

[Exercices de documentation liés au cours théorique de la Semaine 2]

(Écrit par Robert Vanden Eynde dans le cadre du cours INFOS302, Université Libre de Bruxelles)

J'ai créé ces exercices pour faire un parallèle entre la partie théorique (culture générale) et la partie pratique

Cherchez sur internet ! C'est comme ça qu'on apprend beaucoup de choses en informatique, Wikipédia est une bonne source d'info.

Vous montrer aussi des exemples pour que ce qui est discuté dans le cours théorique soit plus concret.

Ce n'est pas matière d'examen.

Les exercices ne sont pas toujours par ordre de difficulté, je vous invite à passer un exo s'il est trop dur.

Cela permet de vous inviter à plus vous documenter tout en restant dans le cadre du cours.

Vous pouvez voir ça aussi comme un complément d'information pour les intéressés.

Ne vous inquiétez pas, je ne compte pas vous donner un tel document chaque semaine.

1) Binaire et comptage de base

1.1)

Trouver une manière de transformer le nombre 1011010011 en décimal

Trouver une manière de transformer le nombre 189 en binaire

(Indice: Ce nombre est-il pair ? Comment sont représentés les nombres pairs en binaire ? Comment diviser par deux en binaire ?)

1.2)

Combien font $1011010011 + 1$ (en binaire) ?

Comment représenter "-1" en complément à deux sur 8 bits ?

Le nombre 10100101 (écrit en binaire complément à deux sur 8bits) représente quel nombre en décimal ? (Optionnellement: Comment faire en complément à un, dire pourquoi c'est peu utile).

1.3)

Compter jusque 255 en hexadécimal.

1011010011 en hexadécimal sans passer par le décimal ?

1.4)

Combien existent-ils d'entiers positifs en 32 bits ? Et en 4 octets ?

Comparez ça avec l'avènement des machines 64 bits sur les ordinateurs de plus de 4Gb de RAM.

1.5) Pour les nombres non entiers, il existe un standard très utilisé parlant de "float" et de "double", quel est ce standard ? Quels sont l'ensemble des nombres pouvant être représentés ? Comme par exemple 1.5, $1/3$, racine de 2, Infini et leurs versions négatives ? Qu'est-ce que "NaN" ?

1.6)

Et en python pour convertir entre les bases et représenter les nombres non-entier ?

(Voir aussi le type "bytes" et "fraction" en python)

2) Caractères et Binaire

- 2.1) Encoder le prénom Robert en ascii, combien de bytes utilisez-vous ? Qu'en est-t-il des caractères de ponctuation et du caractère "à la ligne" (Différence entre Windows et Mac) ? Écrivez un fichier .txt et vérifiez vos dires. Vous pouvez aussi regarder le binaire du fichier avec un logiciel approprié.
- 2.2) Maintenant la même chose pour le prénom Frédérique et ses fameux accents sur ses e (donnant "é").
- 2.3) Que feriez-vous pour encoder son alter ego russe Роберт ? Sachant que le russe a 33 lettres minuscules et 33 lettres majuscules.
- 2.4) Quel était le problème de Windows et ses encodages 8 bits régionaux Windows-1252, Windows-1251, Windows-1253 et autres ?
- 2.5) Maintenant, comment faire pour encoder un texte mélangeant un peu de tous les caractères de toutes les langues du monde ?
- 2.6) Qu'est-ce que U+00E9 et U+2192 ? (Astuce: c'est lié à Unicode, Réponse partielle: ce sont des caractères Unicode, mais lequel ?)
- 2.7) Encoder Robert et Frédérique et Роберт et ← ↓ → ↑ en UTF-8, combien d'octets sont utilisés ? Comment le faire en UTF+16 ? Pourquoi UTF-8 est bien plus utilisé que UTF-16 ? Et comment encoder un emoji comme " 🍌 " ?
- 2.8) Donnez un exemple de suite d'octets qui n'est pas valide en UTF-8
- 2.9) Si vous avez un message (une suite d'octets) en UTF-8 et vous coupez au milieu, comment savoir où se trouve le prochain caractère ? (Vu qu'un caractère peut être encodé en plusieurs bytes, quand on coupe un message en 2 il peut arriver qu'on coupe un caractère en deux).
- 2.10) Comment encoder un symbole unicode comme "→" en html ? (Je vois 3 manières)
- 2.11) Si vous vous intéressez au CKJ (Chinois, Coréen, Japonais), vous seriez intéressé de voir comment sont encodés leurs caractères. Unicode gère ça.
- 2.12) Si vous vous intéressez à l'arabe (qui s'écrit de droite à gauche), vous seriez intéressé de voir comment sont encodés leurs caractères et comment sont gérés les langues écrivant de droite à gauche. Unicode gère ça.
- 2.13) Est-ce que Unicode c'est cool ? (Évidemment que ça l'est, lisez de suite mon article Unicode sur mon blog)

3) Image-Audio-Vidéo vers binaire

3.1)

J'ai un fichier mp4 qui dure environ 2h et pèse 484M

La fin de la vidéo est quasi statique (il n'y a quasi jamais de son et l'image ne change quasi pas)

Je coupe donc la fin de la vidéo, qui dure 1h.

La vidéo pèse maintenant 467M, comment expliquer que la taille n'est pas divisée par 2 ?

PS: Cet exo est vrai, le prof avait oublié de finir l'enregistrement de la séance du vendredi semaine 2 :D

3.2)

Trouvez plusieurs manières d'encoder l'image de taille 3x2 suivante :

rouge vert rouge

noir bleuciel noir

(Trouver des techniques qui marcheraient pour de plus grandes images et qui ne prendraient pas trop d'octets).

Regardez la définition d'un fichier .BMP sur internet, environ comment l'image précédente serait encodée en BMP ?

(pour les plus chevronés vous pouvez faire l'expérience et regarder le binaire du fichier)

3.3) Ouvrez un fichier PNG avec un éditeur de texte, que voyez-vous au début ?

Est-ce que PNG compresse l'image ?

Y-a-t-il de la perte de "qualité" ?

Quant à JPG ? Et GIF ?

Comment est encodé un GIF animé ?

4) HTML/XML/JSON/SVG/Latex

4.1)

Qu'est-ce qu'une balise html ? Donnez quelques exemples

Qu'est-ce qu'un attribut html ? Donnez quelques exemples

Depuis 2010 on parle beaucoup d'html5, quelles balises ont été introduites ? (Et pourquoi ça change la "face du web" ?)

4.2)

Écrire votre cv (ou n'importe quoi) en html, avec des titres, des paragraphes, des textes en gros ou italique. (Utilisez un tuto html ou celui de mon site ou les vidéos sur la chaîne yt de Val)

Placez des liens vers quelques sites web.

(utiliser css vous plongera dans le web des années 2000 et non le web des années 1990).

Mon cv est en html, trouvez-en la source html (Astuce: clic droit, Autre astuce: clic droit inspecter)

4.3)

"J'ai 2 chats gris et un chien labrador"

Décrire en xml, décrire en json (le format est libre à votre imagination :D)

4.4)

Donnez des exemples d'html qui ne sont pas du xml.

4.5)

"J'ai une pièce de ma maison de taille 20m², contenant deux pièces, de tailles 5m², 15m², 5m².

La dernière contient 2 pièces de 4 et 1 m²"

4.6)

Faites votre arbre généalogique en xml,

xml est pratique pour les structures en arbre

(et si votre arbre généalogique n'est pas un arbre, j'ai quelque chose à vous annoncer x))

4.7)

En SVG, créez une image avec un carré, un cercle, un pentagone (et des couleurs quand même).

Vous pouvez soit utiliser un logiciel texte (Comme Notepad++ sous windows) et lire un tuto SVG...

ou soit vous pouvez utiliser le logiciel Inkscape et ouvrir le fichier svg avec un logiciel texte (Comme Notepad++).

Petite note: Inkscape rajoute bcp de données (méta-données) au fichier, rajouter des données supplémentaires est un des avantages du XML (X stands for eXtensive).

Pour les courbes, le svg utilise des courbes de bézier, j'adore les courbes de bézier.

4.8)

Documentez vous sur le langage LaTeX,

pratique pour écrire de beaux syllabus (ou des mémoires) avec plein de formules mathématiques.

Essayez d'écrire quelques formules mathématiques connues comme le théorème de Pythagore ou l'intégrale de 3x

5) Cryptage, Hashage et Signatures (souvent nommé "chiffrage" en français)

5.1) Code César

Encrypter et décrypter Robert en code césar, choisissez une clé

Que feriez-vous pour encoder des phrase ? Avec de la ponctuation et des lettres accentuées ?

Comment craquer votre message codé ? (Depuis le message codé, obtenir le message original)

Vous pourriez aussi faire ça avec une table de vigenère où la clé est un mot.

5.2) DES

Même chose que l'exercice précédent, mais utilisant DES.

5.3) AES

AES est utilisé pour HTTPS,

documentez vous un peu dessus et lisez la petite bande dessinée dessus (comic) (une page).

5.4) Nombres premiers

Qu'est-ce qu'un nombre premier ? Un PGCD ? Un PPCM ?

Utilisez l'algorithme d'Euclide pour trouver le PGCD de deux grands nombres,

comme 456846123 et 432080850

En connaissant le pgcd, le ppcm est trouvable en une petite formule.

5.5) Facteurs premiers,

comment trouver les facteurs premiers des deux nombres précédents ?

Il faut vous dire que pour de vraiment grand nombres, ça prends beaucoup, beaucoup, de temps
Est-ce que ces nombres sont dit "premier entres eux ?" (Réponse partielle: Si leur pgcd vaut 1).

5.5) RSA

Générez une petite paire de clé en RSA avec des petites clés.

Encodez avec la clé publique un petit message (genre "yo") en RSA

Décryptez avec la clé privée ce message en RSA

Comment craquer ce message crypté ?

5.6) Encodage à courbe élliptique et ordinateur quantiques.

Ça existe.

5.5) Qu'est-ce qu'une fonction de hashage (comme md5, sha1, sha256, sha3)

5.6) J'ai un texte ascii de taille 6 ayant le md5 suivant : 4ffe35db90d94c6041fb8ddf7b44df29
quel était ce texte (pas facile) ?

Regardez sur mon twitter aux alentours du nouvel an, j'ai publié un md5,
c'est plus difficile de savoir ce que ça veut dire ^^

5.7) Créez deux fichiers différent ayant le même md5 (moyennement facile)

Créez deux fichiers différent ayant le même sha1 (vraiment difficile)

Créez deux fichiers différent ayant le même sha3 (impossible, ou alors gardez le pour vous :D)

En jouant sur la différence de présentation (par exemple html et son css { display: none }),

un attaquant peut faire croire que deux fichiers sont les mêmes alors que leurs bytes
sont différent. C'est un type d'attaque.

5.8) Les fonctions de hashage sont utilisées :

- pour vérifier que deux (gros) fichiers pas sur le même ordinateur sont exactement les mêmes
(vérifier la taille n'est pas une bonne manière :D)

(calculer le hash des deux côtés et vérifier que le hash est le même estd bien mieux ^^)

- les signatures électroniques

- les tables de hashage, très utile pour faire des dict ou des set en python par exemple.

J'ai un pdf, j'ai un lecteur de carte d'identité belge, j'aimerais le signer électroniquement ! Comment faire ?

J'ai un fichier signé par quelqu'un d'autre, comment vérifier la signaure (que c'est bien lui) ?

Je peux vous envoyer un fichier signé avec ma carte d'identité, ou est-ce une mauvaise idée ?

8) Est-ce que les graphes de la théorie des graphes c'est rigolo ?

8.1) Est-ce que les graphes de la théorie des graphes c'est rigolo ?