

## Examen Protocoles et Services Internet

(durée 1 heure 30, documents interdits)

*Tous les exercices sont indépendants. Les réponses doivent être courtes (environ 3 lignes).*

**Exercice 1.**— (maximum 3 lignes par question) Soit  $u$  une page web sur le serveur  $s$ ,  $u$  contient uniquement des références à des fichiers  $f_1, \dots, f_m$  qui sont tous sur le même serveur. On suppose que le temps pour obtenir  $f_i$  (requête http + temps de la réponse) est  $rtt_i$  et que le temps pour établir une connexion vers le serveur est  $t_s$ .

1. Quel est le temps total pour obtenir la page complète en mode persistant? En mode non-persistant? En mode non-persistant avec un navigateur configuré pour  $k$  connexions en parallèle?
2. On suppose que l'adresse IP du serveur n'est pas dans le cache de l'hôte local. En quoi consiste le temps de la connexion? Le temps de la deuxième connexion vers le serveur sera-t-il identique au temps de la première?

**Exercice 2.**— (maximum 3 lignes par question)

1. A quoi sert un DNS?
2. Peut-il y avoir plusieurs adresses IP associées au même nom?
3. Peut-il y avoir plusieurs noms associés à la même adresse IP?
4. A quoi correspondent les serveurs DNS racines? les "top-level domain" (TLD) serveurs? les "authoritative" DNS serveurs?
5. Quelle est la différence entre le mode récursif et itératif?
6. Pourquoi un DNS est un élément important concernant la sécurité?

**Exercice 3.**— Définir ce que l'on entend par un proxy? A quoi un proxy peut-il servir?

**Exercice 4.**—

1. Alice veut envoyer un message à Bob, quels mécanismes peuvent-ils utiliser pour garantir que seul Bob pourra lire le contenu du message d'Alice.
2. Alice veut envoyer un message à Bob, quels mécanismes peuvent ils utiliser pour garantir que Bob aura aussi la garantie que le message a bien été envoyé par Alice et, de plus, que le message n'est pas un message enregistré et réémis par un tiers.
3. Pourquoi de nombreux protocoles utilisent des systèmes à clés symétriques et limitent l'usage de systèmes à clés publiques?

**Exercice 5.**— Expliquer succinctement en quoi consiste le modèle client serveur. Même question pour le modèle Pair à Pair. Au niveau des connexions avec des sockets (par exemple Java), la notion de pair à pair a-t-elle du sens? Si non pourquoi et si oui de quelle façon?

Pour trouver les données dans un système pair à pair, on peut utiliser des filtres de Bloom ou des DHT (Distributed Hash Table). Comment fonctionnent ces mécanismes?