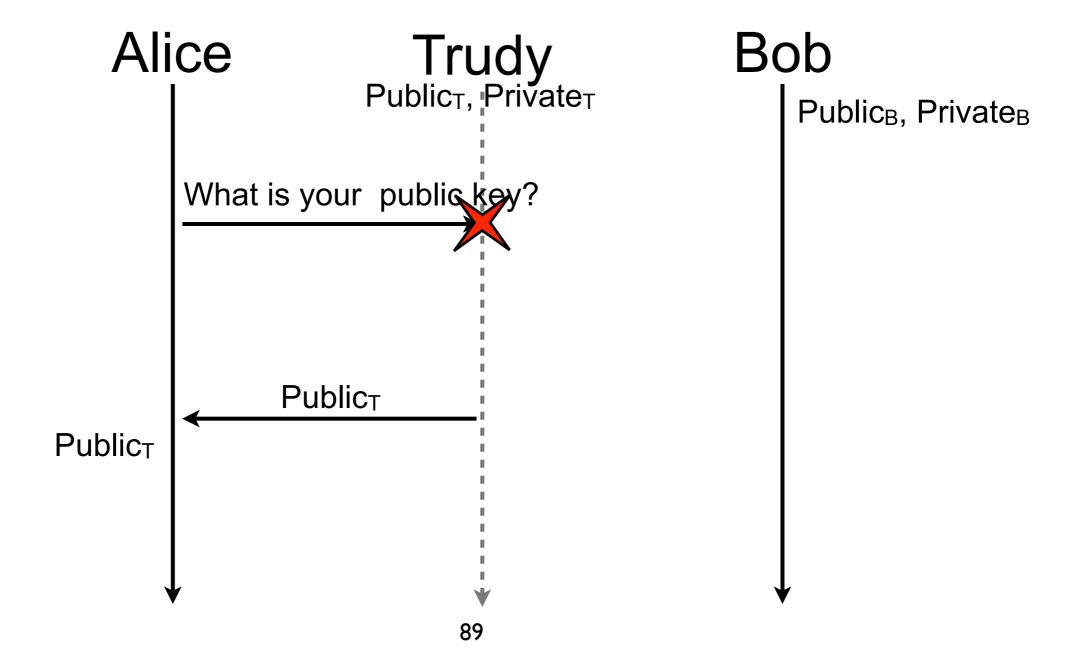




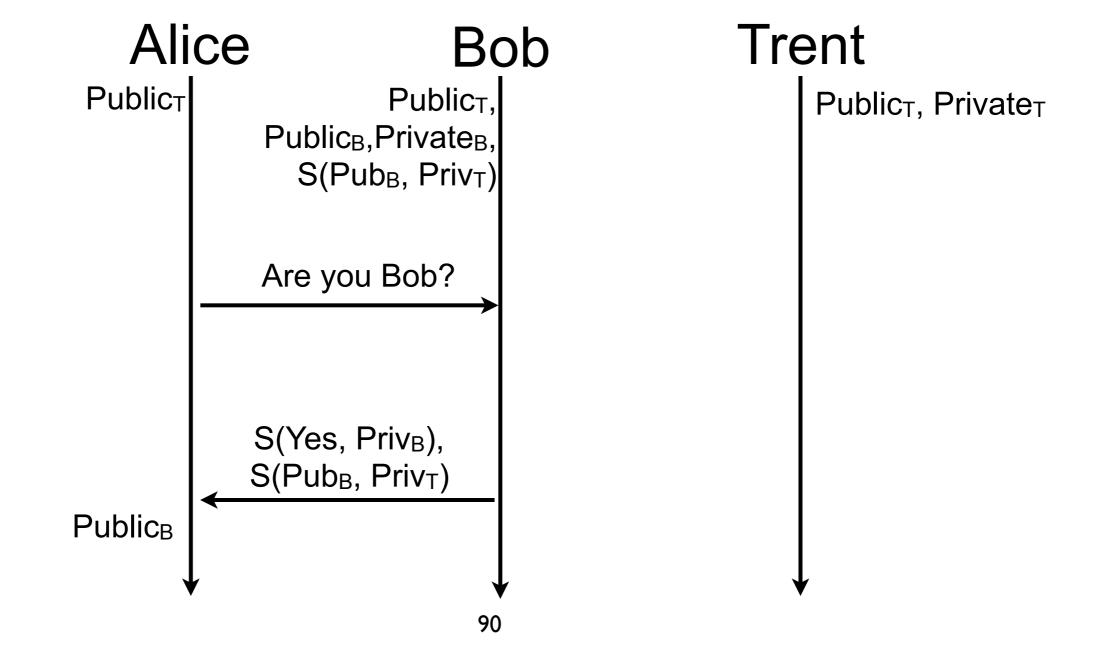




Trudy can send a forged key



Alice and Bob trust a third party (e.g., Trent) for authentication



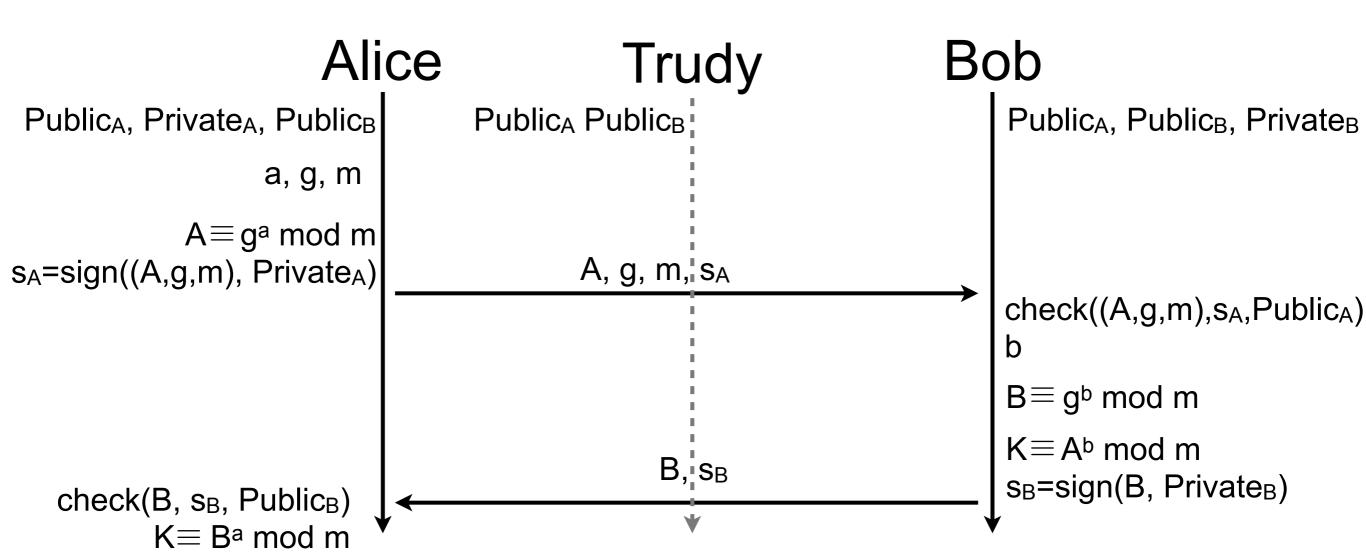
- Practically, Bob sends a certificate (e.g., X.509), not only its public key and signature
- A certificate provides many information to be able to correctly identify and authenticate its subject (e.g., Bob)
  - the subject name and organization
  - the subject public key (and type)
  - the issuer name and organization
  - the certificate validity time (valid not before and not after)
  - the certificate signature and type, signature made by the issuer of the certificate

...

- Certificates are issued once and valid during a given time period, whatever the number of time it is used
- What if the subjects leaves its organization? The private key of the subject is stolen? The private key of the issuer is stolen?
- When a certified key is compromised, the certificate is revoked
  - the issuer maintains the list of revoked certificates
  - that should be checked by the client.

# Diffie-Hellman key exchange (the return)

Trudy cannot perform her attack anymore



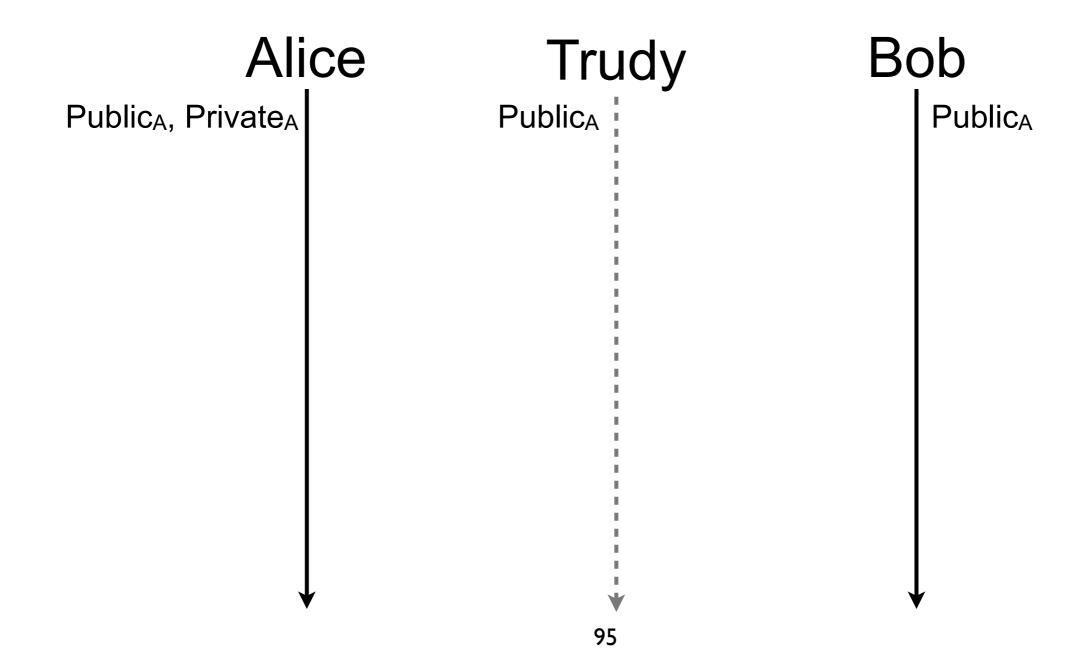
#### Problem solved?

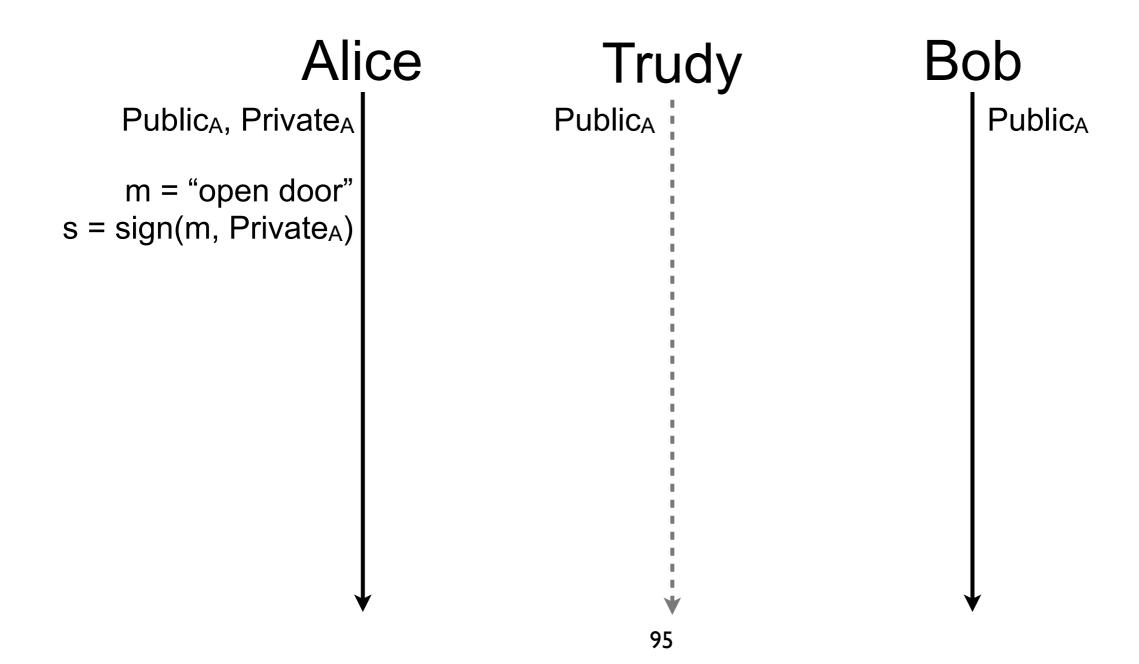
- fill me
- fill me
- fill me

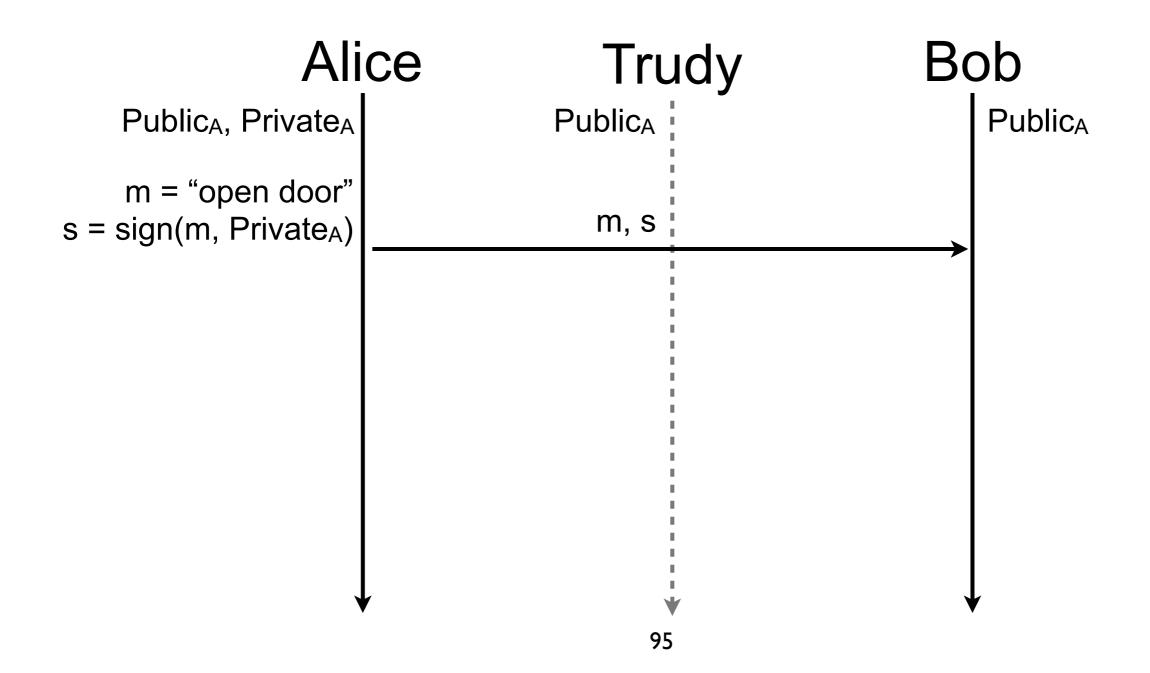
#### Problem solved?

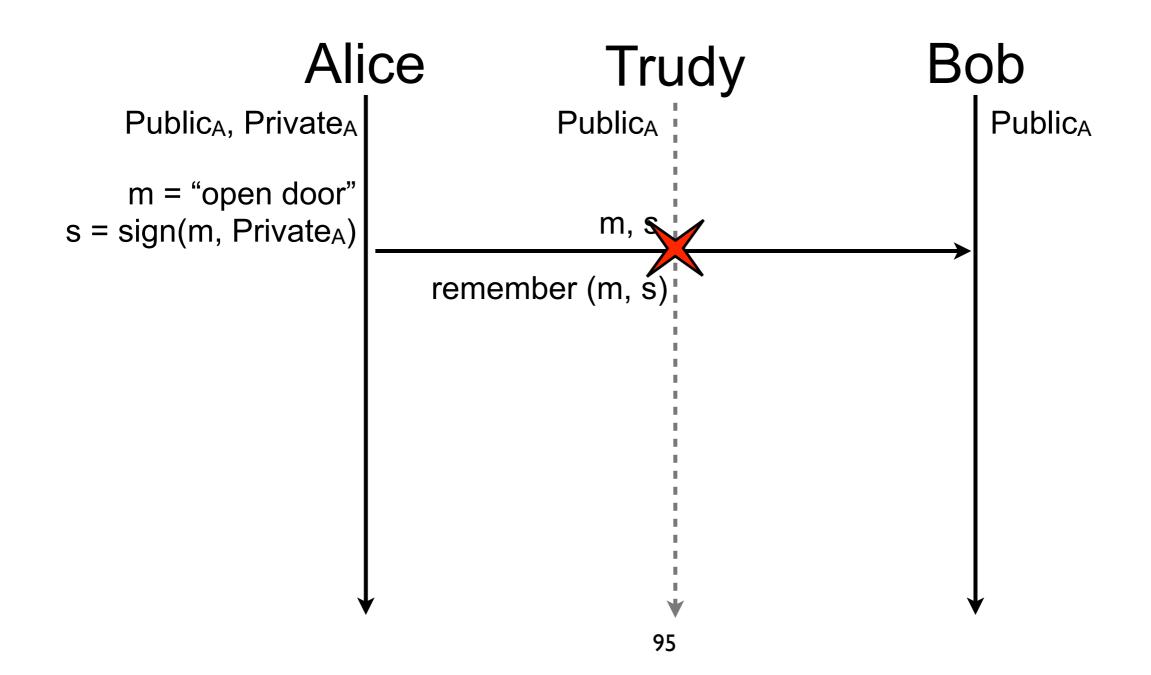
- fill me
- fill me
- fill me

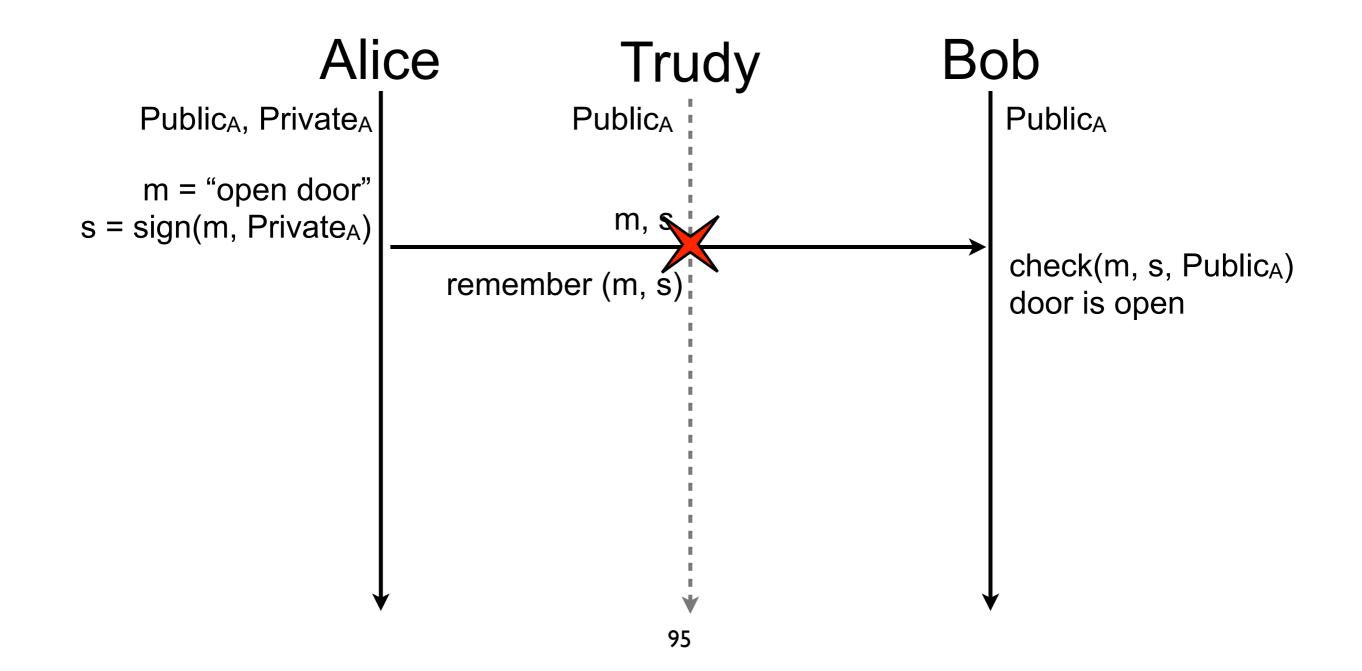
Replay attacks are still possible!

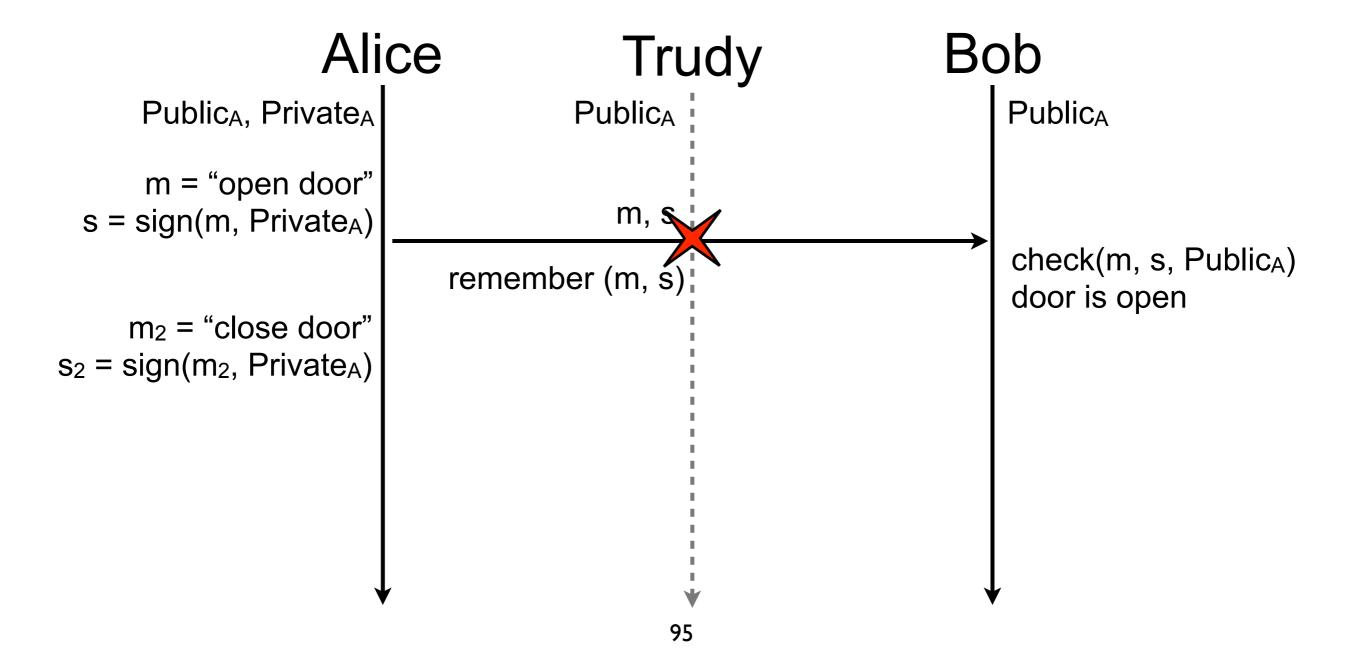


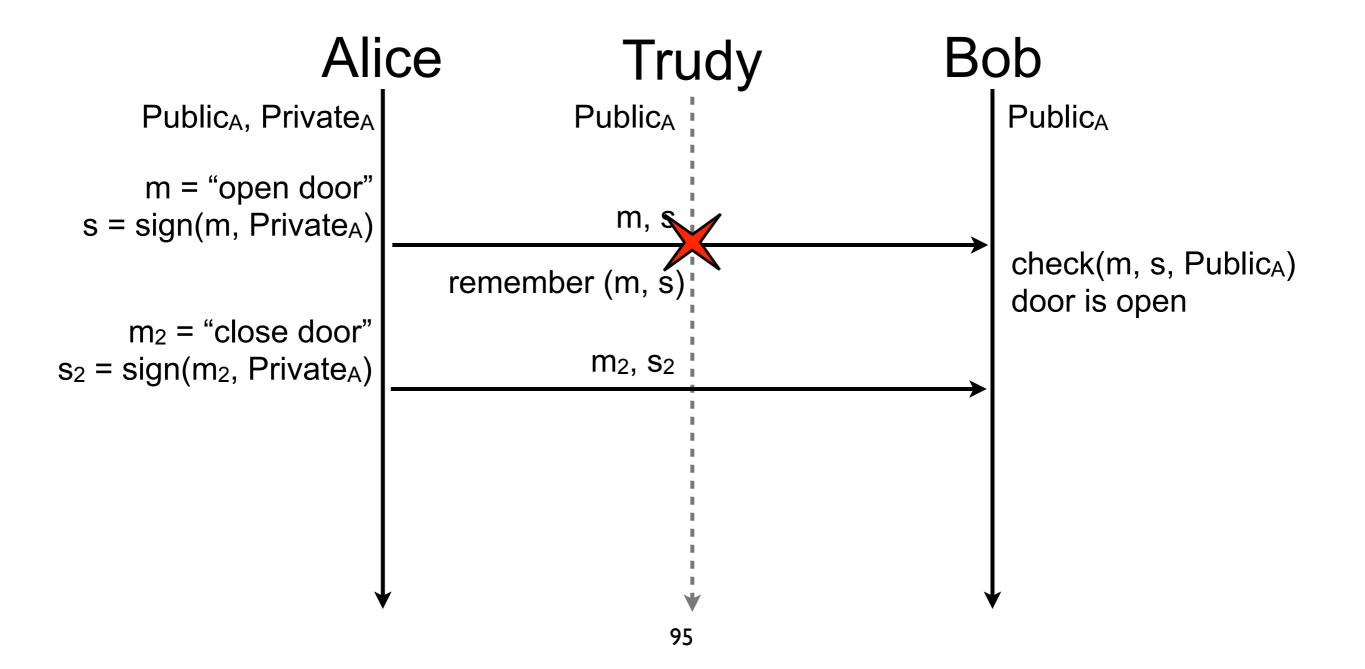


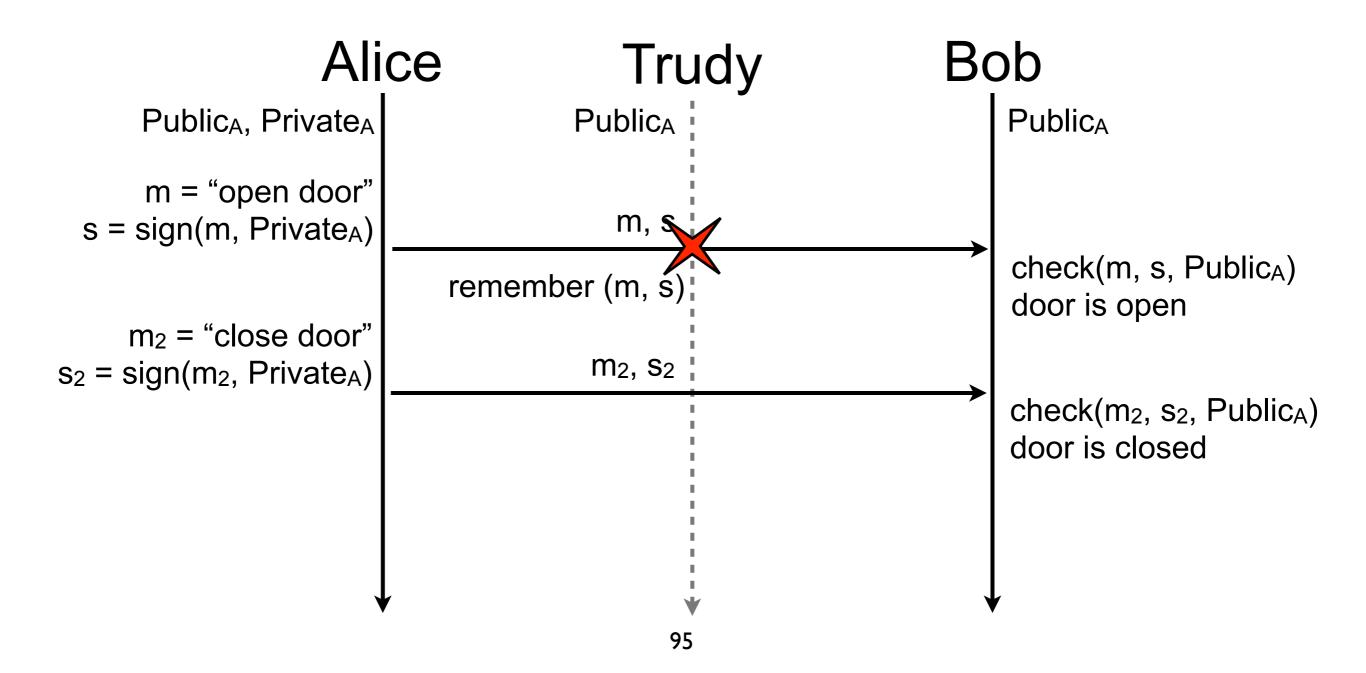


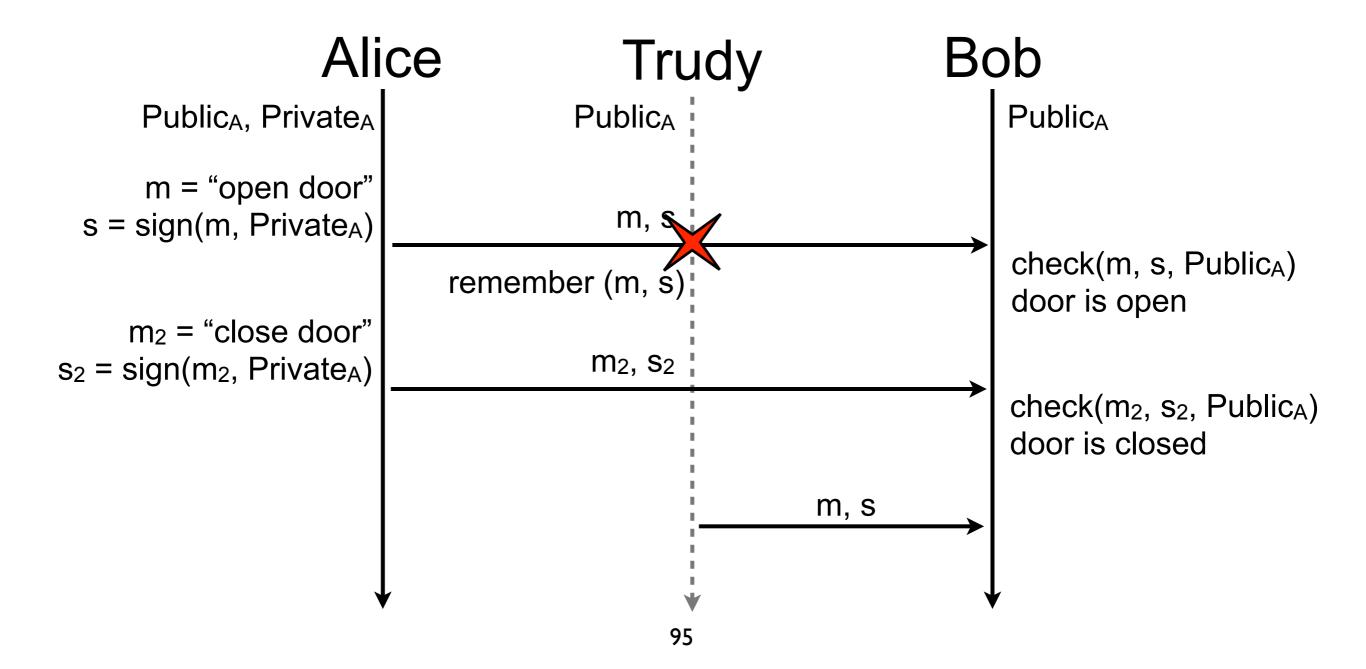


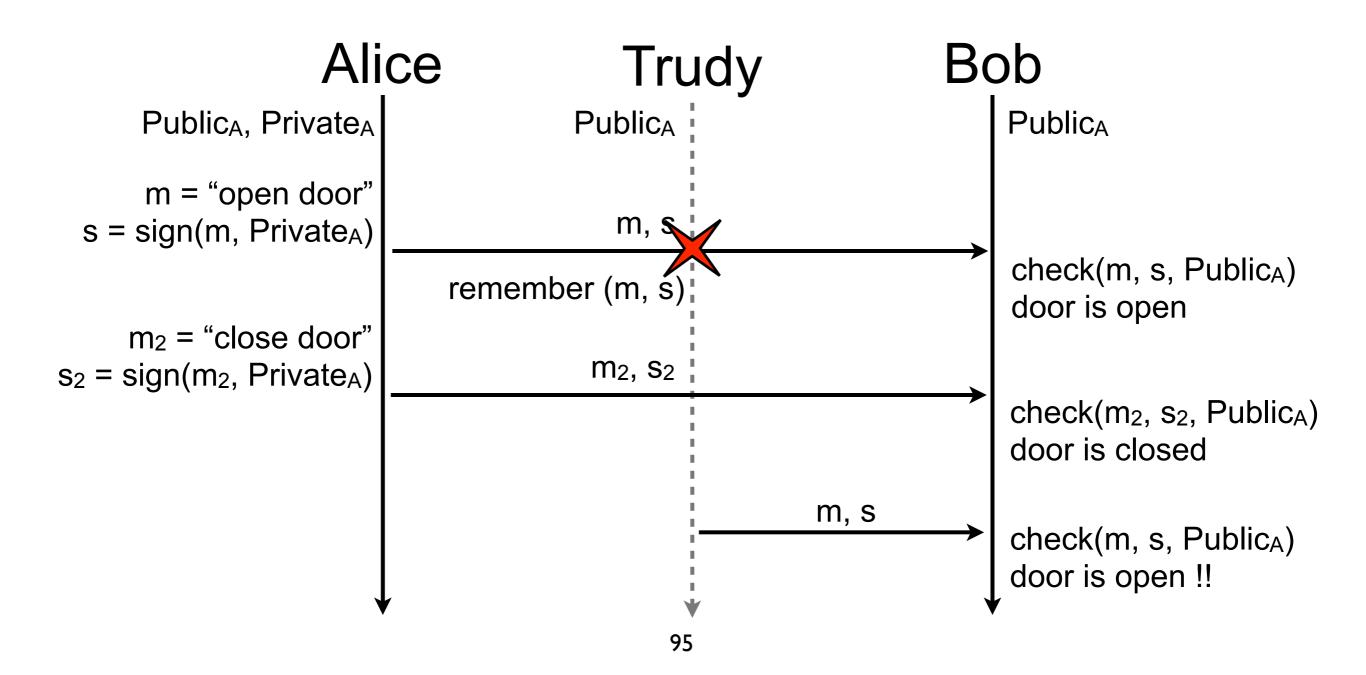










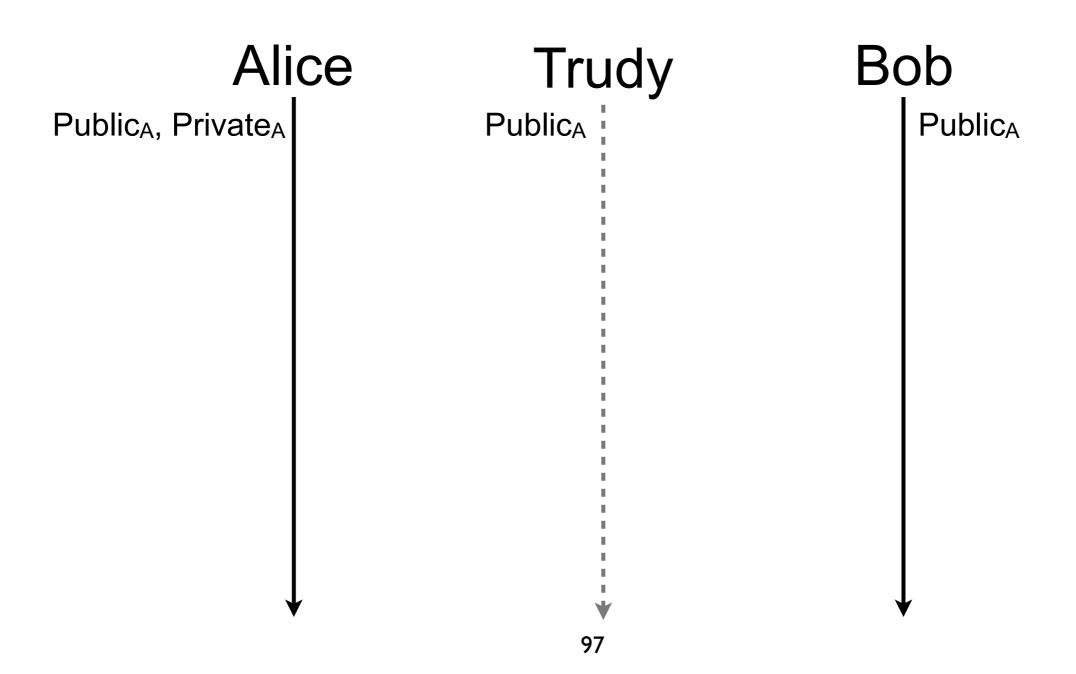


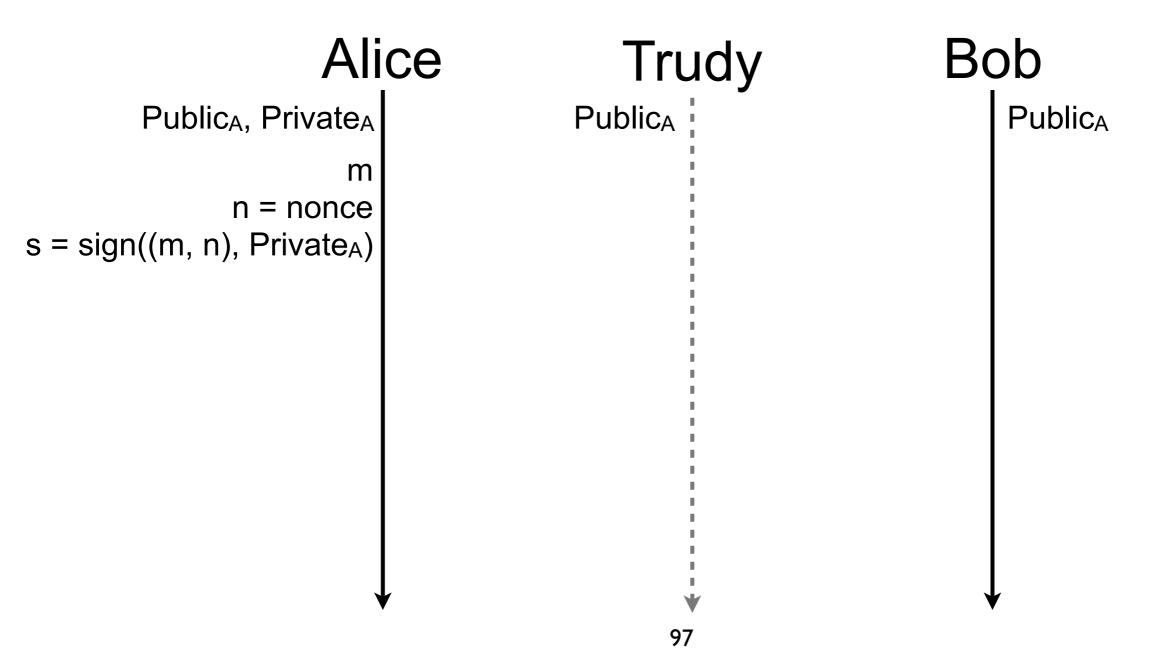
#### Nonce (contd.)

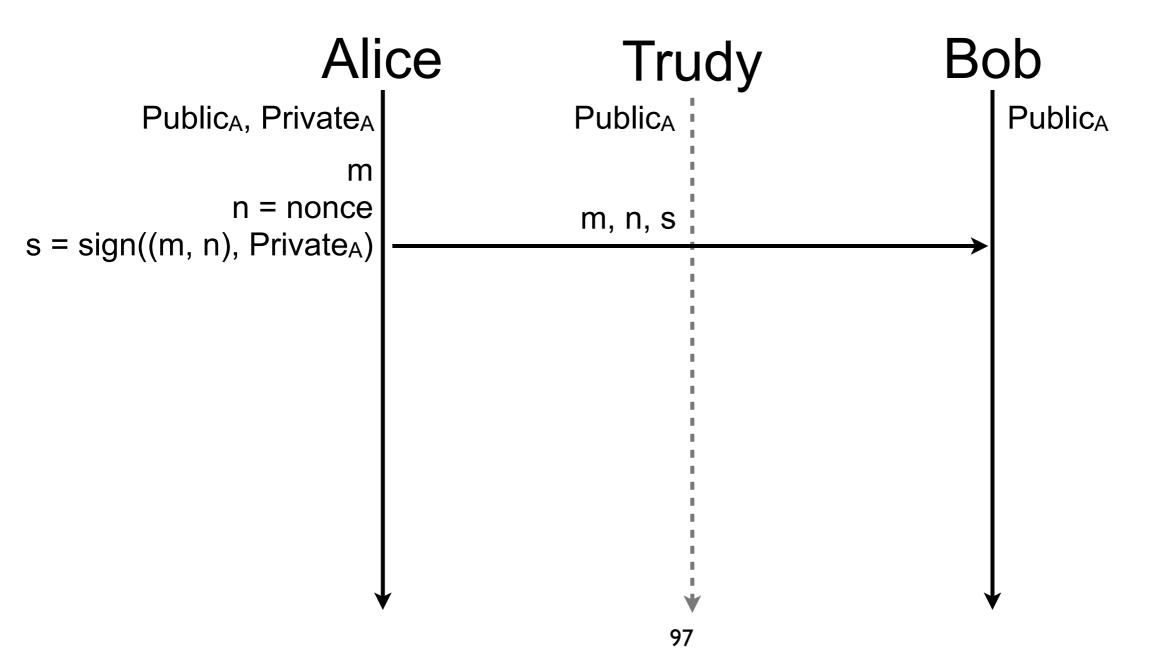
- A nonce is a number used only once
- Three general methods to create nonces
  - sequential number
    - increment after each use
    - keep it in non-volatile storage in case of reboot
  - timestamp
    - current time of the nonce generation
    - be sure clock is not going backward (e.g., winter time)
  - random number
    - low collision probability if the pseudo random number generator is good and random number is big enough (e.g., more than 128 bits)
- Nonce alone is rarely enough to have a good protection
  - not robust to eavesdropping or man-in-the-middle attack

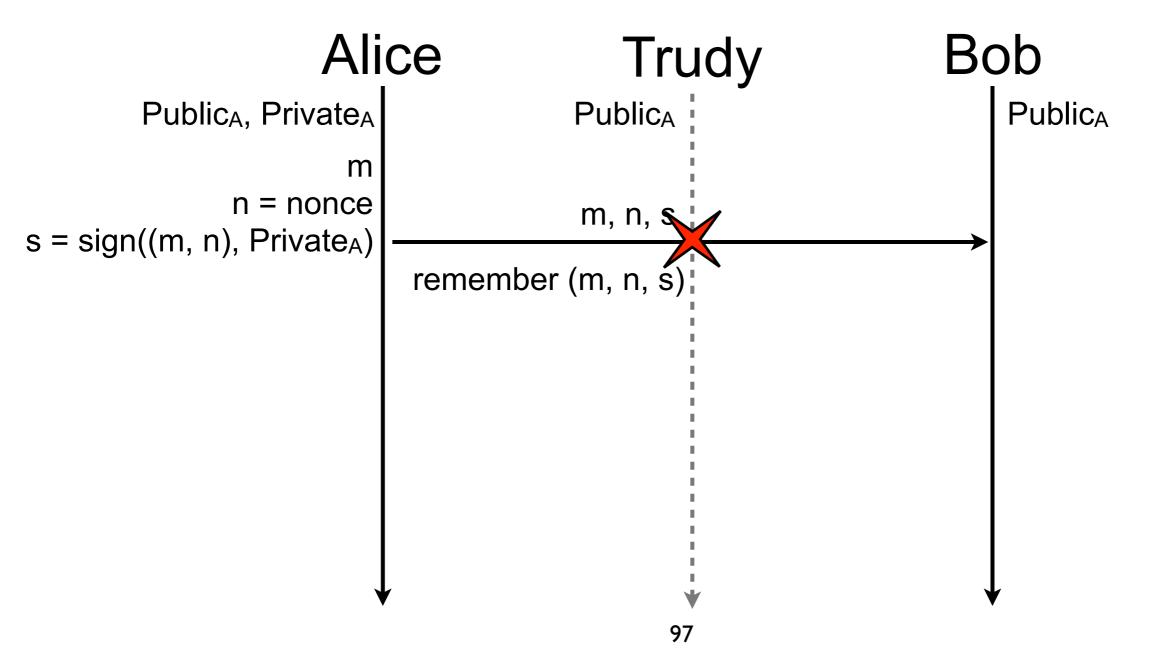
#### Nonce (contd.)

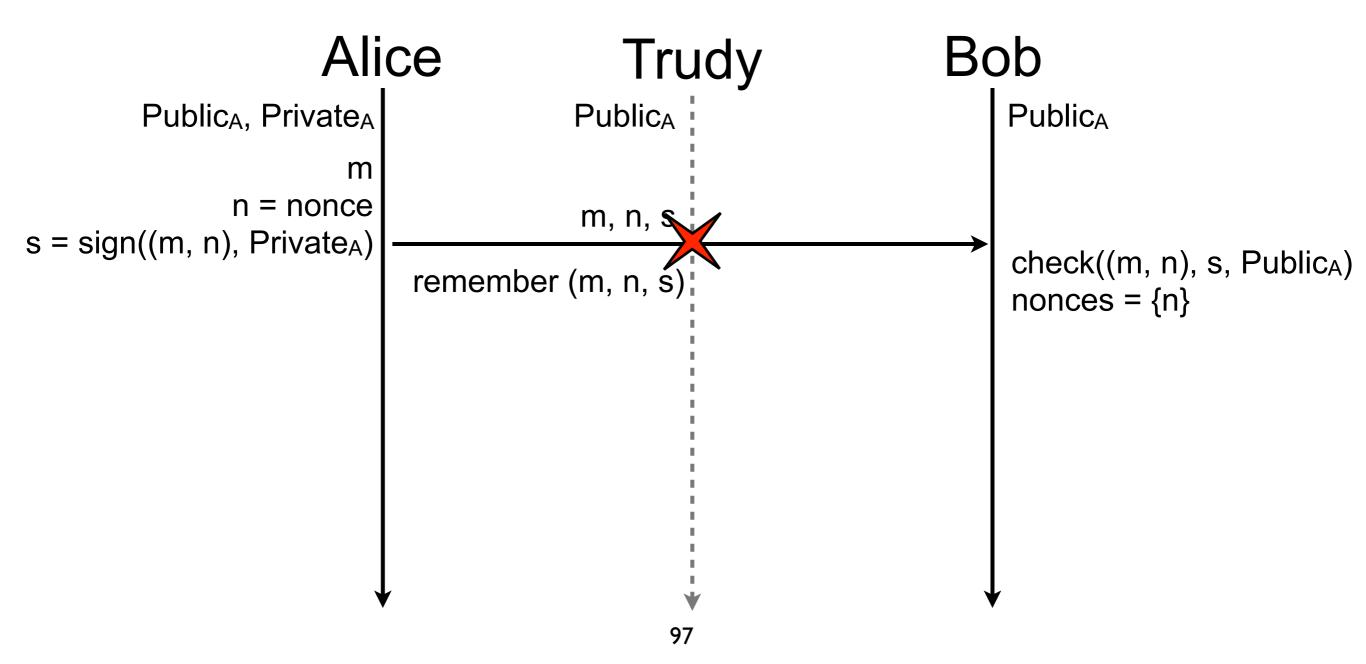
Each message is make unique thanks to the nonce

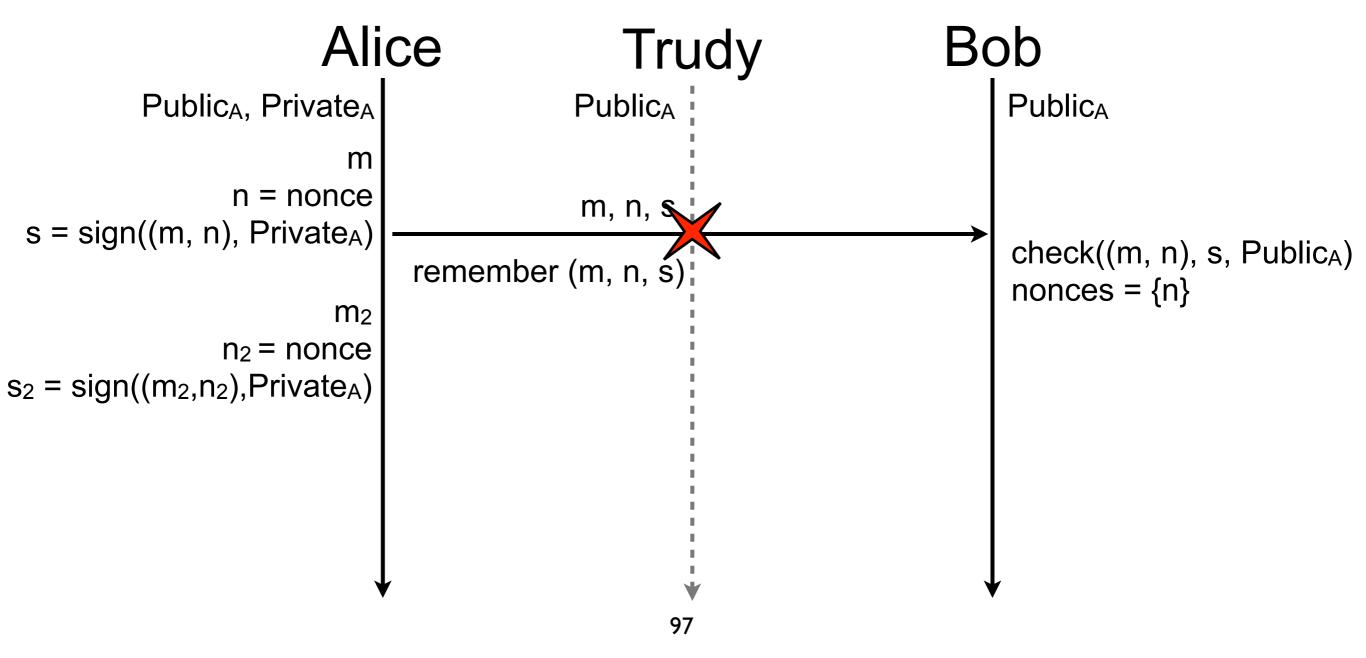


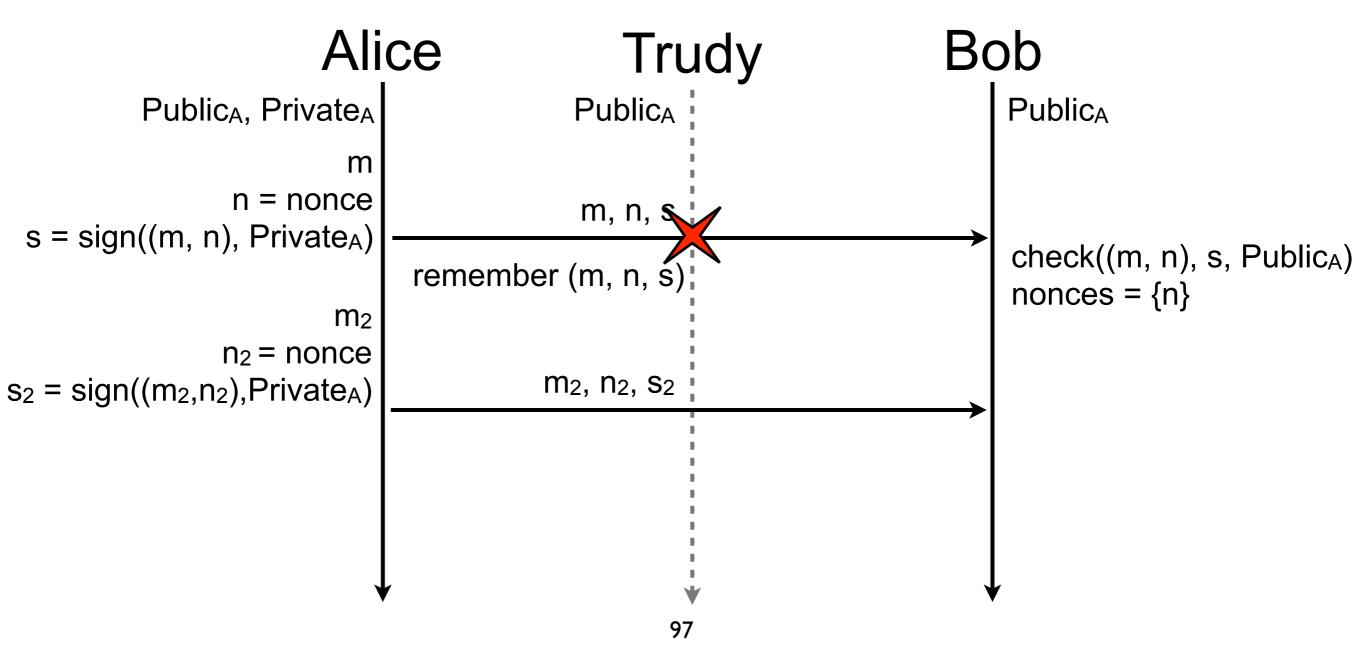


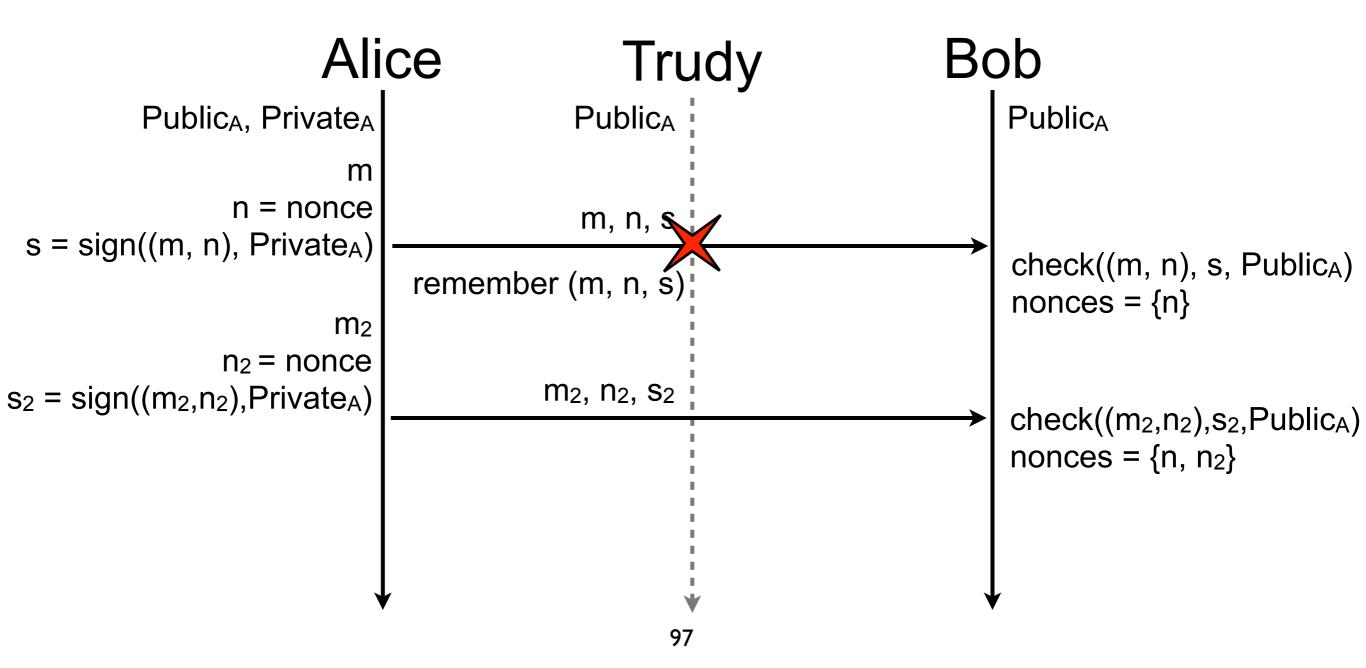


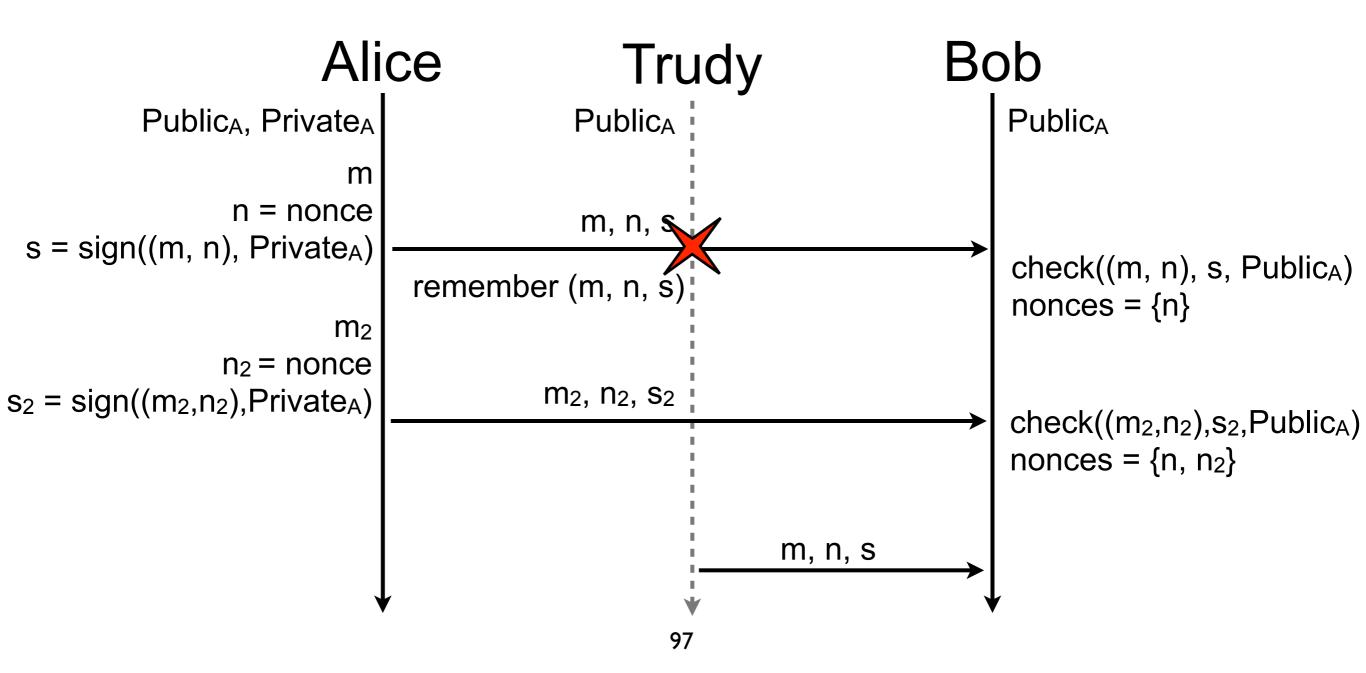


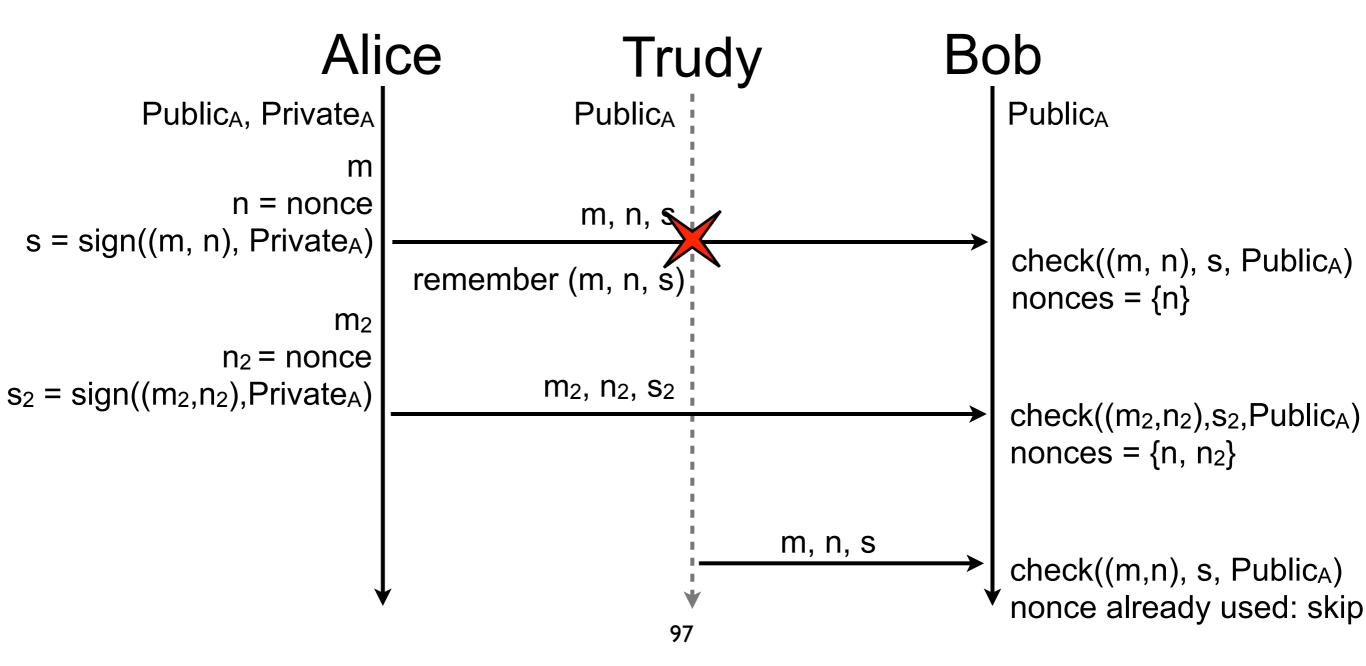


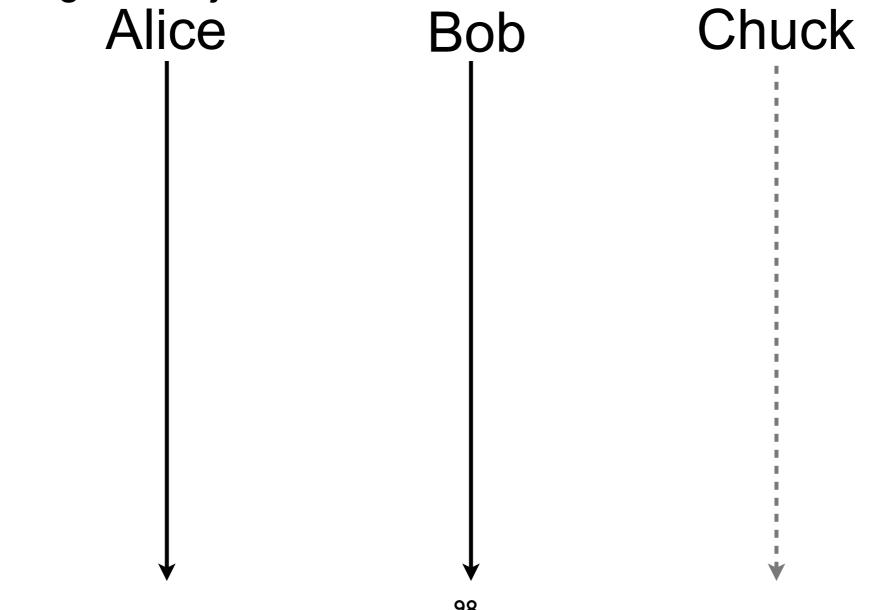


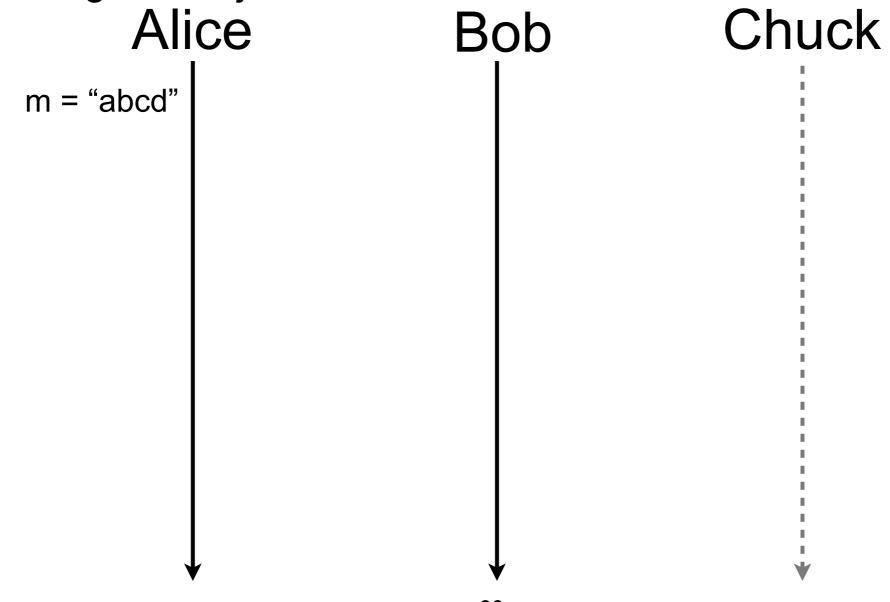


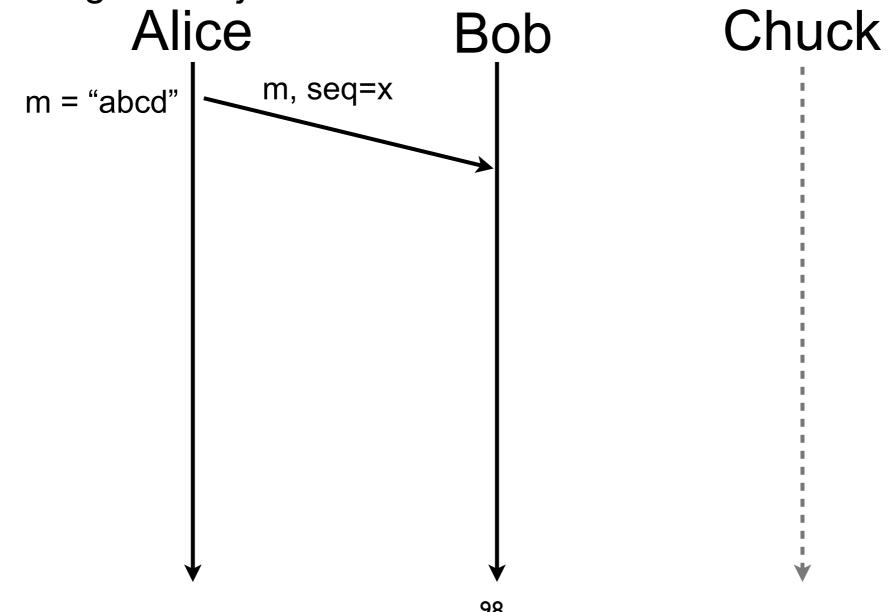


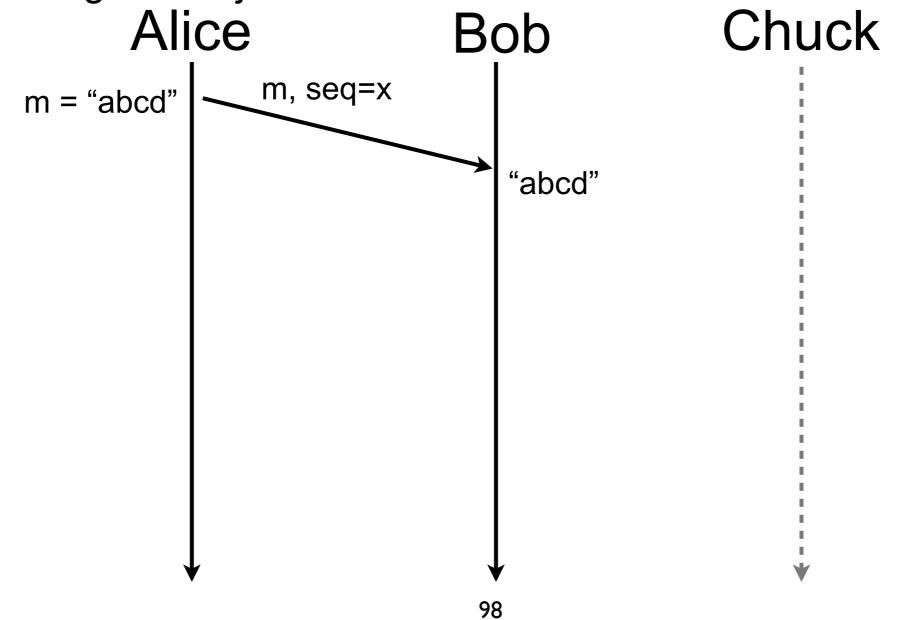


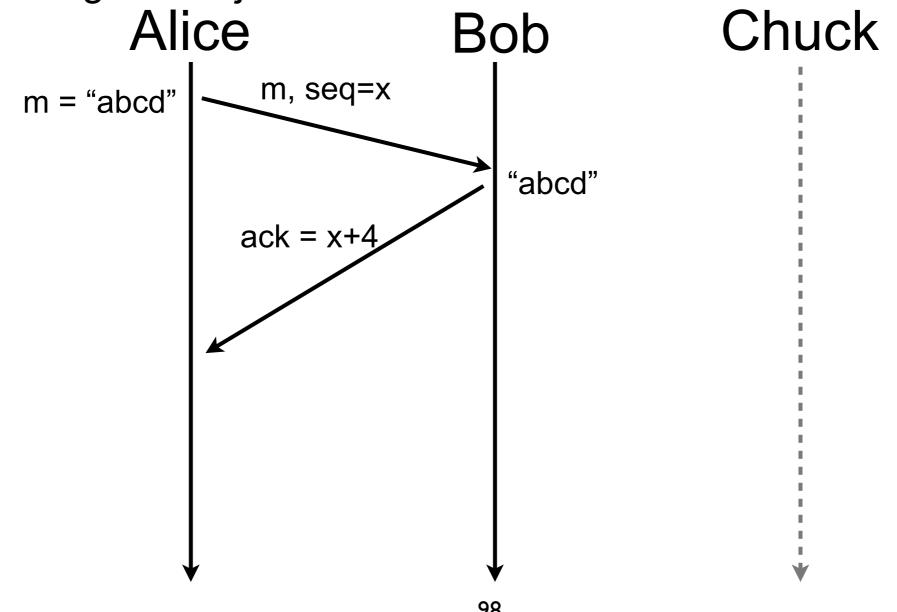


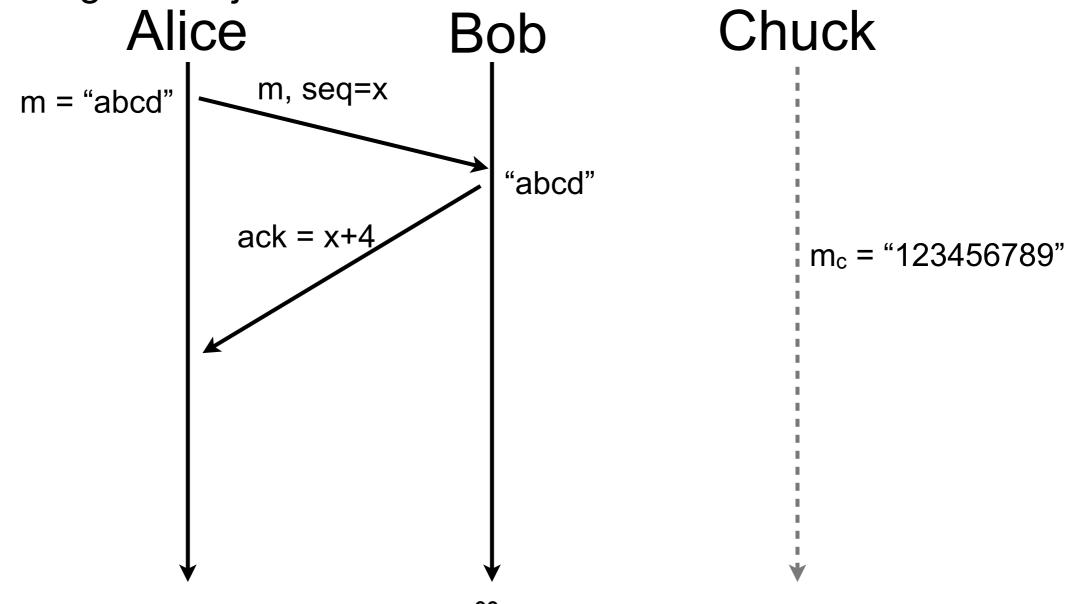


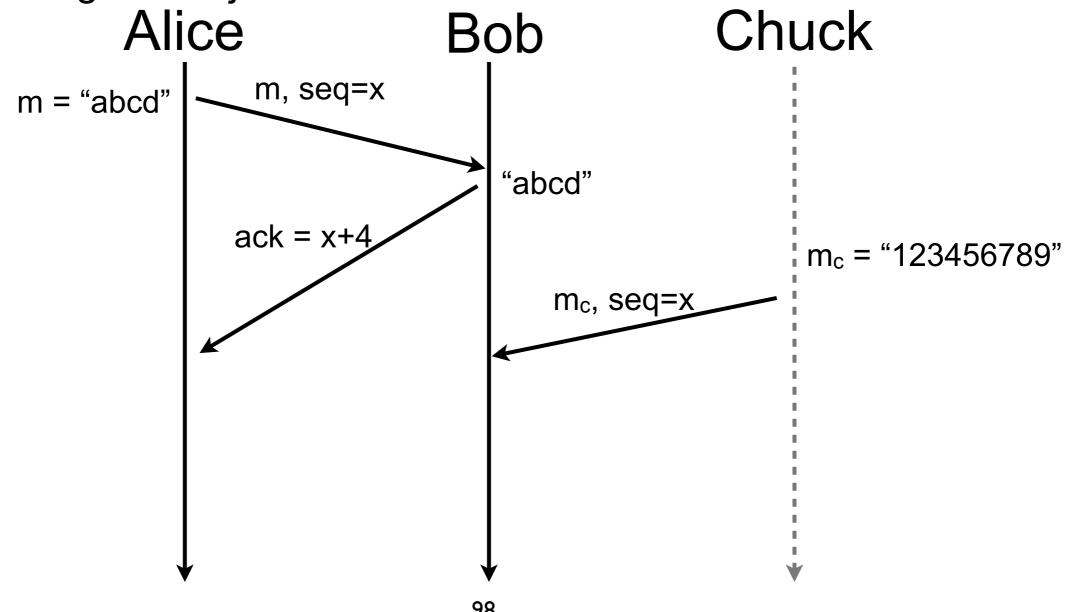


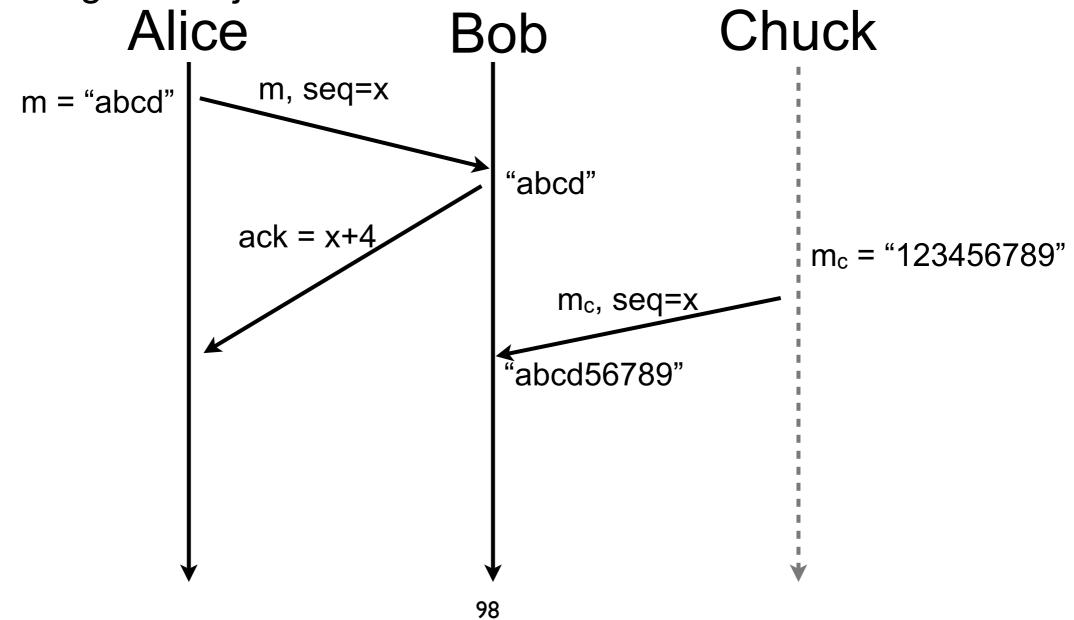


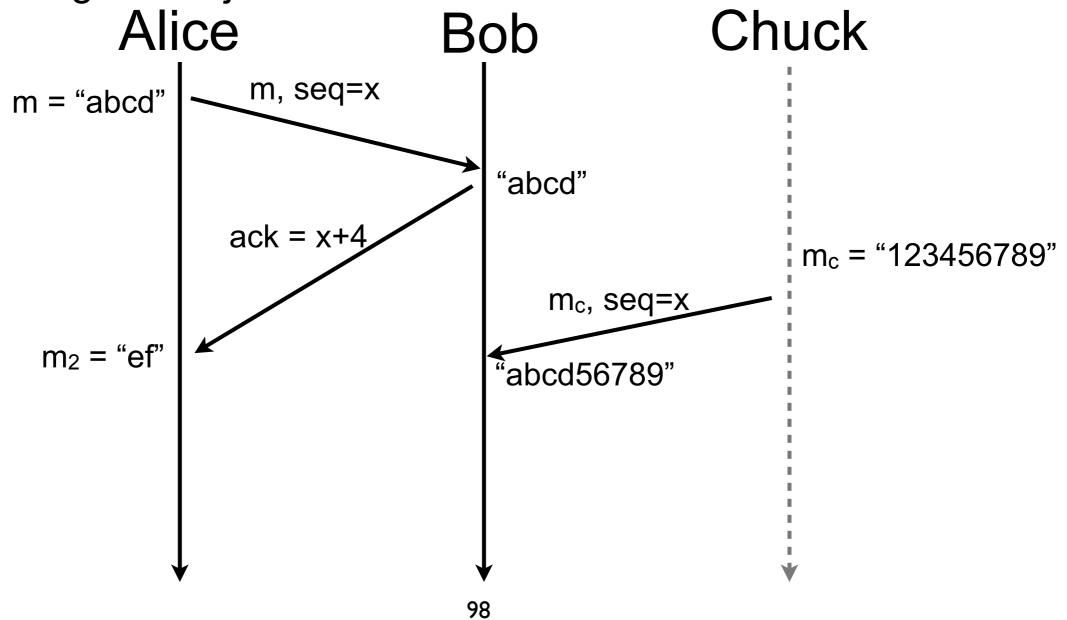


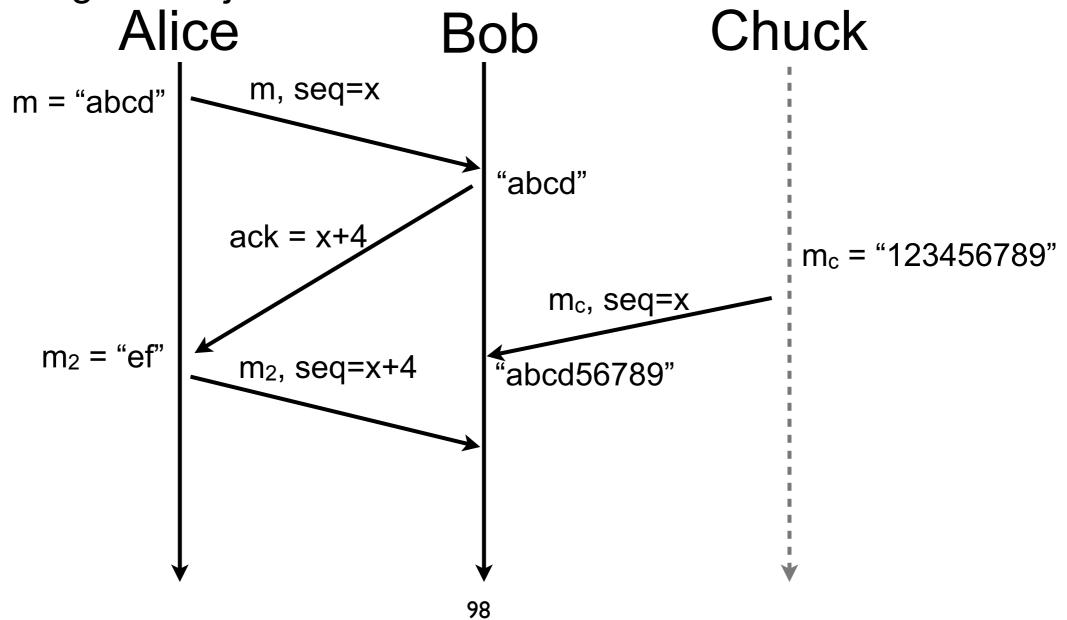


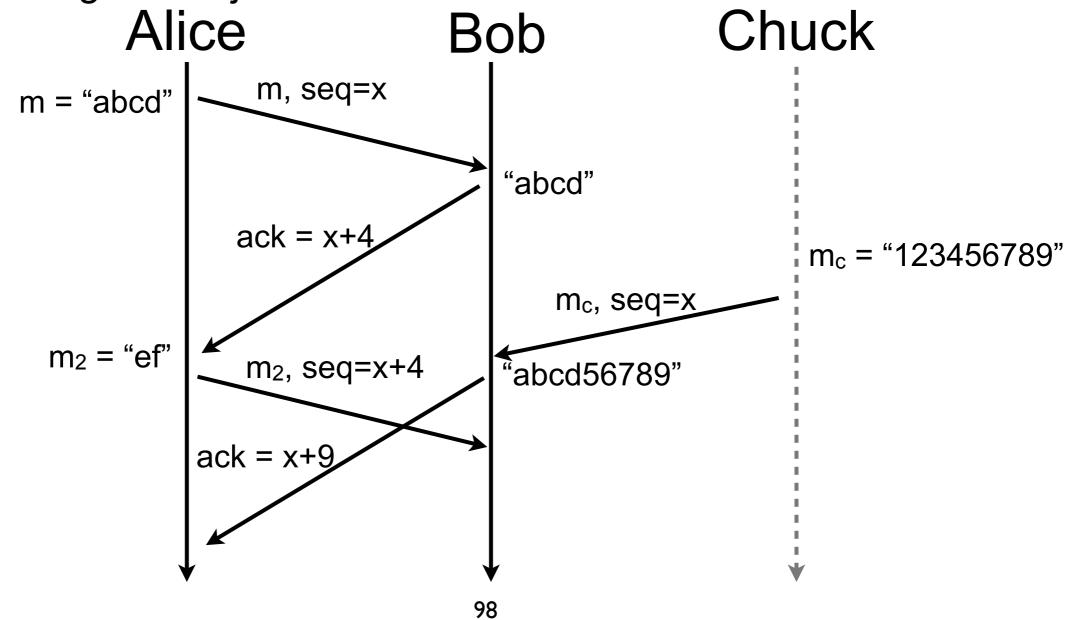


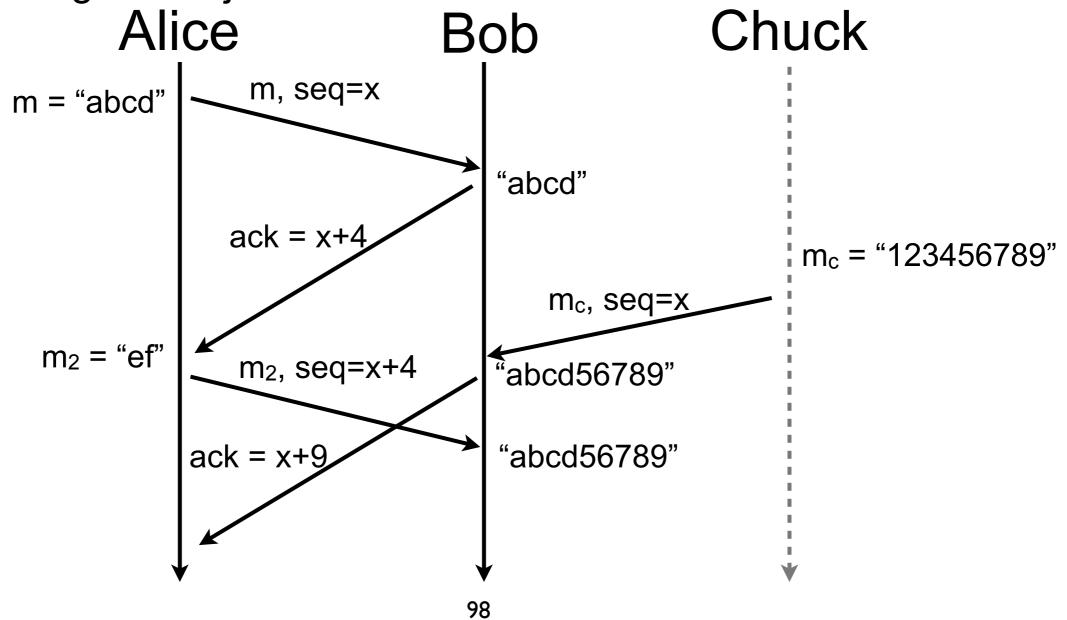


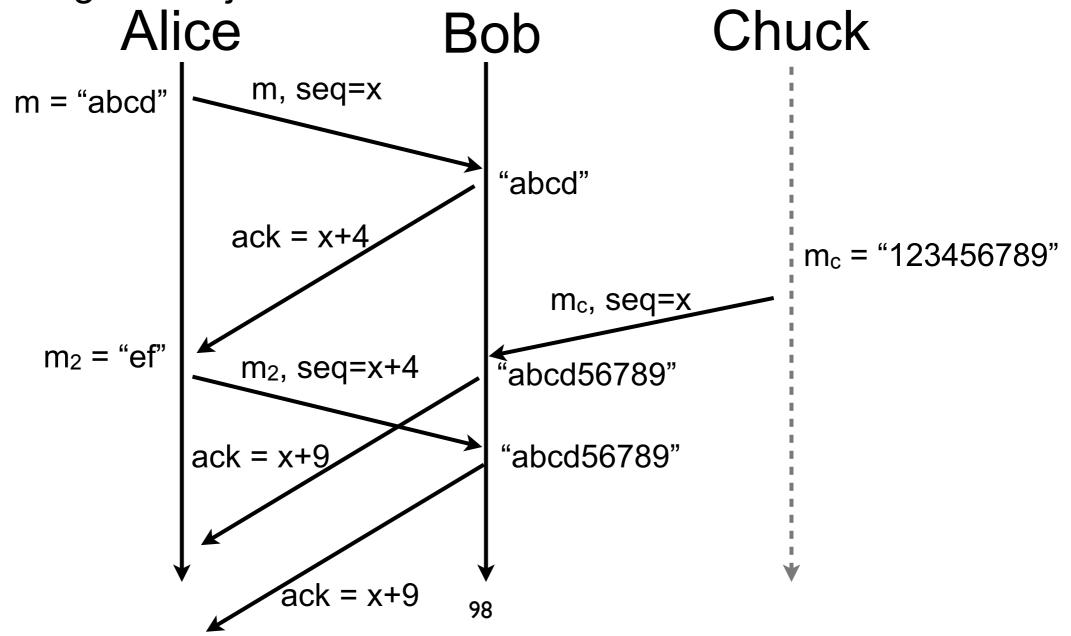


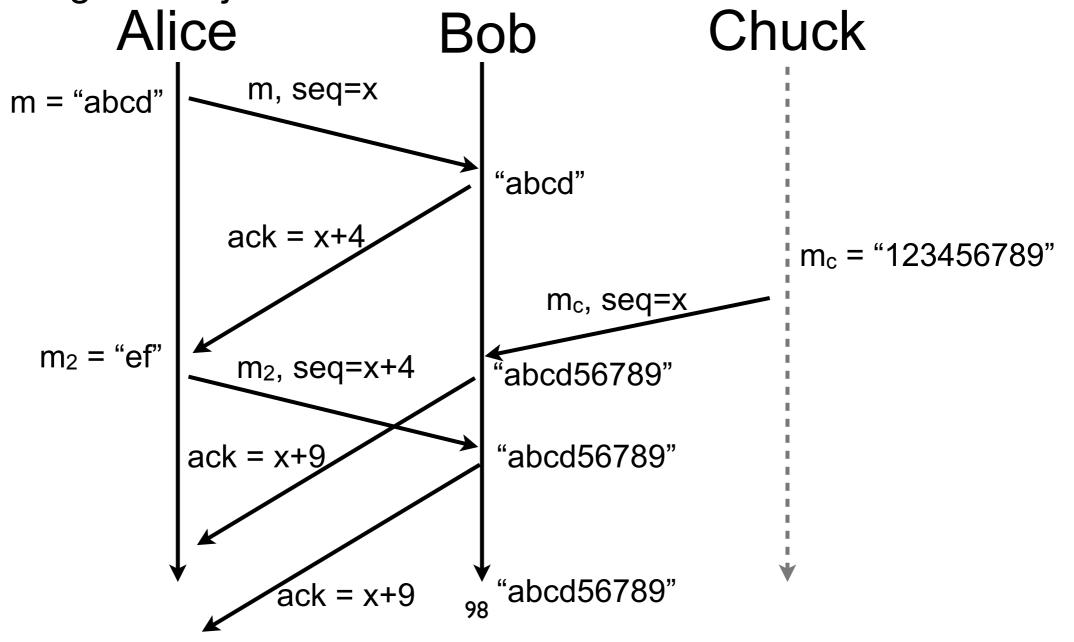












#### Problem solved?

- fill me
- fill me
- fill me

#### Problem solved?

- fill me
- fill me
- fill me

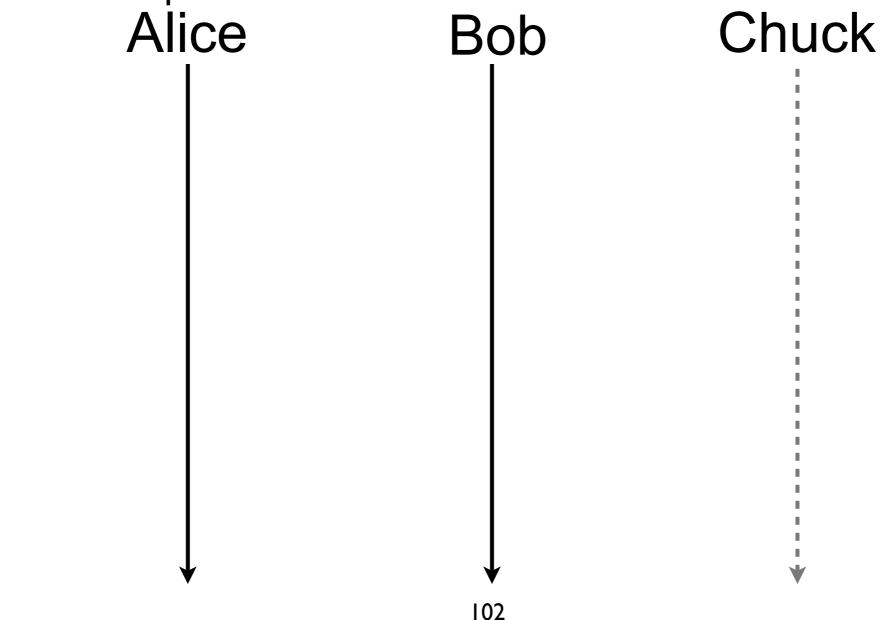
DoS attacks are still possible!

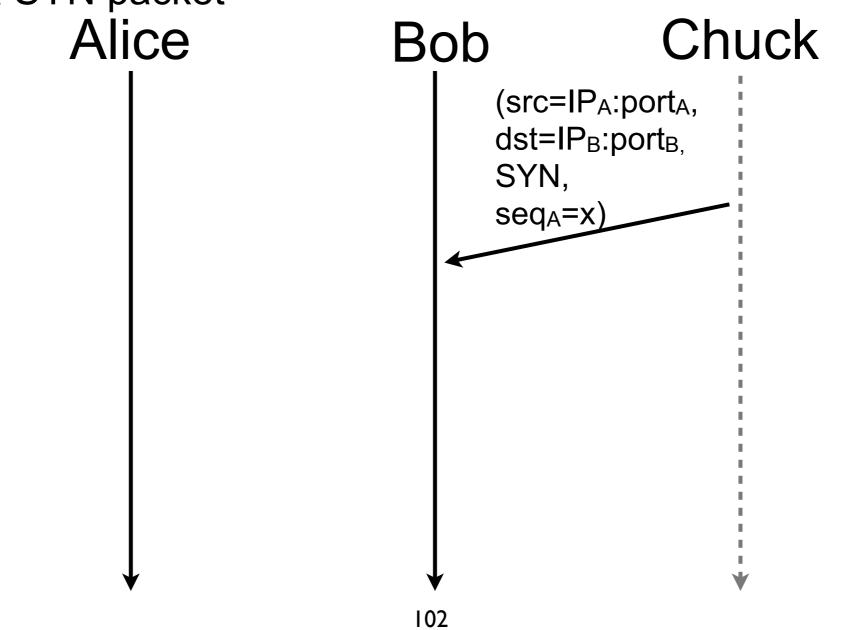
#### Denial of Services

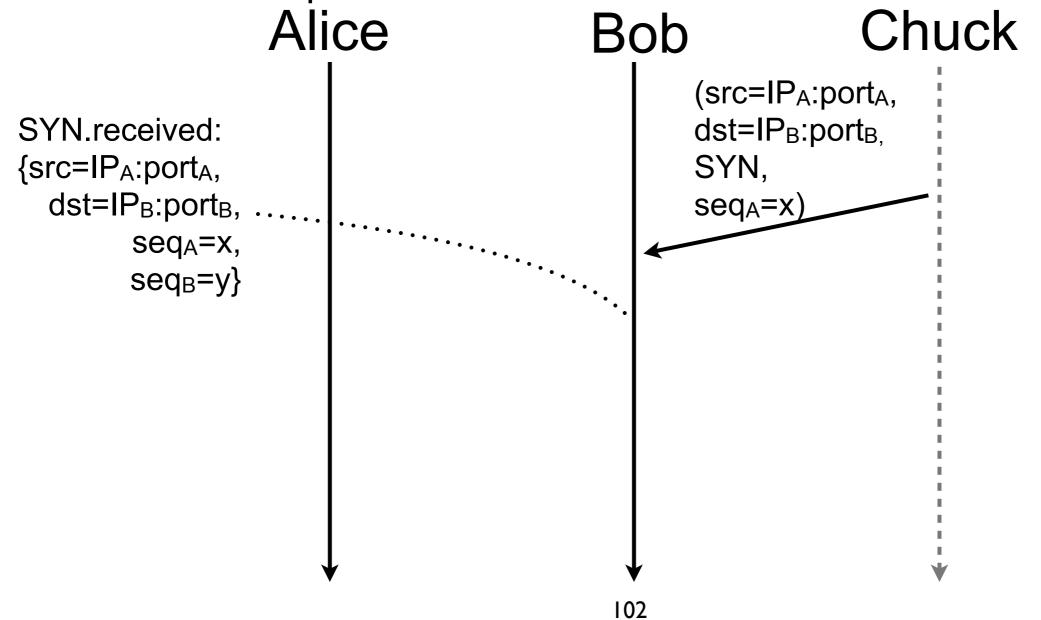
- Resources are always limited
  - e.g., processor, memory, link capacity
- The easiest way of leading a DoS is to overwhelm CPUs, memory, or links of the target
- A more complicated way is to manage an intrusion and neutralize the target
  - imagine you gain administrative access to border router of your network!

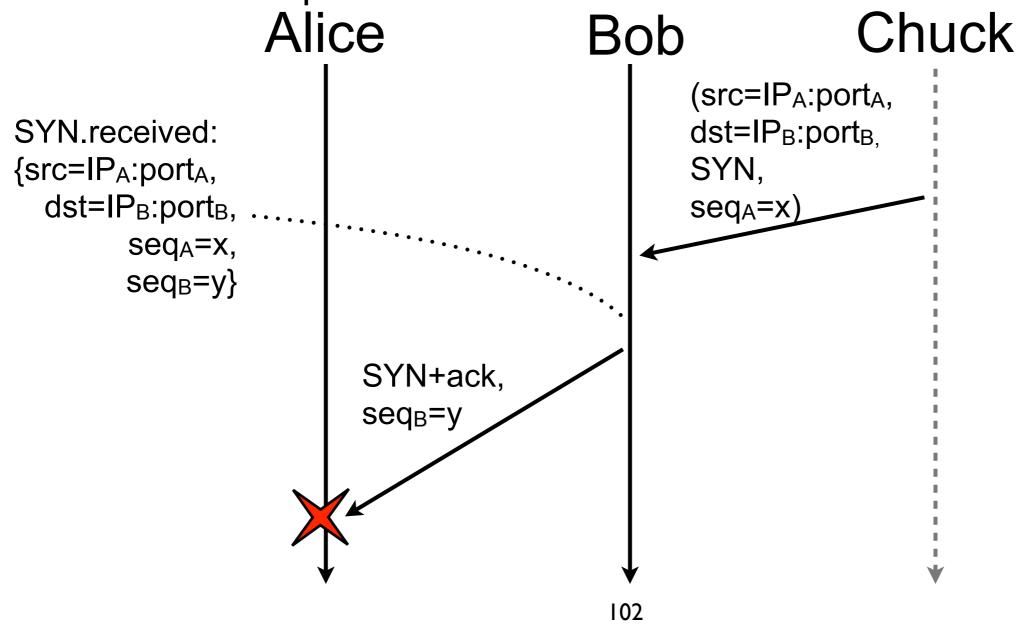
#### Danger of state

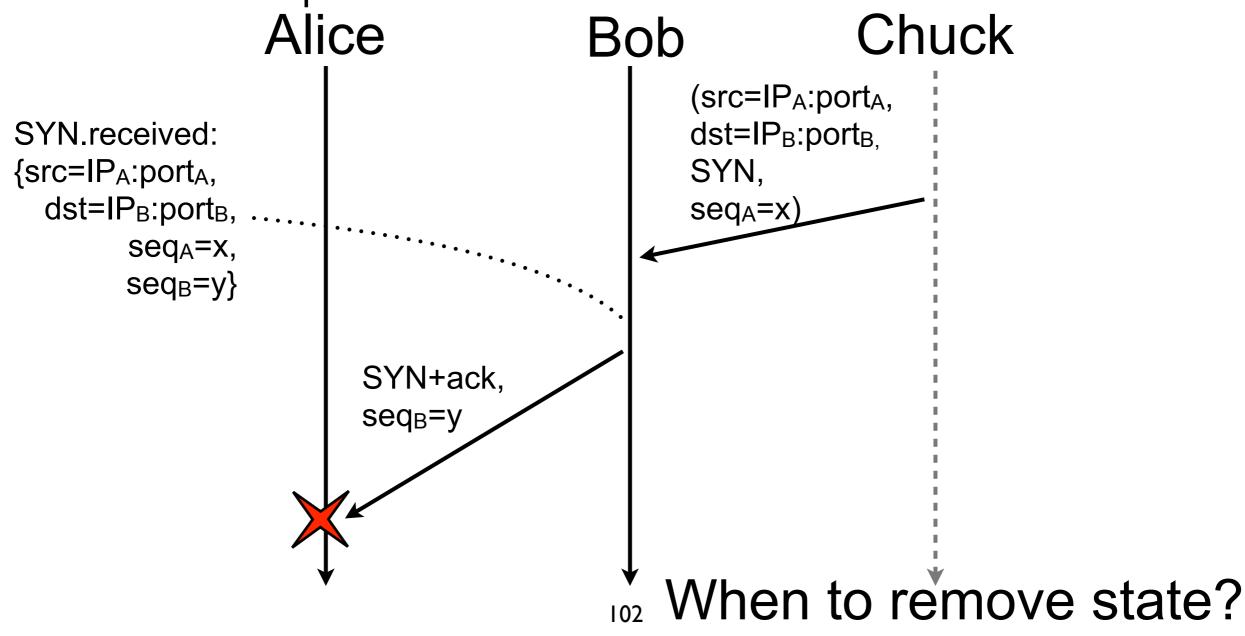
- Establishment and maintenance of session requires state
  - often maintained in "tables" with predefined capacity
- An attacker can saturate state tables by initiating multiple sessions
- Principle
  - require attacker to maintain state before maintaining state yourself
  - in general it is too costly for an attacker to maintain state

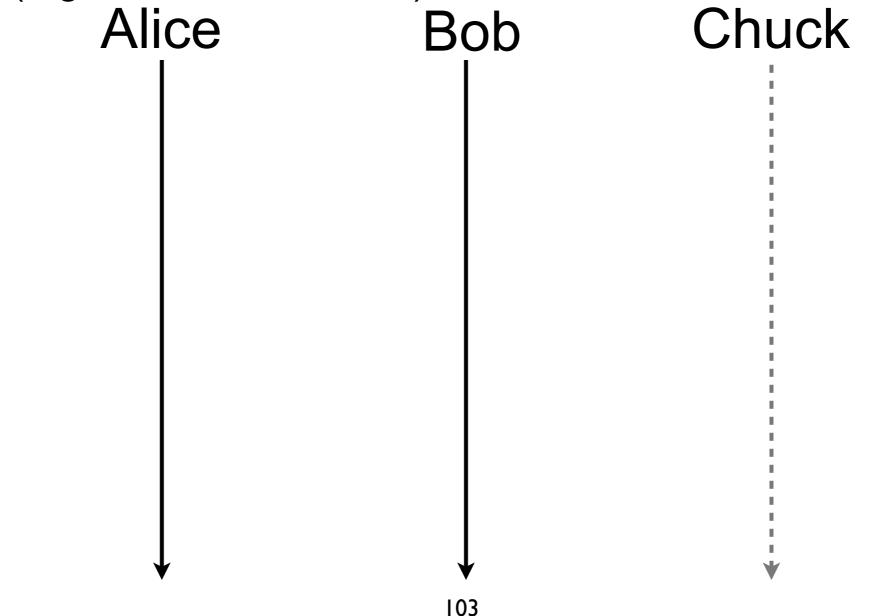


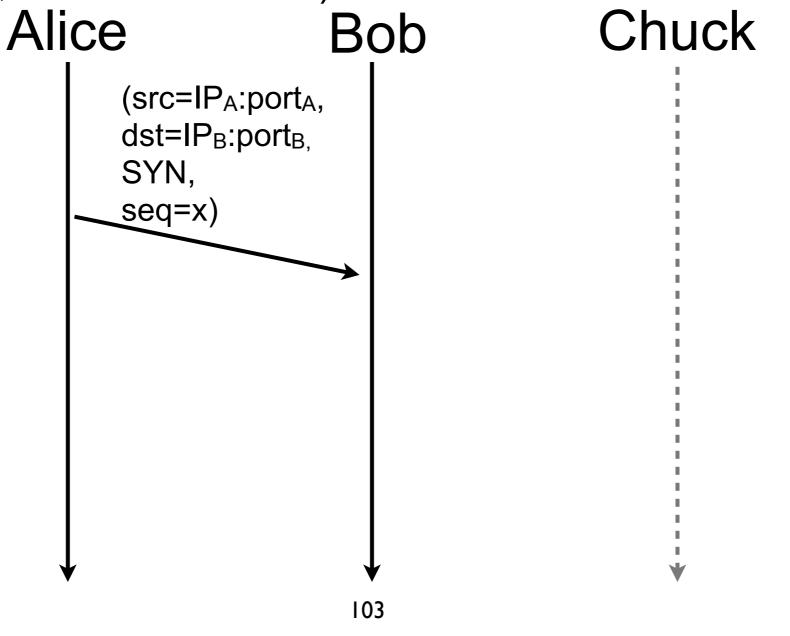


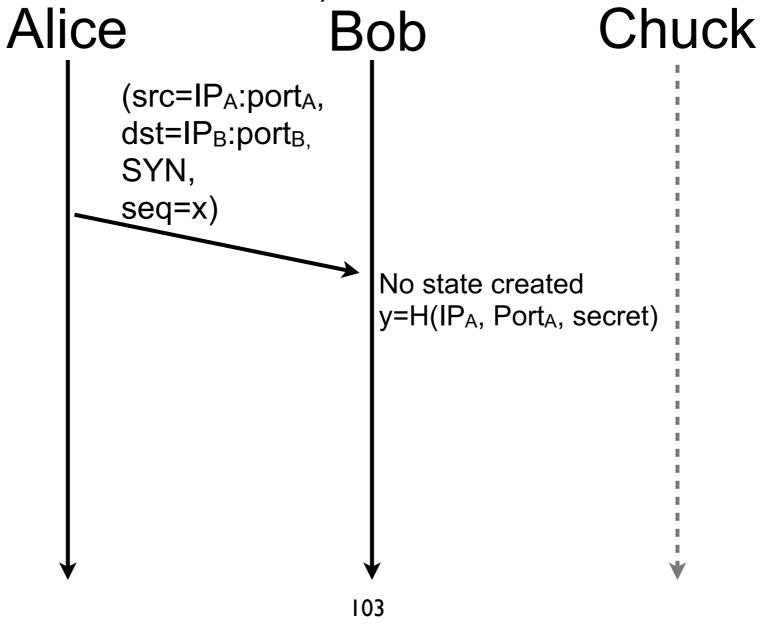


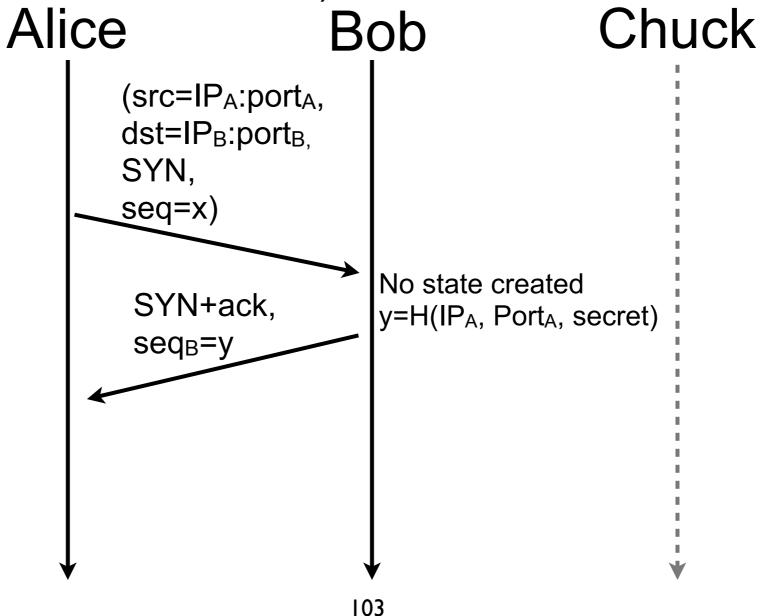






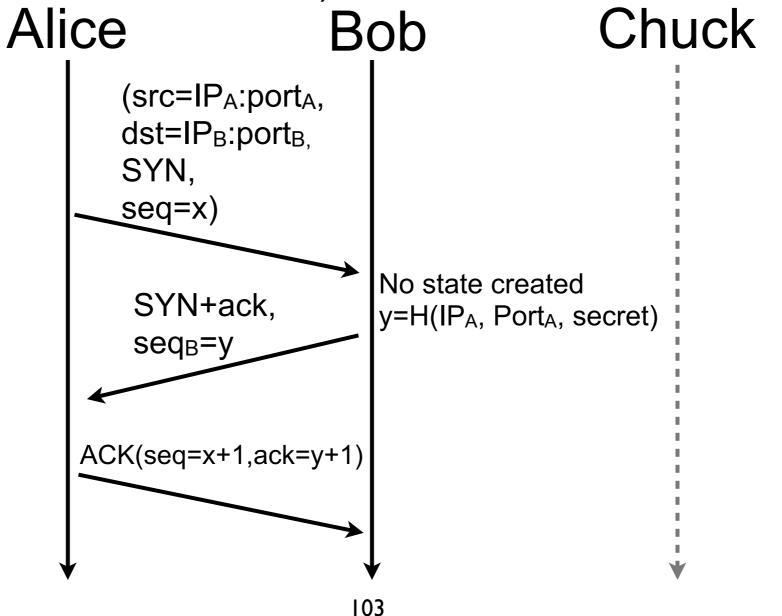






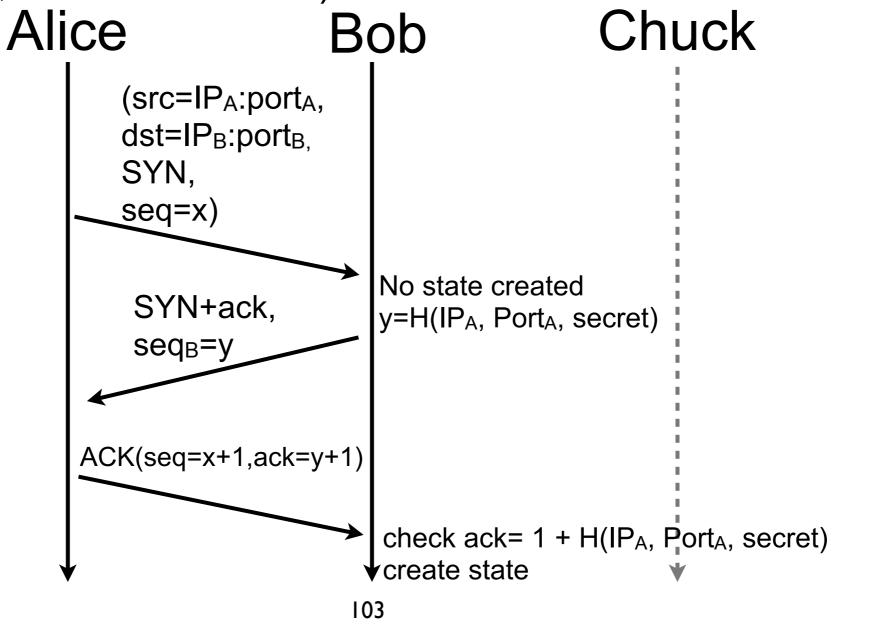
# Danger of state (contd.)

 Always create state at the end of session establishment (e.g., TCP SYN cookie)



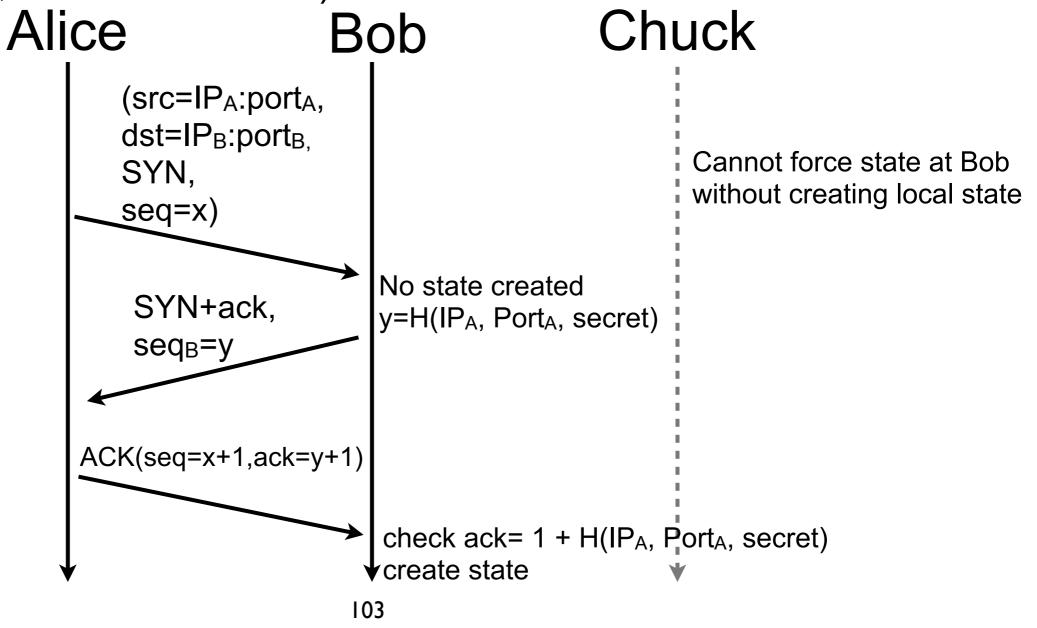
## Danger of state (contd.)

 Always create state at the end of session establishment (e.g., TCP SYN cookie)



## Danger of state (contd.)

 Always create state at the end of session establishment (e.g., TCP SYN cookie)



### Danger of complexity

- Protection mechanism can be complex and can require important processing power
- An attacker can overwhelm her target CPU by triggering protection mechanisms
- Principle
  - require attacker to perform more processing than yourself
  - in general an attacker does not want to have to do heavy computation

# Danger of complexity (contd.)

- Hard, if not impossible, to remove processing requirements but still possible to force the attacker to succeed some challenges to get access. This technique is usually called challenge-response
  - time challenges
    - when an attack is suspected, force the attacker to wait or slow down but the DoS protection can lead to a DoS
      - e.g., rate limiting
  - mathematical challenges
    - ask the initiator to solve a mathematical challenge that is hard to compute but easy to check, this might negatively impact legitimate clients
    - e.g., Bob asks Alice to find a J such that the K lowest order bits of H((N,J)) are zeros. N
      is a nonce and K sets the complexity of the puzzle, both parameters are decided by
      Bob [RFC5201]
  - human processing challenge
    - some services are reserved for users and don't want to be accessed by bots
    - ask Alice to succeed a challenge that is simple for a human but hard for a computer
      - e.g., CAPTCHA

# Danger of complexity (contd.)

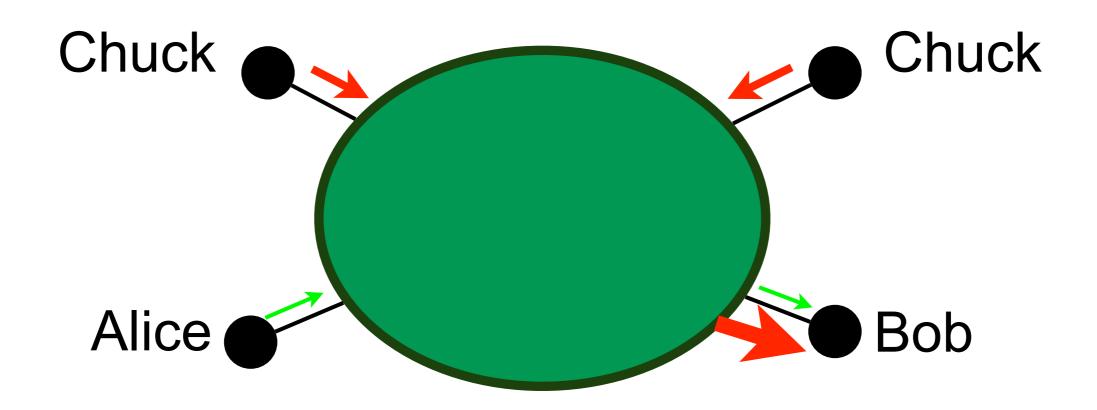
- Hard, if not impossible, to remove processing requirements but still possible to force the attacker to succeed some challenges to get access. This technique is usually called challenge-response
  - time challenges
    - when an attack is suspected, force the attacker to wait or slow down but the DoS protection can lead to a DoS
      - e.g., rate limiting
  - mathematical challenges
    - ask the initiator to solve a mathematical challenge that is hard to compute but easy to check, this might negatively impact legitimate clients
    - e.g., Bob asks Alice to find a J such that the K lowest order bits of H((N,J)) are zeros. N
      is a nonce and K sets the complexity of the puzzle, both parameters are decided by
      Bob [RFC5201]
  - human processing challenge
    - some services are reserved for users and don't want to be accessed by bots
    - ask Alice to succeed a challenge that is simple for a human but hard for a computer
      - e.g., CAPTCHA



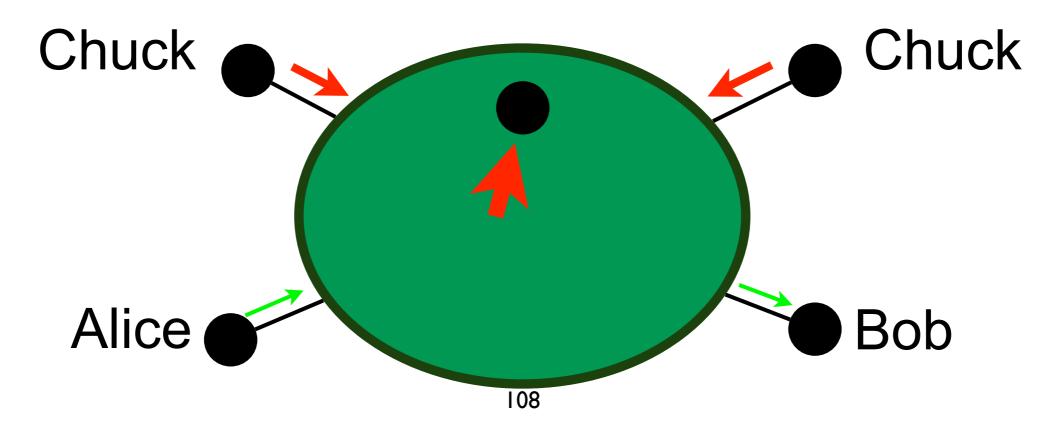
### Link overloading

- Messages are sent to Bob by traversing links
- If an attacker can send packets at a high enough rate, she can saturate links toward Bob and make him unavailable
- Unfortunately, Bob cannot make anything to block packet before they reach him
- Principle
  - tweak the network to not suffer too much of such attacks

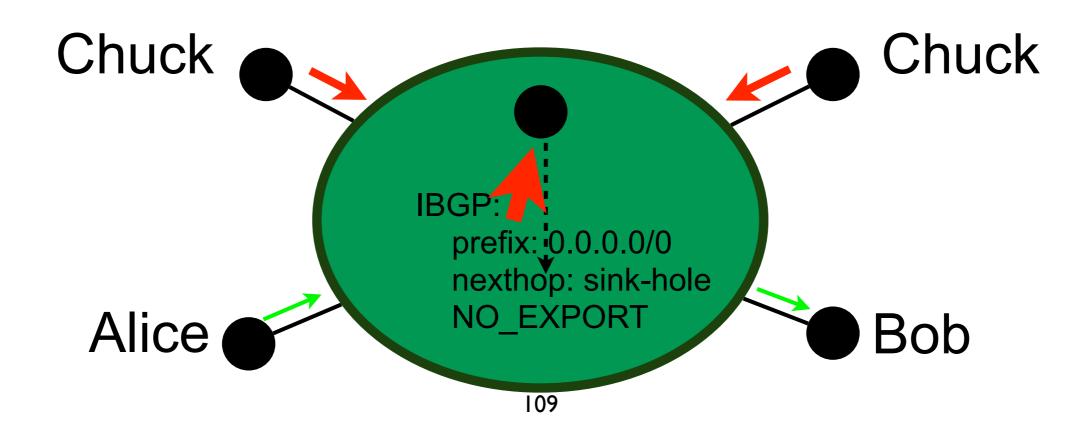
 Example of Distributed Denial of Service (DDoS) attack



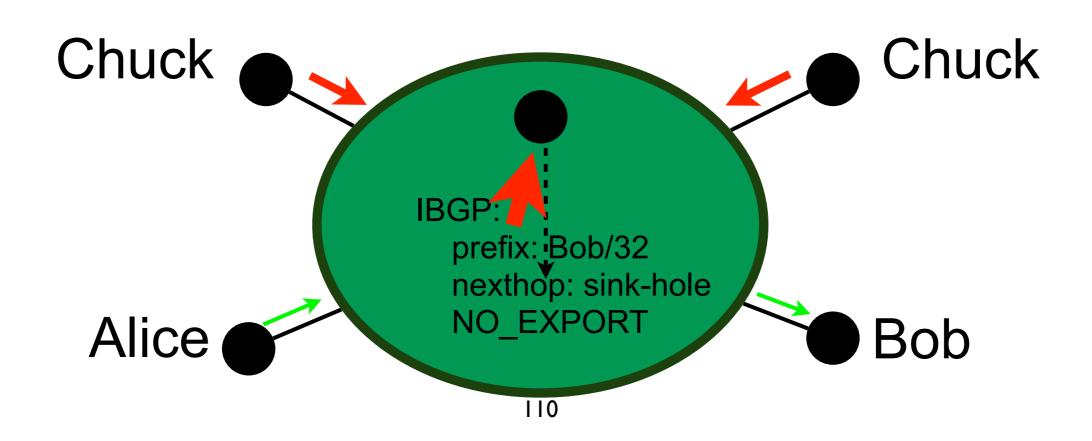
- Attacks are often to random destinations or with random sources
  - backscatter traffic to a sink-hole that can receive a lot of traffic attack without impacting the network



Use the sink-hole to attract bizarre packets



Use the sink-hole to protect the target



- A first parade is to filter illicit traffic before it can harm the target
  - e.g., firewall, access lists
- A set of rules is specified a priori, if the traffic does not match the rules, it is discarded
  - always block everything but what is acceptable

- Filtering based on origin
  - useful to avoid spoofing
    - e.g., block any packet which source address does not belong to the customer cone of a BGP neighbor
  - does not work so well as it depends on every network between the origin and the target
- Filtering based on traffic pattern
  - analyze the traffic and if it deviates from what is normal, drop it
    - e.g., drop malformed packets, rate limit a source if it sends too much SYN packets, ignore mails from well known SPAM servers, block any flow initiated by the outside if there is no server in the network

### Network Intrusion Detection System (NIDS)

- An NIDS aims at discovering nonlegitimate operations
- The NIDS analyses the traffic to detect abnormal patterns
- Upon anomaly detection, the NIDS triggers an alert with a report on the anomaly
- NOC follows procedures upon detection

### Network Intrusion Detection System (contd.)

- Signature based detection
  - a database of abnormal behavior is maintained to construct a signature for each attack
  - if the traffic corresponds to a signature in the database, trigger an alarm
  - risk of false negative (0-day attack)
  - e.g., Snort, Bro, antivirus
- Outlier detection
  - the anomaly detector learns what is the normal behavior of the network
  - went an outlier is detected, an alarm is triggered
  - risk of false positive and false negative
  - e.g., cluster analysis, time series analysis, spectral analysis

- if antivirus(self) == BAD:
  - skip
- else:
  - I am bad

#### Problem solved?

- fill me
- fill me
- fill me

#### Problem solved?

- fill me
- fill me
- fill me

Relay attacks are still possible!

### Relay attack

- In a relay attack, Chuck does not contact Alice directly but goes via Bob
- If the traffic from Bob to Alice is bigger than the traffic from Chuck to Bob, the attack is called amplification attack
- As for DoS, hard to protect correctly against relay attacks
  - use filters (e.g., deactivate ICMP)
  - authentication of the source
    - but correct spoofing protection that doesn't open a relay attack door is very hard to deploy in practice as it requires messages in both directions between parties

#### What did we miss?

#### What did we miss?

- To terminate the session!
  - with the same care as the opening of the session
  - this is often neglected

## Perfect Forward Secrecy

- With perfect forward secrecy (PFS),
   Eve cannot decrypt messages sent
   between Alice and Bob
  - even if she captures every message
  - even if she breaks into Alice and Bob after the communication to steal their secrets (e.g., private keys)

### Perfect Forward Secrecy (contd.)

- PFS is provided using ephemeral keys
  - the ephemeral key is generated and used only during the session
  - the session key is not stored after the communication
  - the session key is independent of stored information (e.g., good PRNG)
  - for long sessions, change the session key regularly

### Perfect Forward Secrecy (contd.)

- 1. Initiate the communication between Alice and Bob
  - authenticity proven with public/private key pairs
- 2. Alice and Bob agree on a secret K
  - use Diffie-Hellman
    - authenticate DH messages with public/private key pairs
- 3. Encrypt/Decrypt messages with symmetric cryptography using K as the key
  - no need to sign as it is encrypted
  - be sure a nonce is used to avoid replay
- 4. If session is too long, back to 2.
- 5. Close the session correctly and be sure K is not stored anywhere

#### Blockchains

### Why?

- Traditional security mechanisms rely on the notion of trust
  - who to be the trusted party (e.g., Trent)
  - concentration of power

### Why?

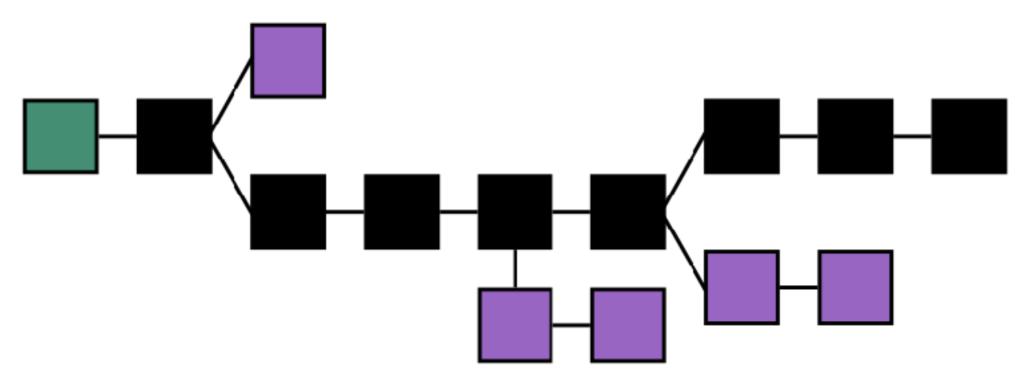
Traditional security mechanisms rely on

Shift to cryptographic proof instead of trust

concentration of power

#### Definition

"A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography."



<sup>1</sup> Blockchain, https://en.wikipedia.org/wiki/Blockchain, 11th Nov. 2017

### First proposed with bitcoin

- Proposed for making Bitcoin transactions while avoiding double spending
  - Nakamoto, Satoshi. "Bitcoin: A peerto-peer electronic cash system." (2008): 28.
- Now blockchains go beyond transactions

### First proposed with bitcoin

 Proposed for making Bitcoin transactions while avoiding double spending

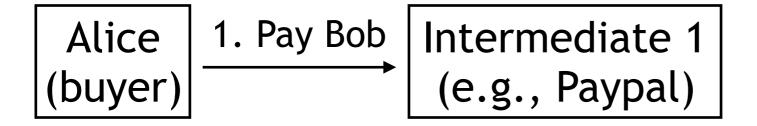
In this presentation we use bitcoin as an example of blockchain

3931<del>0</del>111. (2000). 20.

 Now blockchains go beyond transactions

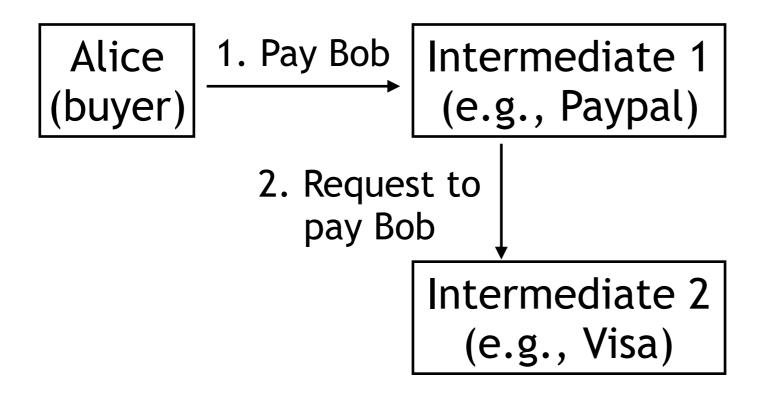
Alice (buyer) Bob (seller)

Alice's bank



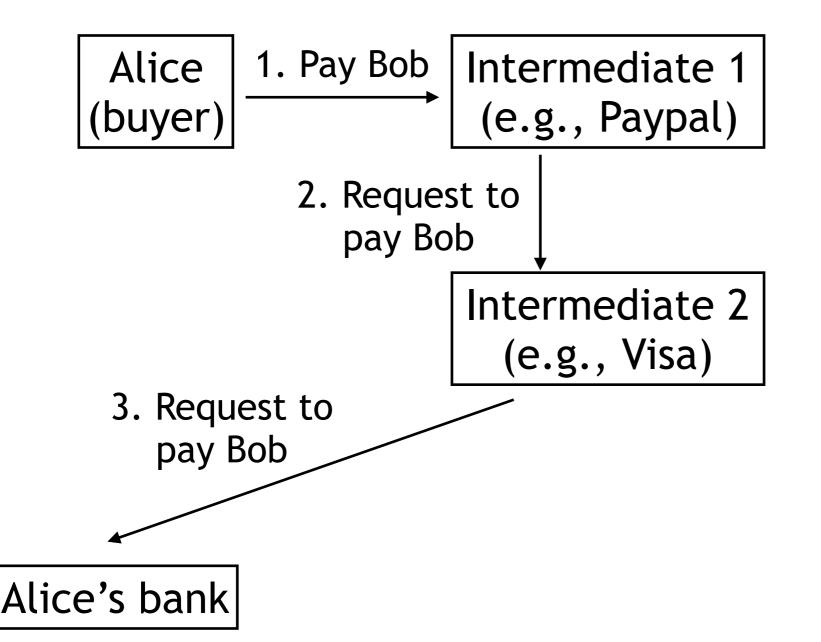
Bob (seller)

Alice's bank

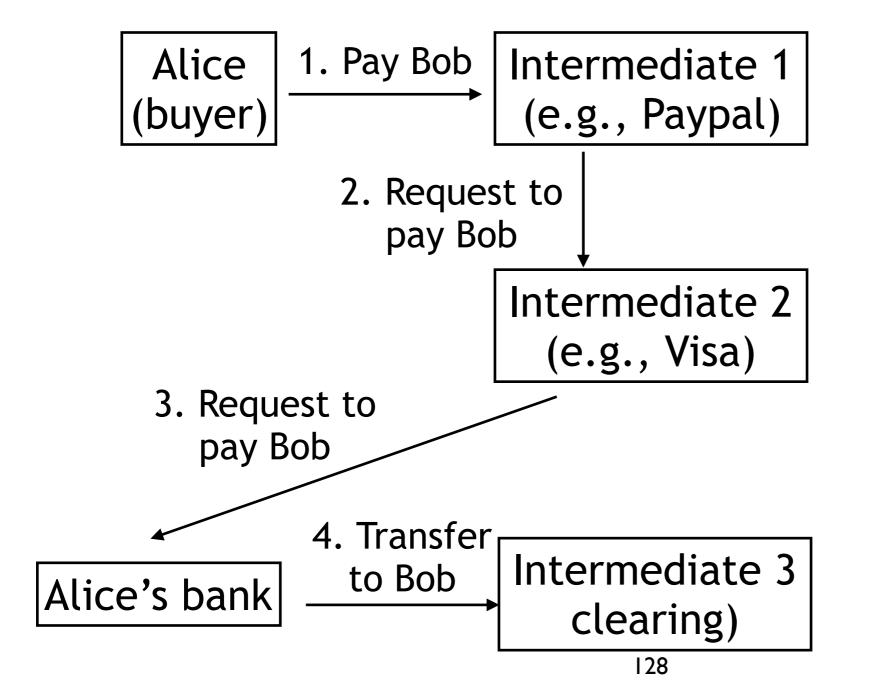


Bob (seller)

Alice's bank

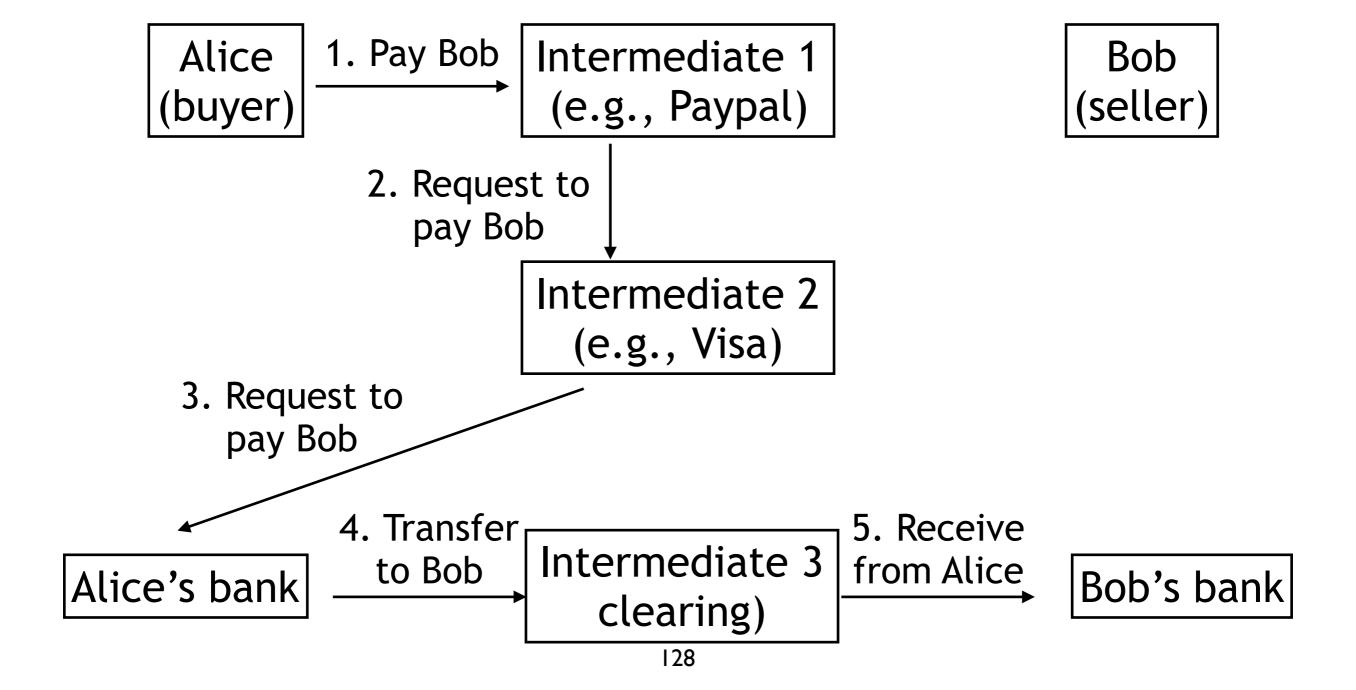


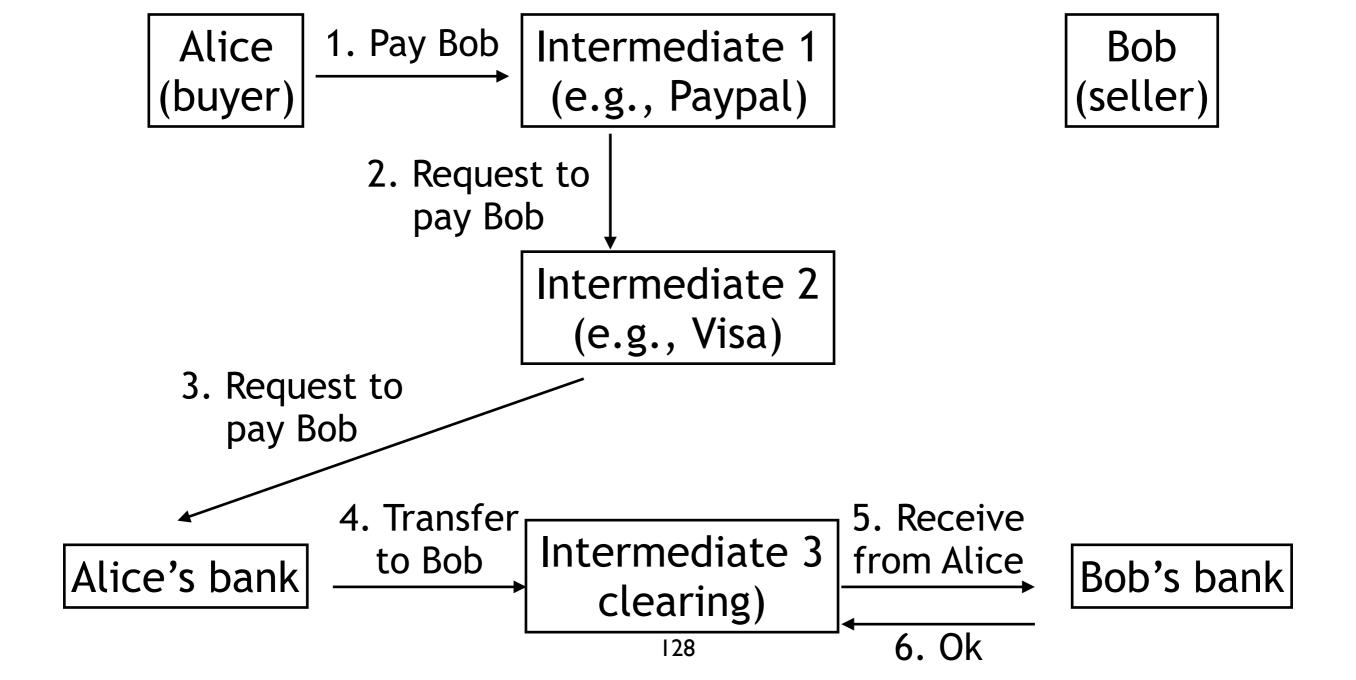
Bob (seller)

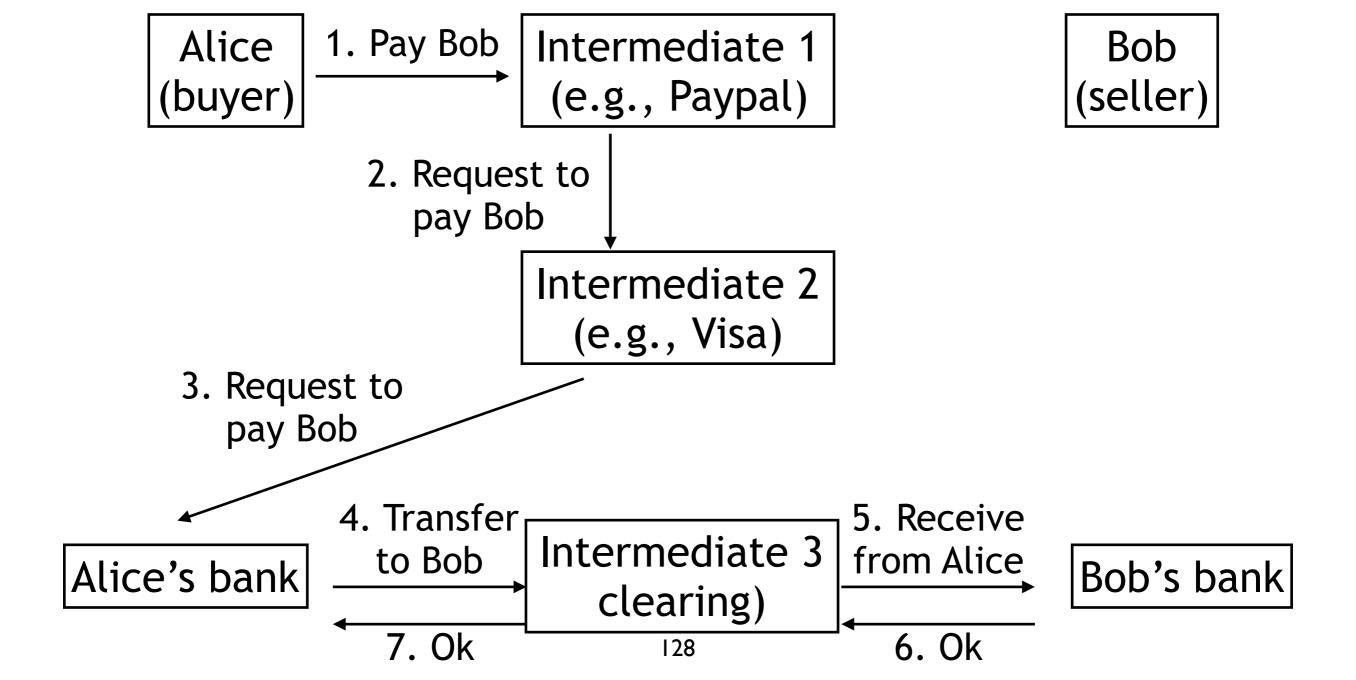


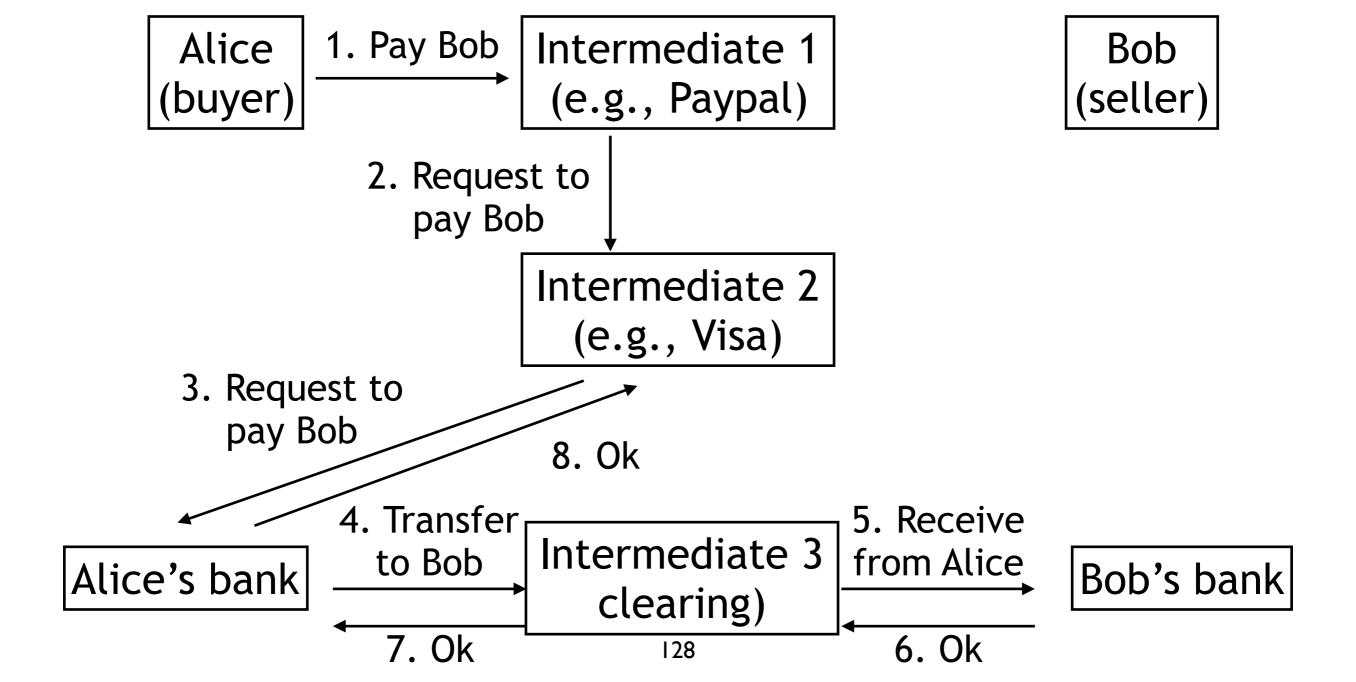
Bob (seller)

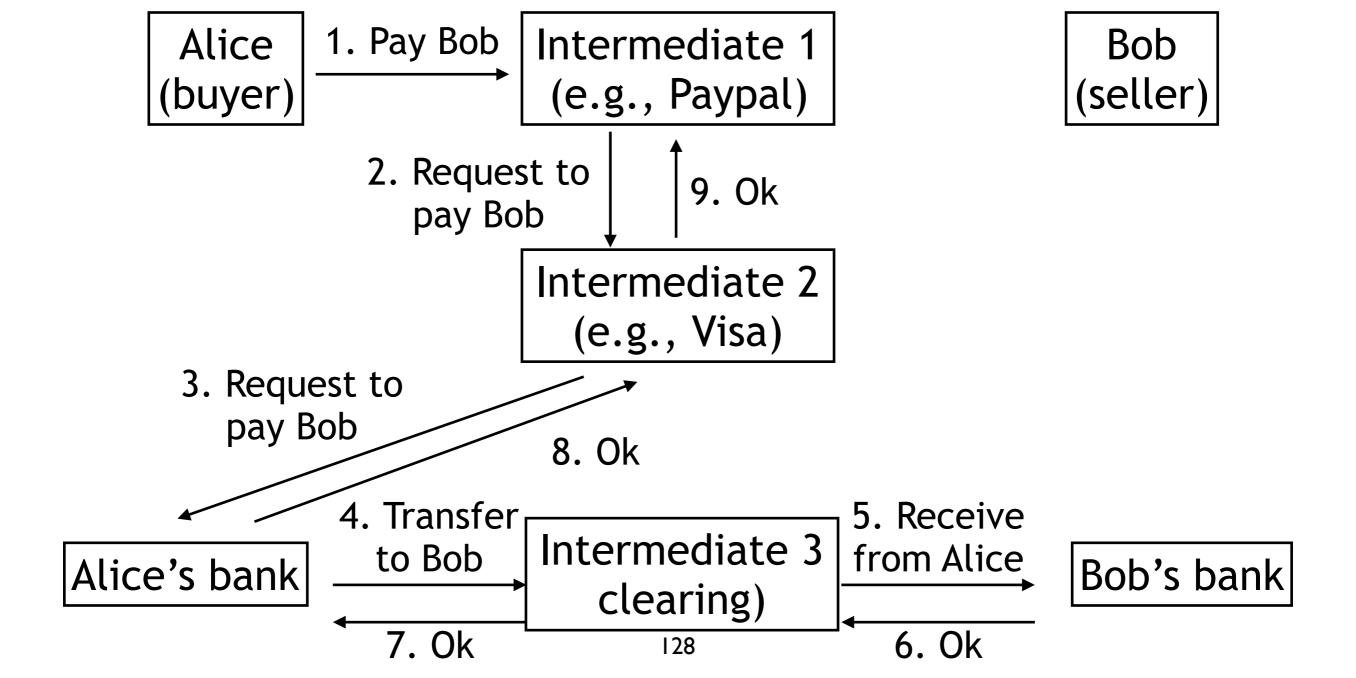
Bob's bank

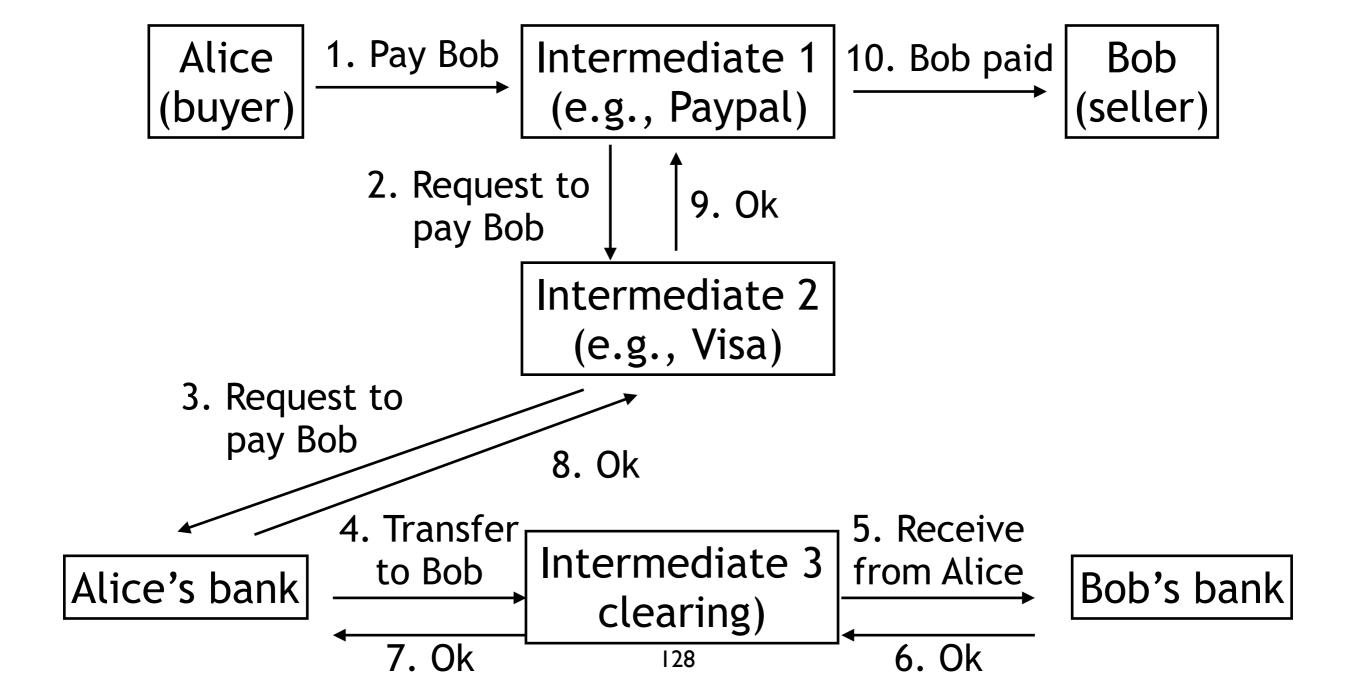


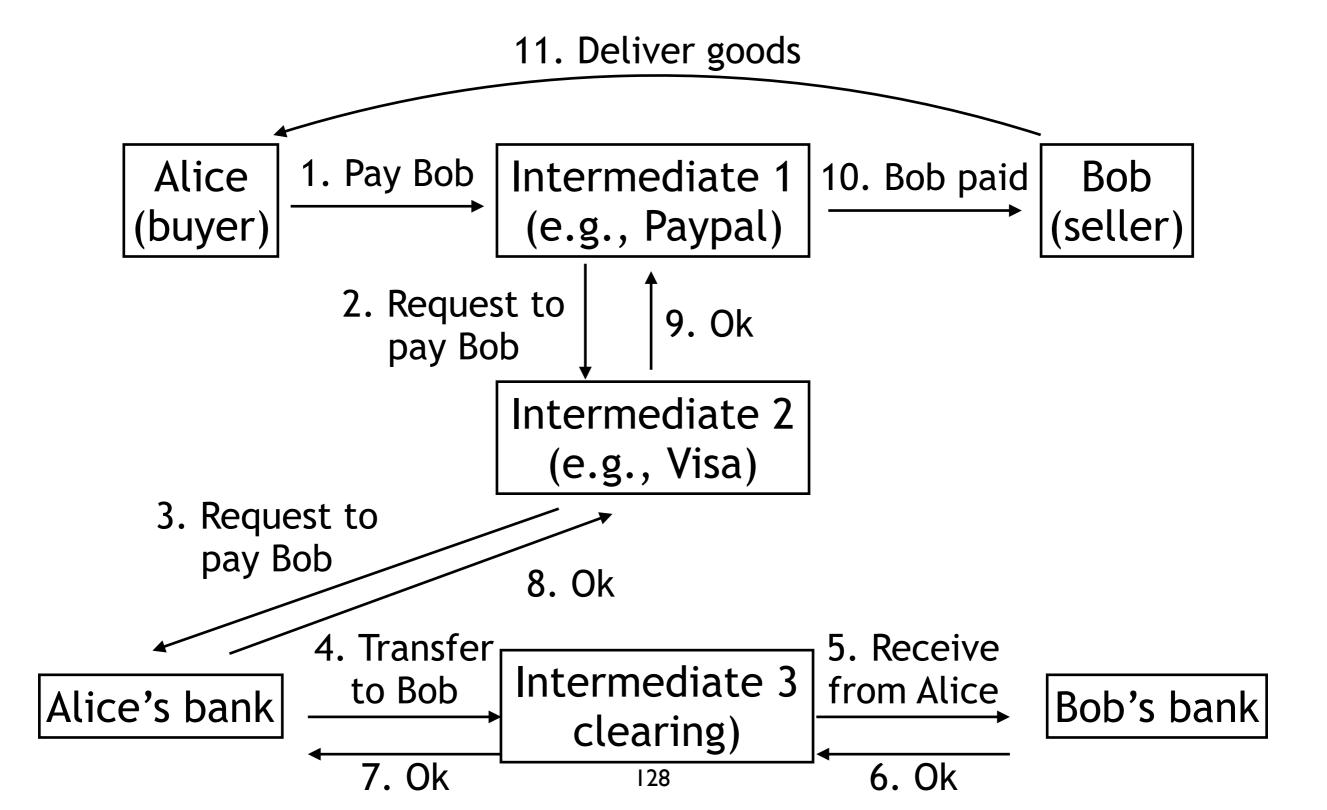








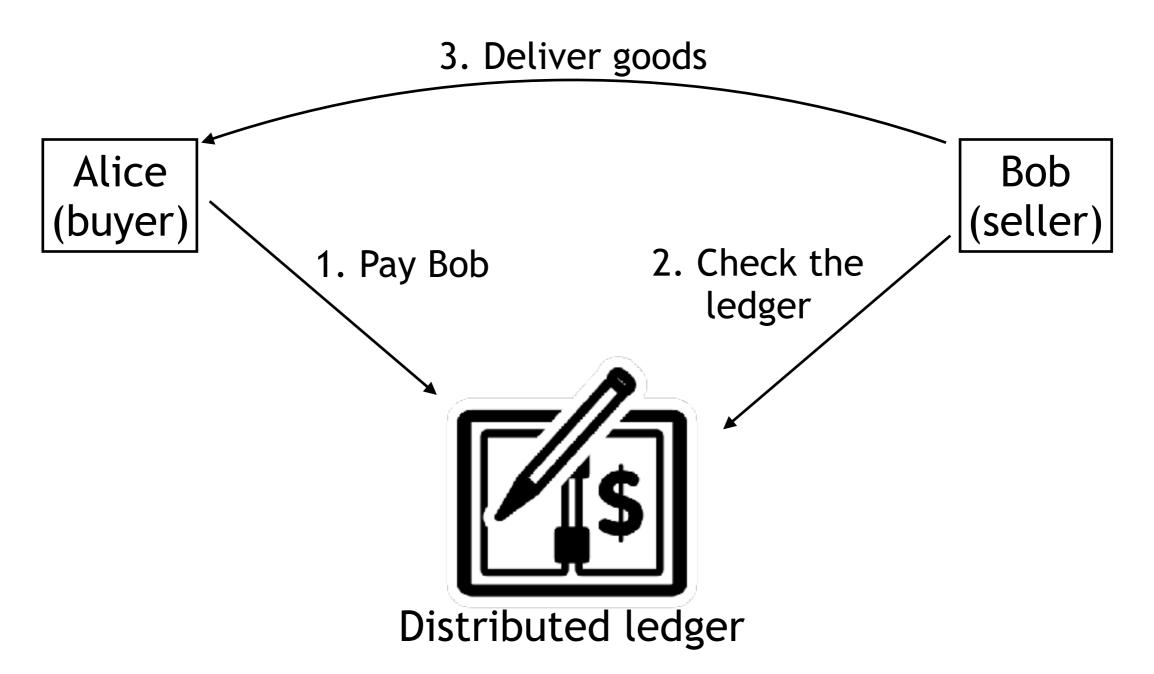




## The role of intermediates: establish trust

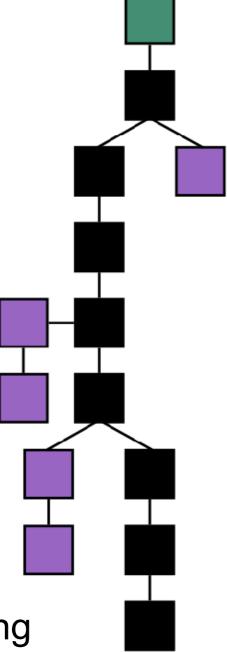
- Alice and Bob don't trust each other
  - need to find a common trusted party
- Banks don't trust each other
  - clearing houses settle transactions
- Each intermediate gets their share and concentrates power

## With the bitcoin: proof



#### Overview

- The blockchain is a list of blocks
  - a block is associated to its cryptographic hash that encompasses
    - the block data
    - the block timestamp
    - the block nonce
    - the hash of the predecessor in the list
      - blocks are "cryptographically linked" preventing them to be tempered
      - the blocks chronology is guaranteed



## Overview (contd.)

- The list of blocks is distributed in the network
  - using a peer-to-peer network (all nodes seem to be connected)
    - supporting broadcast
- Transactions are broadcasted in the network

## Overview (contd.)

- Miners create new block based on the collect transactions
  - a new block is added only if the majority of miners agree
  - every miner collects broadcasted transactions
    - and groups them together to form the data of the block
    - when enough transactions are in the block, the miner computes a valid hash
    - and broadcasts it to the network
  - the first broadcasted new valid block is added as the new head of the blockchain, the fastest miner is the winner
    - the winner is rewarded by gaining some fraction of bitcoin

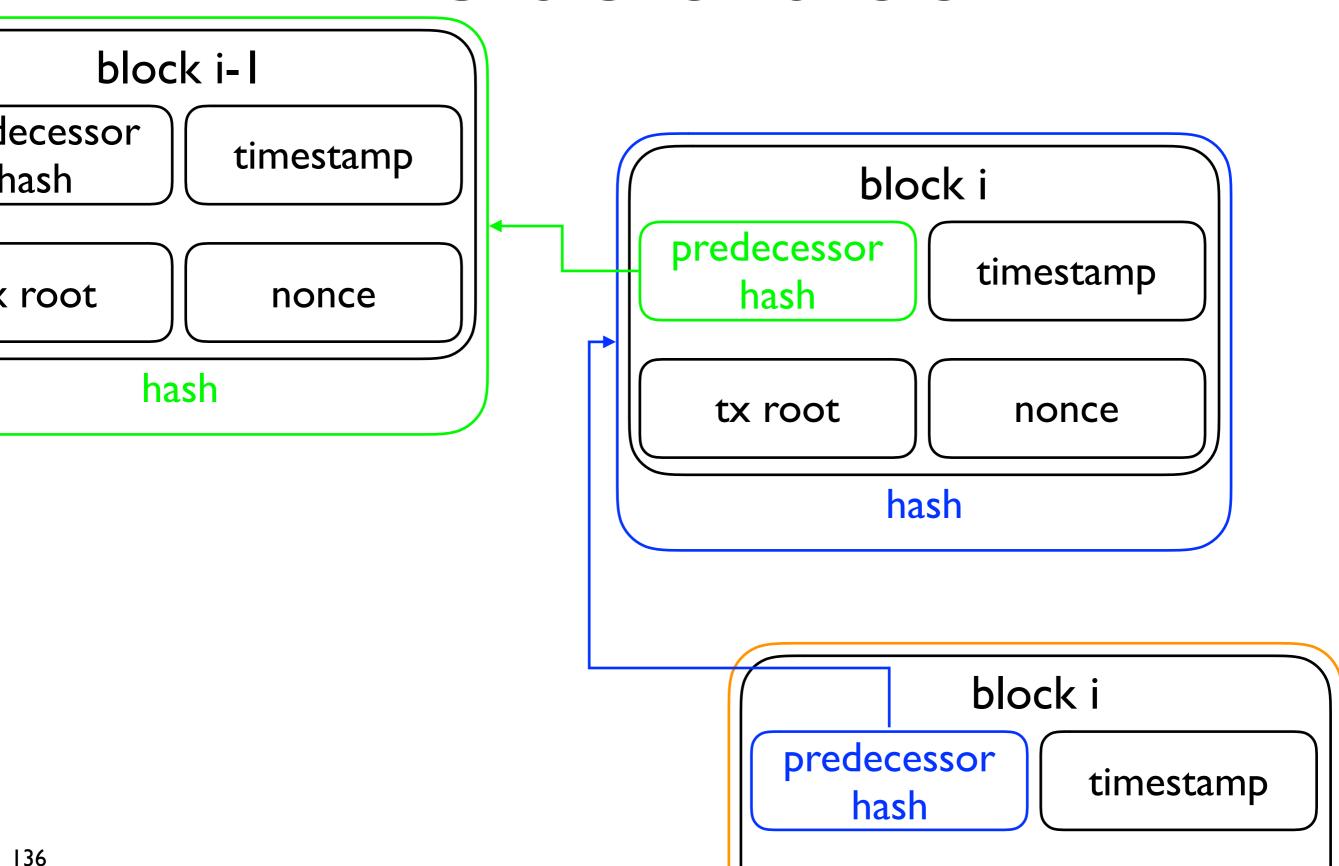
## Making a transactions

- The origin of the transaction
  - adds its bitcoin address
  - adds the bitcoin address of the destination
  - signs the transaction using its private key
  - advertises it in the network
- Anyone can verify the origin of the transaction using the public key
  - and its presence in the blockchain

# How to identity clients in bitcoin?

- Clients have a wallet
  - the wallet is just a private/public key pair
- Identification with a bitcoin address
  - generated for free by any bitcoin user
    - public key = elliptic curve multiplication of the private key
    - bitcoin address = hash of the public key
      - represented with a 26-35 alphanumeric value

## Inside a block



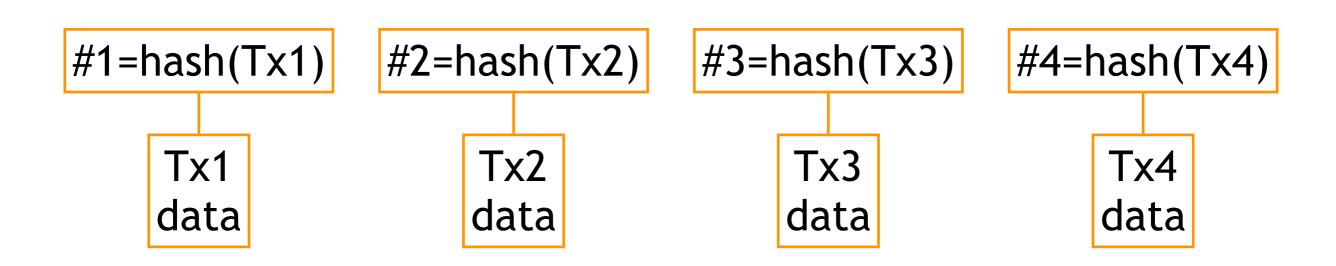
#### Merkel tree

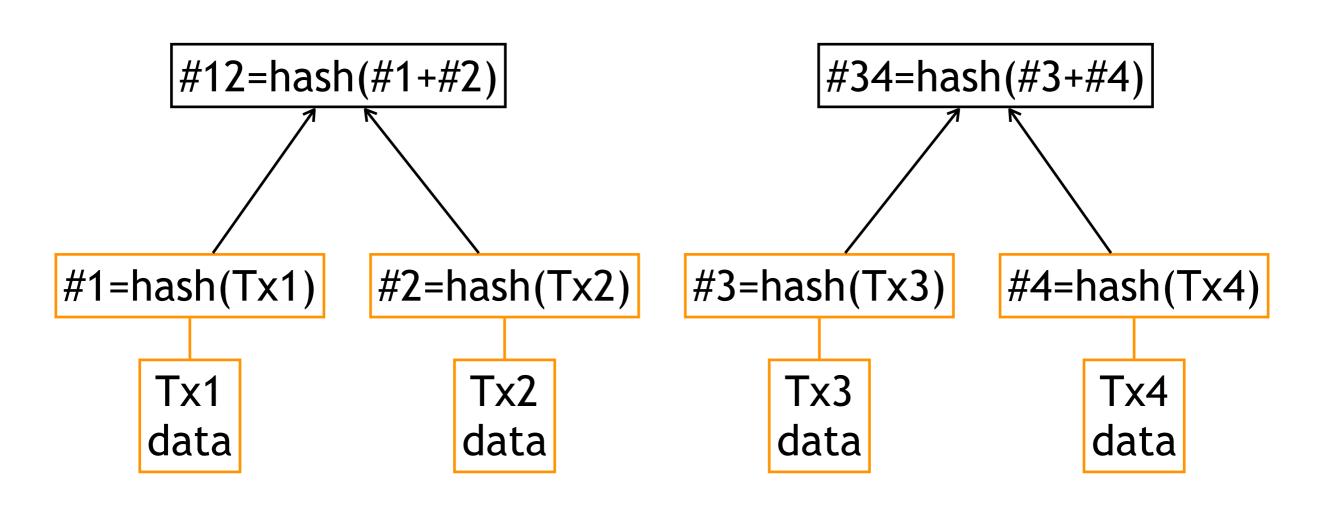
- Transactions are stored in a Merkel tree
- In a Merkel tree
  - the key of a node is the hash of its two children
  - except for the leaves where it is the hash of the data itself
    - in bitcoin, the hash is the SHA-256 hash of the SHA-256 hash of the item to hash

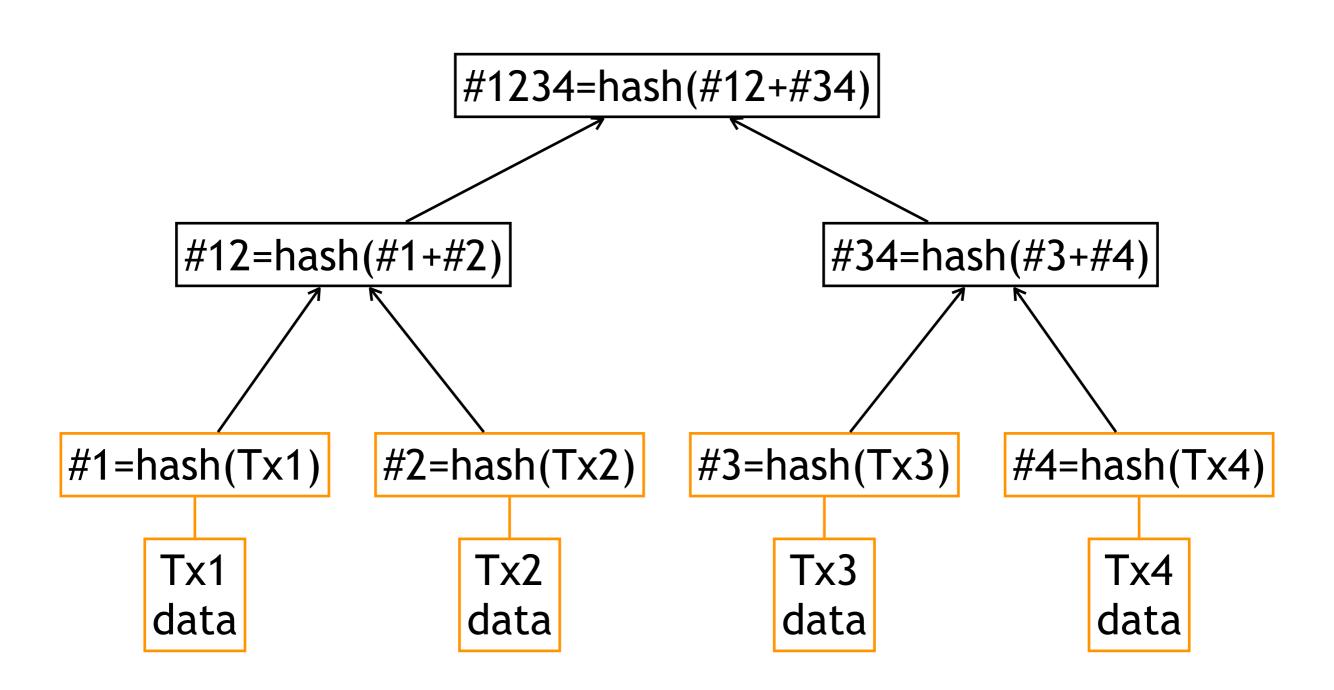
Tx1 data Tx2 data

Tx3 data

Tx4 data







#### Proof of work

- To be accepted, minors must accomplish a proof of work (PoW) on the blocks they advertise
- The PoW is hard to make, easy to check
  - e.g., find a nonce such that the hash of the block is below some target value
    - the target is chosen such that the PoW takes about 10 minutes

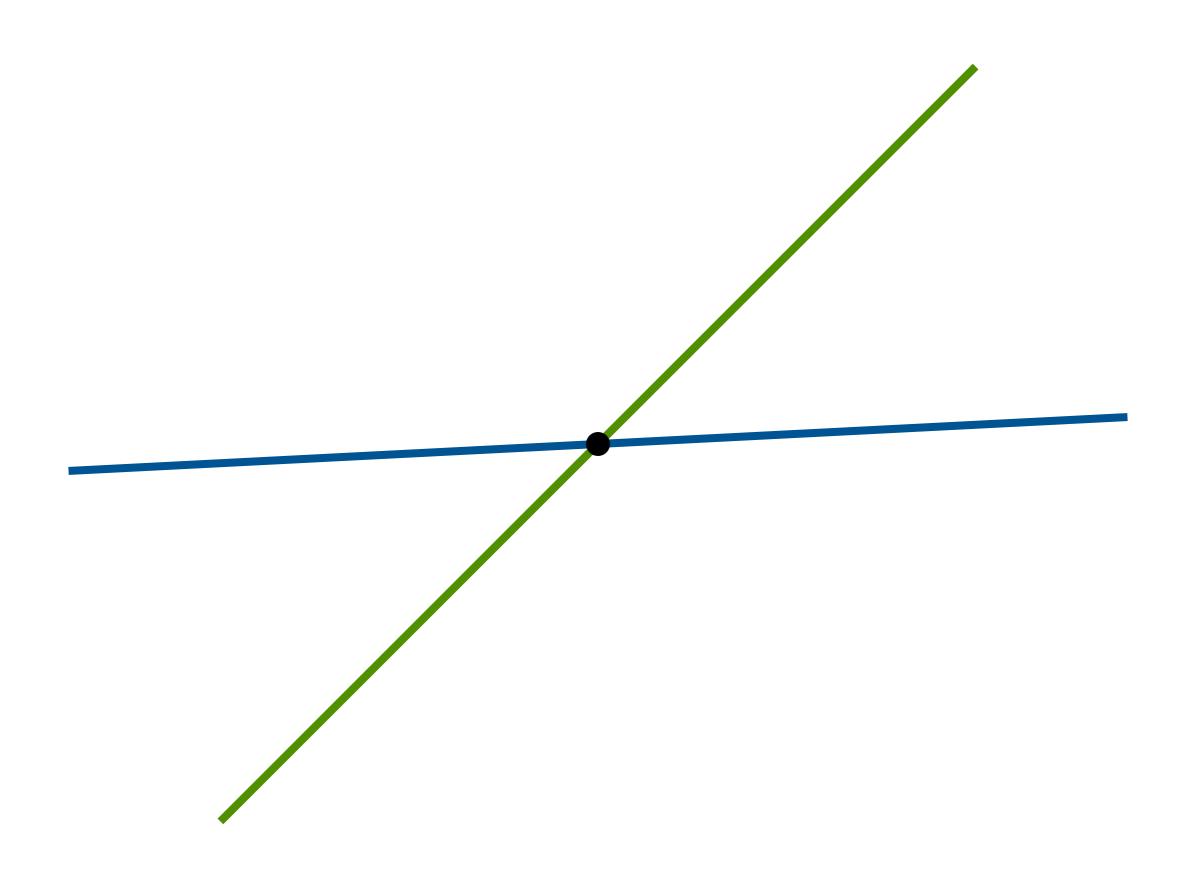
## Branch selection

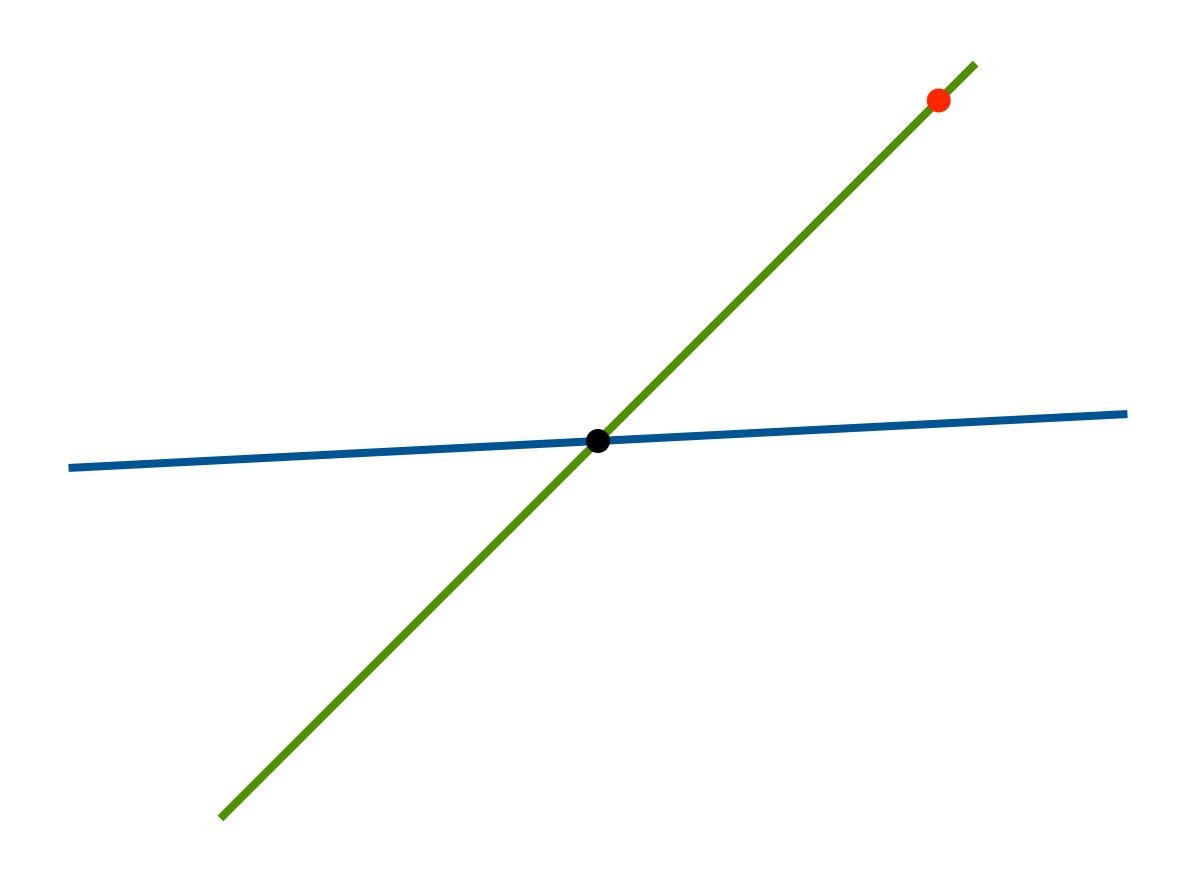
- Multiple branches can be valid (e.g., two minors gave a valid block at the same time)
  - the longest (in terms of complexity) valid branch is selected
  - a block is valid if it has at least 6 successors

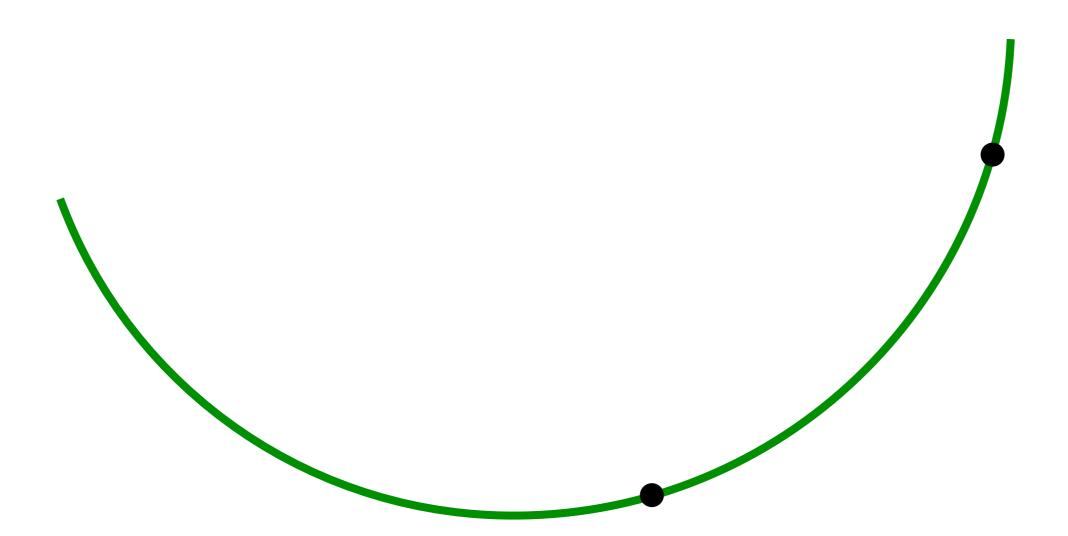
## Privacy

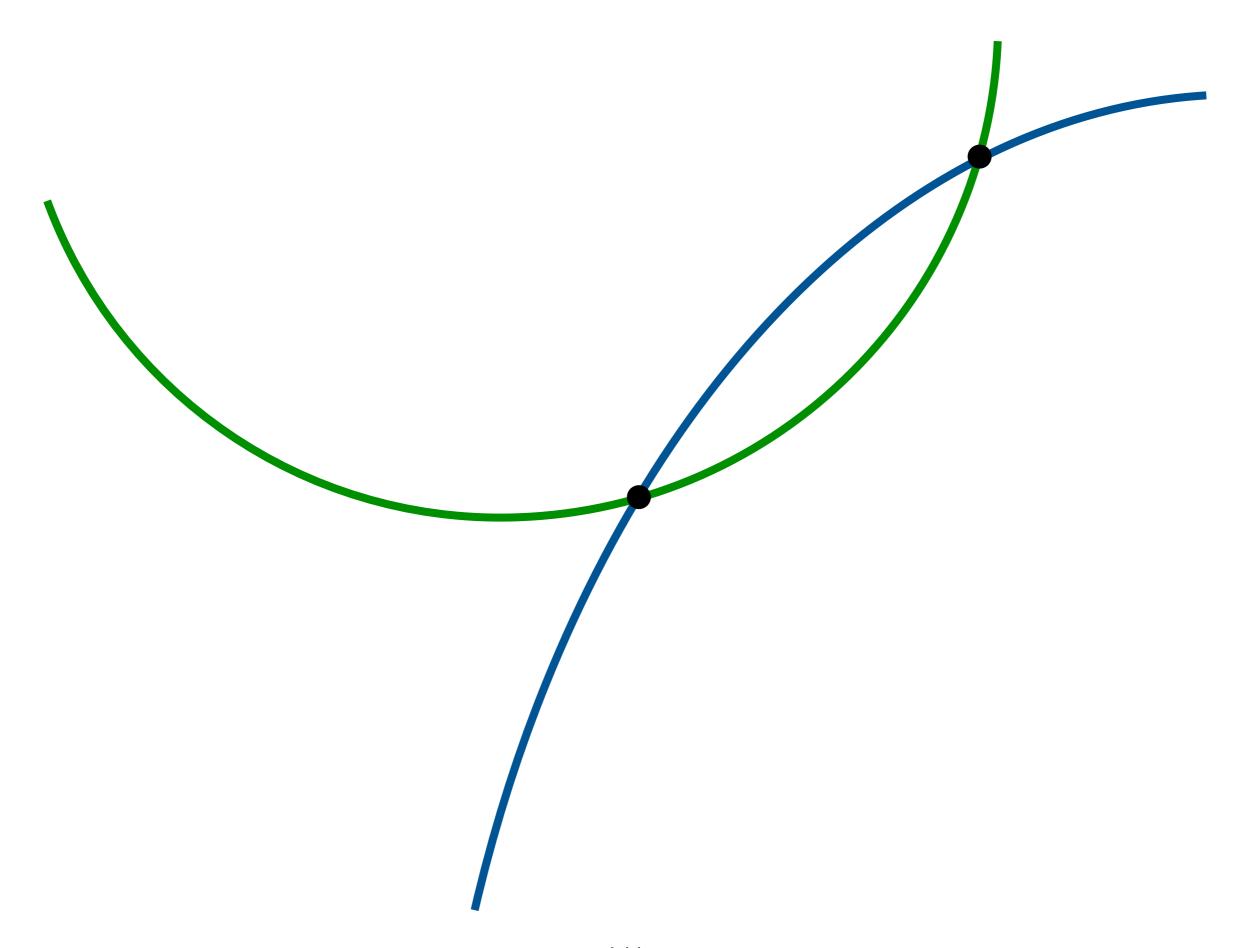
## Sharing secrets

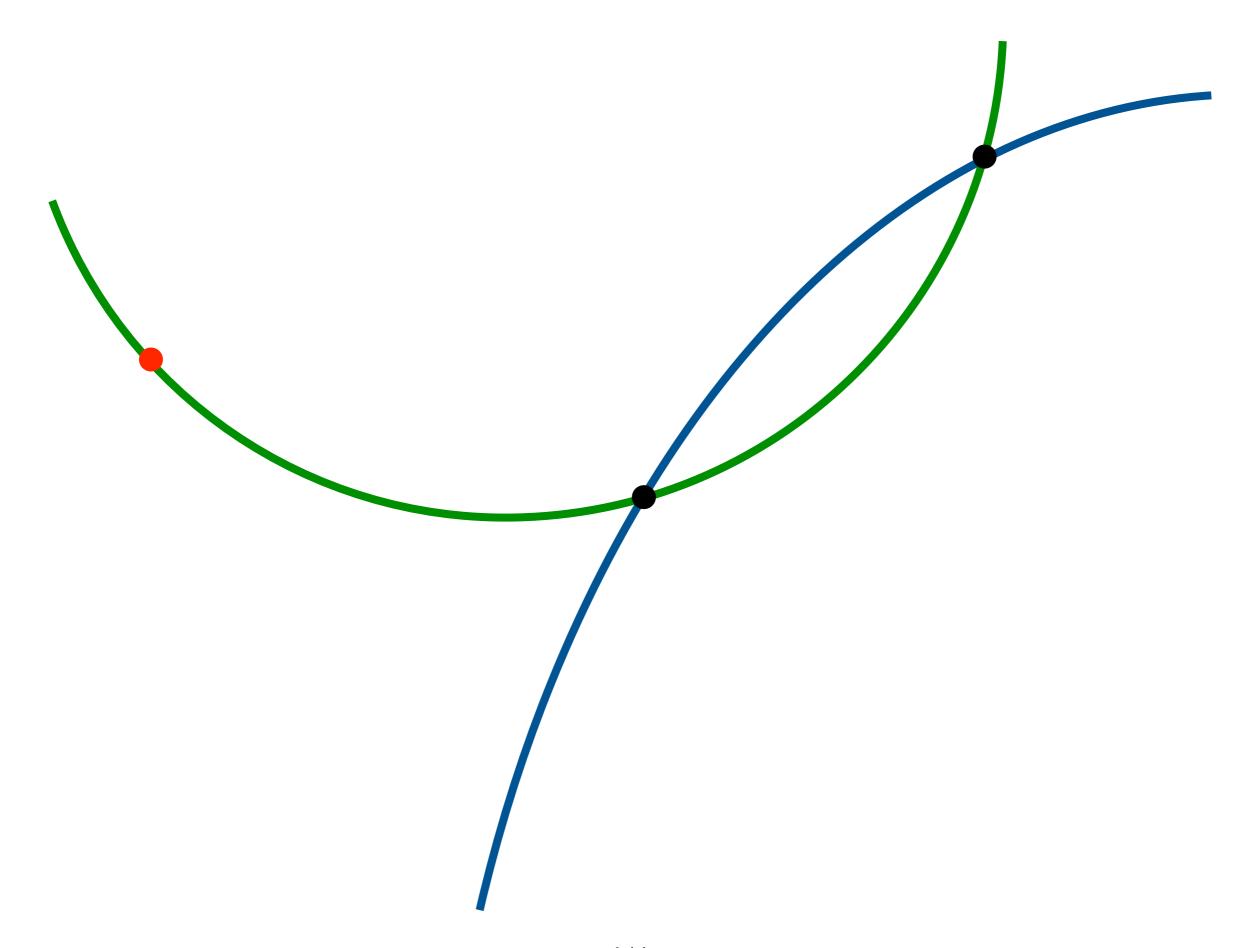
- Context
  - n students work on a top-secret project
  - They cannot trust each other
  - The project is in a digital safe
  - To open the digital safe, at least k out of the n students must be present

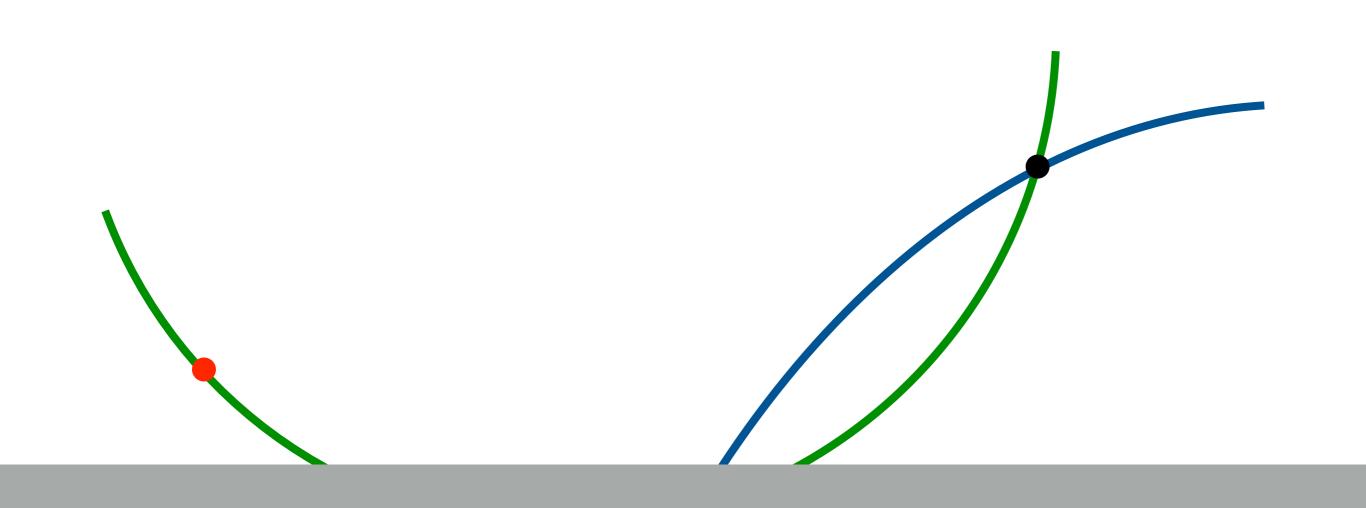








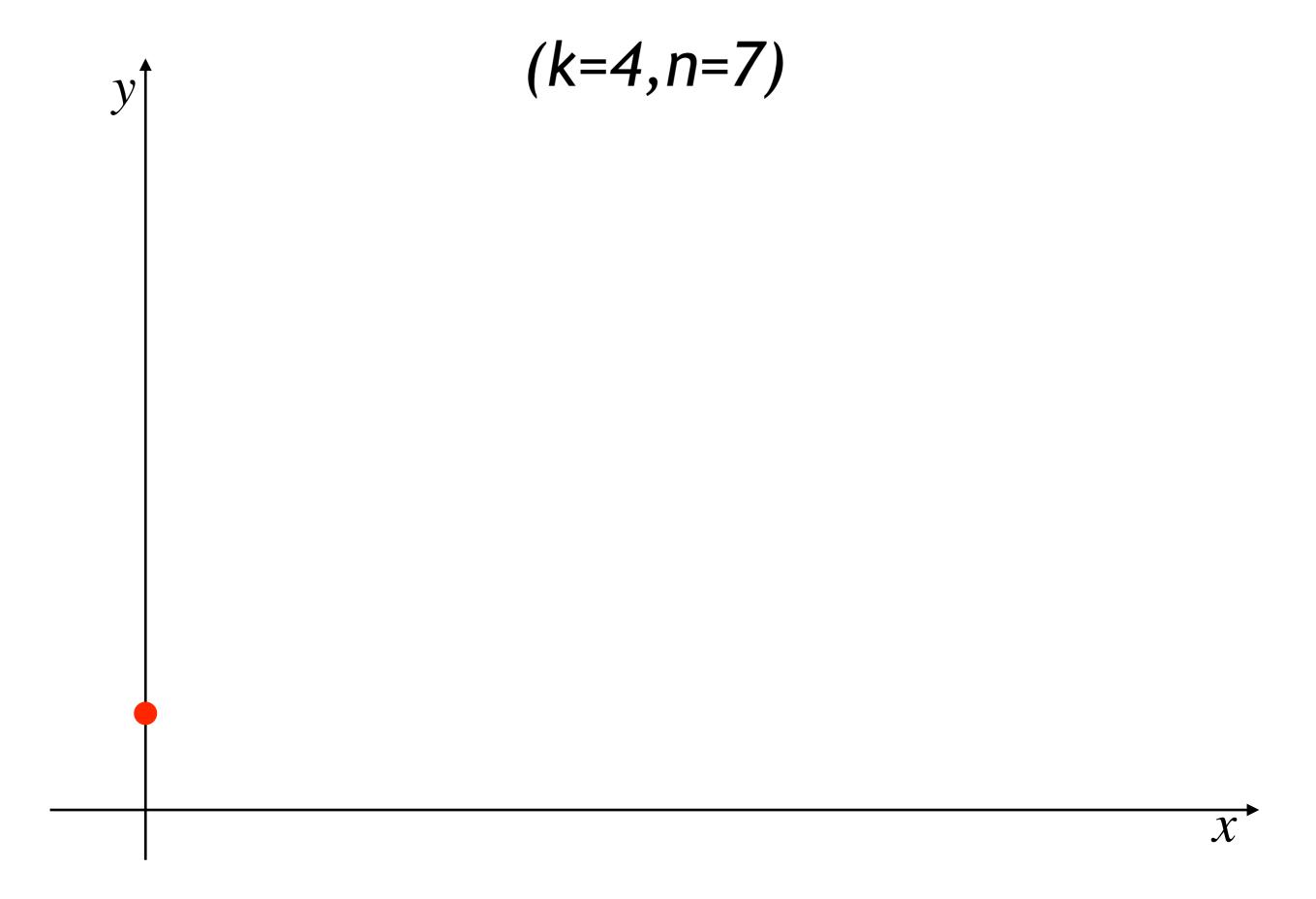


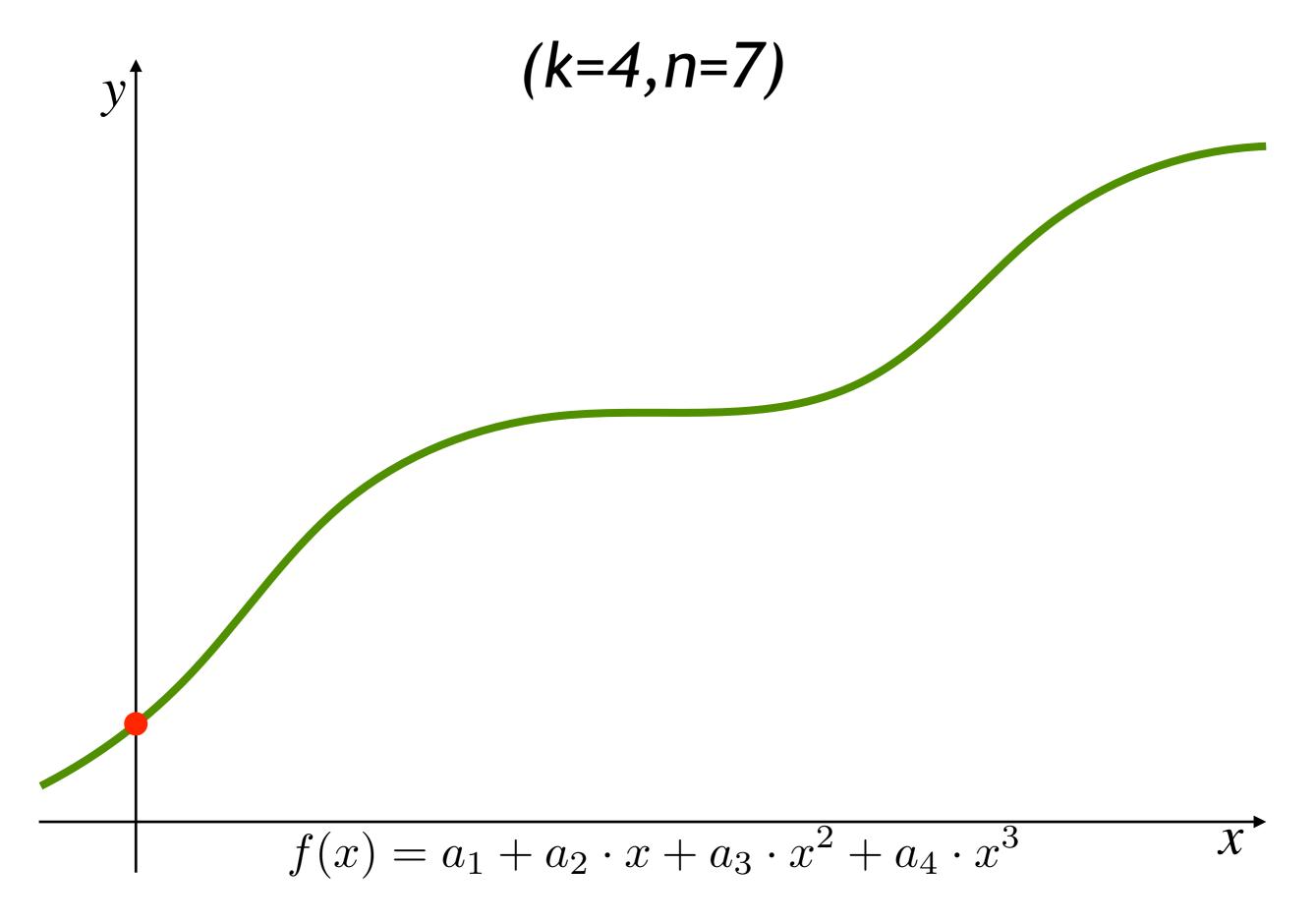


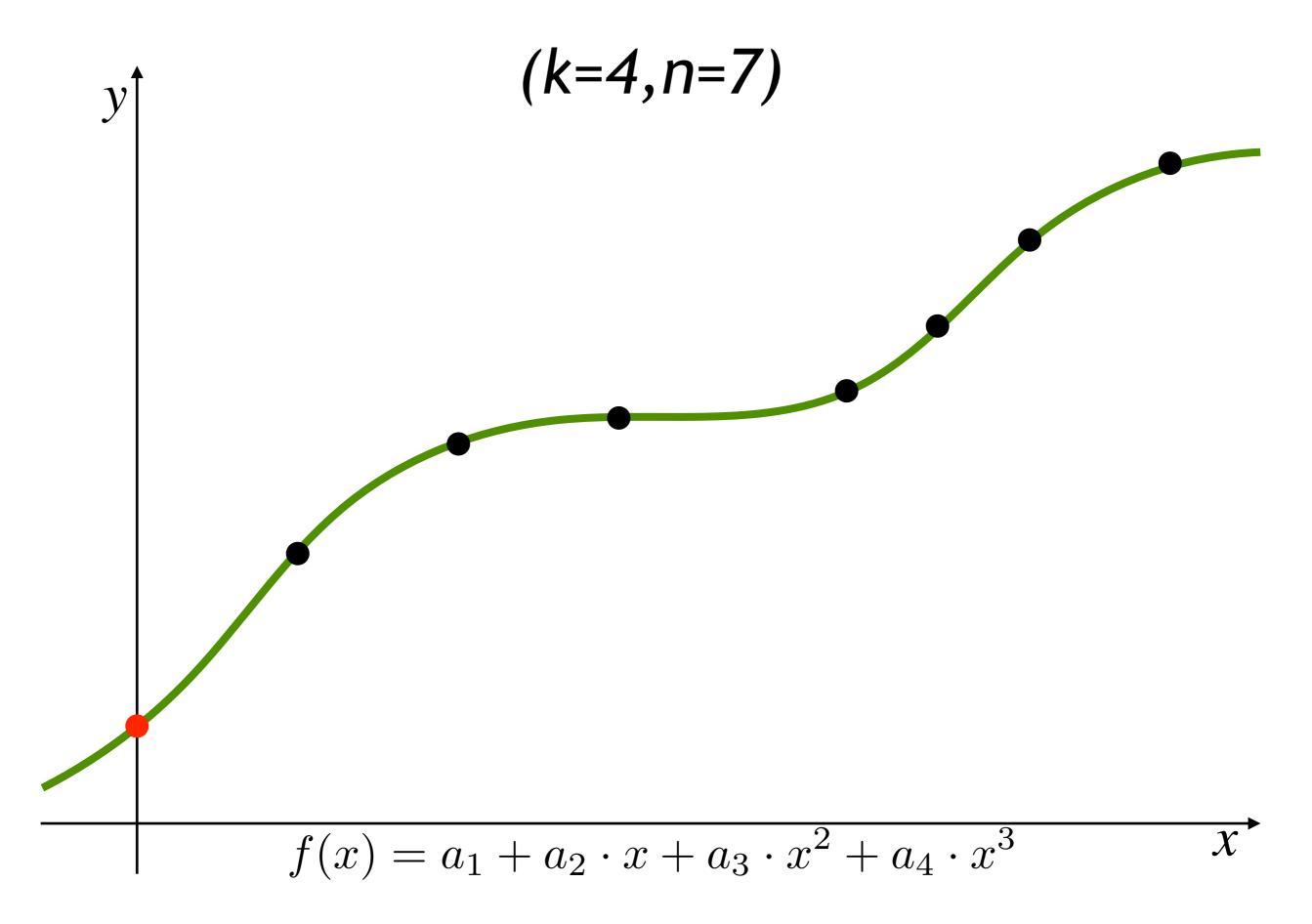
A polynomial of degree k-l is uniquely identified with k points

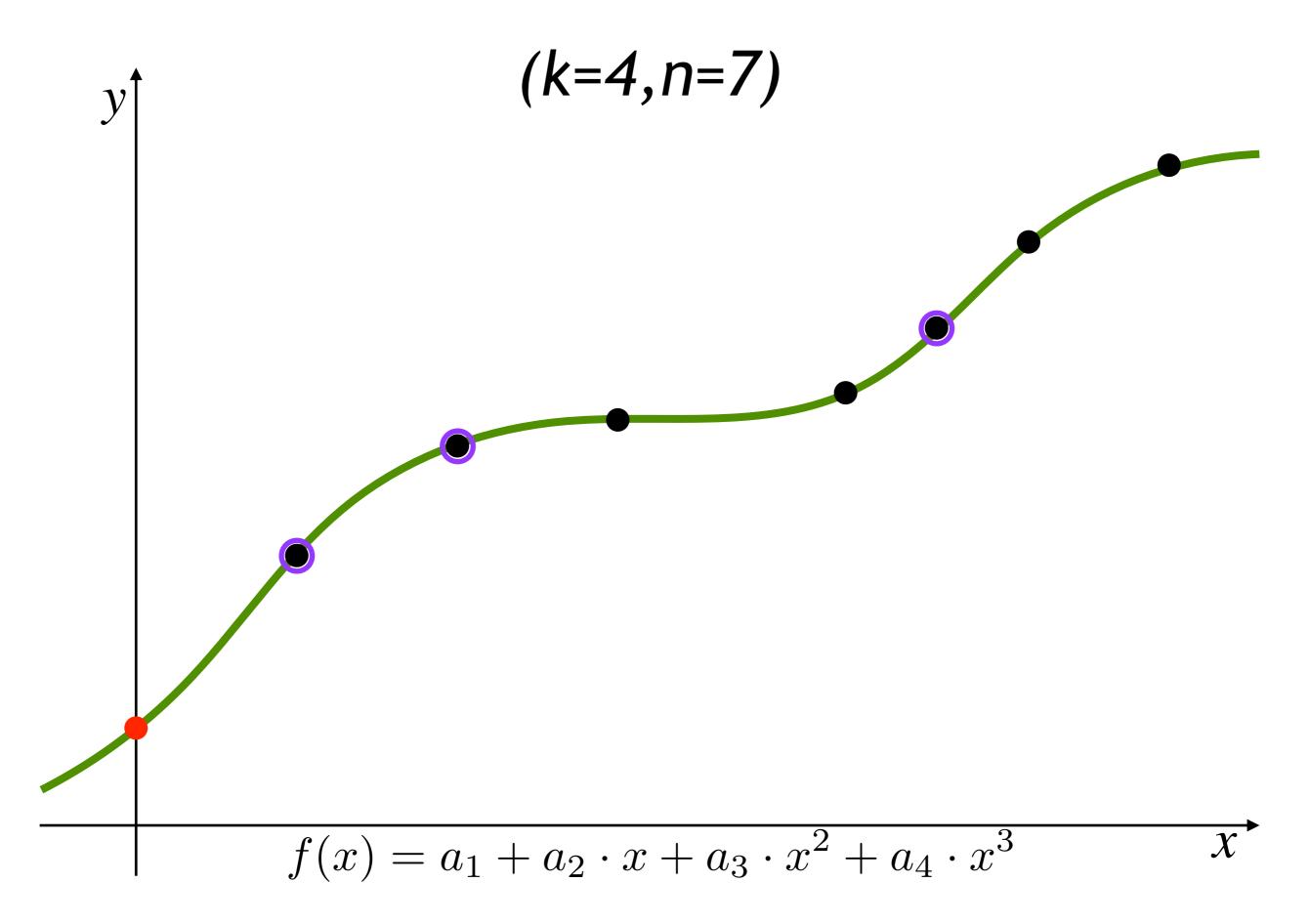
$$(k=4, n=7)$$

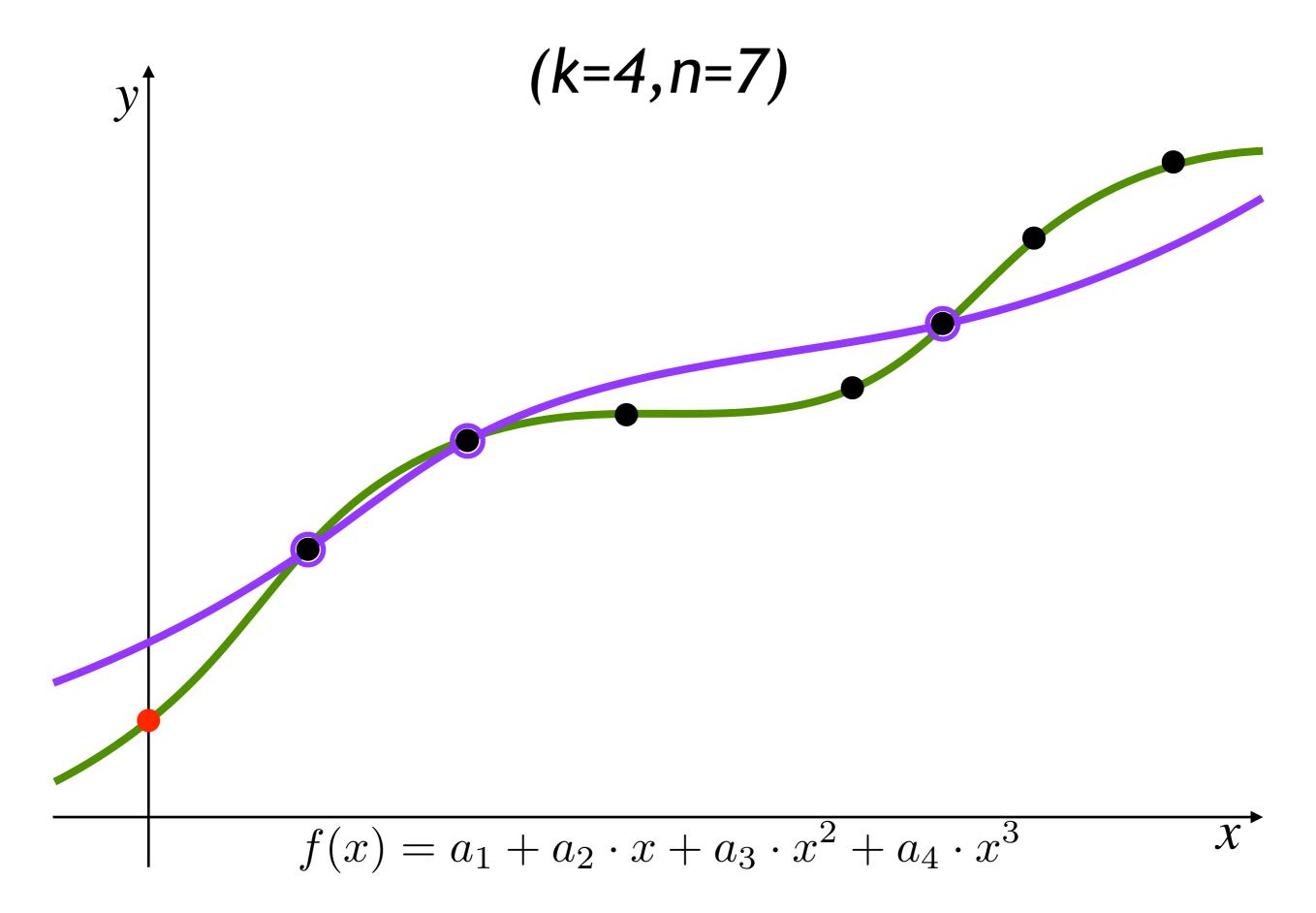
$$(k=4, n=7)$$

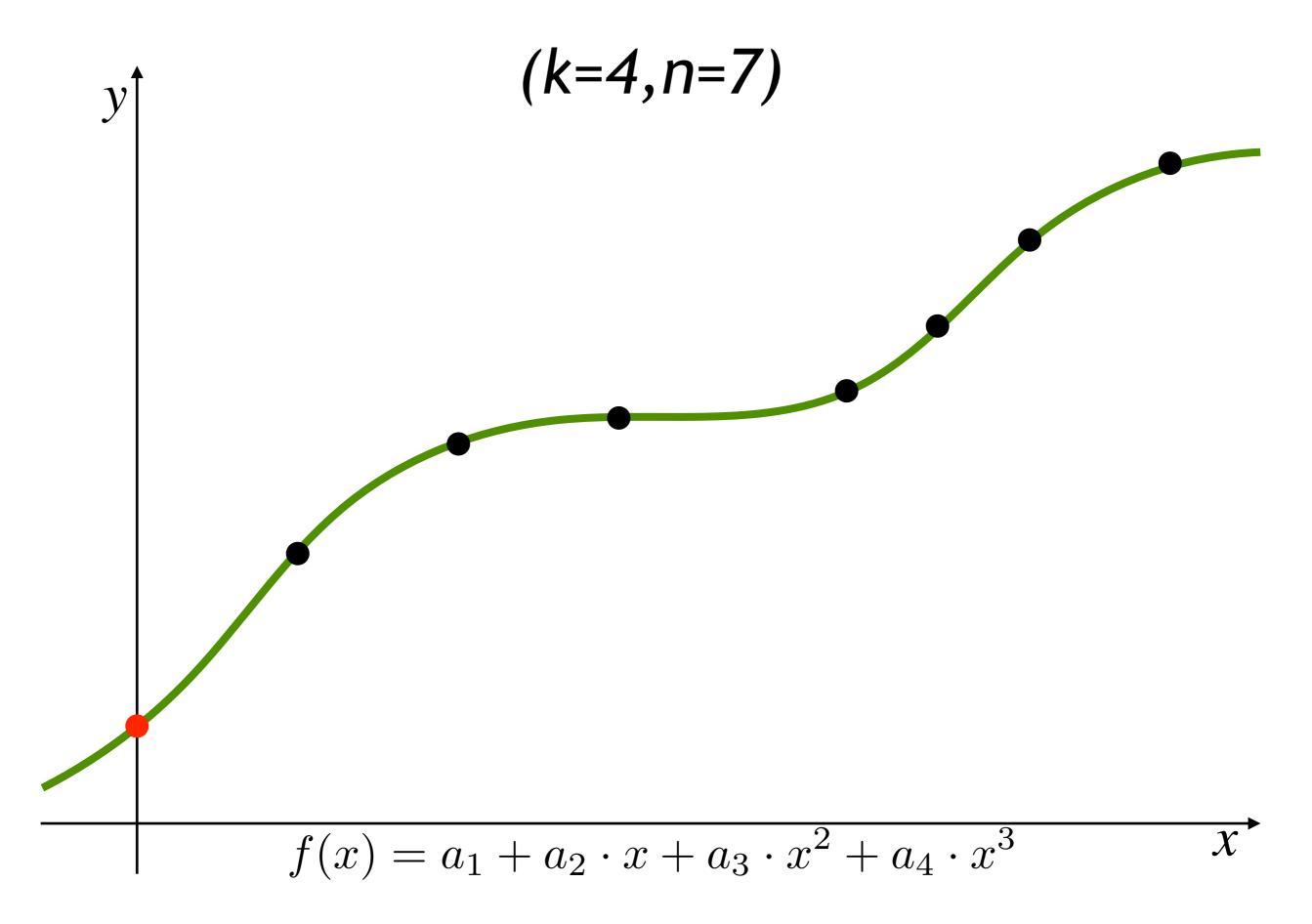


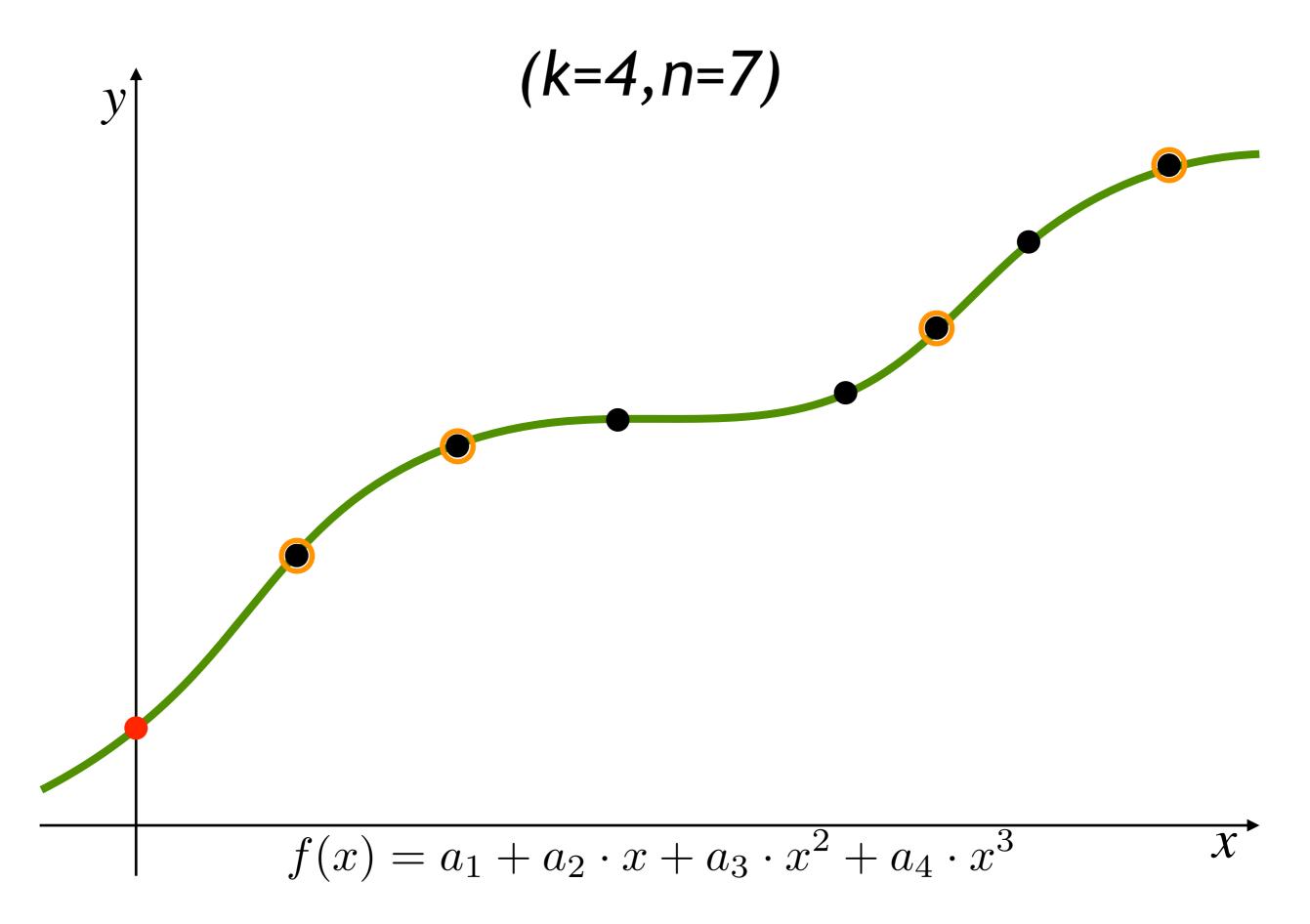


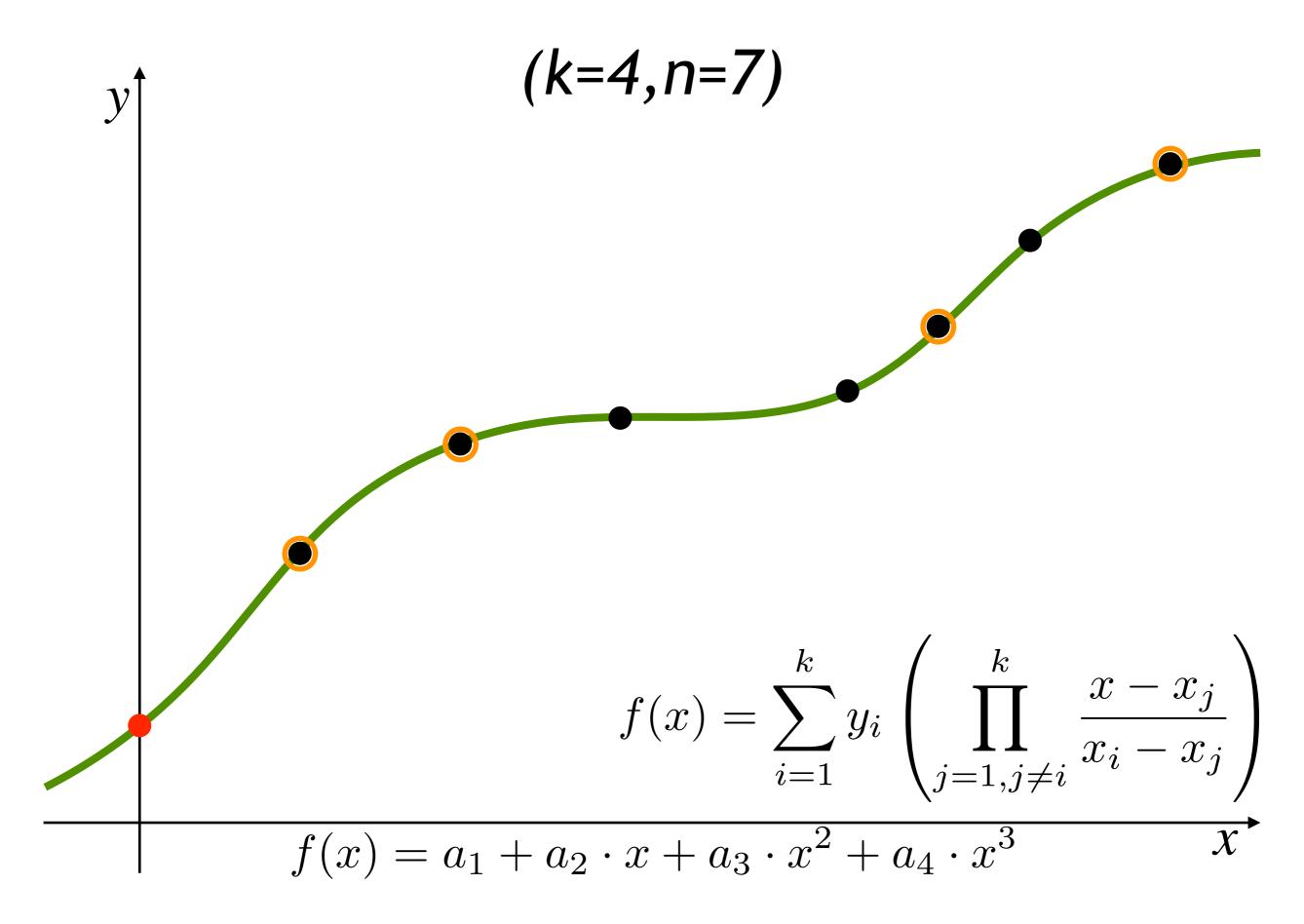


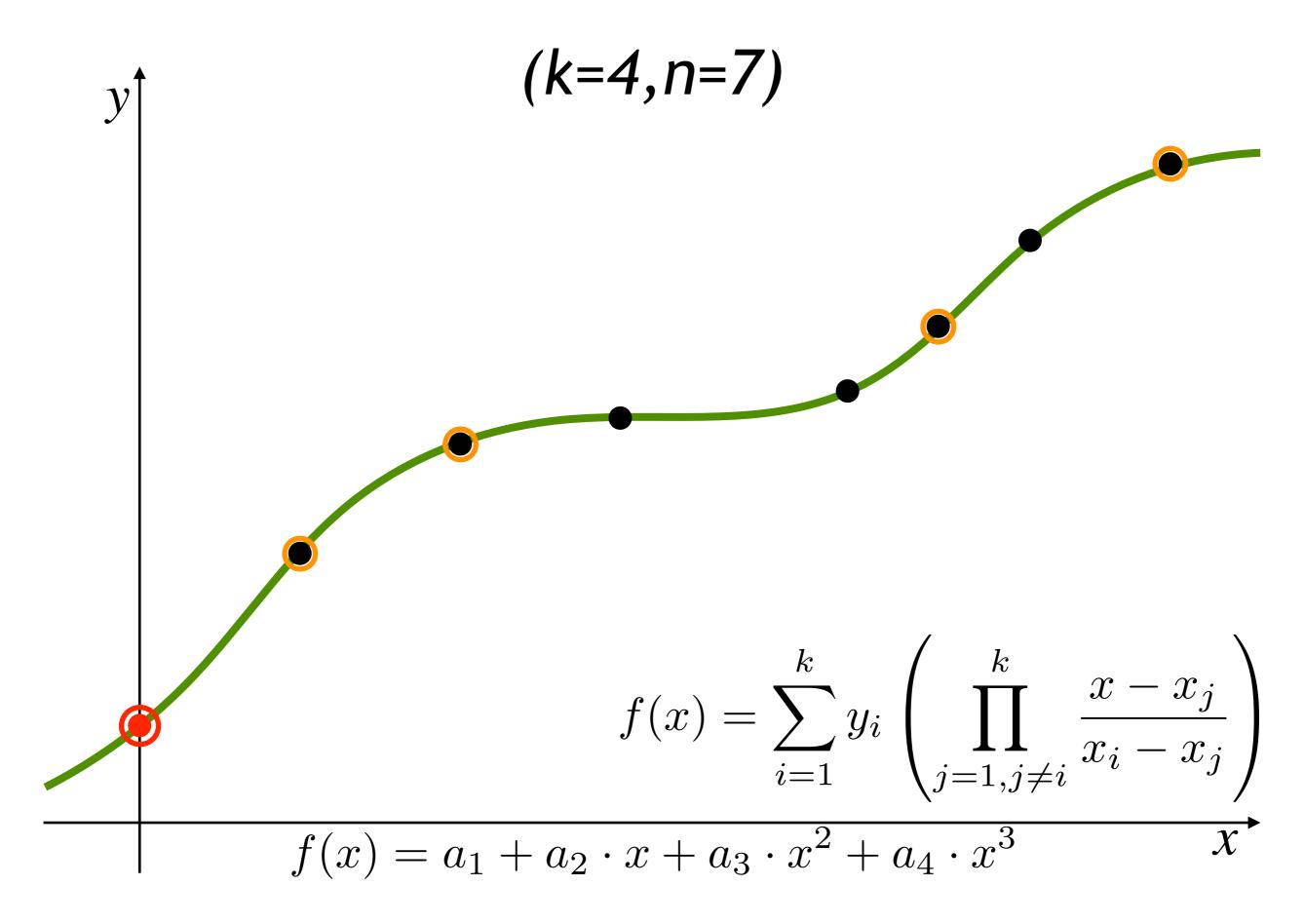












## (k,n) threshold scheme

- $D = [x_1, ..., x_n]$  is a data composed of n pieces
- When at least k pieces x<sub>i</sub> of D are known
  - D can be computed
- otherwise D remains undetermined

## (k,n) threshold scheme

■  $D = [x_1, ..., x_n]$  is a data composed of n pieces

A polynomial of degree k-1 is uniquely identified with k points

- D can be computed
- otherwise D remains undetermined

## Shamir's (k,n) Threshold Scheme

- Let D be our secret (an integer), decomposed in n pieces
- Let p be a prime number  $p > \max(D, n)$
- Generate k-1 random number a<sub>i</sub>

$$\forall i \in [1; k-1] | a_i \in [0; p[$$

Define the polynomial of degree k-1

$$g(x) = D + a_1 \cdot x^1 + \dots + a_{k-1} \cdot x^{k-1}$$

Note that g(0) = D

## Shamir's (k,n) Threshold Scheme (contd.)

Generate n fragments of the secret

$$D_1 = g(1) \mod p$$
,  $D_2 = g(2) \mod p$ , ...  $D_n = g(n) \mod p$ 

- Distribute  $(x_i, D_i)$
- Recompute D from k fragments (x<sub>j</sub>,D<sub>j</sub>) among n using Lagrange polynomial interpolation

$$g(0) = \sum_{i=1}^{k} D_i \left( \prod_{j=1, j \neq i}^{k} \frac{-x_j}{x_i - x_j} \right)$$
$$D \equiv g(0) \mod p$$

#### Example k=3, n=5

**p** = 997

- $f(x) = \sum_{i=1}^{k} y_i \left( \prod_{j=1, j \neq i}^{k} \frac{x x_j}{x_i x_j} \right)$
- Make 5 groups
  - group 1: (1, 547)
  - group 2: (2, 629)
  - group 3: (3, 394)
  - group 4: (4, 839)
  - group 5: (5, 967)

### Example k=3, n=5

- p = 997
- $f(x) = \sum_{i=1}^{k} y_i \left( \prod_{j=1, j \neq i}^{k} \frac{x x_j}{x_i x_j} \right)$
- Make 5 groups
  - group 1: (1, 547)

Collaborate with 2 other groups to compute the secret D

- group 4: (4, 839)
- group 5: (5, 967)

# Example k=3, n =5 (contd.)

Group 1, 3, 4

$$g(0) = 547 \left( \frac{-3}{1-3} \frac{-4}{1-4} \right) + 394 \left( \frac{-1}{3-1} \frac{-4}{3-4} \right) + 839 \left( \frac{-1}{4-1} \frac{-3}{4-3} \right)$$

$$g(0) = 547 * 2 - 394 * 2 + 839 = 1145$$

$$g(0) mod 997 = 148$$

# Example k=3, n =5 (contd.)

To compute it, we took D = 148, p = 997 a prime number, and the polynomial

```
p=997 (prime), a_1=59 (random), a_2=340(random) g(x)=148 + 59x + 340x<sup>2</sup>
```

Such that

$$D_1 = g(1) \mod 997 = 547$$

$$D_2 = g(2) \mod 997 = 1626 \mod 997 = 629$$

$$D_3 = g(3) \mod 997 = 3385 \mod 997 = 394$$

$$D_4 = g(4) \mod 997 = 5824 \mod 997 = 839$$

$$D_5 = g(5) \mod 997 = 8943 \mod 997 = 967$$

## Shamir's (k,n) Threshold Scheme (contd.)

- The size of each fragment does not exceeds the size of the secret
  - as long as p is chosen of the same order as the secret
- Possible to generate new fragments at any time, without altering the others
- Possible to construct hierarchies by attributing more or less fragments
  - the boss has k fragments, the subaltern has k/2, ...
- No assumption as opposed to cryptographic functions

#### Anonymity

- Alice wants to send a message to Bob
  - Communications are unsecured
  - Nobody can know who is the sender (not even Bob)
  - Nobody can know who is the receiver
  - Nobody else than Bob can retrieve the message

#### Mix

- Objectives of a mix
  - Hide correspondences between incoming and outgoing messages
  - Not possible to map a source and an outgoing message (apart for the mix)
  - No possible to map a receiver and an incoming message (apart for the mix)

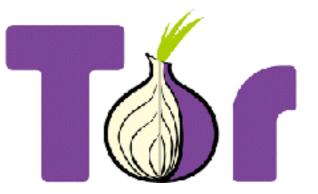
#### Mix (contd.)

- If the mix cannot be fully trusted, use a cascade of mixes
- It works as long as untrusted mixes do not collaborate all together

#### Chaum-net

- Allow to send a sealed message via a cascade of mixes
- In an overlay, each participant has a private/public key pair
- Alice randomly choses a few of them (e.g., 3) to be mixes
- Alice recursively encrypt the message with the public key of each mixes she selected

### Chaum-net



- Allow to send a sealed message via a cascade of mixes
- In an overlay, each participant has a private/public key pair
- Alice randomly choses a few of them (e.g., 3) to be mixes
- Alice recursively encrypt the message with the public key of each mixes she selected

Alice



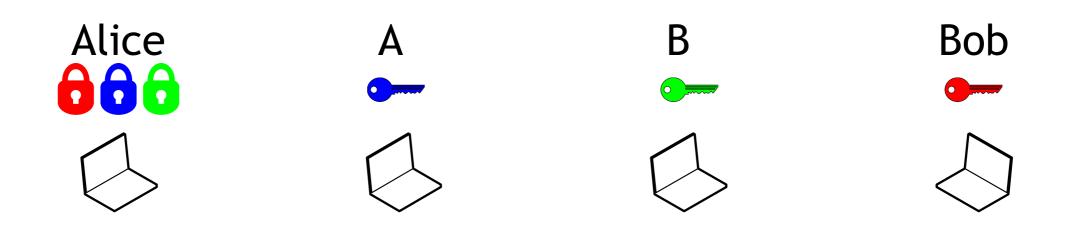
Alice



m

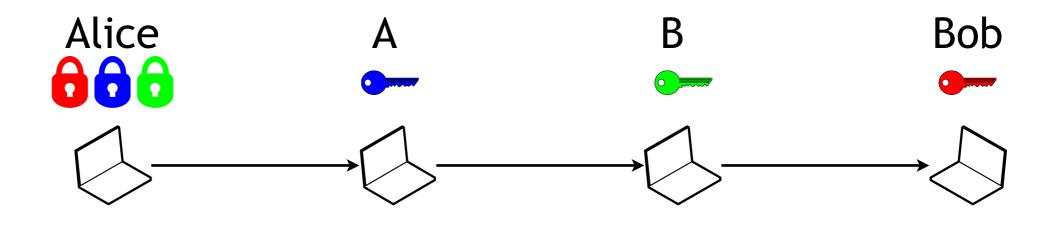
Alice A B Bob

m

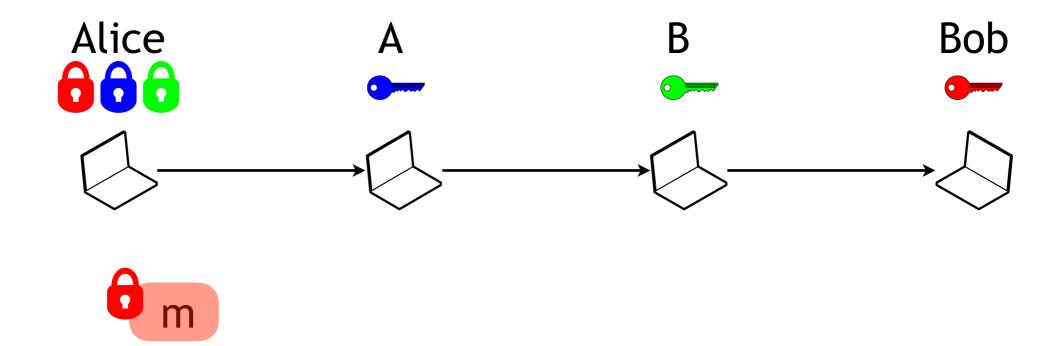


m

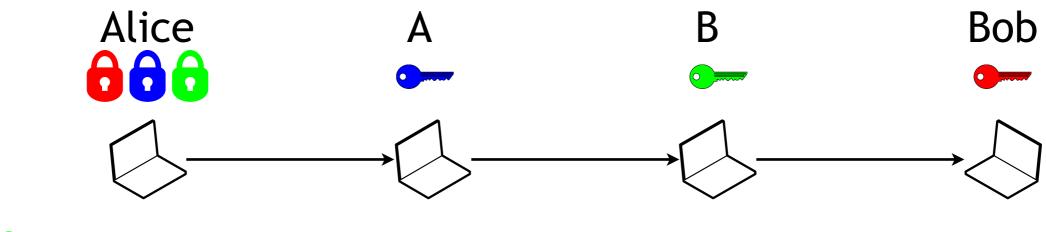
157



m



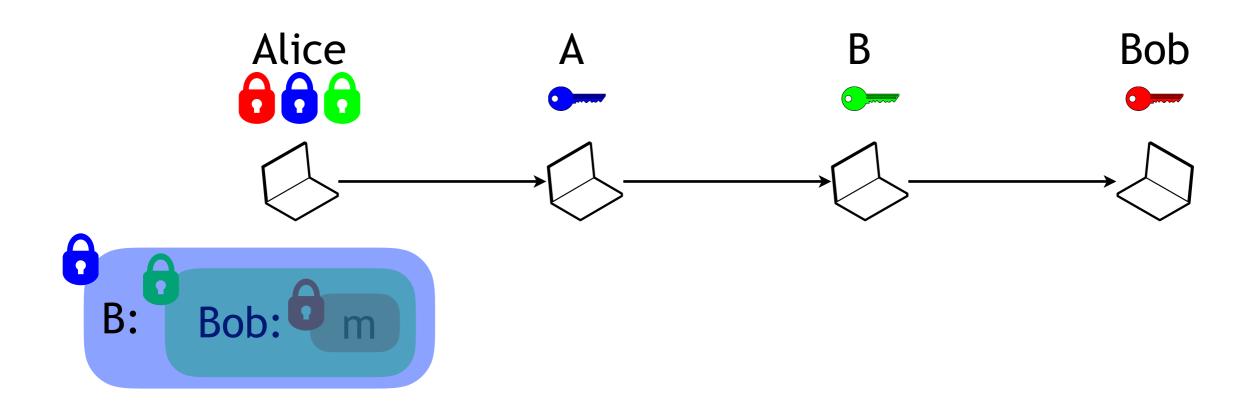
 $K_{Bob}(R_0, m)$ 



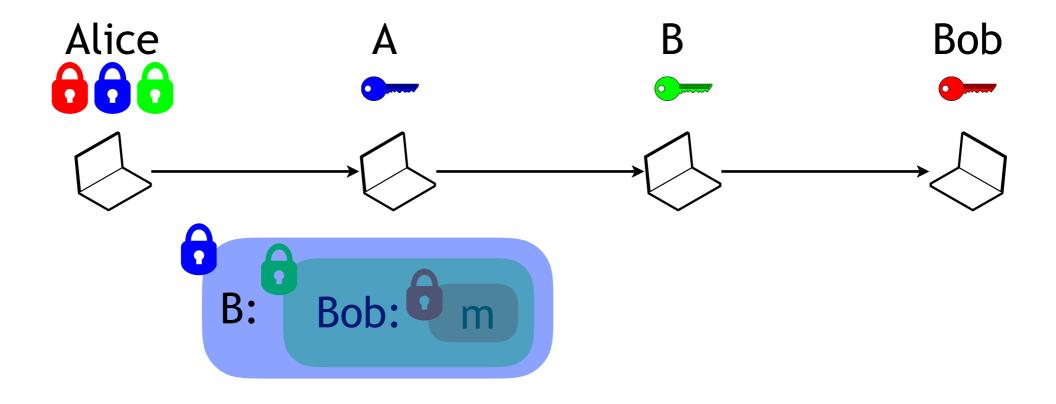


 $K_{Bob}(R_0, m)$ 

 $K_B(Bob, R_I, K_{Bob}(R_0, m))$ 

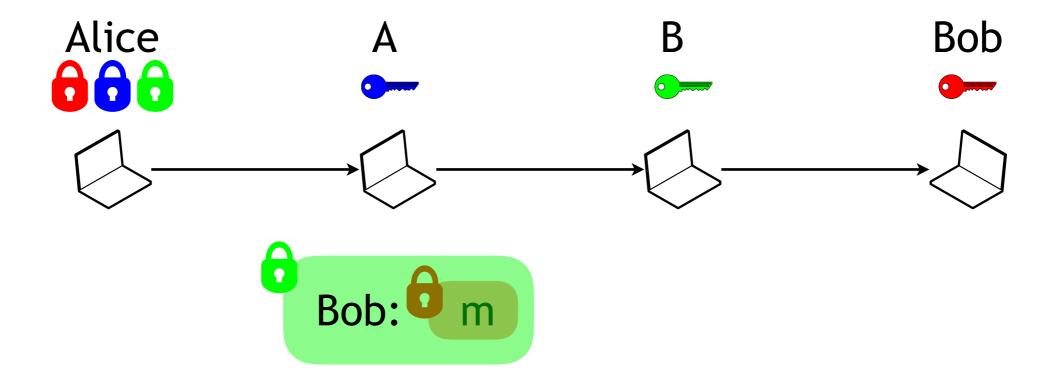


 $K_{Bob}(R_0,m)$   $K_{B}(Bob,R_1,K_{Bob}(R_0,m))$   $K_{a}(B,R_2,K_{B}(Bob,R_1,K_{Bob}(R_0,m)))$ 



 $K_{Bob}(R_0, m)$   $K_{B}(Bob, R_1, K_{Bob}(R_0, m))$ 

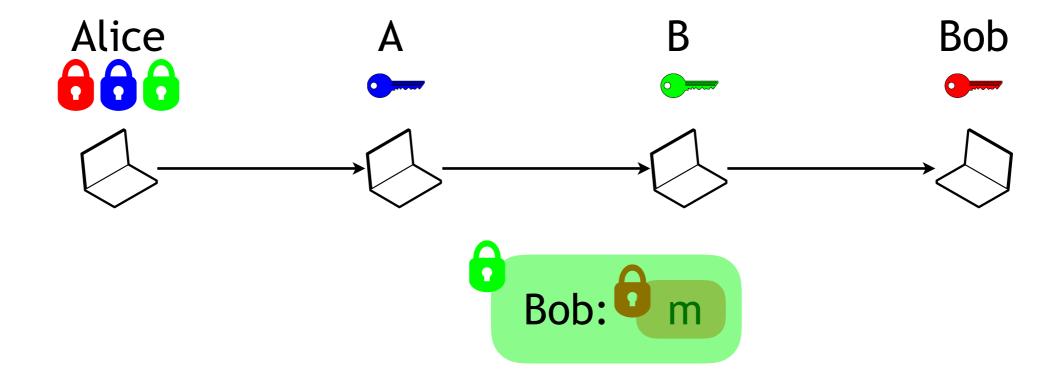
 $K_a(B, R_2, K_B(Bob, R_1, K_{Bob}(R_0, m)))$ 



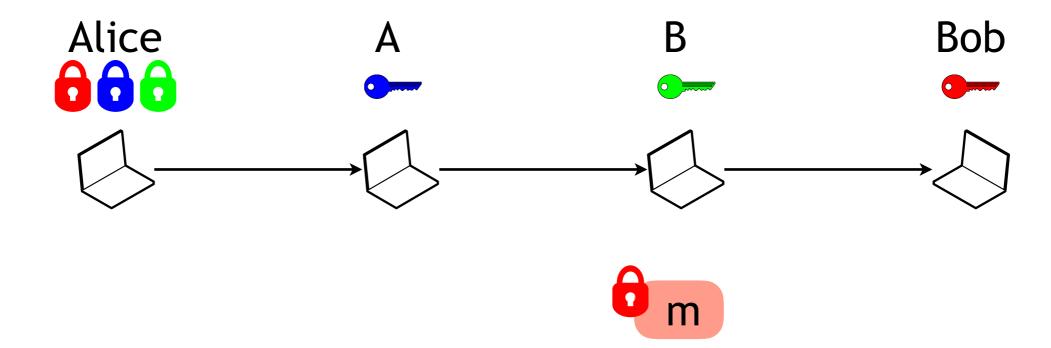
 $K_{Bob}(R_0, m)$ 

 $K_B(Bob, R_I, K_{Bob}(R_0, m))$ 

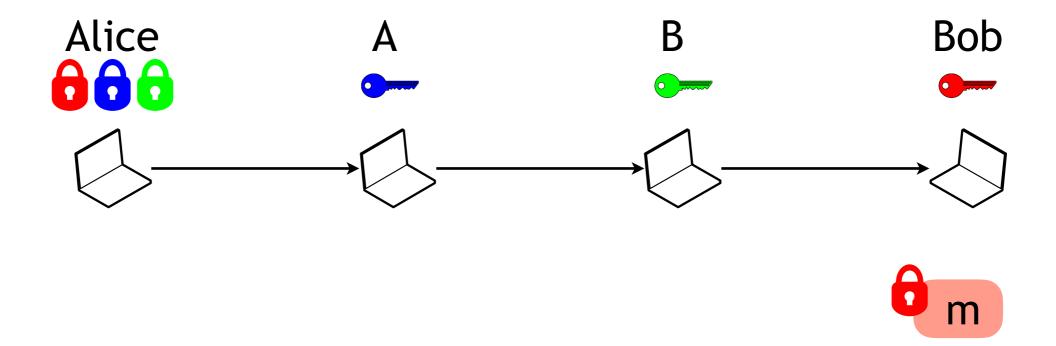
 $K_a(B, R_2, K_B(Bob, R_1, K_{Bob}(R_0, m)))$ 



 $K_{Bob}(R_0,m)$   $K_{B}(Bob,R_1,K_{Bob}(R_0,m))$   $K_{a}(B,R_2,K_{B}(Bob,R_1,K_{Bob}(R_0,m)))$ 

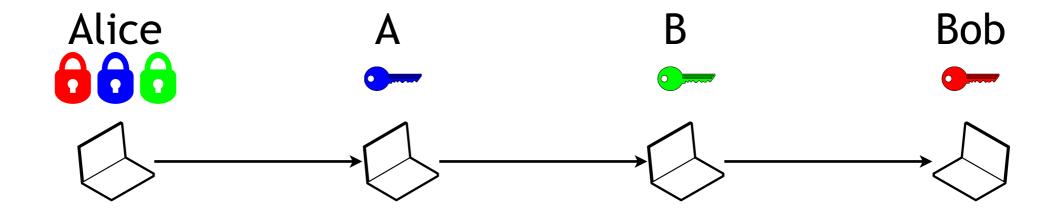


 $K_{Bob}(R_0, m)$   $K_{B}(Bob, R_1, K_{Bob}(R_0, m))$   $K_{a}(B, R_2, K_{B}(Bob, R_1, K_{Bob}(R_0, m)))$ 



 $K_{Bob}(R_0, m)$   $K_{B}(Bob, R_1, K_{Bob}(R_0, m))$   $K_{a}(B, R_2, K_{B}(Bob, R_1, K_{Bob}(R_0, m)))$ 

# Chaum-net example



m

 $K_{Bob}(R_0, m)$   $K_{B}(Bob, R_1, K_{Bob}(R_0, m))$   $K_{a}(B, R_2, K_{B}(Bob, R_1, K_{Bob}(R_0, m)))$ 

# Chaum-net example



Cool, I am anonymous!

m

 $K_{Bob}(R_0,m)$   $K_{B}(Bob,R_1,K_{Bob}(R_0,m))$   $K_{a}(B,R_2,K_{B}(Bob,R_1,K_{Bob}(R_0,m)))$ 

# Chaum-net example



Are you sure?

m

 $K_{Bob}(R_0,m)$   $K_{B}(Bob,R_1,K_{Bob}(R_0,m))$   $K_{a}(B,R_2,K_{B}(Bob,R_1,K_{Bob}(R_0,m)))$ 

# Social behavior

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Eric Schmidt, directeur général de Google, 2009

Je n'ai rien à cacher!

Je n'ai rien à cacher!

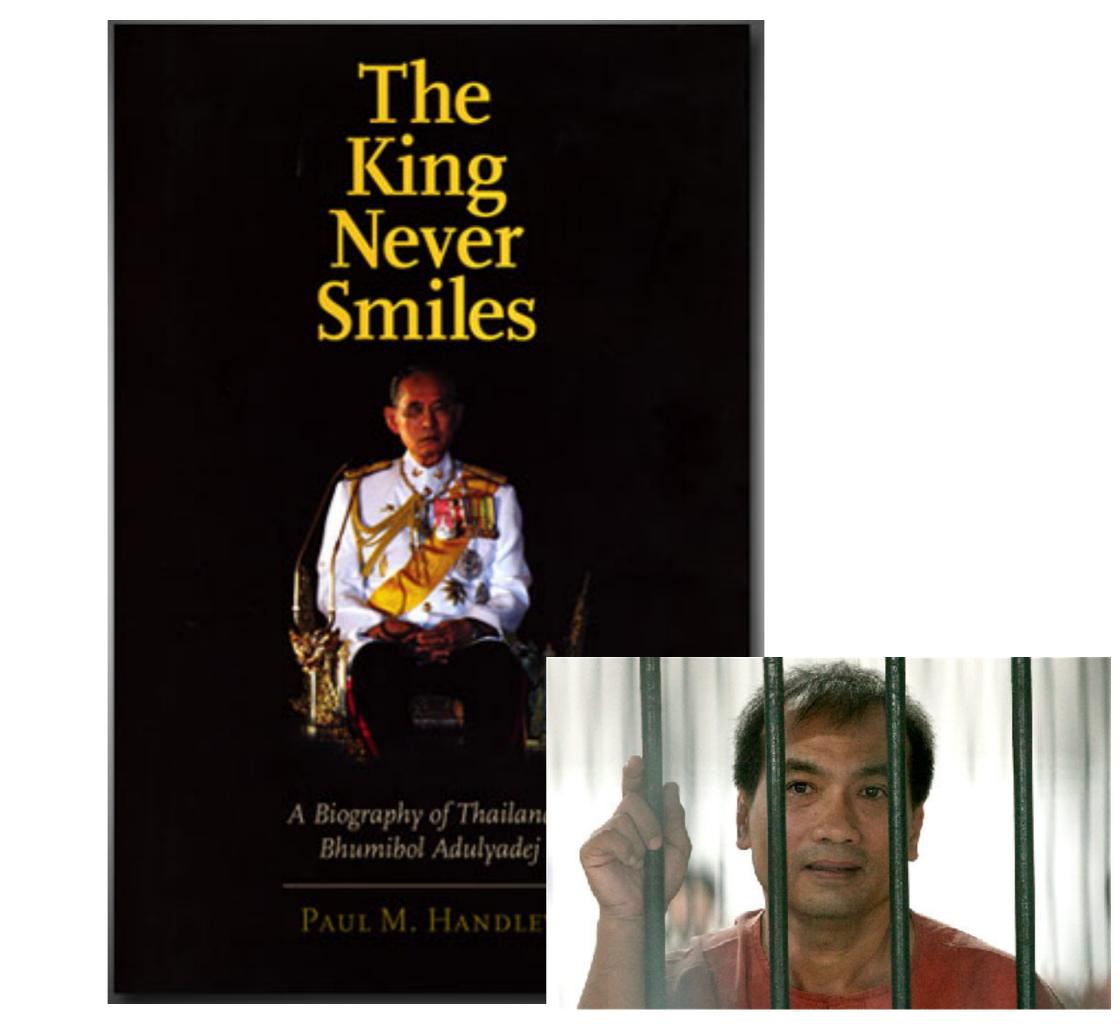
Les définitions de lois et moralité ne sont pas universelles

# The King Never Smiles



A Biography of Thailand's Bhumibol Adulyadej

PAUL M. HANDLEY









# Le site Facebook autorise-t-il les photos de mères en train d'allaiter ?

Oui. Nous reconnaissons la beauté et le caractère naturel de l'allaitement, et nous sommes ravis de savoir qu'il est important pour les mères de partager leurs expériences avec autrui sur Facebook. La plupart de ces photos respectent nos règlements.

Veuillez noter que les photos que nous examinons nous sont presque toutes signalées par d'autres membres qui se plaignent de leur partage sur Facebook.







# Restrictions sur le contenu en France

En France, nous avons restreint l'accès à du contenu signalé dans le cadre de lois interdisant la négation de la Shoah et l'apologie du terrorisme, ainsi que 32 100 cas d'images uniques liés aux attaques terroristes de novembre 2015 à Paris, qui, selon l'OCLCTIC, constituaient des infractions présumées aux lois françaises de protection de la dignité humaine.

# Nombre d'éléments de contenu restreint

37,695



Je suis invisible sur Internet

# Je suis invisible sur Internet

Mais je l'utilise tout le temps et partout







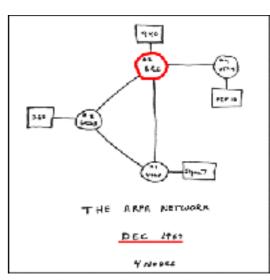
# Je suis invisible sur Internet

Mais je l'utilise tout le temps et partout





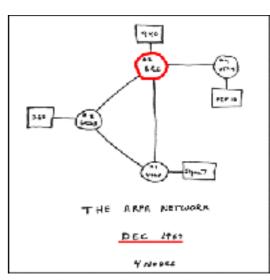
# L'Internet a beaucoup changé



[ARPANET logic map,1969]

# L'Internet a beaucoup changé

de 4 à plus 1 milliard de terminaux



[ARPANET logic map,1969]

En principe l'Internet est décentralisé

# En principe l'Internet est décentralisé

En pratique il est contrôlé par quelques géants...







# En principe l'Internet est décentralisé

En pratique il est contrôlé par quelques géants...





... chez qui il faut s'enregistrer

... chez qui il faut s'enregistrer

Cliquez ici pour accepter

Model of the beginning

# Google Règles de confidentialité et conditions d'utilisation

Donotes que como collectoro Comment nous utilisons issu-

000 ( ) L

# Transparence et liberté de chobo

Données que vous partagad.

# Données que nous partegeons

Olearial day downless

# Champidispolication des potentras Figles de confidentialità

# Modifications

Profiques apric figure is contains Autres responses utiles bies à

# la pomilidanda lité et la la protection dus données

Charles Perforquisited

# Terror disc

Parternal resi

# Bienvenue dans les règles de confidentialité de Google

Labour view Mass are severy end and false and one participated at vos données. Les présentes règles de confidents bévisent à vous indiquer qualles. informations now materials, pour queteration, et nomment messtes ni règles sons importantes et nous espérons que vous prandres le temps de les lins all entirement. Such as que des fundamentés, permettant de gére son distribue à le prodiger voire confident afrai en voire silourist sont d'aponibles dans le section Mon



Monocomore

# Régles de confidentialité.

Date de la damière modification : 25 mars 5016 (voir les versions archivées). Unaquer les examples

Vincinnery and remain American part hater soles de arrans, partier de el patrior de Informations, pour poremuniques avec d'autres personnes ou pour crées des portanus. En nous transmettant das informations, par example en créans un compée Google, vous nous parmetras danelos masestres Rus provinciones al fate de amours et des endos de centrales

plus pertinents et vous sider à dohanger avec d'actres personnes ou à simplifier et accélérar la partage.

over Parties, observative. More controllars que vous, ex buil qui Morbe e de nos revoires, nomprene comment nous utilisons vos connées et de qualles manières vous pouvez protégenante vie privile.

- Nov Highes de confidentiable enuliquest. les données que nous collections et les relacts de cette collecte.
- la facch dont nous utilisons des données.
- comment les mettre à lour.

Houseons et largues of the legality state possible. To define, or view teles passible the parenter of experience of termes "cockies", "achiesses (P", "bellies pixal" os "navigatesta", renseigneo vous polisiólement sur ces. new also. Dies Banglig neue an mes anderen de privasser translate dall habs auch méssa pisées Ainst, que vous soyet nouvei utilitasseur ou un habitual de Google, pranata la tampe de découvrir nos predicates at all your away degrapes for a nih foliation pag is not a composer.

# Données que nous collectoris

Las informations que nous collections pervent à améliann les pervioss proposits à tous nos utilisateurs. Il per l'Argin Malon actions de bace, telles que la largue que viex officies, nu plus annateurs, comme les nes que vans brasse des plus atiles, les persanares qui vans infraesceri le plus con le Mebran les vidéos VouTube out stort suspectibles de vous plairs.

None indicators des données des manéres sussantes

- Informations que vous nous communiques: pour applider à nos services, vous devec souvent créen an articular Changle Plant or our, yours for introduct destribute offices, personnelles, before presented nom, votre adresse erra il votre numito de skliphone ou votre carre de palement qui sont er mytcheen were van einemple. Programmen problem de fander, ber band an wilde de probleme par nois promotins, was proved replement the amen's 4 index on prof 15 ragge public, out prof comprandra votre nom et votra photo.
- Informations purcouns anticolors because value of their was reviews, many anticolors in informations relatives audiservices que yous utilises et à l'usage que yous en faites. D'emples : langua en a largar les antes tito sur Yan Tare, langua varia en la rendra sur a anche Web sur terrat nos sarvices publicitaires som stilla és ou lorsqua vous consulted nos contenus at nos sanoncas, et gue vous ellest use les actions sur refles et Primit est idomations, or ped alles
- Connées referènció l'appareil atilité.

Makes authorite as the district words from in Egypte district control library, per conseque, because the larvest for the synthme disciplination. This development is the support of the informations and we can describe the mobile, you report violent and the side libraries. More demonstrate as exceptibles. d'associar les identifiants de votre apparail ou votre numéro de éléphone à votre compte.

Lorsque vous utilisso nos services ou que your sifiches des contenus fournis per Google, ana collection, et startants des interestimas des tables, les factions journaux de las serverais. Cele

- In land on the source of the foreign property, before one environment.
- des données réalises ou non mondations l'étationnées nombre este nonceute. talifohore, calul de l'appelant, les numitros de transfert. Preure et la ciara des appela, leur dunte les données de routage des SMS et les types d'appais
- des données relatives aux événements l'és à l'appareil que vous utilises, tels que plantages, authorite any afterior, parametres de mattent, by continuous de venir navigateur, date et haute de la requita et UKL de provenance.
- decreases percelon at deather value assignion or othe Comple Congle de Louin unique.

# Sometes de londisation

Lorsque vous utilises des pervioes Goodie, nous sommes susceptibles de collecter et traiter. des recordes actables à sobre producte contre. Neuvollisse se d'illère des trabadiques pour rous localisas y compris fachesse IR, las signaus GPS at disumes capseurs nous permettant informed efficient the less approach, because to the one WH of teconhomise related a bin work à prodmàti.

# Manufacts disconline time unique.

Certains devices another and an automorphism for unique. Committee of less formations concernant votre insis limitor (type de système d'exploitation et numéro de version, per something execut the environs of Completonium some installer our beam broque la servica comacte siguillarement nos serveurs (per exemple, pour demander des mises a construction of question

Not a not yours thre amends it call extended standardes complets by comprisition doubles. personnalie il sur l'appeni pue vous utilites. À l'aide de misse james comma le giociagne su

Note provery the aments a collector et a abottor des cometes fy como a des dométes responded on Egyptet prespondings, Affaile de résonance annuelle shappe se is nevigensur Wab (y compris HTVL S) et les caches de données d'application.

# Contains of Employing temperatures.

conclete:

Not particulate et nou senimes utilisons différentes technologies pour collecter et stocker. es nomeros besque vicio anche y A cincarvine Single, par exemple e indificari des ou des technologies similaires pour identifier votre nevicensur ou votre sociaral. Nous utilizons égallement das factinologies pour collecter et stocker des informations lorsque vous publicité ou les fonctionssible Google oui ouvert appendire our d'autres sites. Notes produit burs size With at our learn poel carbons. Long all lest utiling parallélement à non services. called lanes, belong a committee of the control of the first information of langle things sont associées, par la client Google Analytics ou par Google à Taide de la technologie Google. aux informations relatives are visites our placeurs rates.

Outre texts for exclorer varia concerns all premions obtaining our District effective remay or ferratery, less données que nous requeillons lors que vous êtres connecté à Google peuvant être associées à votre comple Surgio Housiles hallow along an one decilorates personnelles. Pour et sevati plus su manière dont your pouvez accider sux informations associées à votre compte Google, les piver ou les capaning consider la sector frampaience et the textectronic exprésentes règles

# Comment nous utilisons les données que nous collectons.

Las domés que nous collectors nous permetiam de foumir, pinar provider et améliore nos services. males de preside manageme, et de problègio a una diferencia del bacteria que managemente. O nous permenent également de vous proposer des conseque séaprés, rela que des proposes et des

Hour commer susceptibles d'atilizer le nomificant dans voire Profil Google dans tous nos services qui requièrent full ligation d'un Compte Google, Nous pouvons également être amenes à remplacer d'anciens. is a sobre Cample Single, afrique varianque procede de mantere cuberce à foi l'ensemble de nos services. Si d'autres utiliserseurs disposant déjà de voire adresse e-mail, ou de route. rate double principal televino identife, mus some viologibles delea marter les doubles de voirs Prof I Google disposibles publiquement, telles que voirs nom et votre photo.

Securitization that initials Borgly, may poward affoliate round to photode wide public the actions que vous effectues sur Google ou sur des applications tierpes connectées à votre comple Google (bries quelles 4) que vous et flues les ons que vous rédigez en les commentaires que vous poutes) en commerciaco. Hous nous conformerons aux paramitres de partage ou de visibilité que vous définisses. charge discount in County

Largue your contectua Google, nous conservors un emeglatement de votre communication effin de ntena recorde les profiteres que varia remaines. Hono provincia tibre sobre obrese email para sobre tanhinformétés, per ecample, des modifications ou des améliorations à venit de nos pervious.

House milliones les informations formies per les coolies et diames technologies, comme les ballesses pital, pour your offrir un mailleur porfort d'adilitation et améliorer la puelle globale de not services. Borgle Analytics est unites prototo que nos empleyors medie la dans nas propressesso Carregionement de vos préférences l'inquistiques nous permet, par écample, d'efficher nos services dans nous rissocions au cun identificat de copilies ou de technologies similaires à des données sensiblies. descriptions, landque, brestation constrait the resort

Not perferent automotivie analysest you posterula iv pomorialise e-mailei afia de vous proposar des fonctiones liès personnelle ses pur les produits, relieu que des nisultats de recherche personnalisats des

Las informations paracenalles que your fournisses pour fun dans services som suspeptibles d'êtreremovate a comment of the beauty of out to provide a Brought (you do just the bottom of the approximation), you example pour facilitar le paraga de voe informations avec des personnes que vou coome sees. Le cessage mod distributoriste examples contra de contra distributoriste de sistema il conquere d'activité. your identifier nest possible cultived votes accord applichs.

Toute utilization de données dans un but autre que caux qui sont exposés dans les présentes Régles de confidential to accompanies with a construction.

Name had an expectation for communities and the arrespondent families of a force for a familiar and a supplied as a force of le monde. Vos domnées personnalles sont dans suspeptibles d'être traitales sur un serveur situalitiers de

# Transparence et liberté de choix

laut de la page

Les references franciers provides de mode les factios différents franciers provincia Poulse. Moss contractions francier preuve de transparence sur la façon dont nous collectors et utilisons les données qui vous concernant. for previous disposable de fous les éléments pour la production de fourier. Mans pouver par exemple

- Verbrief and a construction of the Construction Construction of the Left also described as the Department toures (les queles etéros pe vois aes reputés son forfate au en rentres entres intenties) que vous voules amagianer dans voirs compta lorsqua vous utilizes des services Google. Vous provide depletion of control or any communities of a depletion may be reclaimed an incidence of modiales dans un coolife ou une rechnologie similaire sur votre appareil mobile lorsque vous at the variation of the control of the control of
- Utiliser Google Caphboard pour whiter et compôler perainarypes de données Mais votre Compte.
- Gelice aux passentons des annonces, vous pouvez ponsulter et modifier vos préférences relatives audiamondes Google qui vous sont préparates sur les sites Google et sur le Web, telles que les actifiquates assumptibles de estat influence. Vana paravez iguile mediatristi de désant vez un tata
- Apole: Pulledrage dispublicacione A velor comple Bingle.
- Contrôler avec qui vous partaged voe donnés par le blats de votre compte Google. Expansion for discrete accorders divine comple Surge deplace as de accorders.
- Cholaisses al le nom et la photo de votre profit parafront dans les recommandations partaglies qui

When an early engineered against the earlier appearance and formula blances have been making a common less. cocides Mails nos services, ou pour éen informé l'orsque nous vous en envoyons. Il convient toutefait de equation professional and make acceptance and better different and professional acceptance of the second acceptance of the second acceptance is a cooling. It is designed participant, participant, delivering professional acceptance in a cooling of the second ac

# Données que vous partagez

De nombre a services Bongle vans proneffent de protogre vas nombre aven d'autres prounte Reposites vous que l'orsque your parte per des informations publiquement, elles peuvent être indisidées parties entires de rectant e tels que florate. Nos sentres sons proposed physicals lagrans. partiagenet de supprimenyop contenue.

# Consultation et mise à jour de vos données personnelles

Largue your call recinos services, nous souhaitors que vous ayec acolas la vos informations escueles Providente, una lescuer sorè que una priviey les métre que applicand ou le supprimes secf si nous devors les conserver à des fins commerciales Hightimes ou si la loi nous l'Impose. Appel de la facilitat de la consection de la facilitat de la consection de la facilitat de la inviter knoon identifier.

Non-more discrepancial and an electric funds are made discrepandity on an executive repetition. systematics, but extensions detorated the official administration decreases for execute développement d'un nouveau système ou une modification majeure d'une procédure extrantés. companied and to consider double development and times, and if interpret into took of a four exempts, dec demandes concernant des données stocbles sur des systèmes de seuvegarde).

Denvelous manages of terrored fundamental base for covering polist, so of constraint or one or Impliquents un effort démasuré. Nous pranons toutes les dispositions pour protéger les données gérées la consensa a primer des domés a filoses par ma services, mas ne seguino a pas inmédiatement. les copies els idualles se trouvert sur nos serveurs actifs ni pelles stociales dans nos syntimes de

# Données que nous partageons

Données que vous partagez

laut de la page

Note no communiques, you common participant and as a desiral spirate, that organisations out des recovered became a consideration and transporter

## + Avec years consumment

More recommendations des données personnelles sons années aut à des enlegations, de programment. Note demonstrate for large pulsives verse consensament. Note demandons togiques with a detaction would be not recognized that has also become presented as well a

# Avec des administrataurs de domaines.

Navine Conside Countries I and accommodate shows the function for execute, of short after compta Google Appa). Facinitalistateur de domaine situi que tout sous-traitent seautent des serve de la cilia describe sobre obranda de como como una documente entre Combr Google (y compris, note marry, your adresse e-mail). Yours administrate, note domaine act

- affichantes statistiques relatives à votre compte, notamment delles concernant les.
- a condicte and temperate and accord
- suspende ou supprimer facella à votre compte;
- autorité au a de adres au acrevées de constité complés é les autorités;
   recevoir les données progras à votre compra pour satisfaire à des obligations légales. of plane of store, policie de superior del siero.

  - restraindre vos drotte de superior fan ou de modificación des doensies ou des paramients de

Prononcasoli plus, vesillar consulte les règles de confrient altré de votre administrates de domains.

Many transport transports character proportion that the part of the control of the part of confence qu'illes traitent pour soire compte, selon sos instructions, conformément sux présentes. Rights de condicional al tre di dans le respent de trade unite consure approprie de securité et de poeridemialital.

# + Pour des raisons (unidiques

Many are and account for department of the control personnes fierces que si nous persons en toute bonne foi que l'appès. l'atilitation, la protection ou

- su conformanti des obligatione légales, réglementaines, judicialmes ou administratives ;
- Interspitation to an attorn distribution on signer, yrompto proconsister disenteels manmaments & callengin
- décales, éviter ou traiter des activités frauduleures, les attaintes à la récurité ou loss problème.
- su pelarun incompetours prietra sux droits, sux biens qu'il la salcurité de Google, de seg. all features as disputitio, employed an el dans le respect de la la

Hous posyone fire amends & partiager publiquement, ainsi qui vac nos pamenaines (Adheurs, annonceurs). consider assembled they information a prince present their prescribed the present referred to discovery. However, , par exemple, partager publiquement des informations relatives auctendances d'utilisation de nos pervices.

Dans le cas où Google prendisit part à une opération de fusion, d'acquisition ou à toute autre forme de informer avant que calles ci ne solars transférées ou soumbses à de nouvelles règles de confidents lié.

# Sécurité des données

Hous matters en outre toates les mesures de sécurist récussaines pour protéger Google ainsi que nos Modern unite factions of foremotivation, disalget in a description medicine adorse. Its doubts que nous ditenors. En particulier:

- Movembillions to physical encourages a fundamental according a 200
- + Nous your proportine une validation en deux ésspecioraque vous accident à votre Compte Google et une formation de Massaction Kernaniere dans Bounte Comme.
- w. How revors the audits internessar knotlede, testadage of tetrationent desilonaes, y compris les mesures de sécurité physiques, afin d'emplicher tout a colo non surprisé la nos
- L'applie sus données personnalles est strictement réservé aux salariés, sous éminants et agents de Simple qui out broatmaty accepte af and less faulter et autre non. Ces presumes soit sources ou de articles colligacions de confidentialital et sont ausceptibles de faire l'objet de sanctions dissiplicates proved alter program in encircum free aus de manque ment à resultigations

# Champ d'application des présentes Règles de confidentialité

Les présentes Règles de confidentialité algophiquent broux les services proposés par Google Inc. et par Chicles, a number A Visit Table, our provinces for may one Storage and less as services proposits our d'autres sites (nos services publicitaires, par exemple), mais eccluent les services : regrespon five lives angress de condicte distillé afoncionnent para les present

Las présentes Régles de confidentialité ne s'appliquent ses sus services proposés per d'autres pocifisis. corpersonnes, incomment components ou con sites qui prevent esse che propose dinsi les resultats d recherche, australies qui persent incompres des services Roppie ou aux autres sites apparatifies à partir dancs services. Les présentes Régles de confidents lité ne couvrert pas les protoues en martiers de potentium des nomées d'antres sonicités nu reganisations qui find la produité de nos revoires et q pacyant cell par dea copilies, das balless gival ou disums technologies pour affichar et propisar des

# Respect el coopération evec des organismes de régulation

None et flore aby different i que nous respendent les présentes Miglies de condute distilé. Nons conse conformora par allieura à plusieura chamas d'autoriguistico. Lorsque nous recevors une réclamation from by more presents, conclude overs for the above point from experience and descent the Manus completion, execut sutorble compléentes, y compris les sarorbles locales chargles de la protection des données, pour describe for Major represent to bounded to character, an expensative participative properties and about

Les présentes Règles de confidentalité pesvent les ameries à changer. Toute diminution de vos droits evertis. Note publishers to the modification due finds the portformialistics nearest owns at dans is our of Extract the notification cyclicative, may put early investigative this extension (you priswhere we storp and a last of the collision are could be a very conference despression. Règles de confidentialité peront archivées et mises à la disposition des utilizateurs.

# Pratiques spécifiques à certains produits.

Les documents sulvants exposent des profoses apéchiques en matière de confidentialité applicables à certains produktiou services Google que vous pouves utiliser

- Reports Change of Change C6.
- + Pley Users
- + Floor
- + Google Apps for Education

Pour obteninglus d'informations sur cartains de nos services les plus populaires, vous pouves consulter.

# Autres ressources utiles lides à la confidentialité et à la protection (Hautrich Lange des données

Vous trouvest d'autres respontes utiles liées à la porfdentains et à la protection des données sur les iges Region of principles de Bougle, indumenent

- + Des informations sunnos sechnologies el principes, qui comprendent notamment des données.
- and offered latery can
- la manière dont nous utilisons les cookles tes technologies are new officers one for white to
- la manière dont nous utili sons la reconsa issance de motificate les visages.
- Web and a Michael and products and tolkness, charaker of southern Local de vérification des paramètres de confidentialité facilité le contrôle de vos principaux.
- concentration to much be finite. + Le Cartre de sécurité Google, qui fournit des informations sur la manière de senforcer la sécurité

+ The page gui explique quelles données vous nous transmettes lors que vous consultes des sites

Nous assurons la confidentialité et la sécurité de vos informations personnelles, et nous yous en donnons le

Accédez aux réponses aux questions courantes concernant la confidentialité et

# Information supplementaries

Technologies et procours. Parameter.

Connex Conjentionles 000<88 Google et la reconnaits ance de

Types de données de Instruction of the pay Surgician

les numéros de carte de Spegle Valor

Comment Name Water alive

Comment Spogle utilize ornous your utilises deals for contamation

produits Specie Réponses sus questions a picurbi

Centre de cenurie Hongle

And the control of the State of the

Monorpole

Newspapers was presented as a

inti/fr/policies/fag/\* in a new tab

the included.

interest on less

MORNOUS VOICE

brinden görten in ministration of

forme e che

(Single-surface) and delication

Nous ne communiquons vos données personnelles à des entreprises, des organisations ou des personnes tierces que dans les circonstances suivantes :

# Avec votre consentement

Nous ne communiquons des données personnelles vous concernant à des entreprises, des organisations ou des personnes tierces qu'avec votre consentement. Nous demandons toujours votre autorisation avant de communiquer à des tiers des données personnelles sensibles.

commentingua utilizana voa constea es de qualles mantiéres vous pouvez protéger votre via privile.

- les données que nous collections et les relacts de cette collecte.
- la facch dont nous utilisons des données.
- comment les mettre à lour.

termes "cockies", "achieses (P", "bellies pixel" ou "naviganeurs", renseigneovous polisiablement aur ces nes ales. Clary Borrgie, mont su mores comitera de privaryes in confederal alli trate sós de mésos privás Ainst que vous soyet nouvei utilitasseur ou un habitual de Google, pranatz la tampe de découvrir nos predicates at all your away degicates for a nih fasted play is now a compacter.

# Données que nous collectoris

Las informations que nous collections pervent à améliann les pervioss proposits à tous nos utilisateurs. Il per l'Argin Malamatiens de bras, leftes que la baque que vios officies, nu plus minuteres, anome les agree and formers her plot of let, but personners prisons in the extent legitive on in Web on the vidéos VouTube out sont suspectibles de vous plains.

- Informations que vous nous communiques: pour accider à nos services, your devec souvent créen an articular Changle Plant or our, yours for introduct destribute offices, personnelles, before presented son, votre adresse email, votre numéro de séléphone ou votre carre de palement qui sont erings lates, were value annuals. Principalism problem to bacter, but formal time tiltra de parlinge que non-proposes, was power endorsed the power a new prof. Strate public outped comprandra votre nom et votre photo.
- Informations processes and enhancement of the consequences are a colorion. informations relatives audiservices que yous utilises et à l'usage que yous en faites. D'emples : langue en us regardes ancenden van Yna Tabe, bassare van senas mender van ans de Websarnos sarvides publicitaires som stillatis de lorsqua vous consulted nos contenus et nos amondas, es gue yourselbed over les antiques au colleges. Permit exchibit rations, on produite
- Connées referènció l'appareil atilité.

Makes authorite as the district words from in Egypte district control library, per conseque, because the larvest for the synthme disciplination. This development is the support of the informations and we can describe the mobile, you report violent and the side libraries. More demonstrate as exceptibles. d'associar les identifiants de votre apparail ou votre numéro de éléphone à votre compte

Lorsque vous utilisso nos services ou que your sifiches des contenus fournis per Google, ana collection, et startants des interestimas des tables, les factions journaux de las serverais. Cele

- In land of the property of the foreign property, before one way confirm to
- des données déclares qui nomination de la fondament de mora et le mora de talifohore, calul de l'appelant, les numitros de transfert. Preure et la ciara des appela, leur dunte, les données de sorage des SMS et les types d'appais
- des données relatives aux événements liés à l'appareil que vous utilises, tels que plantages, authorite any afterior, parametres de mattent, by continuous de venir navigateur, date et haute de la requita et UKL de provenance.
- decreases percelon at deather value assignion or othe Comple Congle de Louin unique.

Lorsque vous utilises des pervioes Goodie, nous sommes susceptibles de collecter et traiter. des recordes actables à sobre positione contre Micro ellisse ve d'Elevère Indicatogres pou rous localisas y compris fachesse IR, las signaus GPS at disumes capseurs nous permettant atomical distribution to appropriate for our WHA less denotes distributed à prodmàti.

# Manufacts disconline time unique.

Certains devices another and an automorphism for unique. Committee of less formations concernant votre insis limitor (type de système d'exploitation et numéro de version, per something execut the environs of Completonium some installer our beam broque la servica comacte siguillarement nos serveurs (per exemple, pour demander des mises a construction of question

Notes par vons être emenés à collecter et à stocket des chanées (y compris des données personnalie il sur l'appeni pue vous utilites. À l'aide de misse james comma le giociagne su

Nous commas susceptibles d'utiliser le nom fourni dans voire Profil Google dans tous nos services qui required full lighter (fun Compts Google, Nous populars stationers) site amenas a remaisse d'anciens. l'ensemble de nos services. Si d'autres utiliserseurs disposant déjà de voire adresse e-mail, ou de route. voirs Prof I Google disposibles publiquement, telles que voirs nom et votre photo.

Stema, dispose of an armode Bounds, consequence of information and important except of the last actions que your effectues sur Google de sur des applications tierdes connecties à votre compte Google (b) tex que to +1 que voio el filtraz, les ovis que virante igravantes da mentales que voia podes) de netro la manes me, y compato dom le corte de la differención de comes con la sabalita y corte de la commercialo. Hous nous conformerore suo paramitres de partage ou de visibilité que vous définisses.

Lorsque vous contectas Google, nous conservors un emiglatement de votre communication efin de tanhinformétés, per ecample, des modifications ou des améliorations à venit de nos pervious.

House milliones les informations formies per les coolies et diames technologies, comme les ballesses pital, pour your offrir un mailleur porfort d'adilitation et améliorer la puelle globale de not services. Complete skyling and an idea production premiors emphysion and the fundamental proprior service L'annightement de vos préférences l'éguladoues nous permet, par écample d'afficher nos pervions dans nous risspecions au our identifiant de copilies ou de technologies similaires à des données sensibles.

Nos symbres automatiste analysent yas contenually comprisites e-mails) afin de vous proposer des fonctiones liès personnelle ses pur les produits, relieu que des nisultats de recherche personnalisats des

Las informations paracenalles que your fournisses pour fun dans services som suspeptibles d'êtreremovate a comment of the beauty of out to provide a Brought (you do just the bottom of the approximation), you example pour facilité le parage de voe informations avec des personnes que pour conscions sees. Le cerus proved distance les sons provenues de conties. De été Citab even des informations person d'unit de

Toute utilization de données dans un but autre que caux qui sont exposés dans les présentes Régles de confidential to accompanies with a construction.

Name had an expectation for communities and the arrespondent families of a force for a familiar and a supplied as a force of le monde. Vos données personnelles sont dans suspeptibles d'être traitales sur un serveur situalithors de

# Transparence et liberté de choix

Les references francier maritée de mode les faitses Milleres à Provincement Peutre, Many content profession preuve de transparence sur la façon dont nous collectors et utilisons les données qui vous concernant. for previous disposable de fous les éléments pour la production de fourier. Mans pouver par exemple

- Vertical for the appropriate Contract to the contract to be presented as a first of the contract to the contract dances (les que les ethos que viux avez republiss ou You'h be un ens dentros un tent est que vous voulec enregistrer dans voirs compte lorsque vous utilises des services Google. Vous modiales dans un coolite ou une technologie similaire sur votra appareil mobile lorsque vous
- Utiliser Google Caphboard pour whiter et compôler perainarypes de données Mais votre Compte.
- Gelice aux passentons des annonces, vous pouvez ponsulter et modifier vos préférences relatives auc annonces Google qui vous soni présentales sur les sites Google et sur le Web, telles que les actifiquates assumptibles de estat influence. Vana paravez iguile mediatristi de désant vez un tata
- Ajorde Pallintage dispubli accome A entre comple Simple
- Contrôler avec qui vous partaged voe donnés par le blats de votre compte Google.
- Cholaisses si le nom et la photo de votre profit parafators dans les recommandations partaglées qui

When properly equipment accomplishes write appellation of a formula blancas have been been problem, a company for cocides Mails nos services, ou pour éen informé l'orsque nous vous en envoyons. Il convient toutefait de

equation por form construction de man review a qualification différent en grant foundament accombination of the con-differentiess has coolines. Ils ne dendrom pas compres, par scennole, de voss priférences linguissiques.

Données que vous partagez

Données que nous partageons

Notes no communiquous ves common parso malvas à overent aprivas, das organisations ou des eronnes Denes que rons les atmonstrares salvantes

# Area years consumment.

programment. Note demonstrate for large pulsives verse consensament. Note demandons togiques entre entre section record de comme compare et des fress des des des des presentations en est de

# Avec des administrataurs de domaines

Research Country Changle and a few particular adjustment of the country from the month, and whealth from compta Google Appa). Facinitalistateur de domaine situi que tout sous-traitent seautent des where Date is the description of the appearant of the proof and the description of the Country Google (y compris, note marry, your adresse e-mail). Yours administrate, note domaine act

- afficher les statistiques relatives à votre compte, notamment delles concernent les.
- a condition to confide provide value accordi
- suspende ou supprimer facella à votre compte;
- professional districts an accepted the weak enoughly of the accepted
- recavoir les données progres à voire compte pour satisfaire à des obligations légales. of plane of store, policie de superior del siero.

  - restraindre vos drotte de superior fan ou de modificación des doensies ou des paramients de

Prononcasoli plus, vesillar consulte les règles de confrient altré de votre administrates de

Many transport from the character proportion files to part Males, as and recognitive and personal exacts confence qu'illes traitent pour soire compte, selon sos instructions, conformément sux présentes. Rights de condicional al tre di dans le respent de trade unite consure approprie de securité et de confidentialital.

# + Pour des raisons (unidiques

personnes fierces que si nous persons en toute bonne foi que l'appès. l'atilitation, la protection ou

- sa conformar à des obligations légales, réglementaines, judiciaines ou administratives.
- Interspitation to an attorn distribution on signer, yrompto proconsister disenteels manmaments & callengin
- décales, éviter ou traiter des activités frauduleures, les attaintes à la récurité ou loss problème.
- su pelarun incompetours prietra sux droits, sux biens qu'il la salcurité de Google, de seg. all features and could be expelled on of dankle respect to lade

Hous posyone fire amends & partiager publiquement, ainsi qui vac nos pamenaines (Adheurs, annonceurs). pouvors, par svemple, partager publiquement des informations missives auctendances d'utilisation de

Dans le cas où Google prendisit part à une opération de fusion, d'acquisition ou à toute autre forme de informer avant que calles ci ne solars transférées ou soumbses à de nouvelles règles de confidents lié.

# Sécurité des données

Nous matters en outres teatres les mesures de sécuriel réfessaines pour protéger Google ainsi que nos Mosters and etual varieties force notification, disalget in material communitorises desidentes que nous ditenors. En particulier:

- Mose of the outerplayed decreases where a finite of the ordering of the
- Hour vous proposons une validation en deux ésspes lorsque vous acoldec à votre Compte Google et une formation de Massaction Kernaniere dans Bounte Comme.
- w. Now revorsities audits interes our broofests, technology of technical desiloniers, y compris les meauses de sécurhé physiques, efin d'emplicher tout a coles non autorisé la nos
- L'apple sus données personnalles est strictement répervé aux salariés, sous énérants et agants de Single-priorities in dynamics afrode technic environment. On personnes and accommon de articles colligacions de confidentialital et sont ausceptibles de faire l'objet de sanctions designations proved allegacy to be consent en such management à recubigations

# Champ d'application des présentes Règles de confidentialité

Les présentes Règles de confidentialité alappliquent à rous les services proposts par Google Inc. et par services proposits our discens sites (nos services publicis hes, par ecemple), mais eccluers les services. regrespon five lives angress de condicte distillé afoncionnent para les present Las présentes Régles de confidentialité ne d'appliquent pas sus services proposés per d'autres sociétais

recherche, et states, qui persent incompres des services Roppie ou aux et tes stres accessibles à partir dancs services. Les présentes Régles de confidents lité ne couvrant pas les particues en martiers de profesionales atomies a Arubes souté tes au arganisations qui fund la profit de le nos cessores pauvant utili sandes copilies, das bei ses gival ou disumes technologies pour afficher et proposer des

# Respect el coopération evec des organismes de régulation

Many editions absolitement in an area, arguestos, by arbeitos Modes de audicidad Many, comconformora par alleura à plusieura chamas d'autoniquistico. Lorsque nous recevors une réclamation that is, many promote and had been facilitative poor flowers with the other control. How completions over sutorble compléentes, y compris les sarorbles locales chargles de la protection des données, pour describe that Major continuously to bounded the character, are considered use the property continuously deliber-

Les prépartes Règles de confidentialité peuvers être ameries à changer. Toute diminution de vos droits evertis. Note publishers to the modification due finds the portformialistics nearest owns at dans is our of Extract the notification cyclicative, may put early investigative this extension (you priswhere we storp and a last of the collision are could be a very conference despression. Règles de confident la lité peront archivées et mises à la disposition des utilizateurs.

# Pratiques spécifiques à certains produits.

Les documents sulvants exposent des persiques apéchiques en mai les de confidentialité applicables à carteins produktiou services Google que vous pouvez stillaer.

- + Pley Users

- + Google Apps for Education

Pour obteninglus d'informations sur cartains de nos services les plus populaires, vous pouvez consulter

Autres ressources utiles lides à la confidentialité et à la protection (Hautrich Lange

Vous trouvest d'autres respontes utiles liète à la porfdentaileile à la protection des données sur les

- + Des informations aurnos sechnologias as principas, qui comprennent notamment des données
- la manière dont nous utilisons les coolies
- les technologies que nous obtavos pour la poblodo
- la manière d'antinque utilisane la reconna les arca de modificials les visages. + The page gui explique quelles données vous nous transmettes lors que vous consultes des sites
- Web and additional new products and tolkneys, the observer sources Local de vérification des paramètres de confidentialité facilité la contrôle de vos principaux
- conception to made technical Le Carrer de sécurité Google, qui fournit des informations sur la manière de serforcer la sécurité

Nous assurons la confidentialité et la sécurité de vos

informations personnelles, et nous vous en donnons le

Accédez aux réponses aux questions courantes concernant la confidentialité et

Comment Name Water alive

les numéros de carte de

# Information supplementaries

Technologies et procours.

Connex Contextionlo 000<88

Google et la reconnaits ance de

Instruction of the pay Surgician

Spegle Valor Comment Spogle utilize ornous your utilises deals for

contamation

produits Specie

Міротнев в из орентіот в a picurbi

Newspapers was presented in the Monorpho Centre de cenurity Hough

And the control of the State of the

inti/fr/policies/fag/\* in a new tab

# Données que nous partageons

Nous ne communiquons vos données personnelles à des entreprises, des organisations ou des personnes tierces que dans les circonstances suivantes :

Avec votre consentement

# Pour des raisons juridiques

moves become automobilities of

Notes par vons être amenés à collecter et à stocket des rionnées (y compris des données

personnalie il sur l'appeni pue vous utilites. À l'aide de misse james comma le gipsique su

Nous ne partagerons des données personnelles avec des entreprises, des organisations ou des personnes tierces que si nous pensons en toute bonne foi que l'accès, l'utilisation, la protection ou la divulgation de ces données est raisonnablement justifiée pour :

- se conformer à des obligations légales, réglementaires, judiciaires ou administratives;
- faire appliquer les conditions d'utilisation en vigueur, y compris pour constater d'éventuels manquements à celles-ci;
- o déceler, éviter ou traiter des activités frauduleuses, les atteintes à la sécurité ou tout problème d'ordre technique;

Données que vous partagez

 se prémunir contre toute atteinte aux droits, aux biens ou à la sécurité de Google, de ses utilisateurs ou du public, en application et dans le respect de la loi.

nos sarvipes publicita has som stilla is ou lors qua your consultatin de contenua at nos annonces, et remaindered of the bound in our more construction for the California for the form of the Laboratory que sons ellestras det antique sur referent Permit excistamentore, on probabe Connées referènce à l'appareil atilisé. Toute utilization de domailes dans un but autre que caux qui sont asposés dans les présentes Régles de confidential to accompanies with a counterplants. May configurate a destinancies relatives à l'apparel que var su fillers, par encapie, le matéle, taivers bride synthme d'apple tration, les identifieres sint ses de l'apparelles les informations at la version d'apparent de la version synthetie de la little de une Marchaelle de la propertie de la company de le monde. Vos domnées personnalles sont dans suspeptibles d'être traitales sur un serveur situalitiers de d'associar les identifiants de votre apparail ou votre numéro de éléphone à votre compte. Transparence et liberté de choix Lorsque vous utilisso nos services ou que your sifiches des contenus fournis per Google, ana collection, et startants des interestimas des tables, les factions journaux de las serverais. Cele Les autonomos francieros partidos de constituiros diferendo Parte constituiros de Rendro Marco Contra de Arte de Arte de Contra de Contr preuve de transparence sur la façon dont nous collectors et utilizons les données qui yous concernant. for previous disposable de fous les éléments pour la production de fourier. Mans pouver par exemple des données dé dives au nommandation détaillantaires, nomme este nomme de Vertical for the amount of common test Contract of the standard color of contract test beneated. talifohorse, calui de l'appelant, les numéros de transfert. Preure et la data das appelas, dances (les que les videos que vous avez republiss ou YouTabe ou vers dentines un bent es) leur dunte, les données de sorage des SMS et les types d'appais que vous voulec enregistrer dans voirs compte lorsque vous utilises des services Google. Vous des données relatives aux événements liés à l'appareil que vous utilises, tels que modiales dans un coolite ou une technologie similaire sur votra appareil mobile lorsque vous plackage, ad eth dany dhan, poverbles de mathed, type et langue de war navigateur, date et haute de la requita et UKL de provenance. Utiliser Google Caphboard pour whiter et compôler perainarypes de données Mais votre Compte. decoratios perceitaris de diferente avagatem o volte Comple Songle de Liquis unique. Gelice aux passentons des annonces, vous pouvez ponsulter et modifier vos préférences relatives auc annonces Google qui vous sons préparales sur les sites Google et sur le Web, telles que les Lorsque vous utilises des services Goodie, nous sommes susceptibles de collecter et traiter actifiquates assumptibles de estat influence. Vana paravez iguile mediatristi de désant vez un tata rous localisms y compris fachesse IR, has signatus GPS at distance dispeture nous permettant Ajude follologe in politicación / volve comple Ringle Contrôl et avec qui vous partages voe donnés par le blats de votre compte Google. alarment efficient to the segment, this pair to forces. Wife dies or homework is seld in word à prodmàti. Cholaisses si le nom et la photo de votre profit parafators dans les recommandations partaglées qui Manufacts disconline time unique. Central services and experience for an oran Egyphortic unique. So an about the informations When properly equipment accomplishes write appellation of a formula blancas have been been problem, a company for concernant votre insis limitor (type de système d'exploitation et numéro de version, per cocides Mails nos services, ou pour éen informé l'orsque nous vous en envoyons. Il convient toutefait de something execut the environs of Completonium some installer our beam equation por form construction de man review a qualification différent en grant foundament accombination of the con-differentiess has coolines. Ils ne dendrom pas compres, par scennole, de voss priférences linguissiques. braque la service contacte siguillarement nos servauts (per exemple, pour demander des

Pour des raisons juridiques personnes il erces que si nous persons en tosta bonne foi que l'appès. Publication, la protection ou se conformar à des obligations légales, séglementaires, judiciaires ou administratives. Interpoliper les routilons dell'autorier vignes, prompts per constate d'enduels manufacturers & college! décales, éviser ou trainer des activités frauduleus su, les attaintes à la sécurité ou tout problème. su pelmunit contre toute pérainte aux droits, aux biens puit le palcuréé de Google, de ses all features and could be expelled on of dankle respect to lade Hous postone fre amends à parteger publiquement, sinsi qui svec nos pamenaines (Adheurs, annonceurs pouvors, par svemple, partager publiquement des informations missives auctendances d'utilisation de Dans le cas où Google prendisit part à une opération de fusion, d'acquisition ou à toute autre forme de informer avant que calles ci ne solará transférées ou soumbres à de nouvelles règles de confidends lié. Sécurité des données Nous matters en outres teatres les mesures de sécuriel réfessaines pour protéger Google ainsi que nos Missilves and ethal was et force and feating dividual to a decreation or unlarge day dracted que nous détenons. En particulier : Movembell and tendenced dynamic sensitive in tente and tendenced are et une formation de Masqueton Reconsecution (Conste Conste- Now revorsities auditable revisal knotkele, techniqued tetratione didestonires, y compris les meauses de sécurhé physiques, efin d'emplicher tout a coles non autorisé la nos

Discola sus données personnalles est strictement réservé aux salariés, sous énérants et agants de

de articles colligacions de confidentialital et sont ausceptibles de faire l'objet de sanctions

Single-priorities in dynamics afrode technic environment. On personnes and accommon

conferce qui les relient pour soire compte, selon sos instructions, conformément sex présentes

Rights de confidentation et dans le respent de trafe volve mesure approprie de seconté et de

poeridentialital.

Champ d'application des présentes Règles de confidentialité.

Les présentes Règles de confidentialité alappliquent à rous les services proposts par Google Inc. et par services proposits our floures sites (not services publicitaires, par ecemple), mais eccluers les services. regrespon five lives angress de condicte distillé afoncionnent para les present

Las présentes Régles de confidentialité ne s'appliquent pas aux san/bes proposés par d'autres pociétais recherche, et states, qui persent incompres des services Roppie ou aux et tes stres accessibles à partir dancs services. Les présentes Régles de confidents lité ne couvrant pas les particues en martiers de payvert utilities des coolités, des ballises gival ou d'autres technologies pour afficher et propies des

0 0 n x

# Respect el coopération evec des organismes de régulation

conformora par allieura à plusieure chamas d'autoniguistics. Lorsque nous recevors une réclamation that he can be decreased, may be discussed by the other many through some for the property of the company of the case of the c sutorbés compléentes, y compris les surorbés locales chargées de la protection des données, pour describe that Major continuously to bounded the character, are considered use the property continuously deliber-

Haut de la page name

the included.

interest on les

Явоца Птерсав.

MORNOUS VOICE

brinden görten in ministration of forme e che

lactide la page

s damendons topiques

contract short the hart conurant dec

nativelie Conde

da domaine art

bations Monley.

rou des seremières de valorisistado e de

Les prépartes Règles de confidentialité peuvers être ameries à changer. Toute diminution de vos droits evertis. Note publishers to the modification due finds the portformialistics nearest owns at dans is our of Extract the notification cyclicative, may pull early in everticement rite extender (y compris, estano servicos, por el tato d'une matinator par email). E es versions artéricanes des presentes Règles de confident le lié seront archivées et mises à la disposition des utilizateurs.

# Pratiques spécifiques à certains produits.

Les documents sulvants exposent des persiques apécifiques en mai les de confidents lité applicables à carteins produktiou services Google que vous pouvez stillaer

- + Pley Users

- + Google Apps for Education

Pour chieninglus d'informations sur cartains de nos services les plus populaires, vous pouvas consulter

Autres ressources utiles lides à la confidentialité et à la protection (et la laboration)

Vous rocurses d'autres respontes utiles lière à la posfdernialité à la protection des données sur les nger, Mayles et principes de Bongle, culoriment

- + Das informations surnos sectinologias as principas, qui comprenhent notamment des données
- la manière dont nous utilisons les coolies
- la manière dont nous utilisans la reconnaissance de motifs, rais les visages.
- Des page qui explique quelles données vous nous transmettes lots que vous consultes des sites
- Web and additional accomplished an absolute and additional and analysis of sources. Lostil de virification des paramètres de confidentialité facilité le contrôle de vos principaux
- Le Carrer de séquiréé Google, qui fournit des informations sur la manière de senforcer la sécurité

Nous assurons la confidentialité et la sécurité de vos informations personnelles, et nous yous en donnons le

Accédez aux réponses aux questions courantes concernant la confidentialité et

# Information supplementaries Technologies et procours. Comment Strade Wallet Little les numéros de carte de

Connex Cogles Sorles 000<88

Google et la reconnaits ance de

Invitation of the not Engle

Spegle Valor Comment Spogle utilize ompus your utilises desprises.

contamples:

Міротана в до question в is picurble

produits Specie

Monorpho

Newspapers was been able to a

Centre de cenurit e Mongle

Chair de mont de de 1974 des

nti/fr/policies/fag/\* in a new tab

... et qui son intégrés à tous les sites



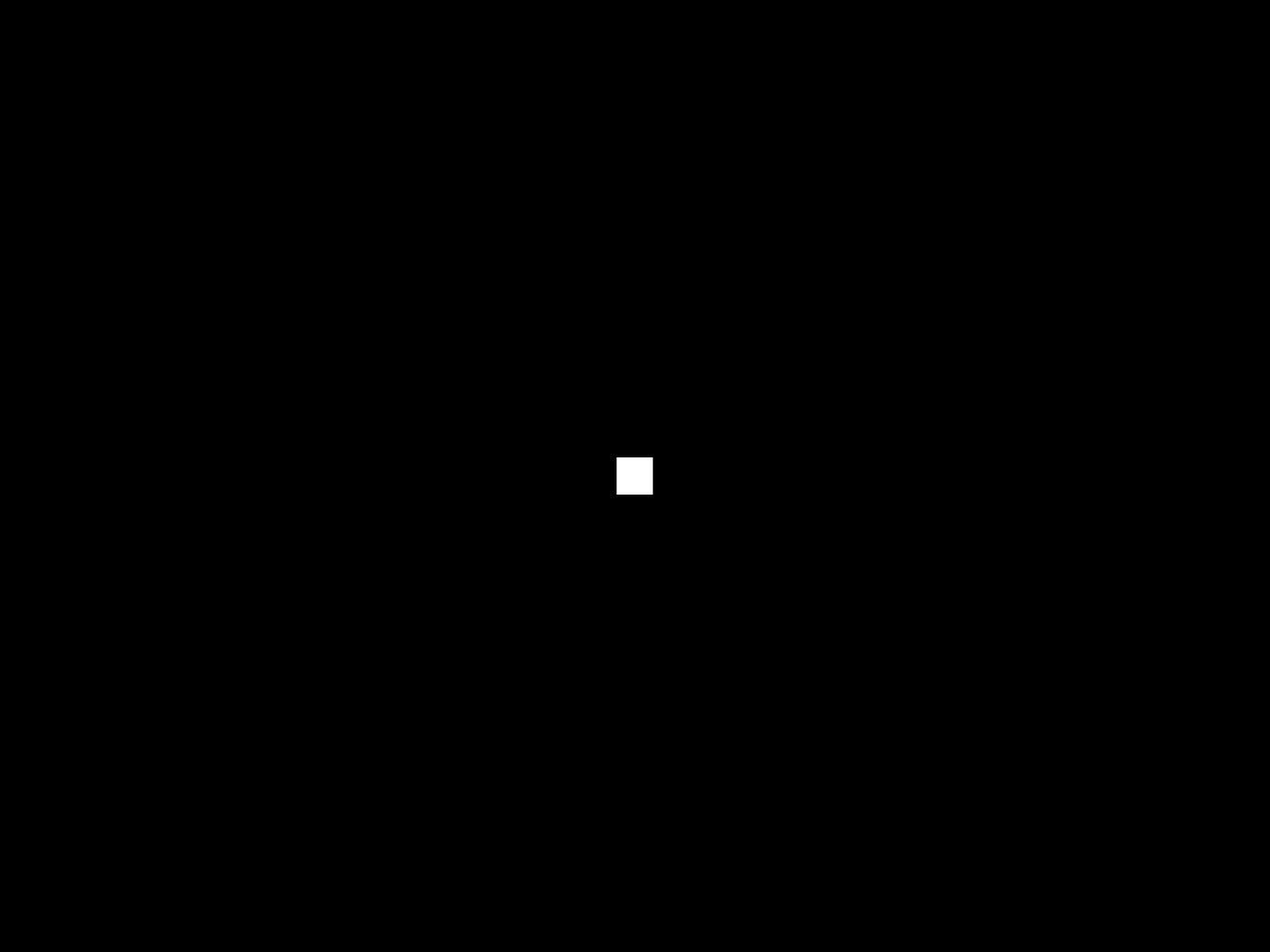
# ... et qui son intégrés à tous les sites

Cliquez ici pour partager

Je n'ai pas de compte

# Je n'ai pas de compte

Je me déconnecte



Risque pour votre vie privée

#### Risque pour votre vie privée

Je leur fait confiance

Qui utilise Skype?

#### Qui utilise Skype?

Logiciel de téléphonie par Internet composé

- d'un annuaire téléphonique publique;
- d'un protocole d'échange de paquets audio sur IP.

Qui utilise BitTorrent?

#### Qui utilise BitTorrent?

Logiciel de partage de fichiers composé

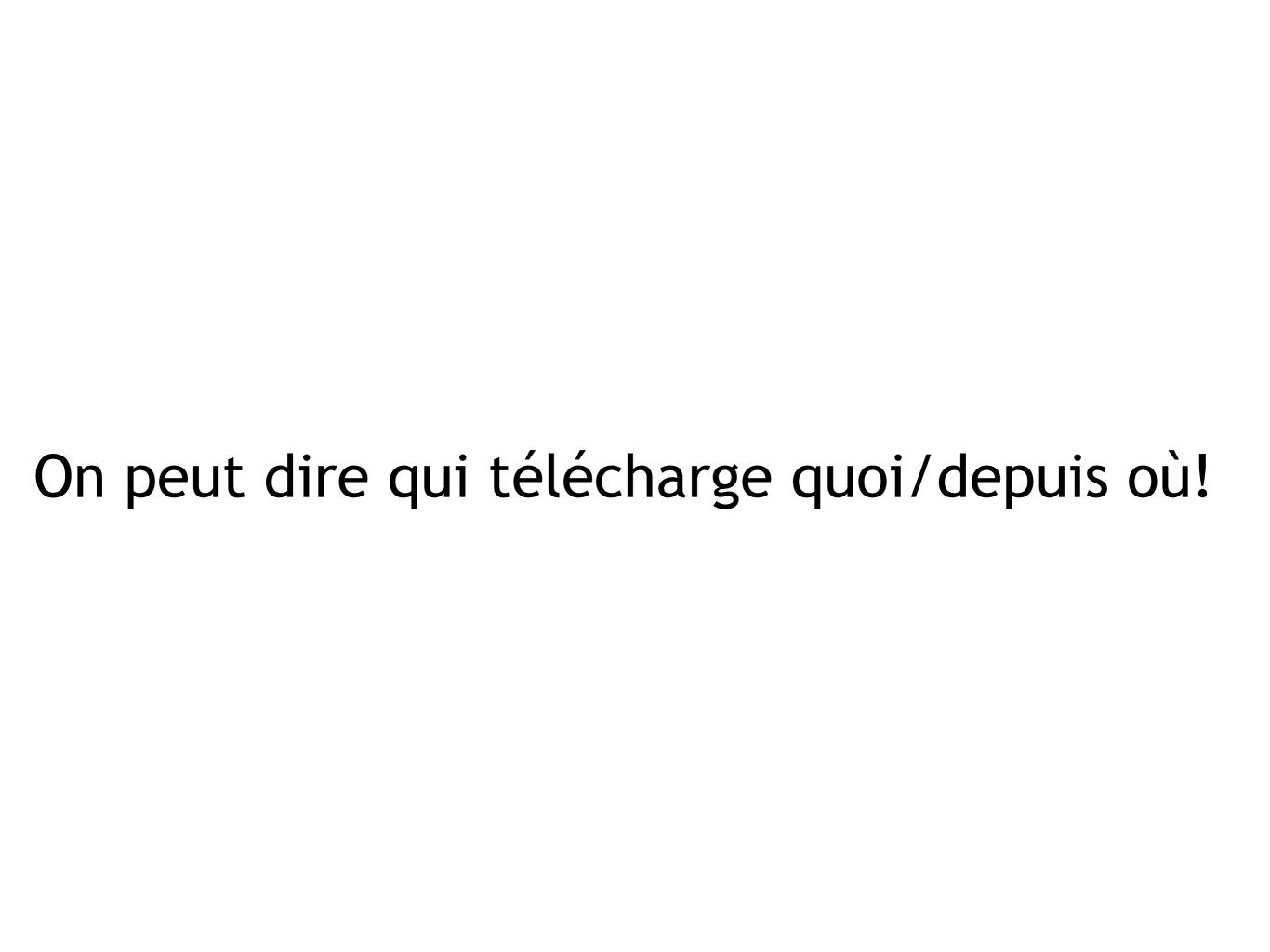
d'un protocole d'échange de paquets de données sur IP.

Qui utilise BitTorrent et Skype?

#### Qui utilise BitTorrent et Skype?

A tout moment il est possible de connaître l'adresse IP

- d'un utilisateur de Skype;
- de machines impliquées dans un téléchargement BitTorrent.





Depuis chez soi

### Overlay networking

### Overlay network

 Constructed on top of another network, called the underlay

Nodes in the overlay appear to be connected independently of the underlay

### Definitions

- Peer
  - A node involved in forming the overlay (can be a computer, an end-user, an application...)
- Leecher
  - A peer that is both client and server
- Seed
  - A peer that is only server

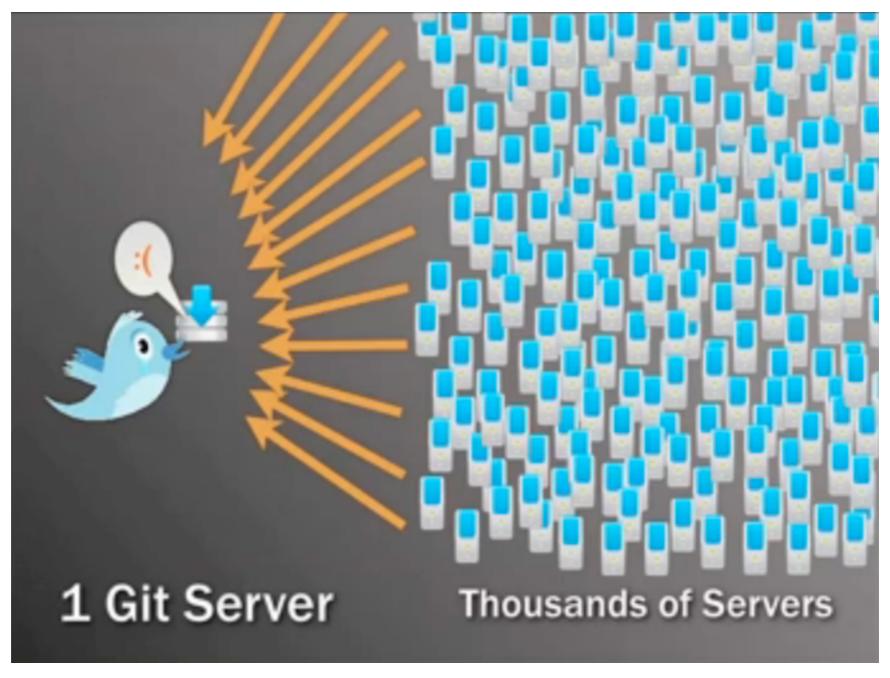
### Definitions (contd.)

- Peer-to-peer (P2P) application
  - No general definition
  - Specific to an application
  - Every peer is client and server
  - Peers form an overlay network
- In general, we define P2P application as overlay network formed by end-users

#### P2P

- P2P applications capitalize on any resource from anybody
  - CPU
  - Bandwidth
  - Storage

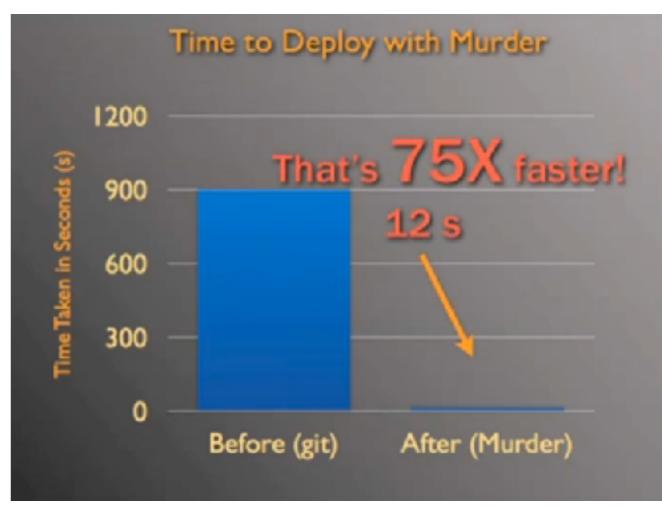
### Before Murder



credit: https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent

### With Murder





credit: https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent

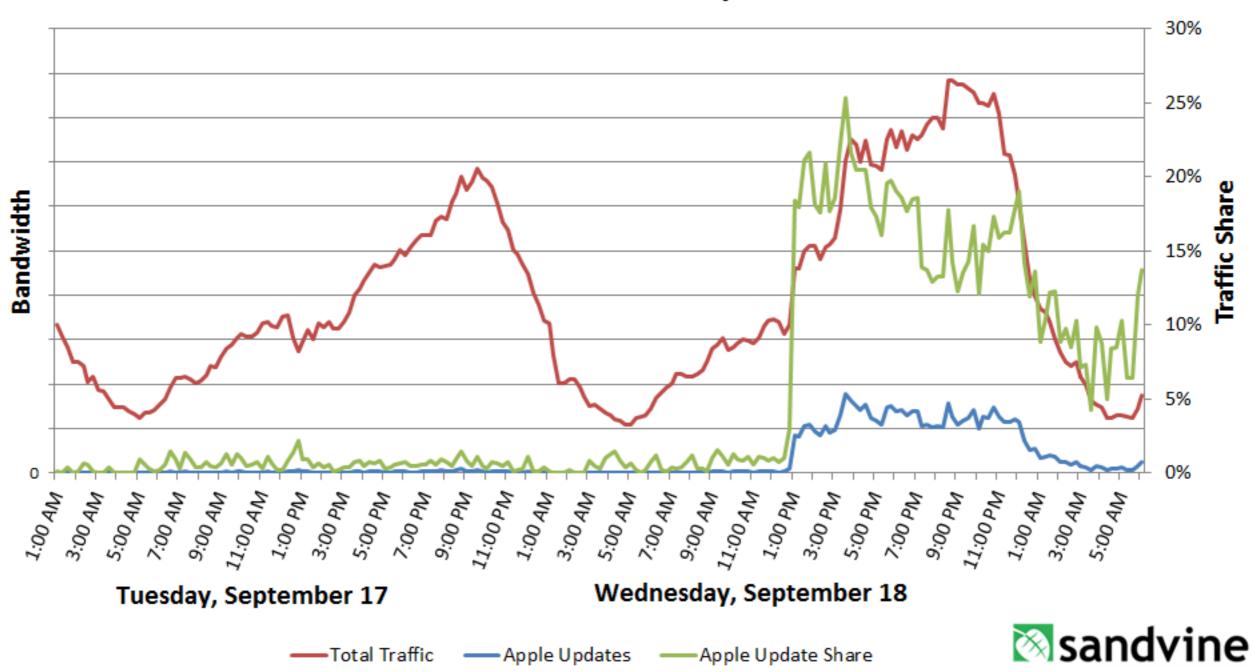
### Content replication

### Definitions

- Service capacity
  - Number of peers that can serve a content
    - = 1 in client-server, constant with time
- Flash crowd of n
  - Simultaneous request of n peers (e.g., soccer match, iOS update...)
- Piece/chunk/block
  - Element of a partition of the content
    - Each piece can be independently retrieved
    - The union of pieces forms the content

### Definitions

iOS 7 Launch Traffic Analysis

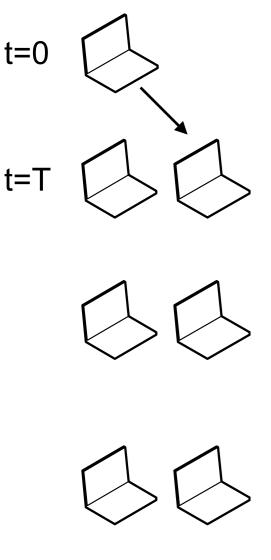


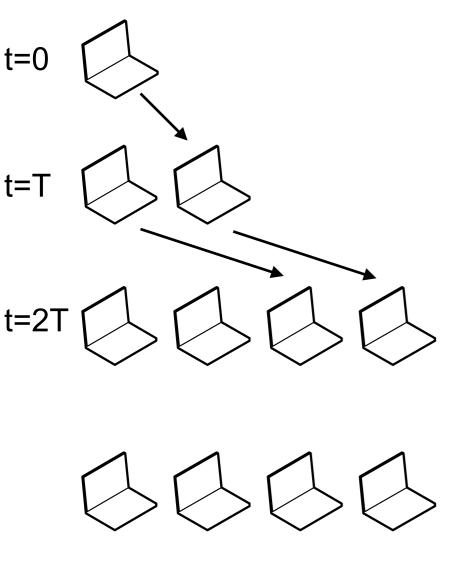
## Interest of P2P to replicate contents

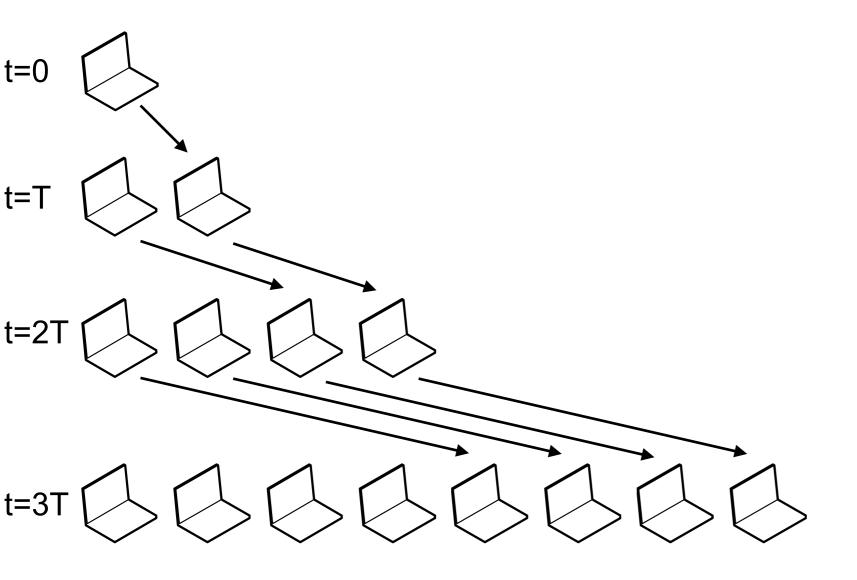
- Service capacity grows up exponentially with time
  - Average download time for a flash crowd n is then in log(n)
  - Average download time decreases in  $\frac{1}{\# \text{ of pieces}}$  when the number of pieces increases
    - if we ignore the overhead

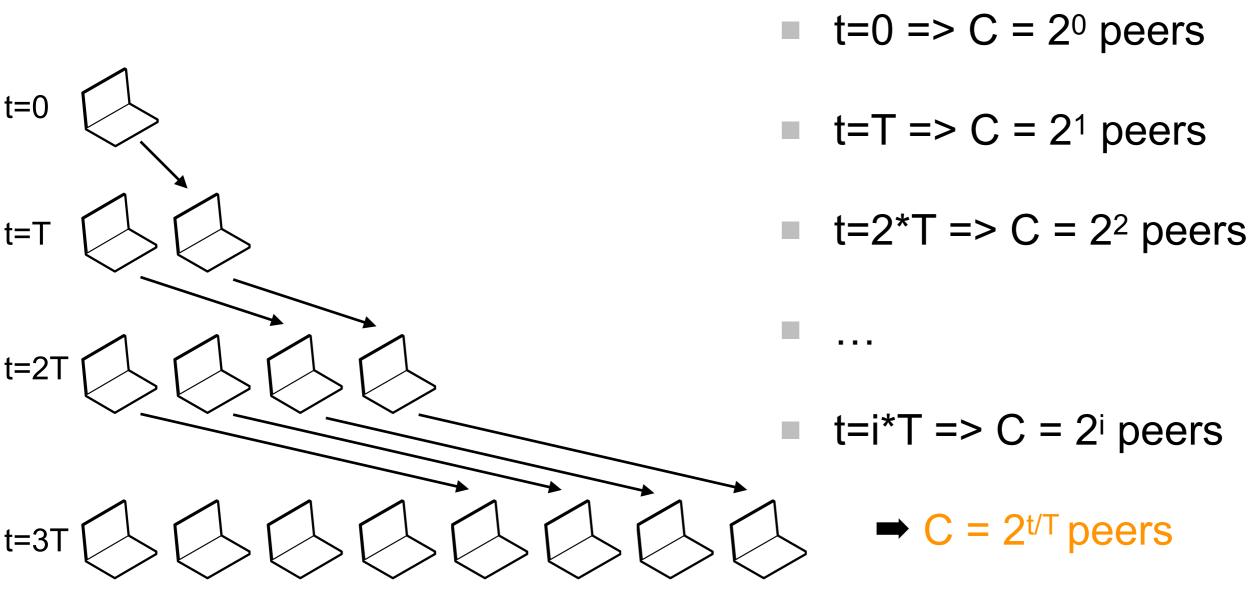
### Content transfer model

- Simple deterministic model
  - Each peer serves only one peer at a time
  - The unit of transfer is the content
  - n-1 peers want the content, with n=2<sup>k</sup>
- T is the time to complete an upload
  - T=s/b, s content size, b upload capacity
- Peer selection strategy with Binary tree
  - global knowledge

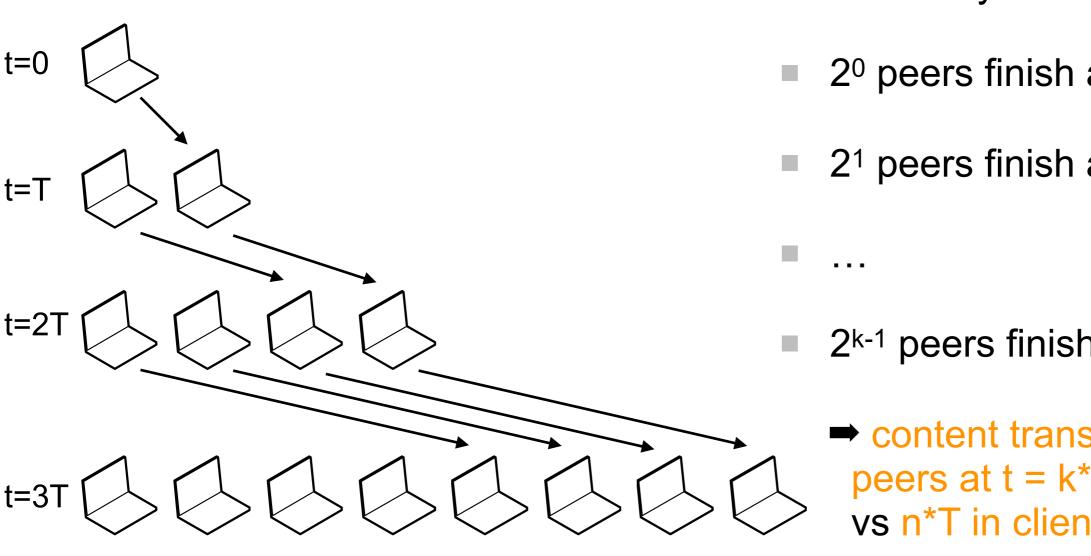








### Finish time



- seed only at time t = 0
- $2^0$  peers finish at t = T
- 2<sup>1</sup> peers finish at t=2T

- 2<sup>k-1</sup> peers finish at t=k\*T
  - content transferred to all peers at  $t = k^*T = T * log_2(n)$ vs n\*T in client-server

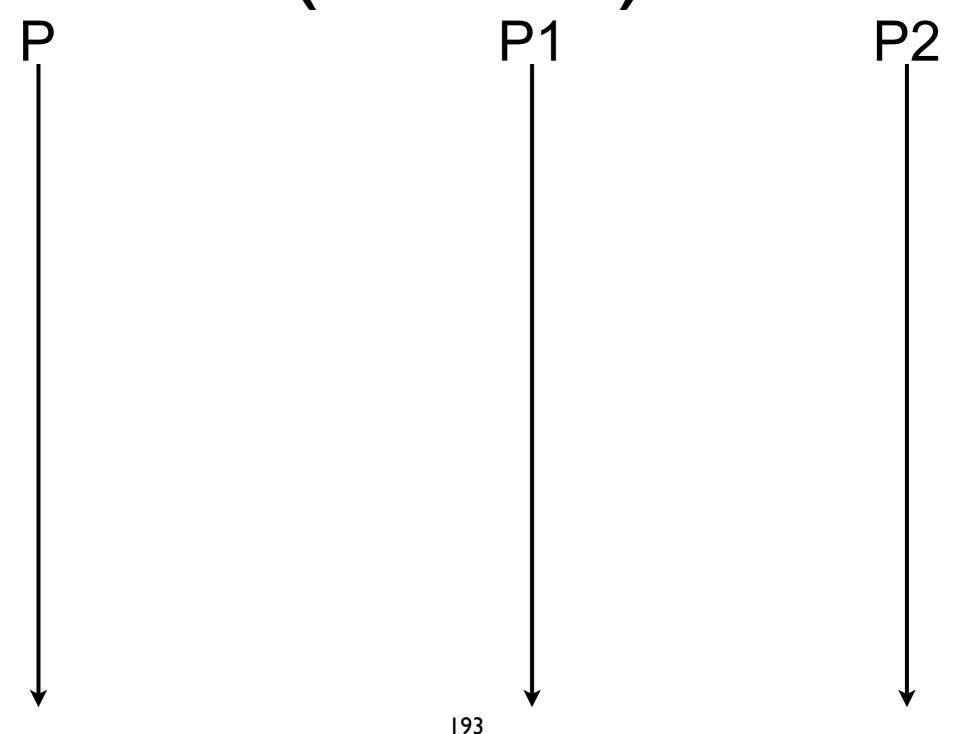
### Can we speed up transfers?

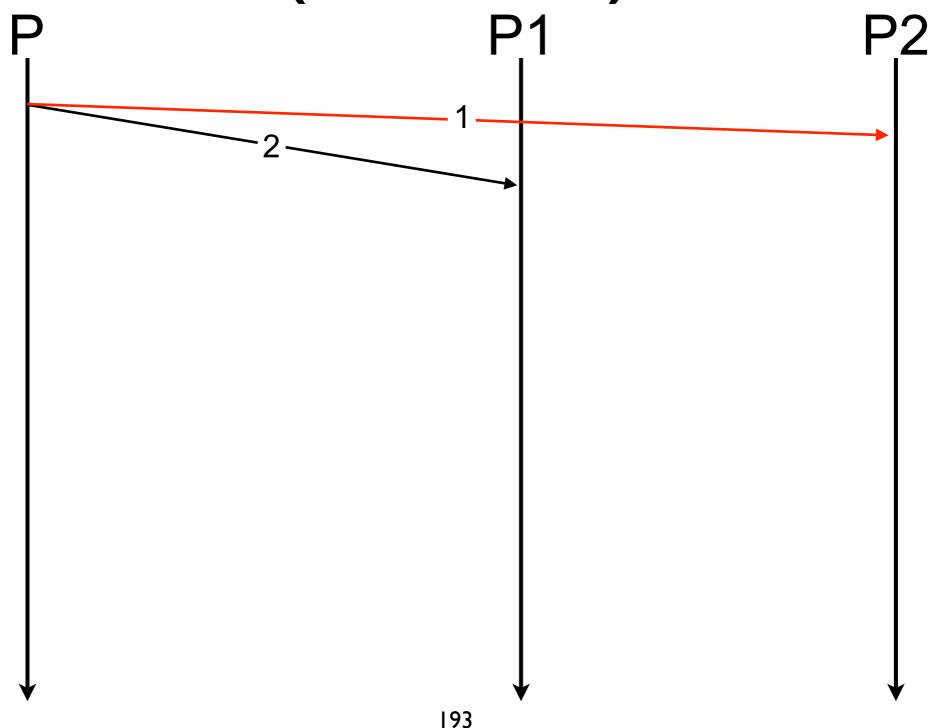
### Piece transfer model

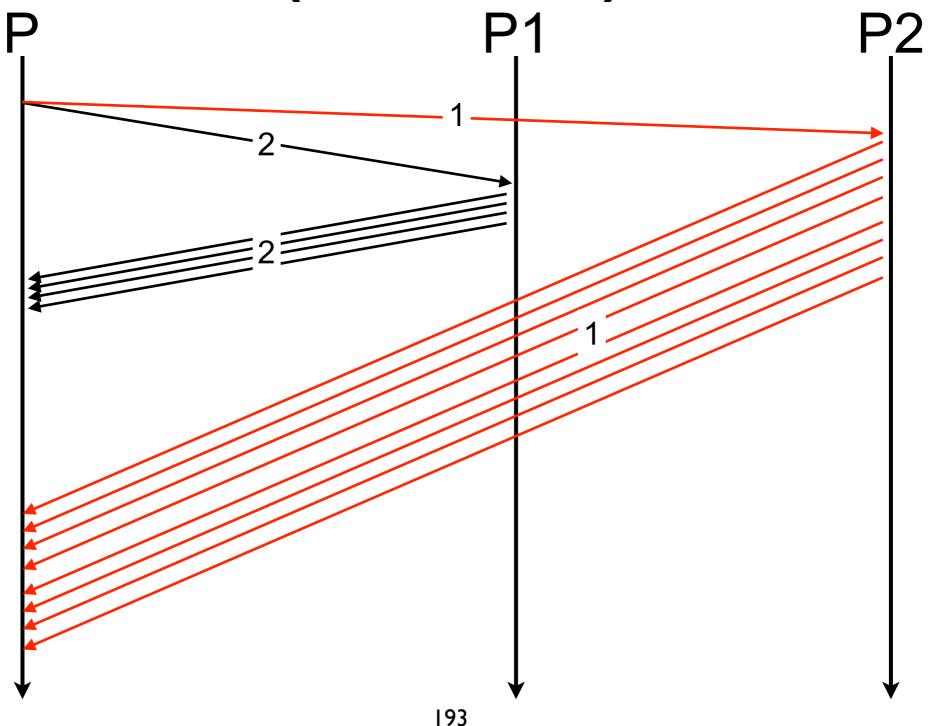
- Same as before but the transfer unit is the piece instead of the content
  - a content is divided into m equal size pieces
  - = m > k
  - Piece downloaded in T/m
  - →content transferred to all peers at t = T \* 1/m \* log<sub>2</sub>(n) + T vs T \* log<sub>2</sub>(n) without piece transfer vs n\*T in client-server

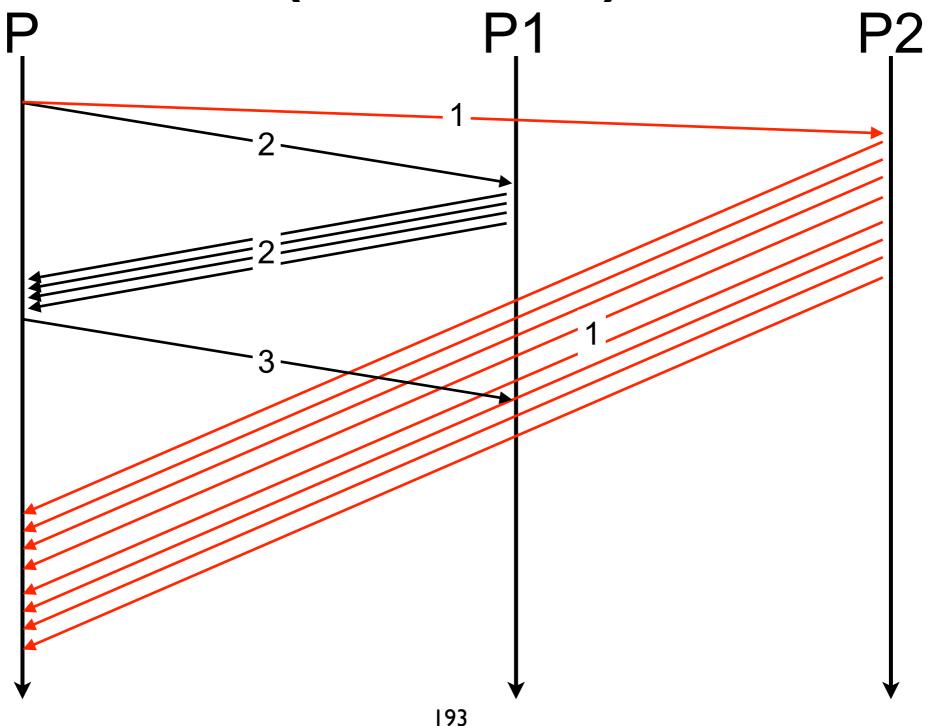
#### Parallel downloads

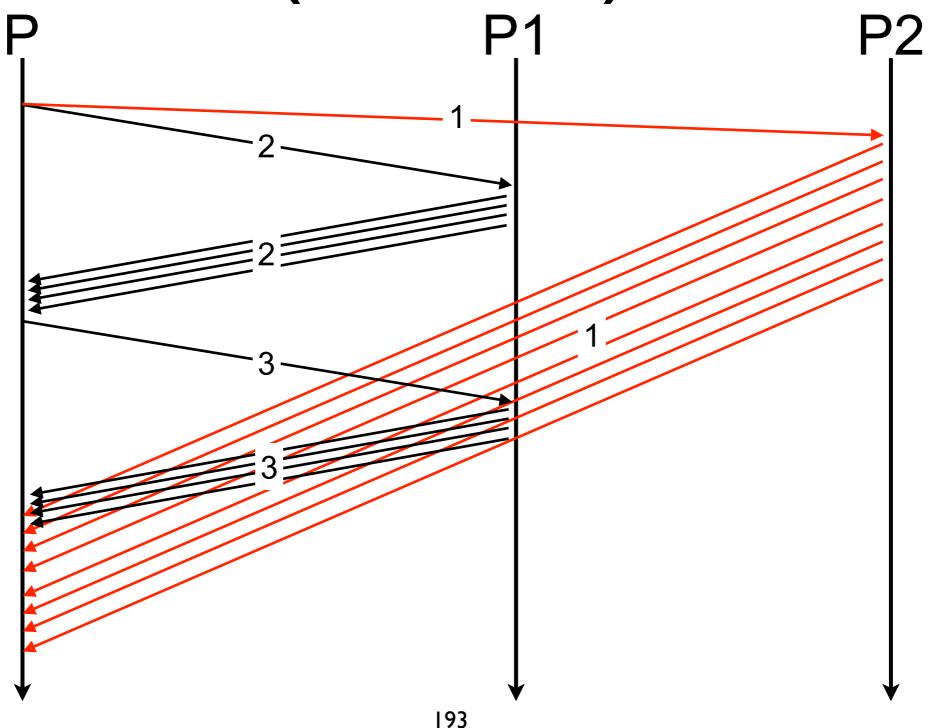
- Download from several peers in parallel
- Strategy
  - request one piece from every server with the content
  - request another piece from the server as soon as the requested piece has been obtained
    - performance is optimal when servers are always busy delivering a piece of data

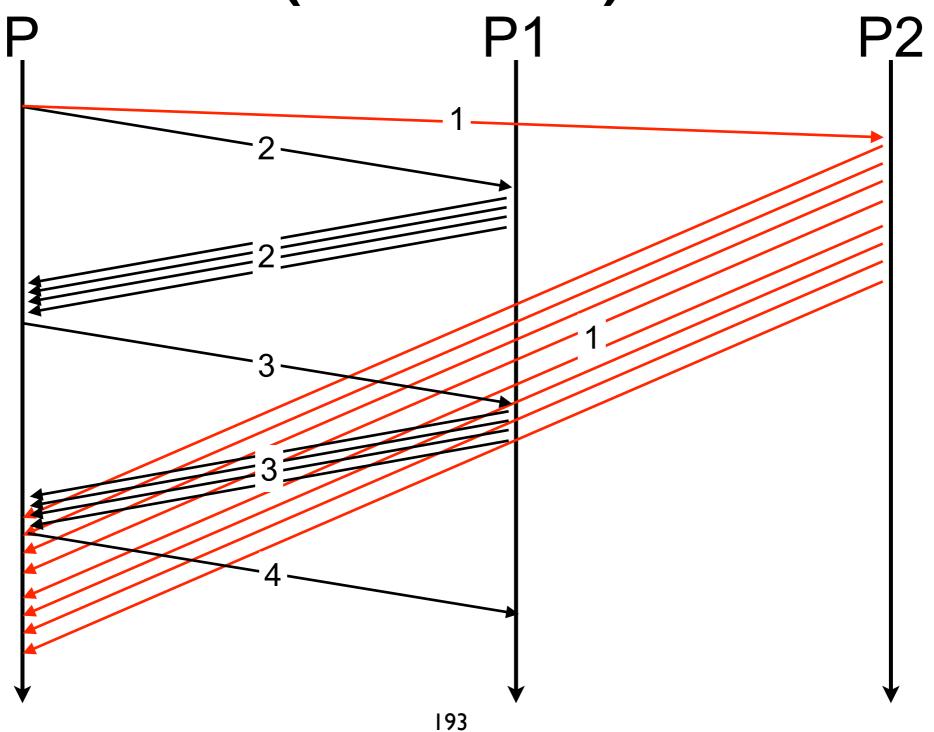


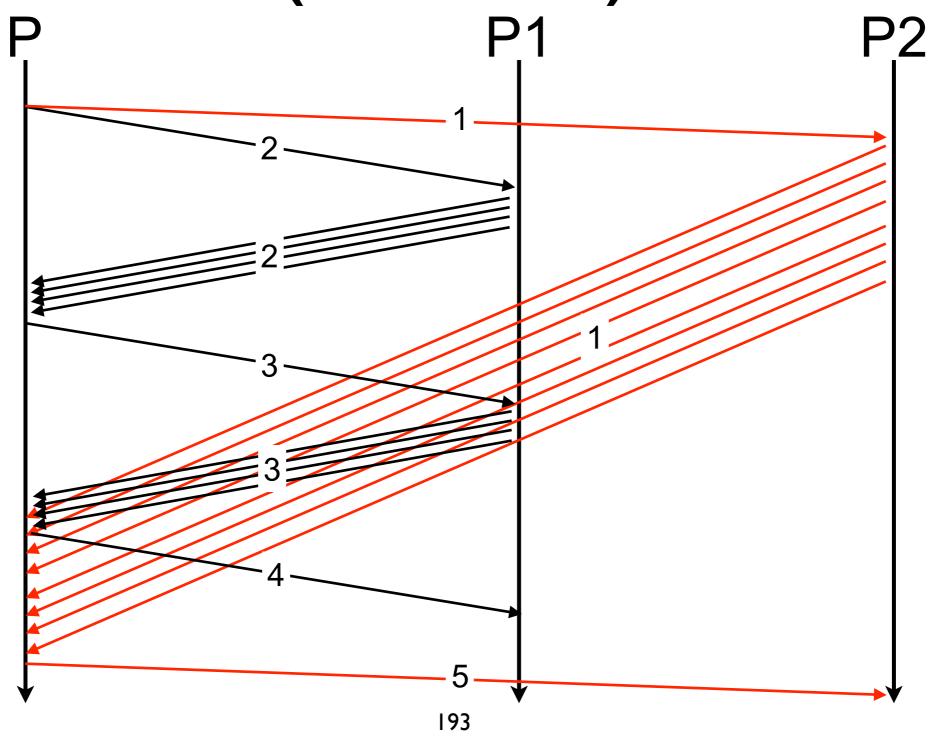


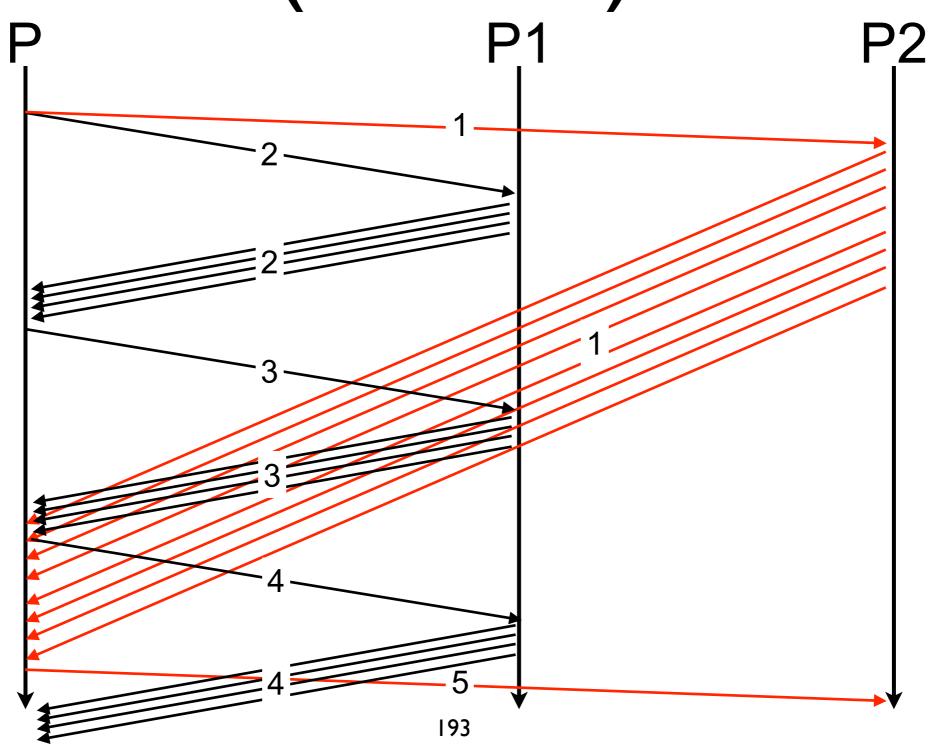


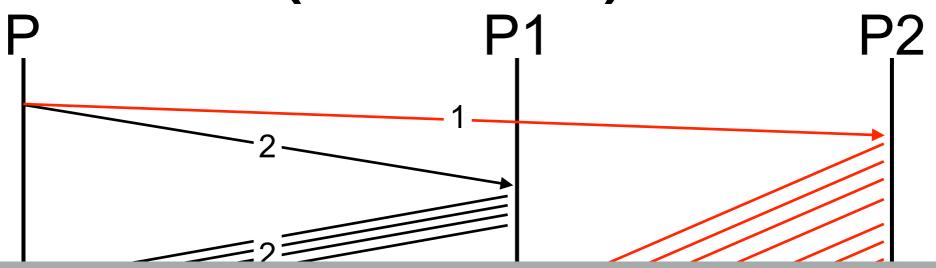




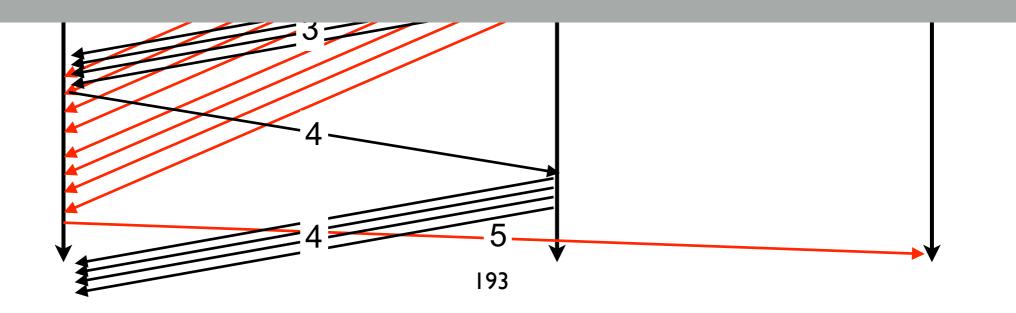






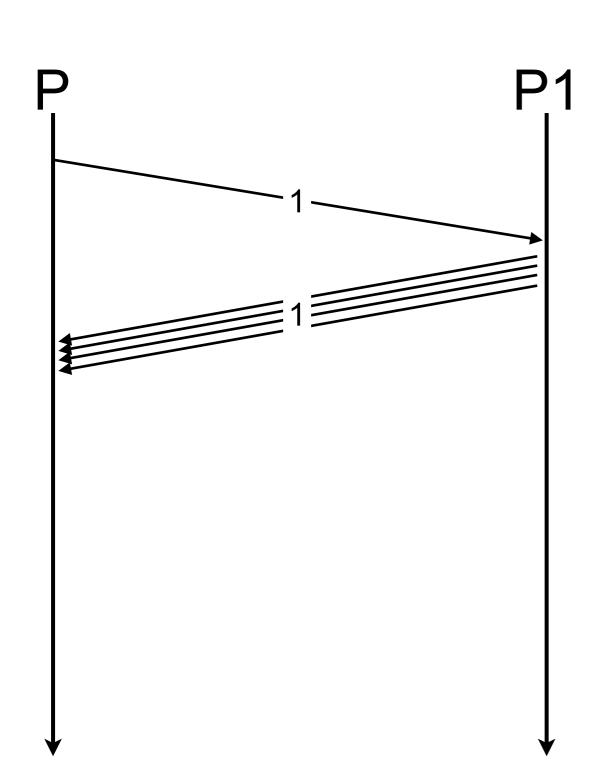


Peers are not always fully utilised!

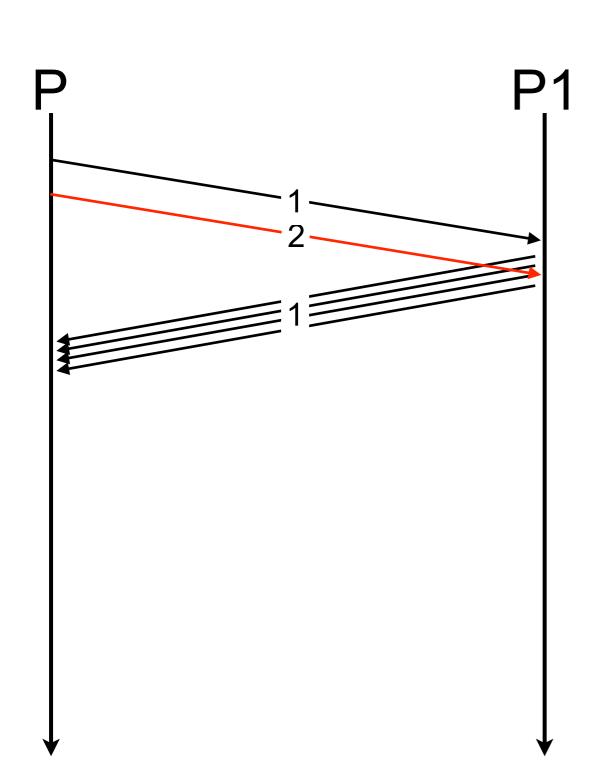


P1

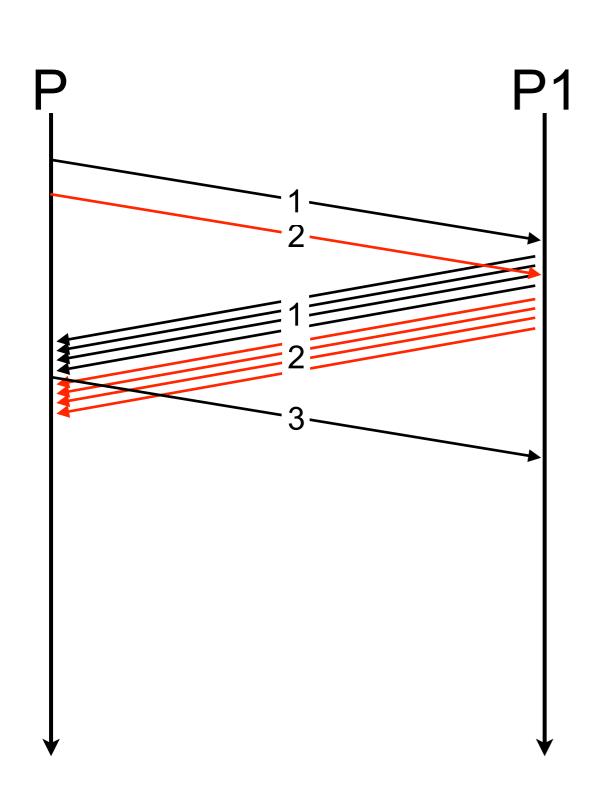
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT



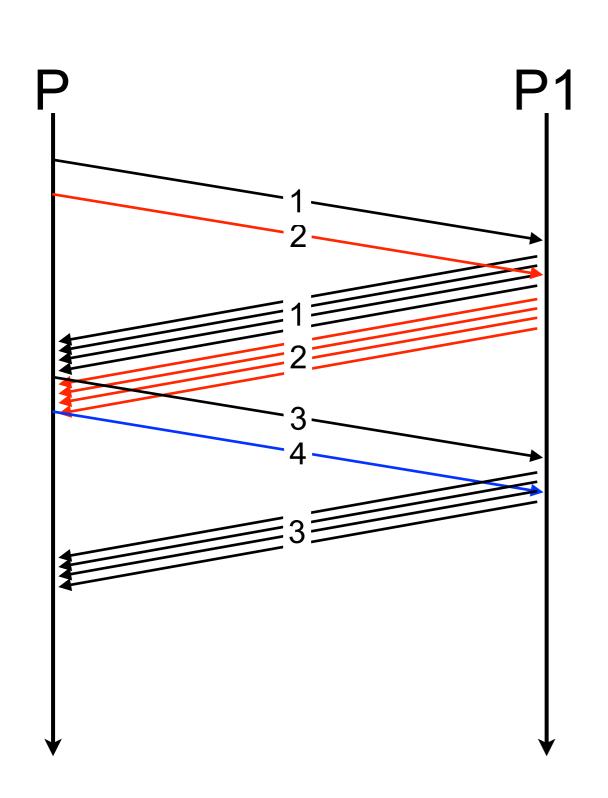
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT



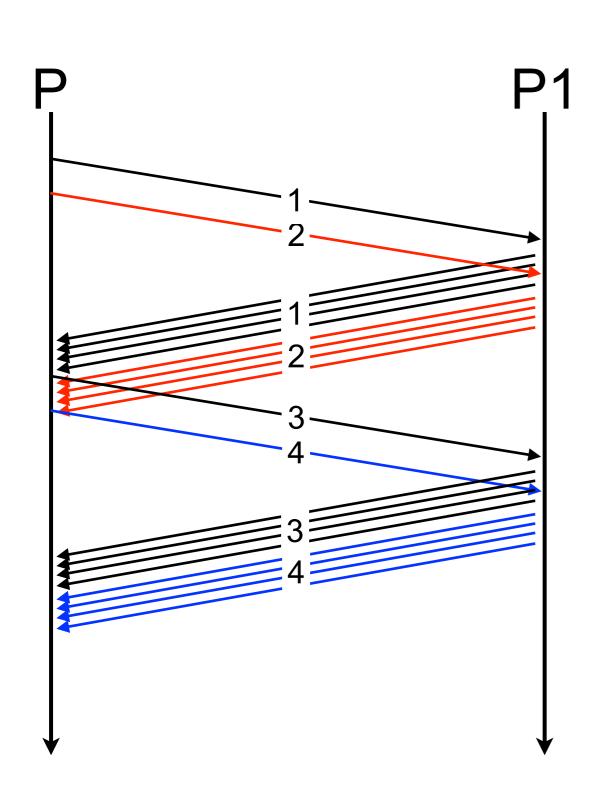
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT



- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT



- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT



- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
  - need to roughly estimate the RTT