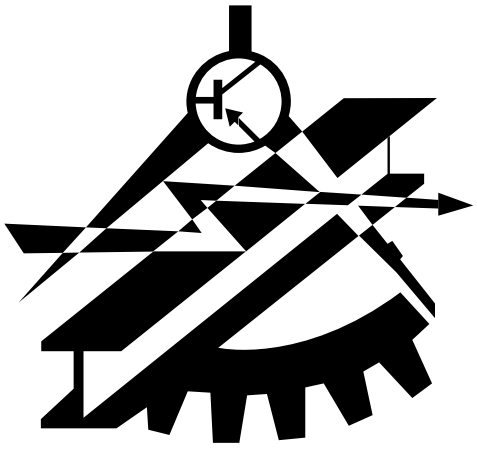


IN2T - Concepts informatiques

Cours 8
Internet

Sébastien Combéfis, Quentin Lurkin

Rappels

- Protocole *Ethernet*
- Protocole Internet (IP)
- *Address Resolution Protocol* (ARP)
- *Dynamic Host Configuration Protocol* (DHCP)

Objectifs

- *Transmission Control Protocol* (TCP)
- *Dynamic Name System* (DNS)
- *HyperText Transfer Protocol* (HTTP)
- *HyperText Transfer Protocol Secure* (HTTPS)

Transmission Control Protocol (TCP)

Problème : protocole IP ne garanti ni l'arrivée ni l'ordre des paquets

- Solution : TCP
- Basé sur IP

  On parle souvent de TCP/IP
- Protocole connecté $\Rightarrow$ 3 phases :
  - Connexion
  - Envoi de données
  - Déconnexion
- garanti l'arrivée et l'ordre des paquets

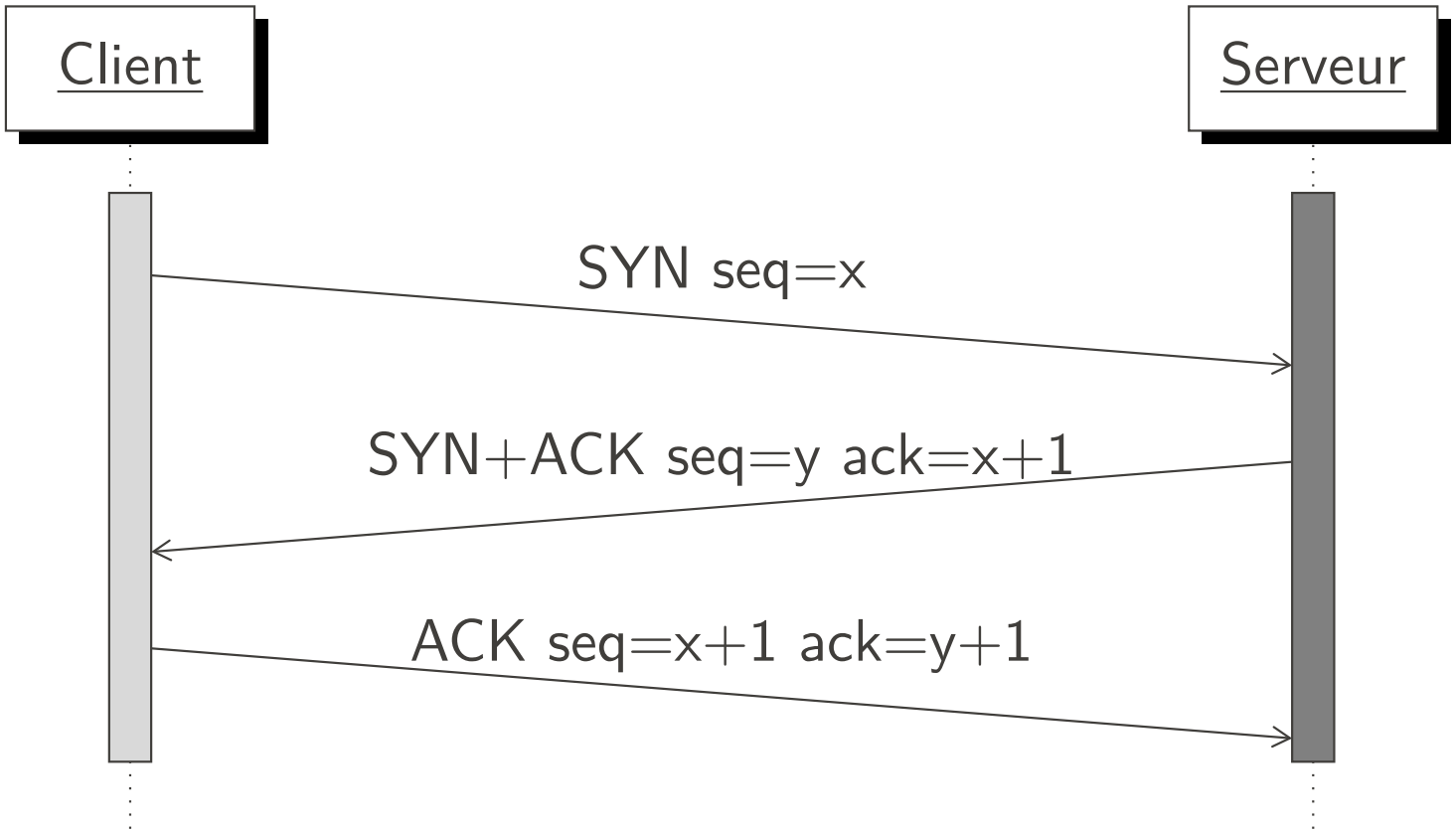
Transmission Control Protocol (TCP)

Les messages contiennent :

- Les numéros de port source et destination
- Des *flags* qui peuvent être à 1 ou à 0
  NS, CWR, ECE, URG, ACK, PSH, RST, SYN, FIN
- Un numéro de séquence
  Pour maintenir l'ordre des paquets
- Un numéro d'acquittement
  Contient le prochain numéro de séquence attendu
- Somme de contrôle
- ...

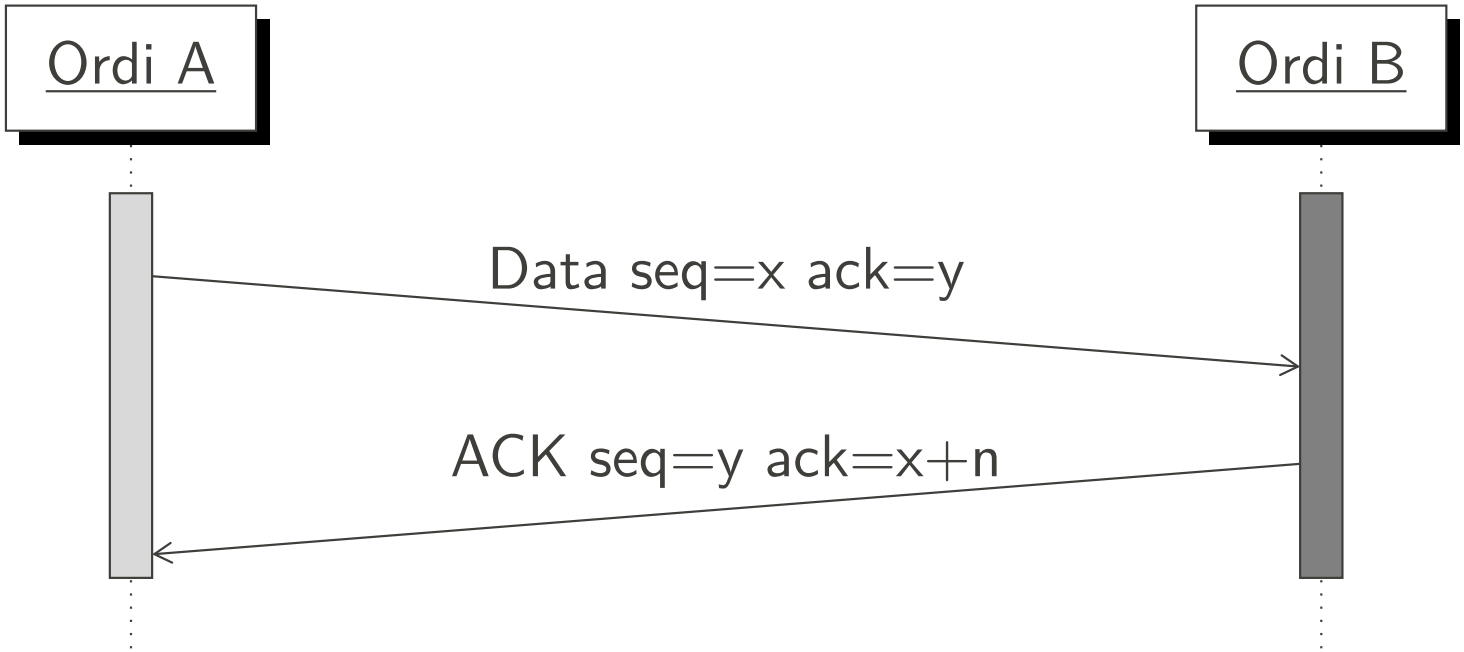
TCP : Connexion

Permet de synchroniser les numéros de séquence. Le client demande une connexion à un serveur qui écoute et peut l'accepter.



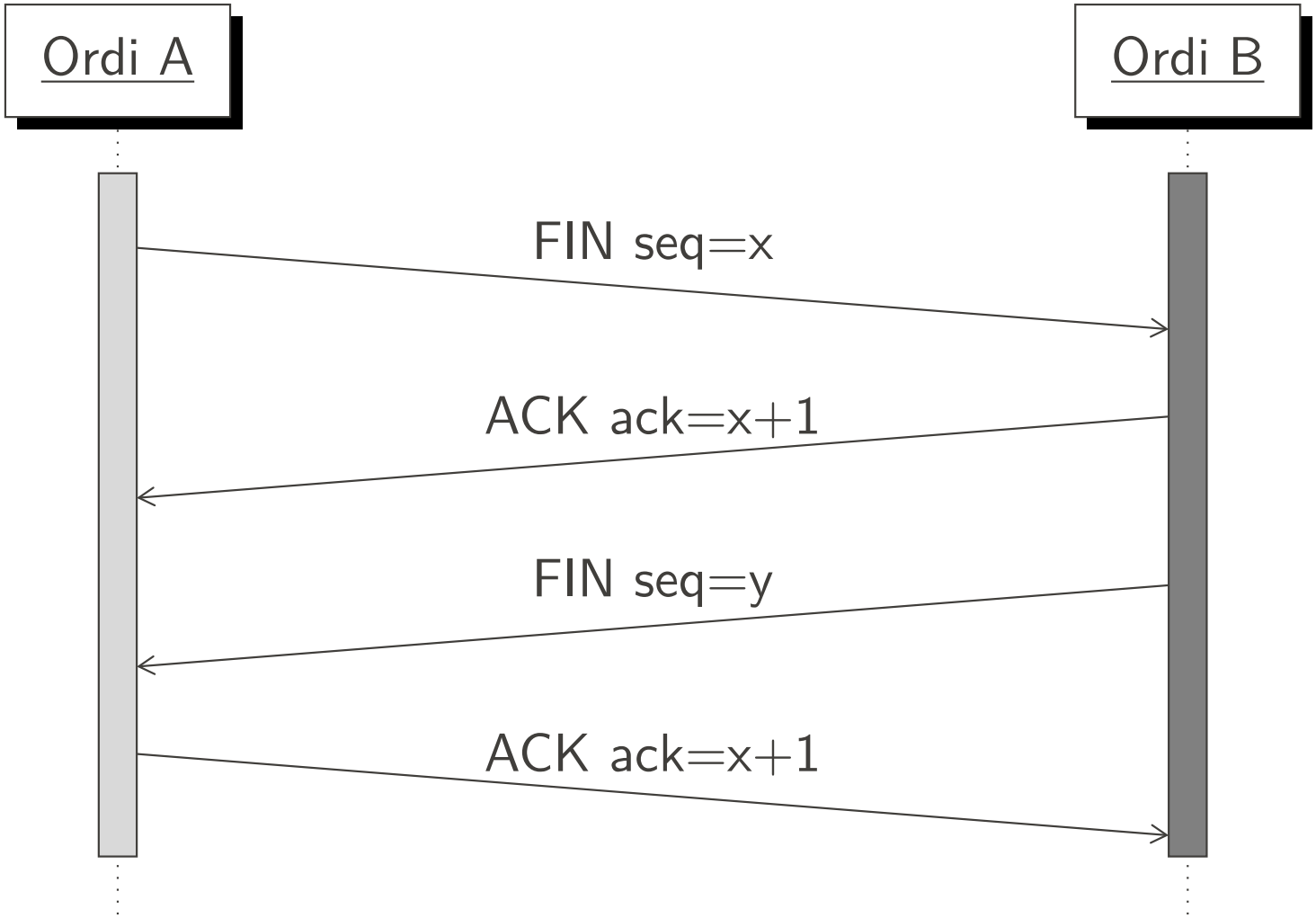
TCP : Envoi de données

Envoi de `n` octets. Dans un sens comme dans l'autre



TCP : Déconnexion

Peut être initiée par l'un ou l'autre des ordinateurs

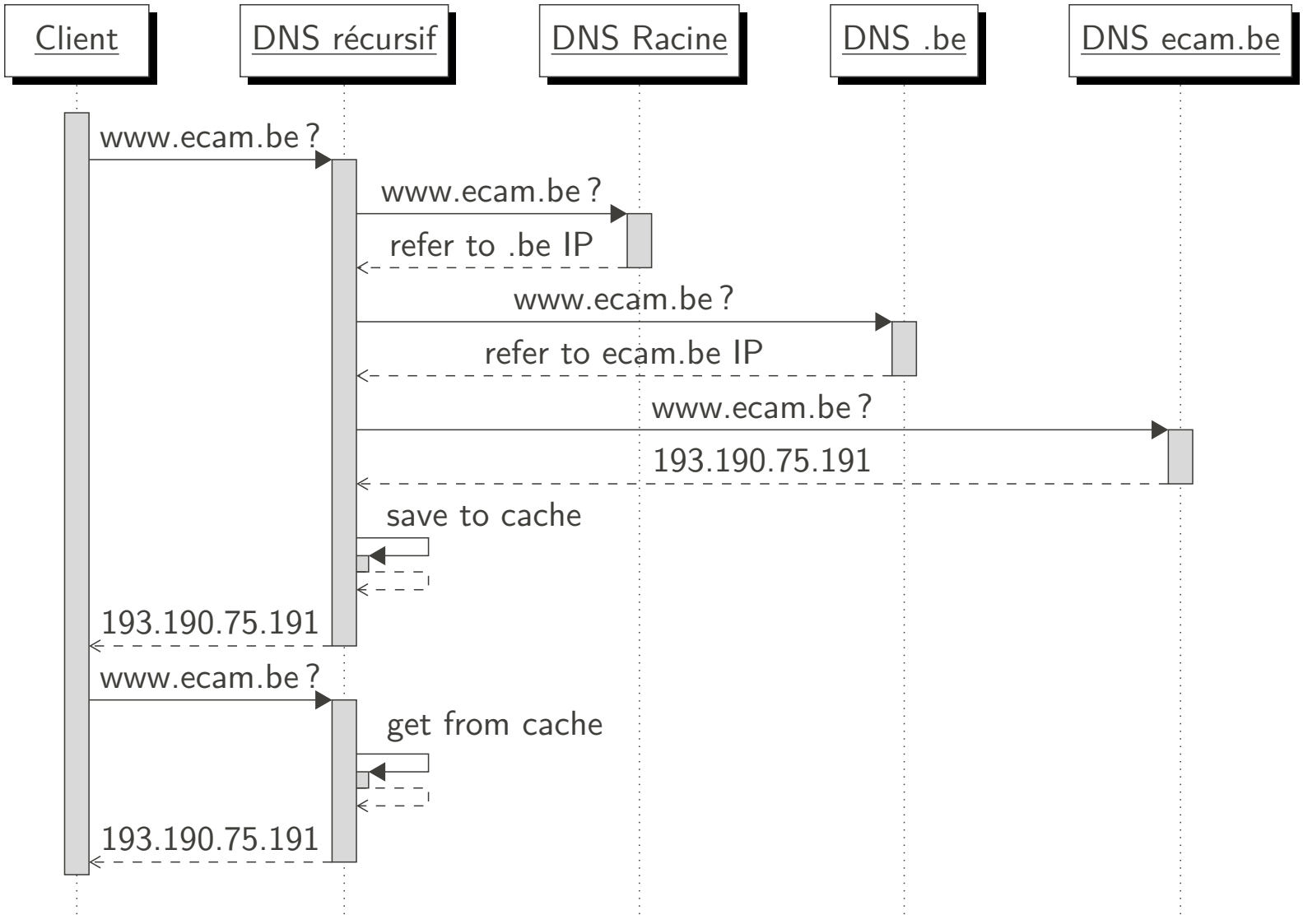


Dynamic Name System (DNS)

Les adresses IP ne sont pas pratiques pour les humains.

- DNS = répertoire qui associe un nom à une IP
  On parle de la résolution d'un nom de domaine
- Les correspondances sont stockées dans une hiérarchie de serveurs
- Des serveurs récursifs s'occupent de parcourir l'arborescence et de maintenir une cache des résolutions effectuées
- Un client obtient l'adresse d'un serveur DNS récursif
  Généralement par DHCP
- Les messages sont envoyés en UDP ou TCP
  UDP fournit uniquement les ports et une somme de contrôle

DNS : Résolution



HyperText Transfer Protocol (HTTP)

- Protocole de haut niveau
- Permet l'accès aux ressources sur internet
- Protocole client/serveur

  Le client envoie une requête, le serveur répond
- La requête et la réponse sont composées d'un entête et optionnellement d'un corp.
- L'entête est du texte, peut être du texte ou du binaire.
- Les requêtes et réponses sont généralement envoyée en TCP

HyperText Transfer Protocol (HTTP)

- La requête commence par l'établissement d'une connexion TCP.
- La requête proprement dite :

```
GET / http/1.1
Host: www.perdu.com
```

- Et la réponse :

```
hTTP/1.1 200 OK
Date: Thu, 22 Nov 2018 19:53:23 GMT
Content-Length: 204
Content-Type: text/html

<html><head><title>Vous Etes Perdu ?</title></head><body>
<h1>Perdu sur l'Internet ?</h1><h2>Pas de panique, on va
vous aider</h2><strong><pre>    * <----- vous &ecirc;tes
ici</pre></strong></body></html>
```

HyperText Transfer Protocol Secure (HTTPS)

2 problèmes :

- La confiance en le serveur DNS

  La bonne résolution des IP en dépends

- Le contenu des requêtes et des réponses passent en clair sur le réseaux

Pour régler ces problèmes, HTTPS utilise 3 concepts :

- Le cryptage
- La signature numérique
- Des autorités de certification

Le cryptage

- Le cryptage se base sur une fonction à sens unique qui utilise une clé d'encryptage `eKey`

  Appelons la ***`encrypt(eKey, message)`*** $\rightarrow$ ***`cryptedMsg`***

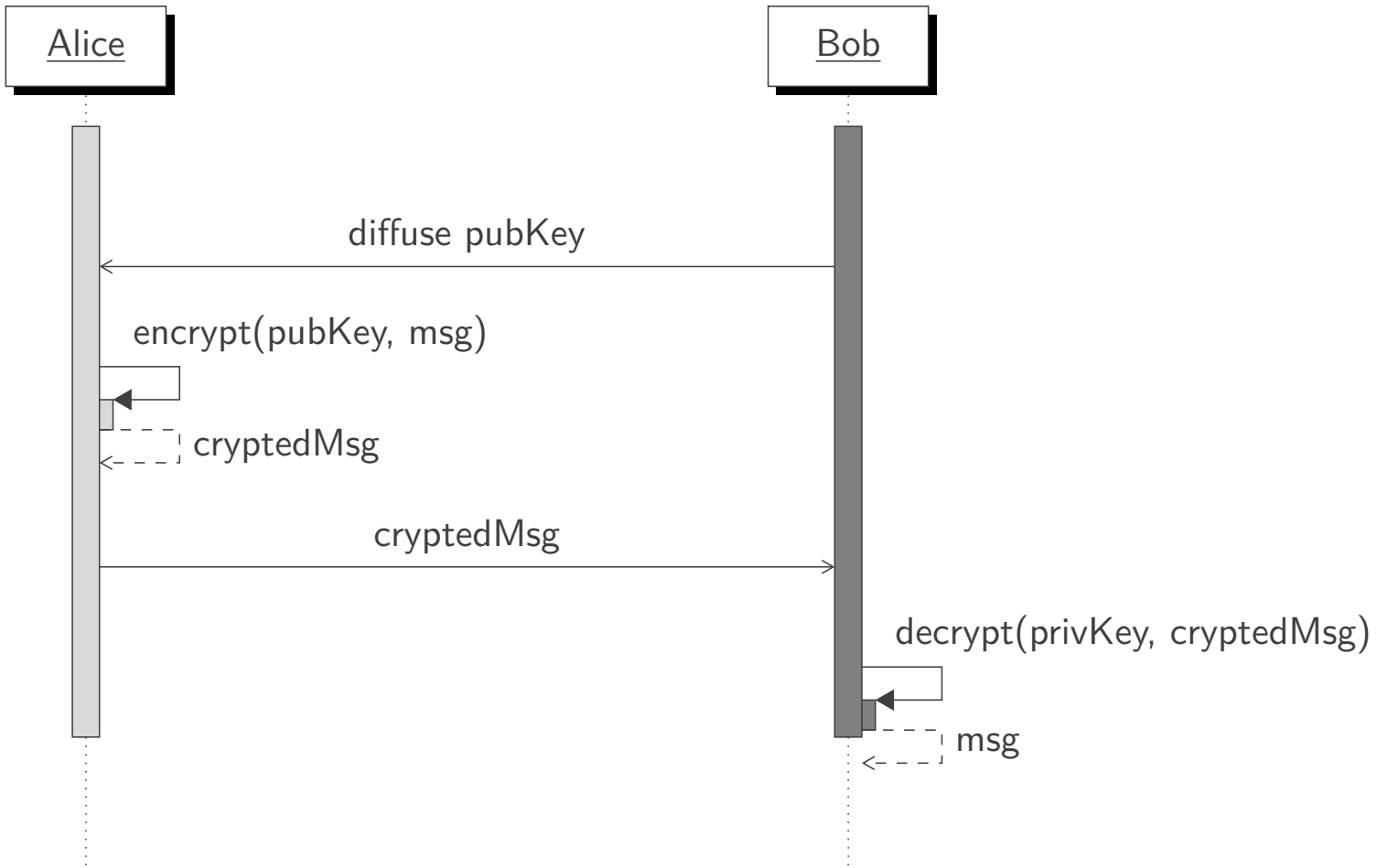
- Il est très difficile (long) de retrouver le `message` à partir de `cryptedMsg` sauf si on connaît `dKey`, la clé de décryptage.

  `decrypt(dKey, cryptedMsg)` $\rightarrow$ ***`message`***

- La clé d'encryptage est appelée clé publique, la clé de décryptage clé privée

- Ce cryptage est appelé asymétrique. Un cryptage symétrique utilise la même clé pour l'encryptage et le décryptage.

Le cryptage

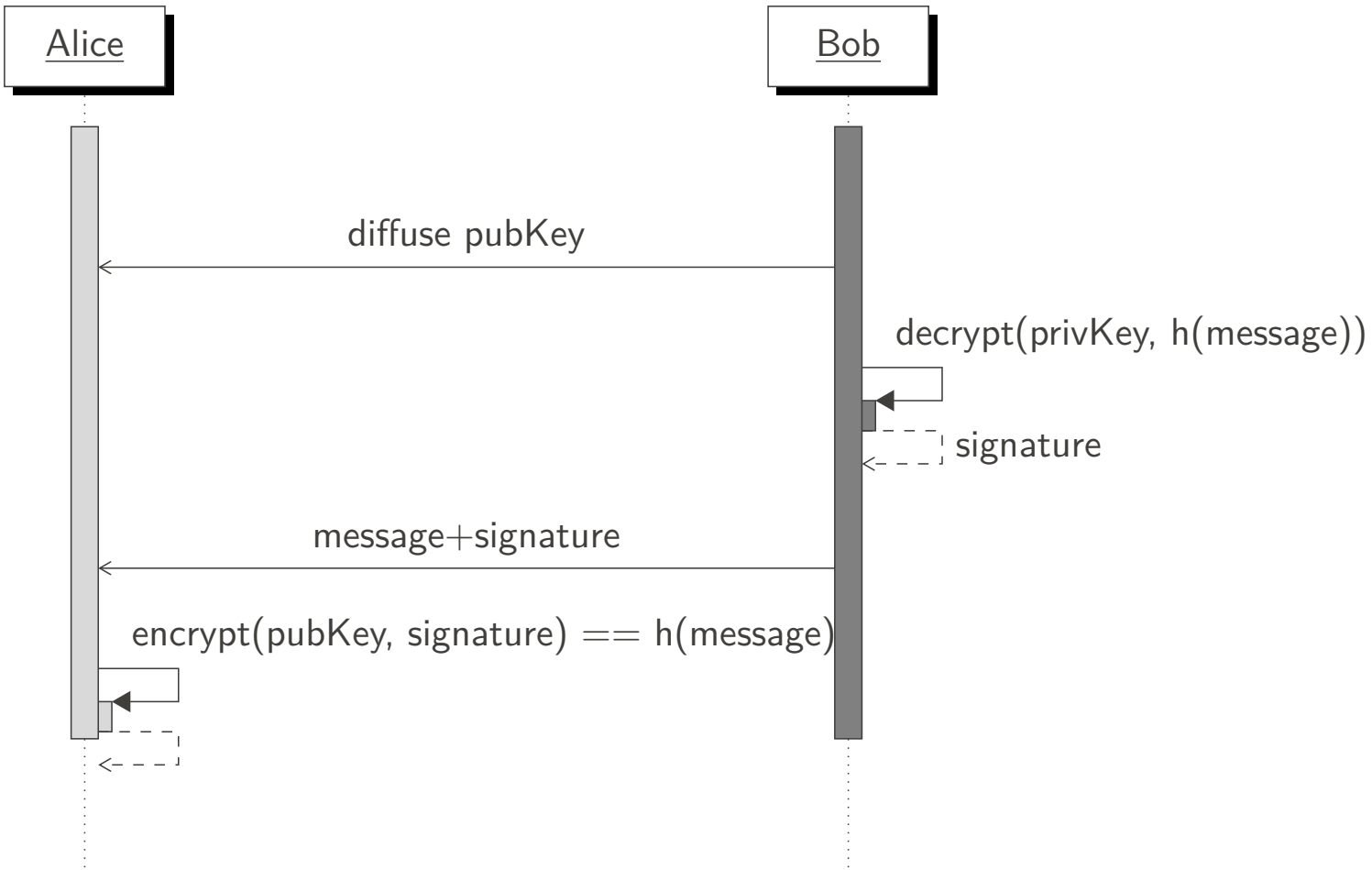

Alice
Bob
diffuse pubKey
encrypt(pubKey, msg)
cryptedMsg
cryptedMsg
decrypt(privKey, cryptedMsg)
msg

La signature numérique

Permet de s'assurer :

- de l'expéditeur d'un message
- que le message n'a pas été modifié

La signature numérique



Les autorités de certification

Fournit des certificats qui contiennent :

- Une clé privée
- Une clé publique
- Le ou les noms de domaine liés au certificat
- La signature de l'autorités de certification

  La signature porte sur la clé publique et les noms de domaine

HTTPS Connexion