Protocoles HTTP et HTTPS

Célian Butré

29 décembre 2020

Table des matières

Bulletin officiel

Contenu	Capacités attendues	Commentaires
Sécurisation des communications	Décrire les principes de chiffrement symétrique (clef partagée) et asymétrique (avec clef privée/clef publique). Décrire l'échange d'une clef symétrique en utilisant un protocole asymétrique pour sécuriser une communication HTTPS.	Les protocoles symétriques et asymétriques peuvent être illustrés en mode débranché, éventuellement avec description d'un chiffrement particulier. La négociation de la méthode chiffrement du protocole SSL (Secure Sockets Layer) n'est pas abordée.

Introduction

Brève introduction sur le contexte général et les motivations : internet et le web, premier protocole HTTP, pas assez sécurise, etc.

On peut citer ici les sources utilisées dans tout le document, comme par exemple [1], et [2] (que l'on peut aussi citer ponctuellement dans le document si on ne s'en sert juste pour une information ou figure).

C'est également ici que l'on peut introduire les acronymes importants utilisés tout le long ou une partie du document :

`HTTP` (« *Hyper Transfert Protocol* » ou « *protocole de transfert d'hyper texte* » en français) et `HTTPS` (« *Hyper Transfert Protocol Secure* » ou « *protocole de transfert sécurisé d'hyper texte* » en français)

Quelques rappels TeX / LaTeX : figure et algorithme (à terme : figure et algo à supprimer de l'intro)

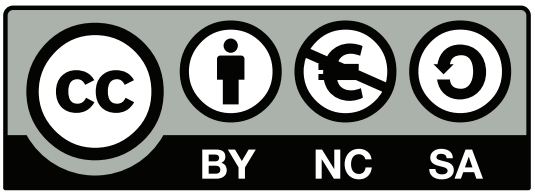

FIGURE 1 – Titre de la figure : logo de la licence libre CC BY-NC-SA.

Algorithme 1 : Nom de l'algorithme.

Entrée : entrée de l'algo
Sortie : sortie de l'algo

```
// un commentaire à la C++
une variable ← une valeur
Rédiger_rapport(param1 = n élèves)
TantQue une condition avec un ou en gras Faire
    faire_un_truc
    faire_un_autre_truc
Si une condition Alors
    bloc du si
Sinon
    bloc du sinon
Retourner un truc si l'algo a bien taffé
```

On peut faire référence dans le texte (et il le faut) à la figure ou à l'algorithme avec Fig. `ref{fig1}` ou Algo. `\ref{algo1}` (fig1 et algo1 étant les clés/label associés), ce qui donne : Fig. 1 et Algo. 1.

1 Protocoles de communications

Une phrase d'intro pour expliquer le rôle de cette partie : notions très générales, dont `HTTP` et `HTTPS` sont des implantations techniques de certaines de ces idées.

1.1 Protocoles simples

— Notion de réseau
— Notion d'échange et de communication informatique
— Notion de protocoles de communication (au sens large : « bonjour », « bonjour », etc)
— Notion et définition de protocole informatique
— Nécessité de protocoles de communication

1.2 Protocoles cryptés

Notion de cryptographie et necéssité de crypter les communications.

Figure 2 – Titre de la figure.

2 Le protocole HTTP

Mini-spoiler en une phrase : en gros c'est quoi HTTP.

2.1 Contexte

— Web
— Tim Berners-Lee
— Motivation et utilisation du protcole

2.2 Description du protocole HTTP

Algorithme 2 : Protocole HTTP.

2.3 Exemple d'échange suivant le protocole HTTP

Figure 3 – Établissement d'une communication via le protocole HTTP.

3 Le protocole HTTPS

Mini-spoiler en une phrase : en gros c'est quoi HTTPS.

3.1 Motivation

— Problèmes et failles de HTTP
— Sécurité

3.2 Protocole TLS

Figure 4 – Établissement d'une liaison TLS.

3.3 Description du protocole HTTPS

HTTP + TLS = HTTPS

Algorithme 3 : Protocole HTTPS.

FIGURE 5 – Établissement d'une communication via le protocole HTTPS.

3.4 Exemple d'échange suivant le protocole HTTPS

Références

[1] *Site Pixees*, D. Roche. https://pixees.fr/informatiquelycee/n_site/nsi_term_archi_secu.html

[2] *Site Le Web Pédagogique*. https://lewebpedagogique.com/dlaporte/category/nsi-1ere/

[3] *Wikipédia*, article « Hypertext Transfer Protocol ». https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[4] *Wikipédia*, article « Hypertext Transfer Protocol Secure ». https://en.wikipedia.org/wiki/HTTPS

[5] *Wikipédia*, article « Transport Layer Security ». https://fr.wikipedia.org/wiki/Transport_Layer_Security

[6] *Chaîne youtube Comprendre le* SSL/TLS, Y. Bidon. https://www.youtube.com/playlist?list=PLYsJ-3MUn_eeYwSgJ3Z_hfrIzGqYOGAaj