Cryptographie

Leopold Tran

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 : depuis l'Antiquité, besoin de protéger des secrets et des communications, 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 :

algo / méthode RSA (du noms des auteurs de l'algorithme : Riverst, Shamir et Adleman).
Quelques rappels TeX / LaTeX : figure et algorithme (à terme : figure et algo à supprimer de l'intro)

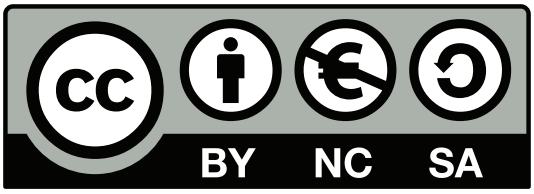

FIGURE 1 – Titre de la figure : logo de la licence libre CC BY-NC-SA.

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 Cryptographie

1.1 Un peu d'histoire

- Motivations
- Importance de la crypto, indépendemment de la période historique (aussi important à l'antiquité ou au moyen-âge que dans le monde numérique actuel)
- Intérêt porté à la crypto par certains mathématiciens importants : antiques (?), arabes du moyen-âge (Ibn al-Durayhim, Al-Kindi), Turing, les polonais du début de la guerre, etc

FIGURE 2 – Une photo d'Enigma ?

1.2 Idée générale et quelques méthodes cryptographiques

Notion / définition de cryptographie / cryptage / code :

Chiffrement / déchiffrement :

Aspects mathématiques : quel type de mathématiques est utilisé ? (arithmétique)

Présentation de quelques méthodes simples : code de César, Vigenère, etc.

2 Cryptographie à clé symétrique, ou à clé privée

Mini-phrase spoiler : c'est quoi le principe de clé symétrique ? (un gamin de 10 ans doit pouvoir comprendre ici).

2.1 Principe

Notion de clé privée :

Principe de la communication à clé privée : à expliquer de manière simple (quasiment toujours formulée classiquement avec Alice et Bob qui veulent communiquer et s'échanger de l'info, et éventuellement une espionne Eve). On peut faire référence à la figure.

FIGURE 3 – Principe de chiffrement à clé privée.

2.2 Quelques exemples

Vigenère, Enigma, etc

Algorithme 2 : Un algo simple type code de César ?

3 Cryptographie à clé asymétrique, ou à clé publique

Mini-phrase spoiler : c'est quoi le principe de clé publique ? (un gamin de 10 ans doit pouvoir comprendre ici).

3.1 Principe

Notion de clé publique :

Principe de la communication :

Lien avec la crypto à clé privée : RSA peut par exemple servir à s'échanger une clé privée

FIGURE 4 – Principe de chiffrement à clé publique.

3.2 Quelques exemples

RSA (avec un *c.f. section suivante*), DSA (autres ?)
Utilisation et importance aujourd'hui.

4 La méthode RSA

4.1 Contexte

Motivation :

Origine : Rivest, Shamir et Adleman

Utilisation : énorme aujourd'hui

4.2 Principe général

Méthode / algo **(très général sans les détails)** RSA.

Algorithme 3 : Algorithme RSA.

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 « Cryptography ». `https://en.wikipedia.org/wiki/Cryptography`

[4] *Wikipédia*, article « Symmetric-key algorithm ». `https://en.wikipedia.org/wiki/Symmetric-key_algorithm`

[5] *Wikipédia*, article « Public-key cryptography ». `https://en.wikipedia.org/wiki/Public-key_cryptography`

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