
Introduction à l'informatique

Julien Tesson

Université Paris-Est Créteil
UFR Droit

2015

Présentation

Julien Tesson

Maitre de conférence (Informatique)

Mail : `julien.tesson@u-pec.fr`

cours bientôt sur `http://tesson.julien.free.fr`

Bureau : Laboratoire LACL

C2I Niveau 1

- ▶ Possible en candidat libre
- ▶ Inscrivez-vous via **internet**
- ▶ Programme partiellement repris dans ce cours

C2I Niveau 2 - Métiers du droit

- ▶ Pas disponible à l'UPEC
- ▶ Si vous êtes intéressés, faites remonter l'information

-
- 1 Architecture
 - 2 Codage de l'information
 - 3 Algorithme - Programme
 - 4 Fichiers et format de documents
 - 5 Cryptographie
 - 6 Logiciel libre
 - 7 Réseaux Informatiques
 - 8 Sécurité

Plan

- ① Architecture
 - Description générale
 - Processeurs
 - Mémoires
- ② Codage de l'information
- ③ Algorithme - Programme
- ④ Fichiers et format de documents
- ⑤ Cryptographie
- ⑥ Logiciel libre
- ⑦ Réseaux Informatiques

Plan

- 1 Architecture
 - Description générale
 - Processeurs
 - Mémoires

Architecture - des formes diverses



De l'ordinateur de bureau

...

au smartphone

Architecture - des formes diverses



Architecture - Matériel (Hardware)

3 composants principaux

- ▶ Processeurs (CPU : Central processing unit)



calcul +
mémoire cache (très rapide, très chère)

- ▶ RAM : Mémoire vive



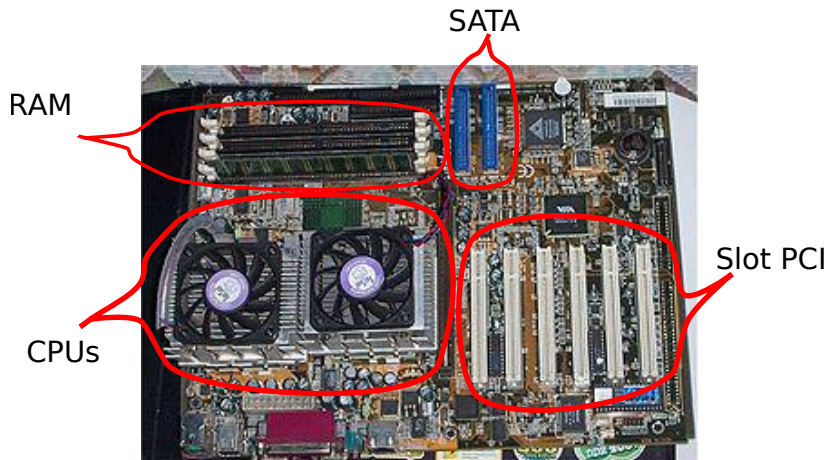
mémoire rapide, volatile

- ▶ HDD, SDD : Disque dur



mémoire lente, permanente

Architecture - support classique



Architecture

- ▶ Des périphériques : *écran, clavier, souris, imprimante, projecteur, lecteur de media amovibles ...*
- ▶ La connectique (ports, slots) interne (*pci-express, sata, ...*) ou externe
 - ▶ usb 1/2/3 : périphériques/stockage
 - ▶ e-sata : stockage (disques durs externe))
 - ▶ RJ45 *ethernet* : réseau
 - ▶ VGA, HDMI, DisplayPort

Attention aux numéros de versions (usb 1/2/3 , HDMI 1/2,...) et aux formes de connecteurs (usb A/B/micro/mini/...)



- ▶ Connexion sans fil : Wi-Fi (*réseau local, internet*), bluetooth (*périphériques, connexion courte distance*)

Plan

1 Architecture

Description générale

Processeurs

Mémoires

Le processeur (CPU)

- ▶ ensemble de transistors, organisés pour calculer
- ▶ Jeu d'instructions fixes
 - ▶ arithmétique
 - ▶ lecture/écriture (mémoires/périphériques),
 - ▶ choix d'instruction suivante
- ▶ synchronisés par une *horloge*
chaque instruction termine en un nombre prédéfini de *tics* d'horloge
- ▶ plusieurs opérations différentes possibles sur un même *tic* d'horloge

Mesures de puissance

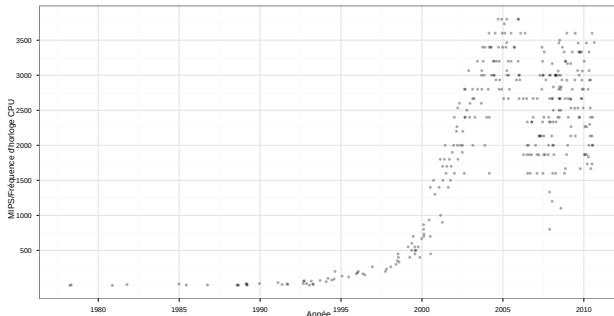
Préfixes multiplicateurs - Système international

Kilo (K) 10^3 , Méga (M) 10^6 , Giga (G) 10^9 , tera (T) 10^{12} , Péta (P) 10^{15} , Exa (Z) 10^{18}

Puissance de calcul

- ▶ Hz : Fréquence d'horloge du processeur
- ▶ Flops (Floating point Operation per Second) : nombre d'opération par seconde
- ▶ valeur usuelle 2015 : environ 3-4 GHz, 50-200 Gflops (4 cœurs, 10^{11} ops)
- ▶ super-calculateurs Top 5 mondial : 10 Peta-Flops (10^{15} ops)
- ▶ Cerveau humain estimé entre 10^{13} et 10^{19} ops

Évolution des processeurs - fréquences

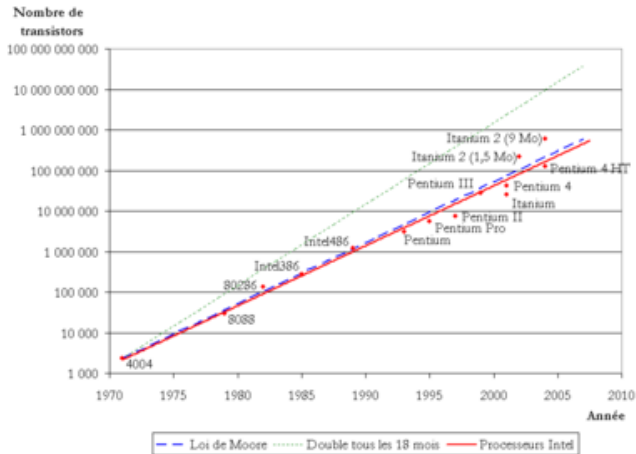


Accélération des circuits

Nombre de cycle de calcul en une seconde (fréquence d'horloge)

- ▶ doublé tous les 18 mois jusqu'en 2004
- ▶ puis problèmes de dissipation de la chaleur et de consommation

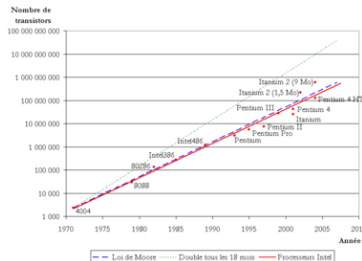
Évolution des processeurs - nombre de transistors



Loi de Moore (1975)

Tout les 2 ans, doublement du nombre de transistors dans un cpu.

Évolution des processeurs



Conséquence de la loi de Moore

- ▶ Processeurs plus complexes
- ▶ Multiplication du nombre d'opérations par cycle
- ▶ processeurs multi-cœurs

Prochaine limite : transistors de la taille d'un atome
Fait en laboratoire, d'ici 30 ans à l'échelle industrielle ?

Du GPU à l'accélérateur



GPU - Graphical Process Unit

- ▶ Carte graphique
- ▶ Matériel initialement dédié à l'affichage de scènes 3D
- ▶ Milliers d'unités de calcul simples
- ▶ Complexe à programmer

Plan

1 Architecture

Description générale

Processeurs

Mémoires

Mesure et caractéristiques

Unité de mémoire

Octet (fr) ou Byte (en)

Kilo (Ko) 10^3 , Méga (Mo) 10^6 , Giga (Go) 10^9 , téra (To) 10^{12} ,
Péta (Po) 10^{15} , Exa (Zo) 10^{18}

caractéristique

- ▶ vitesse de lecture/écriture (octets/seconde)
- ▶ volatile/persistante

Mémoire volatiles¹

Cache processeur

- ▶ Mémoire proche du processeur (sur la puce, donc très chère)
- ▶ très rapide, en fonction du niveau (L1, L2, L3)
- ▶ $L1 < 128 \text{ Ko/coeur}$
- ▶ $L2 < 1 \text{ Mo/coeur}$
- ▶ $L3 < 20 \text{ Mo}$ partagé

RAM - Random Access Memory

- ▶ Mémoire de travail de l'ordinateur
- ▶ Relativement rapide
- ▶ Volatile
- ▶ Actuellement de l'ordre de 4 à 16 Go
- ▶ Évolution suit la loi de Moore

1. Informations perdues à la mise hors-tension

Disque dur

- ▶ Support de sauvegarde, non-volatile
- ▶ Accès aux données lent
- ▶ Grande capacité de stockage, suit la loi de Moore

HDD - Hard drive Disc

SSD - Solide State Disc

Disque dur

HDD - Hard drive Disc

- ▶ plateau magnétisé en rotation
- ▶ plusieurs tête de lecture
- ▶ Actuellement de l'ordre de 500 Go - 1 To
- ▶ Durée de vie : 5-7 ans

SSD - Solide State Disc

Disque dur

HDD - Hard drive Disc

SSD - Solide State Disc

- ▶ Similaire aux cartes mémoire (flash/SD)
- ▶ Pas de parties mobile
- ▶ Lecture/écriture beaucoup plus rapide
- ▶ Nombre limité d'écritures possibles sur une cellule mémoire
- ▶ Actuellement de l'ordre de 128-256 Go
- ▶ Évolution suit la loi de Moore
- ▶ Durée de vie : ???

Plan

- 1 Architecture
- 2 Codage de l'information
 - Qu'est ce qu'un codage ?
 - Mesure d'une quantité d'information
 - Codage de texte
 - Codage d'images
 - Codage de sons
- 3 Algorithme - Programme
- 4 Fichiers et format de documents
- 5 Cryptographie
- 6 Logiciel libre

Codage de l'information

Comment des informations aussi diverses que du son, des images ou du textes peuvent-elles être manipulées par un ordinateur ?

Codage de l'information

Comment des informations aussi diverses que du son, des images ou du textes peuvent-elles être manipulées par un ordinateur ?

Un indice, on utilise le terme *numérique* pour parler de l'informatique

Plan

② Codage de l'information

Qu'est ce qu'un codage ?

Mesure d'une quantité d'information

Codage de texte

Codage d'images

Codage de sons

Codage de l'information

Definition (code)

Système de symboles permettant de représenter une information dans un domaine technique

Definition (codage)

Ce qui permet de passer d'une représentation de données à une autre.

Un codage est caractérisé par

- ▶ une liste de symboles
- ▶ une méthode d'interprétation

Attention : différent de chiffrement/cryptage !

Codage en informatique

En informatique

- ▶ codages binaires
- ▶ (deux symboles : 1, 0).
- ▶ Représentés dans le matériel par un état physique (transistor, surface magnétique, ...).

Plan

② Codage de l'information

- Qu'est ce qu'un codage ?

- Mesure d'une quantité d'information

- Codage de texte

- Codage d'images

- Codage de sons

Mesure de quantité d'information

- ▶ une unité d'information = un bit (2 valeurs possibles, 0/1).
- ▶ un groupe de 8 bits = un octet (256 valeurs possibles)
- ▶ 1000 o = 1 Kilo-octet
- ▶ 1000 Ko = 1 mega-octet, ...
- ▶ kilo (Ko), mega (Mo), giga(Go), tera(To), peta(Po)

Ne pas confondre : bit (b) et byte (B, nom anglais pour octet)

Quantité d'information - Ordre de grandeur

Ordre de grandeur (en 2012)

- ▶ Ko : registres d'un processeur, e-mail (1~50Ko)
- ▶ Mo : cache d'un processeur (1~5Mo), photo(1~10Mo), mp3 de 5 minutes(~5Mo), film compressé(~500Mo), CD (~700Mo)
- ▶ Go : RAM (2-32 Go), DVD(5Go), Blue-ray Disk(25Go), Clés USB (2-500Go), Disque durs SSD (64~ 500 Go)
- ▶ To : Disque durs standards (0,5~ 3To)

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

2

0

1

2

Codage binaire

2 symboles : 0,1

1

1

1

1

1

0

1

1

1

0

0

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

$$\begin{array}{ccccccc} & 2 & & 0 & & 1 & & 2 \\ = & 2000 & + & 0 & + & 10 & + & 2 \end{array}$$

Codage binaire

2 symboles : 0,1

1 1 1 1 1 0 1 1 1 0 0

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

$$\begin{array}{ccccccc} & 2 & & 0 & & 1 & & 2 \\ = & 2000 & + & 0 & + & 10 & + & 2 \\ = & 2 \times 10^3 & + & 0 \times 10^2 & + & 1 \times 10^1 & + & 2 \times 10^0 \end{array}$$

Codage binaire

2 symboles : 0,1

1 1 1 1 1 0 1 1 1 0 0

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

$$\begin{array}{ccccccc} & 2 & & 0 & & 1 & & 2 \\ = & 2000 & + & 0 & + & 10 & + & 2 \\ = & 2 \times 10^3 & + & 0 \times 10^2 & + & 1 \times 10^1 & + & 2 \times 10^0 \end{array}$$

Codage binaire

2 symboles : 0,1

$$\begin{array}{cccccccccccc} = & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ & 2^{10} & 2^9 & 2^8 & 2^7 & 2^6 & 0 \times 2^5 & 2^4 & 2^3 & 2^2 & 0 \times 2^1 & 0 \times 2^0 \end{array}$$

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

$$\begin{array}{ccccccc} & 2 & & 0 & & 1 & & 2 \\ = & 2000 & + & 0 & + & 10 & + & 2 \\ = & 2 \times 10^3 & + & 0 \times 10^2 & + & 1 \times 10^1 & + & 2 \times 10^0 \end{array}$$

Codage binaire

2 symboles : 0,1

$$\begin{array}{cccccccccccc} & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ = & 2^{10} & 2^9 & 2^8 & 2^7 & 2^6 & 0 \times 2^5 & 2^4 & 2^3 & 2^2 & 0 \times 2^1 & 0 \times 2^0 \\ = & 1024 & 512 & 256 & 128 & 64 & 0 \times 32 & 16 & 8 & 4 & 0 \times 2 & 0 \times 1 \end{array}$$

Codage des nombres

Codage alphabétique

42 symboles dans l'alphabet français

deux mille douze

Codage décimal positionnel

10 symboles : 0,1,2,3,4,5,6,7,8,9

$$\begin{array}{ccccccc} & 2 & & 0 & & 1 & & 2 \\ = & 2000 & + & 0 & + & 10 & + & 2 \\ = & 2 \times 10^3 & + & 0 \times 10^2 & + & 1 \times 10^1 & + & 2 \times 10^0 \end{array}$$

Codage binaire

2 symboles : 0,1

$$\begin{array}{cccccccccccc} & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ = & 2^{10} & 2^9 & 2^8 & 2^7 & 2^6 & 0 \times 2^5 & 2^4 & 2^3 & 2^2 & 0 \times 2^1 & 0 \times 2^0 \\ = & 1024 & 512 & 256 & 128 & 64 & 0 \times 32 & 16 & 8 & 4 & 0 \times 2 & 0 \times 1 \\ = & 2012 & & & & & & & & & & \end{array}$$

Plan

2 Codage de l'information

Qu'est ce qu'un codage ?

Mesure d'une quantité d'information

Codage de texte

Codage d'images

Codage de sons

Codage - Exemples

ASCII - American Standard Code for Information Interchange

1 caractères = 7 bits :

'a' = 000 1101 (61)

'b' = 000 1110 (62)

'c' = 000 1111 (63)

'd' = 001 0000 (64)

⋮

Unicode

- ▶ 8 bits, 16 bits, 32 bits
- ▶ Beaucoup plus de caractères (caractères accentués, sinogrammes, arabe, cyrillic, ...)
Σ, Γ

Plan

2 Codage de l'information

- Qu'est ce qu'un codage ?

- Mesure d'une quantité d'information

- Codage de texte

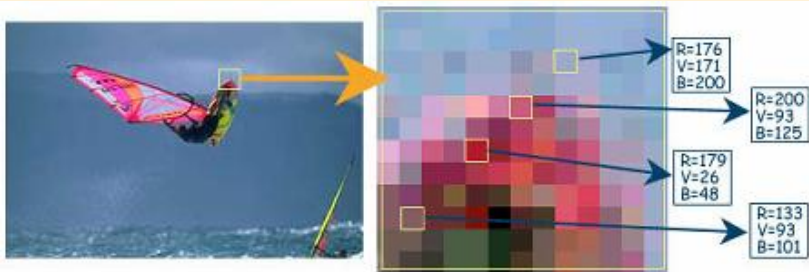
- Codage d'images

- Codage de sons

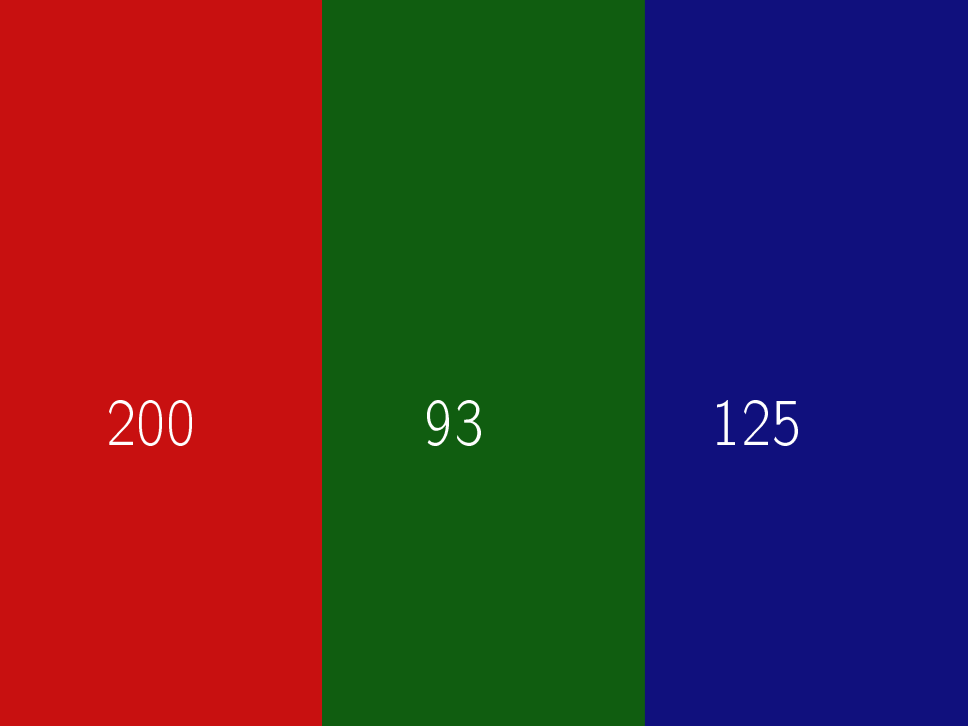
Codage - Exemples

Image

1 pixel = 3 valeurs (Rouge Vert Bleu) = 3×1 octet



176 171 200 → 1011 0000 1010 1011 1100 1000

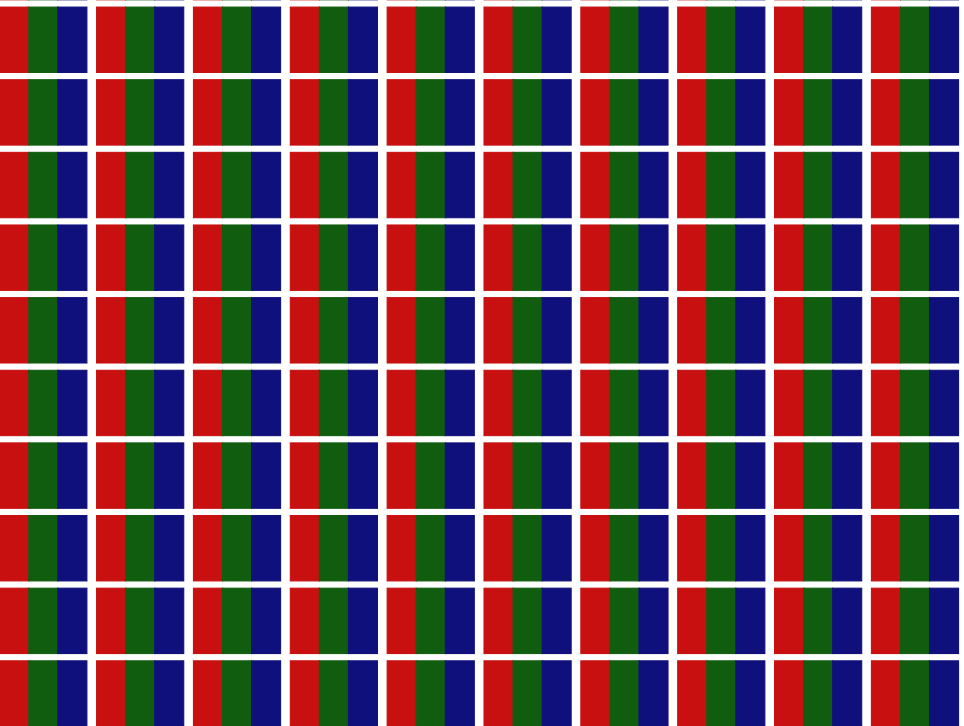


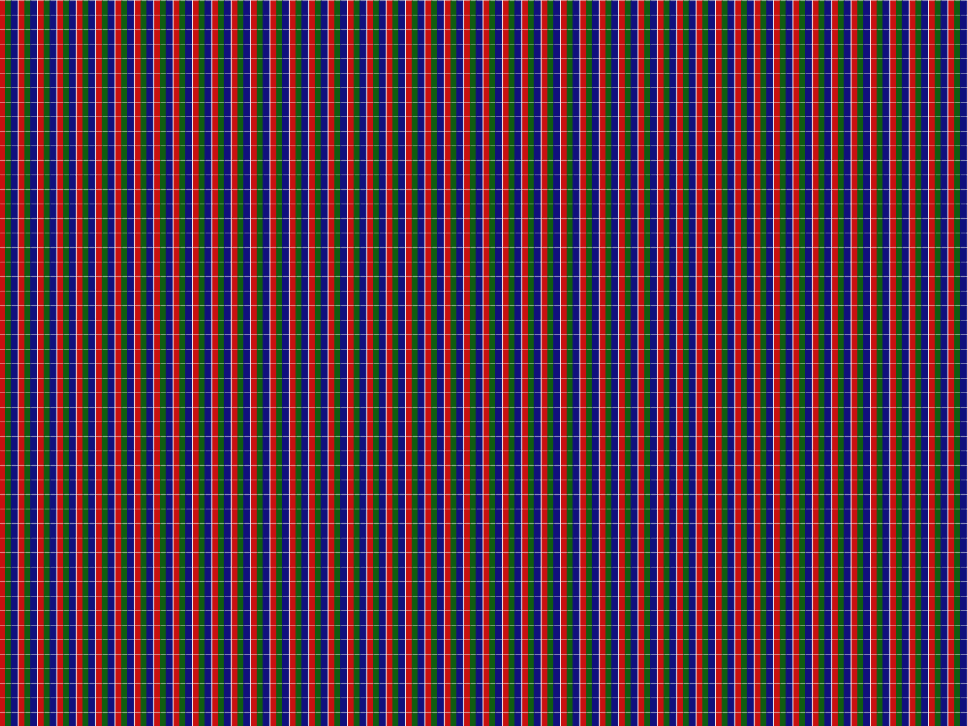
200

93

125







176

171

200

Plan

2 Codage de l'information

- Qu'est ce qu'un codage ?

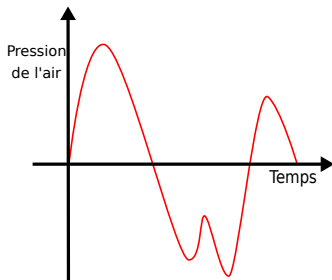
- Mesure d'une quantité d'information

- Codage de texte

- Codage d'images

- Codage de sons

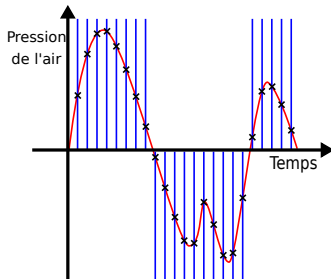
Codage - Son



Signal sonore

Variation de la pression de l'air, capturée par le micro

Codage - Son

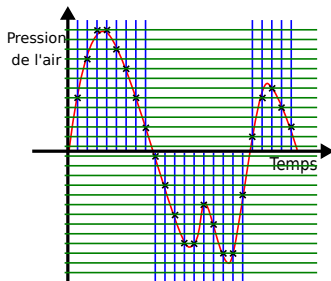


Échantillonnage temporel

Numérisation^a de la hauteur de la courbe à intervalles de temps réguliers

a. Enregistrement sous forme de nombre dans un codage binaire

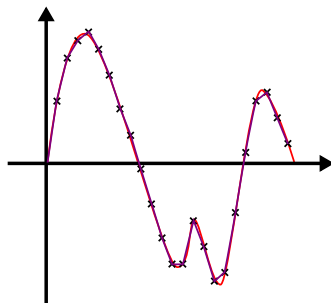
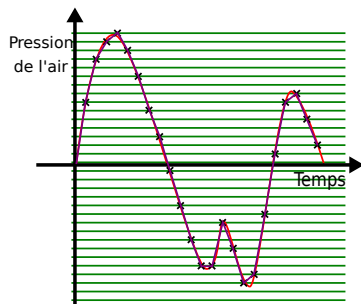
Codage - Son



Résolution des échantillons

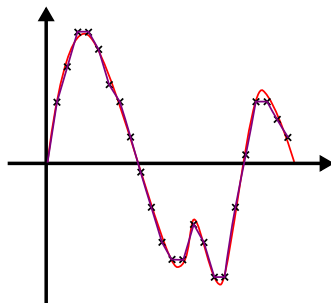
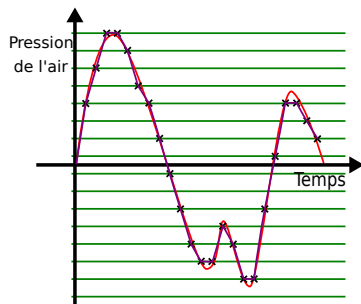
Le nombre de bits utilisés pour coder la hauteur de la courbe en chaque point (limite la précision des échantillons)

Codage - résolution



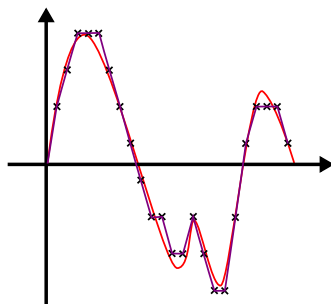
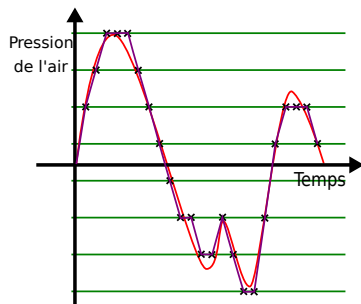
Courbe obtenue avec une résolution de 5 bits

Codage - résolution



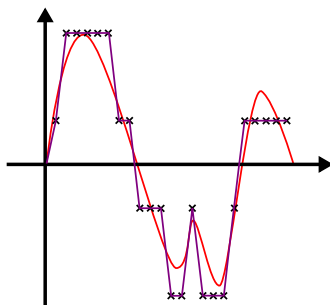
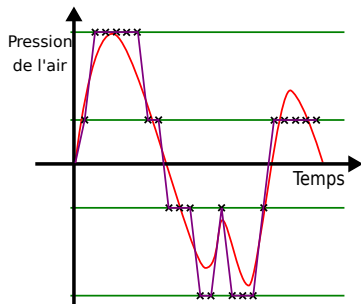
Courbe obtenue avec une résolution de 4 bits

Codage - résolution



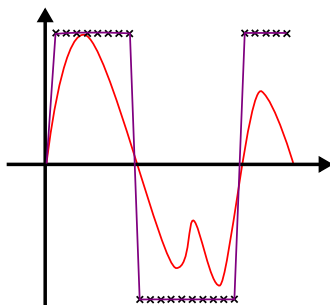
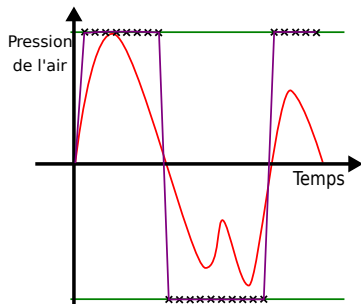
Courbe obtenue avec une résolution de 3 bits

Codage - résolution



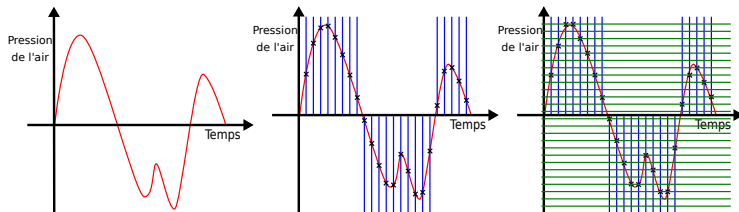
Courbe obtenue avec une résolution de 2 bits

Codage - résolution



Courbe obtenue avec une résolution de 1 bits

Codage son



Échantillonnage

La **précision** (donc la qualité du son) dépend de :

- ▶ Fréquence d'échantillonnage (nombre de points par secondes)
- ▶ Nombre de bits utilisés pour coder chaque échantillon

Donc de la **quantité d'informations** (bits) enregistrées

Plan

- 1 Architecture
- 2 Codage de l'information
- 3 **Algorithme - Programme**
 - Aux origines du logiciel
 - Algorithme
 - Programme
 - Cycle de vie d'un logiciel
 - Système d'exploitation
- 4 Fichiers et format de documents
- 5 Cryptographie
- 6 Logiciel libre

Plan

- ③ Algorithme - Programme
 - Aux origines du logiciel
 - Algorithme
 - Programme
 - Cycle de vie d'un logiciel
 - Système d'exploitation

D'Al-Khawarizmi au Logiciel

Algorithme - origine

Nom dérivé de celui du mathématicien, géographe, astrologue et astronome perse Al-Khawarizmi (~ 783-850) auteur de kitabu 'l-mukhtasar fi hisabi 'l-jabr wa'l-muqabalah

(كتاب المختصر في حساب الجبر والمقابلة)

- ▶ Popularisation du système décimal positionel (chiffre arabes)
- ▶ Recensement et formalisation de nombreuses méthodes de calcul
- ▶ Un des fondateurs de l'algèbre (discipline systématisant les méthodes de résolution de problèmes mathématiques)

Algorithme - définition

Programme

Logiciel

D'Al-Khawarizmi au Logiciel

Algorithme - origine

Algorithme - définition

Suite d'instructions non-ambiguë, exécutables *mécaniquement*, visant à résoudre un problème.

Programme

Logiciel

D'Al-Khawarizmi au Logiciel

Algorithme - origine

Algorithme - définition

Programme

Suite d'instructions s'exécutant sur un ordinateur.

Logiciel

D'Al-Khawarizmi au Logiciel

Algorithme - origine

Algorithme - définition

Programme

Logiciel

Dérivé du mot logique, le suffixe met en opposition le logiciel au matériel.

Il s'agit d'un ou plusieurs programmes et fichiers permettant d'utiliser le matériel. Sur les architectures modernes, on distingue deux types de logiciels :

- ▶ Le système d'exploitation
- ▶ Les applications

Plan

③ Algorithme - Programme

Aux origines du logiciel

Algorithme

Programme

Cycle de vie d'un logiciel

Système d'exploitation

Algorithme

recette de cuisine - pb : tarte au pommes

- ▶ Déroulez votre pâte dans votre moule.
- ▶ Percez-la avec une fourchette.
- ▶ Faites préchauffer le four thermostat 6/7.
- ▶ Lavez les pommes, épluchez-les, coupez-les en fine tranches.
- ▶ disposez-les en les chevauchant.
- ▶ Répartissez le sucre vanillé sur toute la surface.
- ▶ Enfournez la tarte à mi-hauteur.
- ▶ Laissez cuire 30 minutes.

Plan

③ Algorithme - Programme

Aux origines du logiciel

Algorithme

Programme

Cycle de vie d'un logiciel

Système d'exploitation

Programme

Definition

Algorithme conçu pour s'exécuter sur un ordinateur.

- ▶ Définit dans un langage de programmation par le programmeur (programme source / code source)
- ▶ Transformé en programme exécutable par un compilateur (programme exécutable)

Exemples

- ▶ Gestionnaire de fenêtres, drivers, BIOS
- ▶ Calculatrice, Démineur, Traitement de texte

Plan

③ Algorithme - Programme

Aux origines du logiciel

Algorithme

Programme

Cycle de vie d'un logiciel

Système d'exploitation

Cycle de vie d'un logiciel

Analyse

Recueil des besoins auprès des utilisateurs, définition du problème à résoudre

conception

programmation

Mise en production, Maintenance

Cycle de vie d'un logiciel

Analyse

conception

Choix des algorithmes, des fonctionnalités

programmation

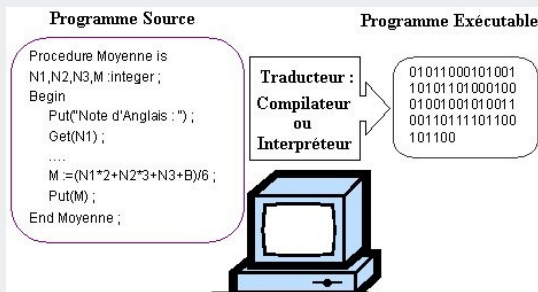
Mise en production, Maintenance

Cycle de vie d'un logiciel

Analyse

conception

programmation



Mise en production, Maintenance

Cycle de vie d'un logiciel

Analyse

conception

programmation

Mise en production, Maintenance

Tests, correction d'erreurs, ajout de fonctionnalités.

Nécessite l'accès au code source.

Plan

③ Algorithme - Programme

Aux origines du logiciel

Algorithme

Programme

Cycle de vie d'un logiciel

Système d'exploitation

Système d'exploitation

Système d'exploitation(Operating system, OS)

Ensemble de programmes assurant la liaison entre les ressources matérielles, l'utilisateur et les applications.

Tâches dévolues aux SE

- ▶ Accès mémoires
- ▶ Gestion des droits d'accès
- ▶ Répartition des ressources entre les programmes (temps processeur, quantité de mémoire, accès au réseau)
- ▶ Accueil de l'utilisateur au démarrage de la machine

Système d'exploitation

Exemples

- ▶ Windows (Microsoft)
- ▶ GNU/Linux
- ▶ GNU/BSD
- ▶ Mac OS (Apple)

Plan

- 1 Architecture
- 2 Codage de l'information
- 3 Algorithme - Programme
- 4 Fichiers et format de documents
Formats de fichiers & compression
- 5 Cryptographie
- 6 Logiciel libre
- 7 Réseaux Informatiques
- 8 Sécurité

Système de fichiers

Definition (fichier)

Suite d'informations physiquement stockées sur un support.

Point de vue utilisateur

Ensemble d'informations, exploitable à l'aide d'un logiciel adapté, identifié par un chemin, un nom et une extension

- ▶ chemin : suite de noms de répertoires
- ▶ extension : caractérise le format des données du fichier

Système de fichiers

Definition (fichier)

Point de vue utilisateur

Ensemble d'informations, exploitable à l'aide d'un logiciel adapté, identifié par un chemin, un nom et une extension

- ▶ chemin : suite de noms de répertoires
- ▶ extension : caractérise le format des données du fichier

Chemin vers un fichier dans le système

- ▶ sous windows
`c:\Users\julien\Documents\cours\initiation_info.pdf`
- ▶ sous mac
`/Users/julien/Documents/cours/initiation_info.pdf`
- ▶ sous linux
`/home/julien/Documents/cours/initiation_info.pdf`

Système de fichiers

Definition (fichier)

Suite d'informations physiquement stockées sur un support.

Point de vue utilisateur

Ensemble d'informations, exploitable à l'aide d'un logiciel adapté, identifié par un chemin, un nom et une extension

- ▶ chemin : suite de noms de répertoires
- ▶ extension : caractérise le format des données du fichier

Definition (Système de fichiers - file system)

Organise les données sur un support physique et les met en relation avec un ensemble d'entités logiques

Système de fichiers

Partitions

Un même support physique (disque dur) peut être divisé en plusieurs disques logiques (partitions).

- ▶ Co-existence de plusieurs OS
- ▶ Possibilité de séparer fichiers utilisateur/données système

Recommandation pour le nommage de fichier

Afin d'assurer la *portabilité* des répertoires et des fichiers d'un système à l'autre, quelques recommandations sur leur noms :

- ▶ pas d'accents
- ▶ pas de caractère tels que '\ " | { } [] () % \$ & @ # > <
- ▶ pas d'espace, utilisez _

Plan

- ④ Fichiers et format de documents
 - Formats de fichiers & compression

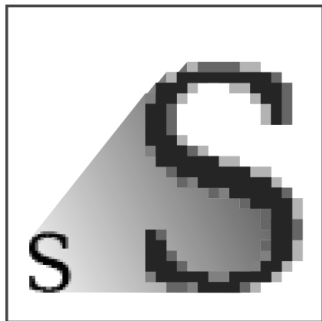
Formats de fichiers

Definition

Le format de fichier spécifie comment l'information est codée et organisée dans le fichier.

L'extension du fichier est utilisée pour spécifier le format, elle aide le système à décider quelle application utiliser pour ouvrir un fichier.

Exemples de formats de fichiers - image



Matriciel
.jpeg .gif .png

tableau de pixels



Vectoriel
.svg

composition de formes géométriques

Formats de fichiers - compression

formats de fichiers compressés

- ▶ Réorganisation des données pour minimiser la mémoire utilisée.
- ▶ Décompression nécessaire pour lire le fichier.
- ▶ Gain de place, perte de temps (temps de décompression).

Avec ou sans perte

Deux type de compression :

sans perte les informations sont simplement réorganisées de façon à prendre moins de place

avec perte On oublie quelques informations jugées non-nécessaire

Le format JPEG est un format **compressé avec perte**, le taux de compression peut être réglé :

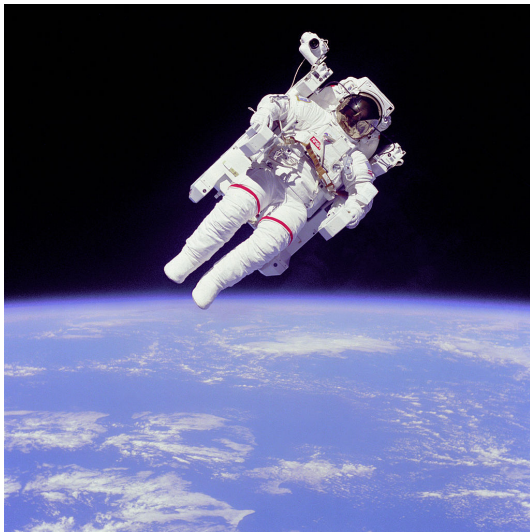


image faiblement compressée

Le format JPEG est un format **compressé avec perte**, le taux de compression peut être réglé :

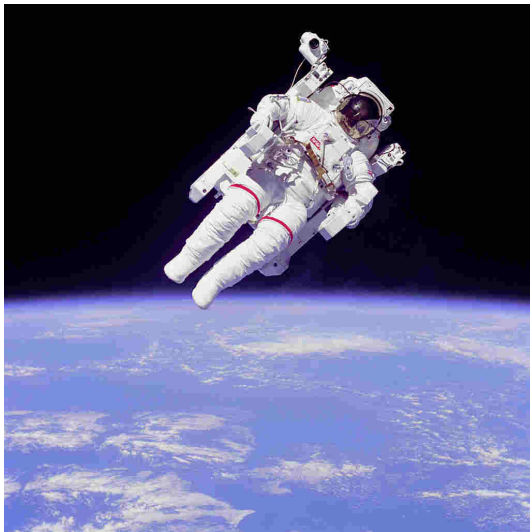


image compressée, apparition d'aplat de couleurs

Le format JPEG est un format **compressé avec perte**, le taux de compression peut être réglé :

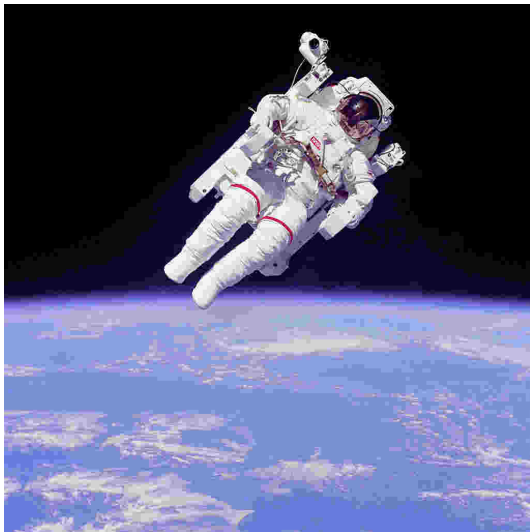


image plus compressée, aplat de couleurs et perte de détails

Le format JPEG est un format **compressé avec perte**, le taux de compression peut être réglé :

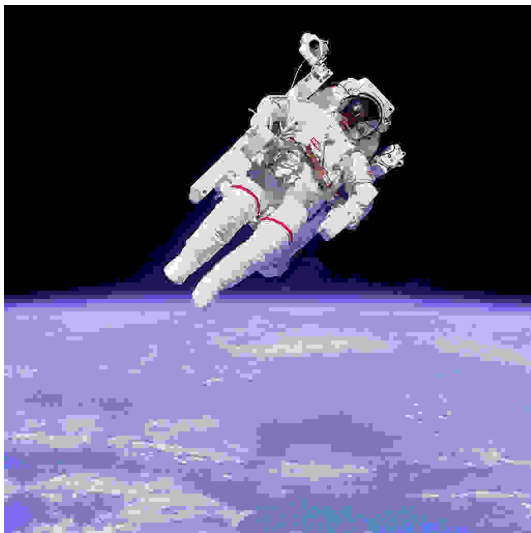


image très fortement compressée

Son - compression

Le format MP3 est un format audio **compressé avec perte**.
le taux de compression peut être réglé ; plus la compression est importante plus la *qualité* du son est dégradé.

Le format FLAC est un format audio **compressé sans perte**.

Taille d'un fichier audio de 3 minute 30	
MP3 ou Ogg vorbis, qualité correcte	FLAC
3,5 Mo	16 Mo

Autres formats de Documents I

Texte

.txt	texte brute sans mise en forme
.rtf	(rich text format) texte avec mise en forme
.doc	document texte Microsoft Word
.docx	document texte Microsoft Word, format ouvert
.odt	document texte LibreOffice/OpenOffice
.htm .html	page web au format HTML (HyperText Markup Language)
:	

Autres formats de Documents II

Tableurs

.xls	Microsoft Excel
.xlsx	Microsoft Excel, format ouvert
.ods	LibreOffice/OpenOffice
⋮	

Présentation

.ppt	Microsoft Power point
.odp	LibreOffice/OpenOffice
⋮	

Autres formats de Documents III

Formats de fichier LibreOffice : Open Document Text (odt); Open Document Spreadsheet (ods); Open Document Présentation (odp); ...

Dans les fichiers

ouvrons quelques fichiers ...

Plan

- 1 Architecture
- 2 Codage de l'information
- 3 Algorithme - Programme
- 4 Fichiers et format de documents
- 5 Cryptographie
 - Définition et principes généraux
 - contexte
 - Cryptographie symétrique
 - Cryptographie asymétrique
 - En pratique
- 6 Logiciel libre

Cryptographie

Plan

5 Cryptographie

- Définition et principes généraux

- contexte

- Cryptographie symétrique

- Cryptographie asymétrique

- En pratique

Définition

Cryptographie

La **cryptographie** s'attache à protéger des messages (assurant confidentialité, authenticité et intégrité) en rendant un message inintelligible à tout autre que ses destinataires.

Ne pas confondre avec la stéganographie

Cryptanalyse

La **cryptanalyse** est la science qui consiste à tenter de déchiffrer un message sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé **décryptage** (ou cassage, attaque).

Principe de Kerckhoffs

Principe

Le procédé de cryptographie doit pouvoir tomber entre les mains de l'ennemi.

Autrement dit, seul la clef protège le message, l'algorithme de chiffrement peut être public.

Analogie

Lorsque j'utilise une serrure pour fermer un coffre, peu m'importe que l'on sache comment fonctionne le mécanisme. L'important, c'est qu'on ne puisse pas l'ouvrir sans la clef.

Plan

5 Cryptographie

- Définition et principes généraux

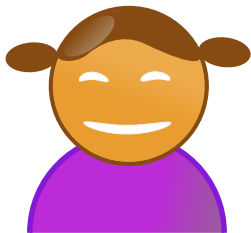
- contexte

- Cryptographie symétrique

- Cryptographie asymétrique

- En pratique

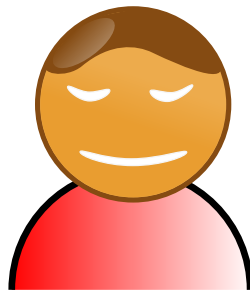
Les acteurs



Alice



Bob



Charlie

Les autres éléments

Message clair

Suite d'informations intelligibles pour un humain ou interprétables par un logiciel.

Message chiffré

Suite d'informations chiffrée, inintelligibles pour un humain et non-interprétables par un logiciel.

Algorithme de chiffrement/déchiffrement

Méthode permettant de passer du message clair au message chiffré (et inversement) à l'aide d'une clef

Clef

Information, représentée par une suite de bit, permettant de chiffrer ou déchiffrer un message.

Propriétés recherchées

Intégrité

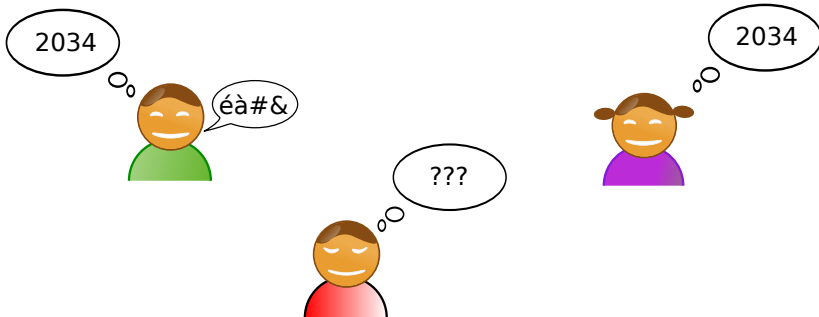
L'intégrité est l'assurance que les informations transmises ne subissent aucune altération volontaire ou accidentelle.



Propriétés recherchées

Confidentialité

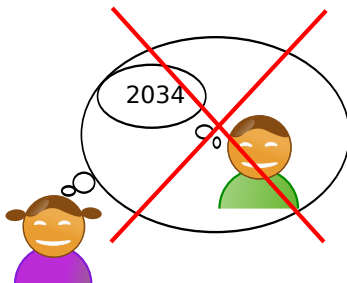
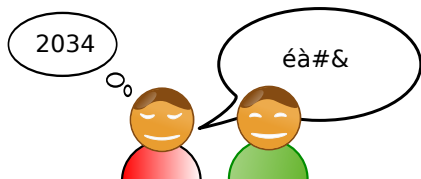
La confidentialité est le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé.



Propriétés recherchées

Authenticité

L'authentification est la procédure qui consiste, en informatique, à vérifier l'identité d'une entité.



Plan

5 Cryptographie

- Définition et principes généraux
- contexte

- Cryptographie symétrique

- Cryptographie asymétrique

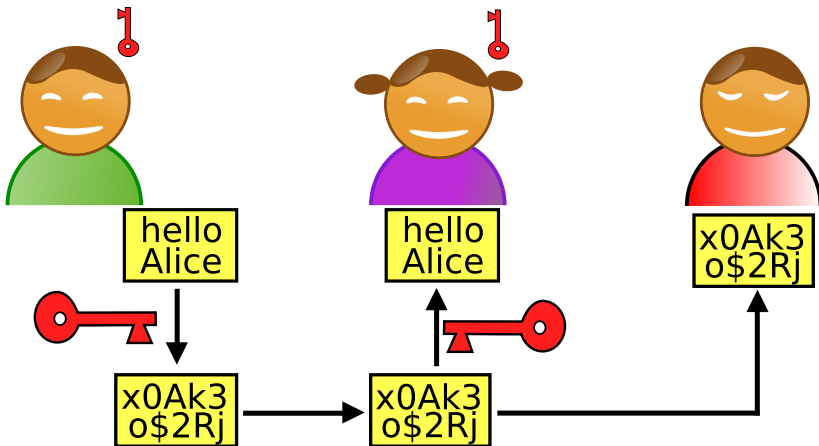
- En pratique

Cryptographie Symétrique

Définition

Une seule clé pour chiffrer et déchiffrer le message.

La clé est un secret partagé par Alice et Bob.



Cryptographie Symétrique

Définition

Une seule clé pour chiffrer et déchiffrer le message.

Analogie

Un coffre, plusieurs copies de la clef. Toute personne possédant une copie de la clef peut voir ce qu'il y a dans le coffre.

Inconvénients

Pour partager la clé, Alice et Bob doivent se rencontrer avant l'échange chiffré.

Plan

5 Cryptographie

Définition et principes généraux
contexte

Cryptographie symétrique

Cryptographie asymétrique

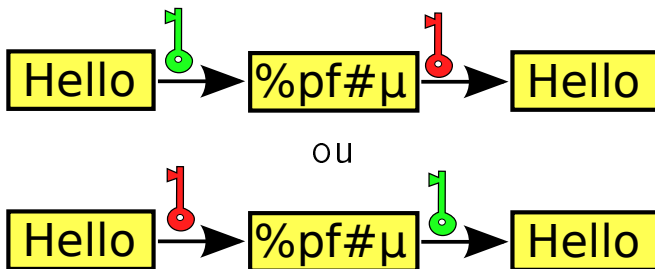
En pratique

Cryptographie Asymétrique

Cryptographie asymétrique (cryptographie à clé publique)

Méthode de chiffrement reposant sur l'utilisation de deux clefs, l'une permettant de chiffrer le message et l'autre de le déchiffrer.

Une clef sera publique  (diffusée) et l'autre privée  (gardée secrète).



Cryptographie Asymétrique

Cryptographie asymétrique (cryptographie à clé publique)

Méthode de chiffrement reposant sur l'utilisation de deux clefs, l'une permettant de chiffrer le message et l'autre de le déchiffrer.

Une clef sera publique  (diffusée) et l'autre privée  (gardée secrète).

Analogie

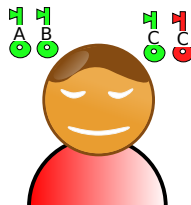
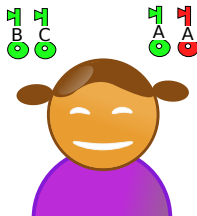
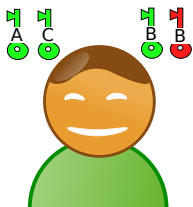
Coffre avec trappe anti-retour, je met le message dans le coffre par la trappe (chiffrement avec une première clef), mais j'ai besoin de la clef du coffre pour obtenir le message (déchiffrement avec une seconde clef)

Cryptographie Asymétrique

Cryptographie asymétrique (cryptographie à clé publique)

Méthode de chiffrement reposant sur l'utilisation de deux clefs, l'une permettant de chiffrer le message et l'autre de le déchiffrer.

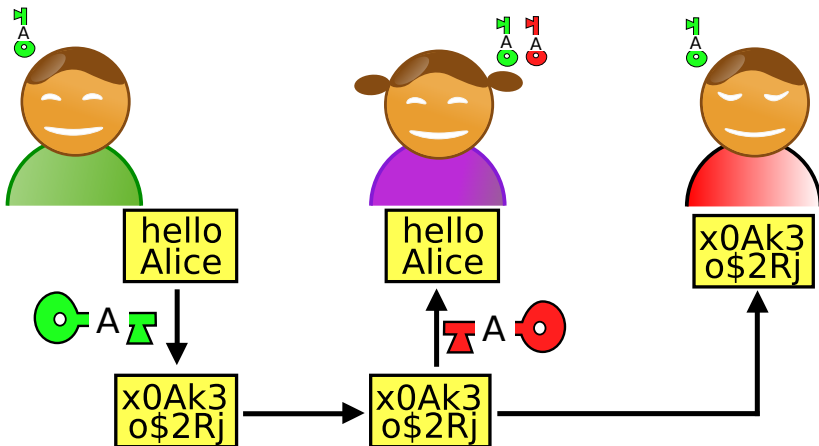
Une clef sera publique  (diffusée) et l'autre privée  (gardée secrète).



Cryptographie Asymétrique

Confidentialité

Chiffrement avec la clé publique, déchiffrement avec la clé privée



Cryptographie Asymétrique

Confidentialité

Chiffrement avec la clé publique, déchiffrement avec la clé privée

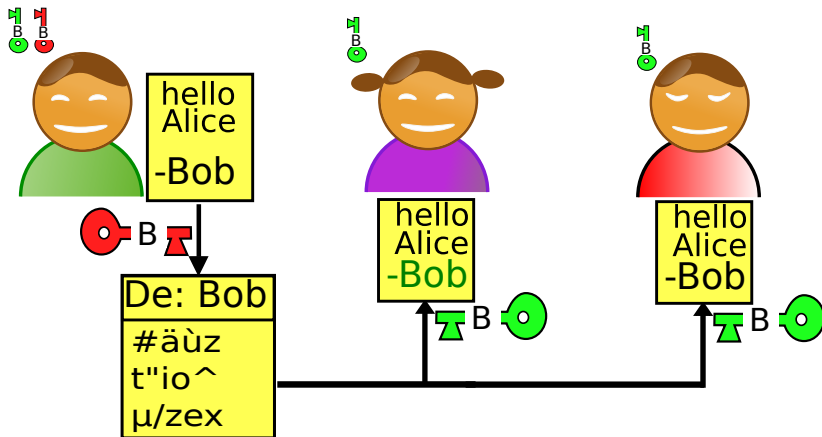
Analogie

Coffre avec trappe anti-retour disponible publiquement, tout le monde peut mettre des messages, seul le destinataire peut l'ouvrir.

Cryptographie Asymétrique

Authentification et intégrité

Chiffrement avec la clé privée, déchiffrement avec la clé publique



Cryptographie Asymétrique

Authentification et intégrité

Chiffrement avec la clé privée, déchiffrement avec la clé publique

Analogie

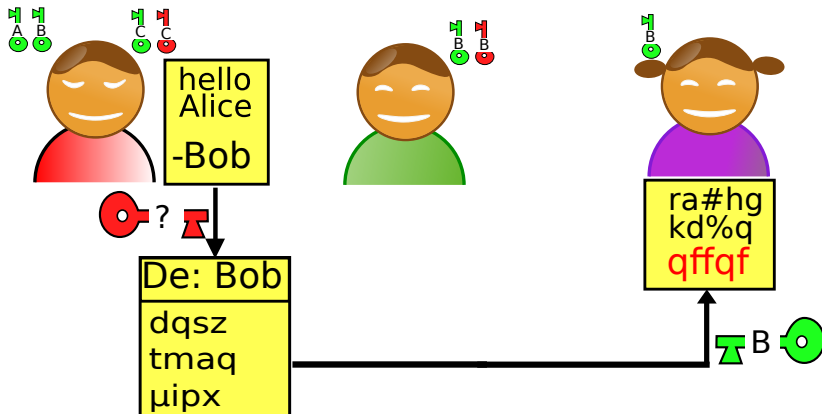
Panneau d'affichage public fermé à l'aide d'une clef : seul le processeur de la clef peut y mettre des messages (utilisation de la clef privée), la présence du message dans le panneau (déchiffrement du message par la clef publique) assure l'identité de l'émetteur.

Cryptographie Asymétrique

Authentification et intégrité

Chiffrement avec la clé privée, déchiffrement avec la clé publique

Charlie ne peut plus se faire passer pour Bob, il n'a pas la clef pour mettre le message dans le panneau.



Plan

5 Cryptographie

- Définition et principes généraux
- contexte

- Cryptographie symétrique

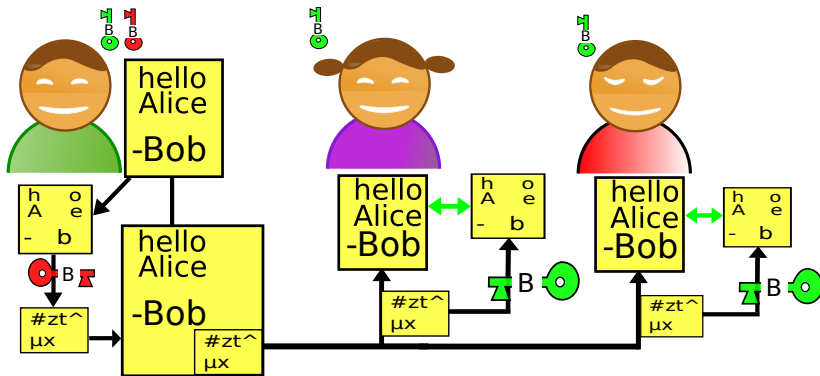
- Cryptographie asymétrique

- En pratique

Cryptographie Asymétrique

Authentification et intégrité avec message en clair
(fonctionnement usuel)

Chiffrement d'un condensat du message avec la clé privée,
déchiffrement avec la clé publique



Cryptographie Asymétrique

Inconvénients

Nécessite plus de ressource de calcul que le chiffrement symétrique

Standards de chiffrement

Symétrique

Taille de clés minimum pour un chiffrement sûr : 100 bits

- ▶ *DES (Data Encryption Standard)*, triple DES (obsolètes)
- ▶ **AES** (Advanced Encryption Standard) 128, 192 ou 256 bits

Asymétrique

- ▶ **RSA** (Rivest Shamir Adleman), **DSA**
- ▶ Taille de clés minimum pour un chiffrement sûr : **2048** bits
- ▶ Utilisé pour l'établissement de connections sécurisées entre machines (https,ssh,...)

Limites légale

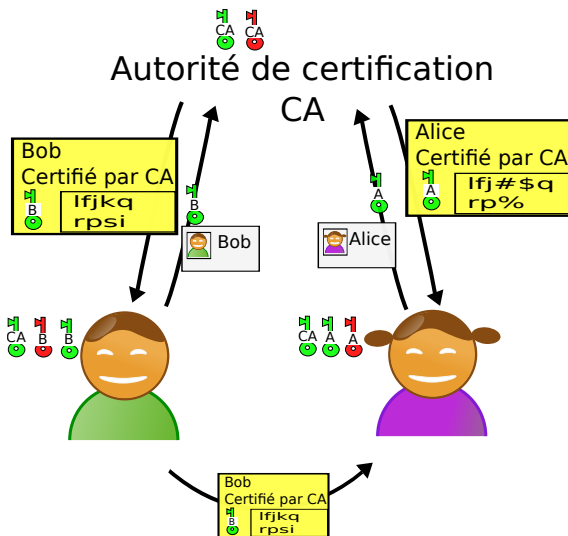
- ▶ **Usage libre** depuis 2004 (avant 2004, arme de catégorie 2).
- ▶ Exportation d'outils de cryptographie contrôlée

Infrastructure à clefs publique (PKI)

Objectif

Construire une infrastructure de confiance pour obtenir une clef publique.

Infrastructure à clefs publique (PKI)



PGP - OpenPGP - GPG

Pretty good Privacy

But : Permettre à tous de protéger sa vie privée

Concepteur : Phil Zimmermann

Fonctionnement

Logiciel pour générer les clefs, chiffrer/déchiffrer des données, mettre en ligne les clefs publiques, obtenir des clefs publique en ligne.

GPG : version Logiciel Libre (Gnu Privacy Guard)

Intégration

- ▶ Logiciel seul (GPA - Gnu Privacy Assistant)
- ▶ Logiciel de messagerie (extension Enigmail dans thunderbird)

GPG

DEMO

Plan

- 1 Architecture
- 2 Codage de l'information
- 3 Algorithme - Programme
- 4 Fichiers et format de documents
- 5 Cryptographie
- 6 Logiciel libre**
- 7 Réseaux Informatiques
- 8 Sécurité

Logiciel - Droit d'auteur

Les logiciels sont soumis au droit d'auteur

- ▶ Droit moral : reconnaissance de la paternité, respect de l'intégrité
- ▶ Droit patrimonial : monopole d'exploitation économique pour une durée variable

Licence d'utilisation

Restreint les usages possibles d'une copie d'un logiciel. Elle peut limiter par exemple :

- ▶ le nombre d'utilisateurs simultanés
- ▶ le nombre de machines sur lesquels il peut être installé/utilisé
- ▶ la modification, la copie et la redistribution

Logiciel libre

Logiciel libre - Licence assurant 4 libertés

- ▶ Liberté d'utiliser

Logiciel libre

Logiciel libre - Licence assurant 4 libertés

- ▶ Liberté d'**utiliser**
- ▶ Liberté d'**étudier**

Logiciel libre

Logiciel libre - Licence assurant 4 libertés

- ▶ Liberté d'**utiliser**
- ▶ Liberté d'**étudier**
- ▶ Liberté de **modifier**

Logiciel libre

Logiciel libre - Licence assurant 4 libertés

- ▶ Liberté d'utiliser
- ▶ Liberté d'étudier
- ▶ Liberté de modifier
- ▶ Liberté de diffuser

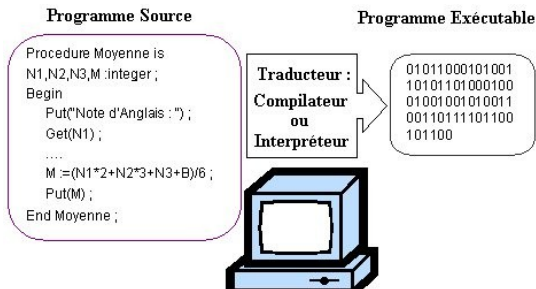
Logiciel libre

4 libertés

- ▶ Liberté d'utiliser
- ▶ Liberté d'étudier
- ▶ Liberté de modifier
- ▶ Liberté de diffuser

Accès au Code source

Nécessité d'accéder au code source



	Libre			
Utiliser	Oui			
Étudier	Oui			
Modifier	Oui			
Diffuser	Oui			

	Libre	Freeware Gratuitiel		
Utiliser	Oui	Oui		
Étudier	Oui	Non		
Modifier	Oui	Non		
Diffuser	Oui	Limitée		

	Libre	Freeware Gratuiciel	shareware partagiciel	
Utiliser	Oui	Oui	Limitée	
Étudier	Oui	Non	Non	
Modifier	Oui	Non	Non	
Diffuser	Oui	Limitée	Limitée	

	Libre	Freeware Gratuiciel	shareware partagiciel	Propriétaire
Utiliser	Oui	Oui	Limitée	Limitée
Étudier	Oui	Non	Non	Non
Modifier	Oui	Non	Non	Non
Diffuser	Oui	Limitée	Limitée	Non

CopyLeft

Définition

Le copyleft est l'autorisation donnée par l'auteur d'un travail soumis au droit d'auteur (œuvre d'art, texte, programme informatique ou autre) d'utiliser, d'étudier, de modifier et de copier son œuvre, **dans la mesure où cette autorisation reste préservée.**



Licences libres → Obligations

Toujours citer l'auteur, parfois diffuser à nouveau sous licence libre

Licences libres

Licence	Obligations
GPL, CeCILL	Diffuser toute modification ou réutilisation du code sous la même licence (licences virales)
LGPL, CeCILL-C	Diffuser toute modification sous la même licence
BSD, CeCILL-B	Ré-utilisable dans n'importe quel contexte, seule la citation des auteurs est obligatoire

Et l'utilisateur ?

- ▶ Pérennité
- ▶ Qualité/Extensibilité
- ▶ Sécurité

Pérennité

Non-dépendance à l'éditeur logiciel

- Possibilité de *Fork* (séparation d'un logiciel en deux versions évoluant séparément)



- Choix systèmes d'exploitation
- Format de fichier ouverts (possibilité de les utiliser dans d'autres logiciels)

Assurée uniquement si le nombre d'utilisateur est important

Qualité/Extensibilité

Code source accessible et modifiable par de très nombreux programmeurs :

- ▶ Corrections de bugs
- ▶ Ajouts de nouvelles fonctionnalités

Qui peuvent être mis à la disposition des utilisateurs rapidement

N'importe qui peut contribuer à la traduction du logiciel

Code source accessible par de très nombreux programmeurs :

- ▶ Possibilité de détecter des bugs
- ▶ Possibilité de détecter des comportement malveillants/inappropriés

Quelques logiciels libres

- ▶ Les systèmes d'exploitation GNU/Linux (Redhat, Debian, Ubuntu, Mint, Mandriva, Gentoo, ...)
- ▶ Navigateurs web : Mozilla Firefox, Chromium, ...
- ▶ Clients de messagerie : Mozilla Thunderbird, Kmail, Evolution, ...
- ▶ Clients de messageries instantanées : aMSN, pidgin, Miranda, Trillian, ...
- ▶ Suite office : Open Office/ Libre Office, Koffice, ...
- ▶ Retouche photo : Gimp

Modèle économique

Gratuité du logiciel ?

« *Le logiciel libre est gratuit, **une fois qu'il a été payé*** »

François Elie

Président de l'ADULLACT

- ▶ Mutualisation des investissements
(financement par consortium)
- ▶ Vente de services
(installation, formation, maintenance, extension)

Au delà du logiciel

Licence libre

- ▶ Creative commons
- ▶ Licences Art libre

Utilisable pour toutes les œuvres soumises au droit d'auteur

À lire

“Circulaire Ayrault” sur les logiciels libres, sections 1, 2 et 3

Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

- Réseaux privés virtuels

Plan

7 Réseaux Informatiques

Structure des réseaux

Protocoles de communication : la base des réseaux

Organisation des communications sur les réseaux

Exemple du chargement d'une page web

Proxy

Réseaux privés virtuels

Réseaux informatiques

Definition (Réseau local - LAN)

Réseau informatique déployé sur une étendue limitée (une pièce, un bâtiment, ...).

Usages

- ▶ Partage de ressources (imprimante, scanner, serveur de fichiers, ...)
- ▶ Communication entre les postes sur ce réseau
- ▶ Accès à d'autres réseaux (dont internet) via une passerelle

Réseaux informatiques

Definition (Réseau étendu - WAN)

Réseau informatique déployé à plus grande échelle qu'un réseau local.

Usages

idem LAN + communications entre des sites répartis sur une zone géographique étendue.

Exemple : RENATER, Infrastructures de fournisseurs d'accès à internet, ...

Internet

Definition (Internet)

Interconnexion de réseaux (LAN/WAN), déployé à l'échelle de la planète, accessibles "publiquement".

Usages

En théorie les mêmes que les LAN, à l'échelle de la planète (voir au-delà).

Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

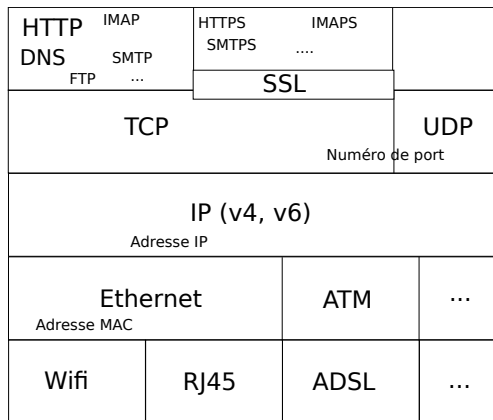
- Réseaux privés virtuels

Protocole de communication

Définition

Conventions décrivant la structure de la communication entre deux programmes, deux machines.

Protocoles utilisés sur internet

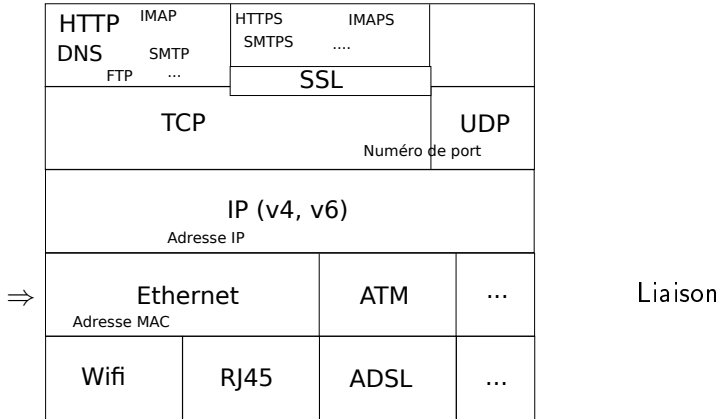


⇒

Organisation physique :

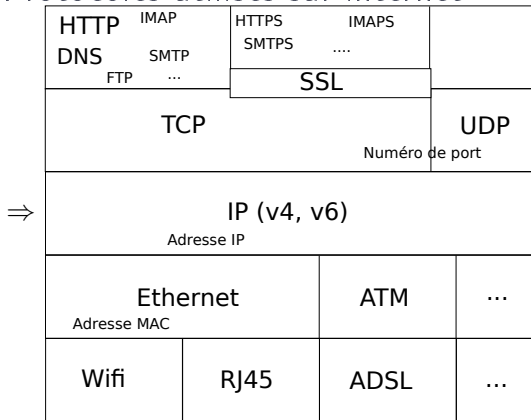
- ▶ Dépendant du *support* (WiFi, cable, fibre optique, ...)
- ▶ Gérée par le matériel
- ▶ interférences, Conversions Analogique ↔ Numérique, ...

Protocoles utilisés sur internet



- ▶ Échange de données binaires et Intégrité des données
- ▶ Lien entre les machines d'un même réseau local
- ▶ Protocole **Ethernet** : Adresse MAC = identifiant unique attribué au matériel par le constructeur

Protocoles utilisés sur internet

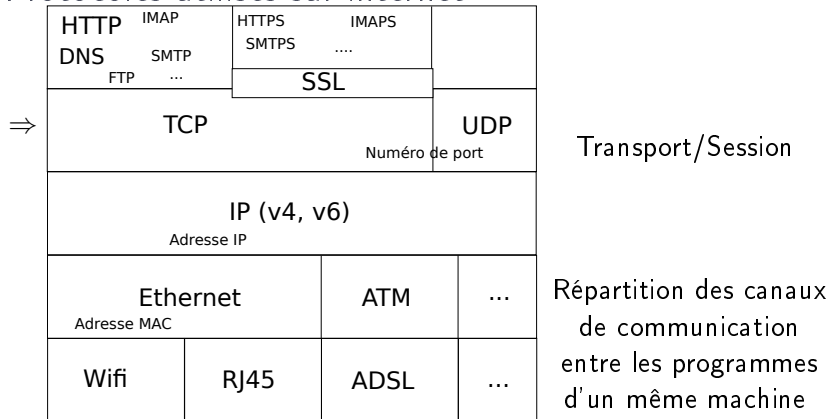


Réseau

- Interconnexion entre les réseaux
- Découverte de chemin entre les machine du réseau

- Les chemins passent toujours par plusieurs passerelles
- Protocole **IP** (Internet Protocol) : Adresse IP = identifiant unique sur le réseau, attribué par le gestionnaire du réseau pour une durée limitée
- IPv4 : 175.19.2.253 | IPv6 : fe80 :0000 :021d :d9ff :fe26 :0acd
- Communication non-ordonnée

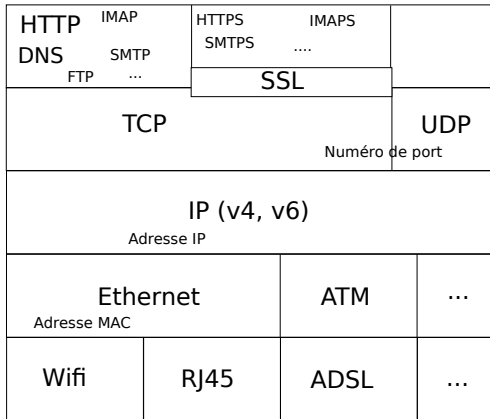
Protocoles utilisés sur internet



- ▶ Attribution de **port** à une application souhaitant communiquer
- ▶ Protocole **TCP** (communications ordonnée),
UDP (non-ordonnée)
- ▶ **SSL** (Secure Socket Layer)/**TLS** (Transport Layer Security) :
cryptographies asymétrique et symétrique pour assurer
confidentialité et authentification

Protocoles utilisés sur internet

⇒



Applications

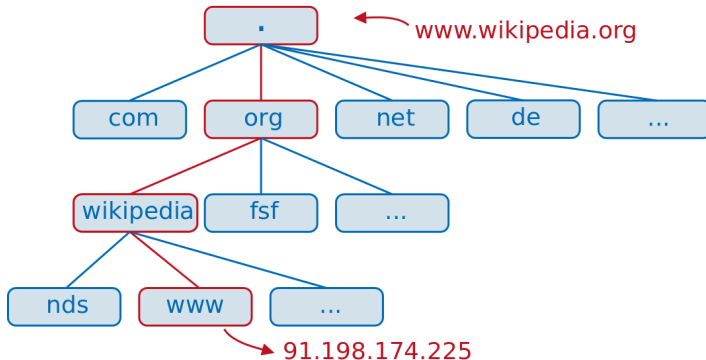
Protocoles spécifiques
à chaque type
d'applications

- ▶ **http** : page web, **https** : page web, connexion sécurisée
- ▶ **ftp**, **sftp**, **ftps** : transfert de fichiers
- ▶ **smtp** : envoi de mail, parfois sécurisé (**SSL**, **TLS**)
- ▶ **pop3**, **imap** : réception de mail, parfois sécurisé (**SSL**, **TLS**)

Domain Name Service

DNS

Service permettant d'obtenir l'adresse IP d'une machine à partir de son nom de serveur.



Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

- Réseaux privés virtuels

Organisation des communications sur les réseaux

Client-Serveur

Le serveur attend l'arrivée des clients (connexions) et rend le service demandé (envoi d'une page web par exemple)

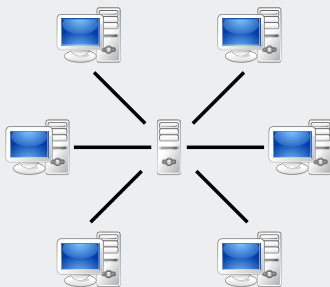
Pair-à-pair (Peer to Peer, P2P)

Chaque machine du réseau est à la fois client et serveur

Organisation des communications sur les réseaux

Client-Serveur

Le serveur attend l'arrivée des clients (connexions) et rend le service demandé (envoi d'une page web par exemple)



Pair-à-pair (Peer to Peer, P2P)

Chaque machine du réseau est à la fois client et serveur

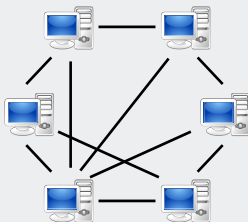
Organisation des communications sur les réseaux

Client-Serveur

Le serveur attend l'arrivée des clients (connexions) et rend le service demandé (envoi d'une page web par exemple)

Pair-à-pair (Peer to Peer, P2P)

Chaque machine du réseau est à la fois client et serveur



Une requête peut transiter par plusieurs nœuds du réseau

Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

- Réseaux privés virtuels

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL :
 - ▶ protocole : http
 - ▶ serveur : tesson.julien.free.fr
 - ▶ emplacement : /teaching/
 - ▶ fichier : index.php
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS** :
tesson.julien.free.fr → 212.27.63.133
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS** :
tesson.julien.free.fr → 212.27.63.133
- ▶ Connexion **TCP** : 212.27.63.133 :80
(80 = port attribué aux serveurs web)
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur `get /teaching/index.php`
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ Affichage de la page

Exemple

`http://tesson.julien.free.fr/teaching/index.php`

- ▶ Analyse de l'URL
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ **Interprétation** du fichier par le navigateur
- ▶ Affichage de la page

Exemple

<http://tesson.julien.free.fr/teaching/index.php>

- ▶ Analyse de l'URL
- ▶ Requête **DNS**
- ▶ Connexion **TCP**
- ▶ Envoie d'une demande au serveur
- ▶ le serveur renvoie par la même connexion le contenu de la page
- ▶ Interprétation du fichier par le navigateur
- ▶ **Affichage** de la page



Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

- Réseaux privés virtuels

Compléments réseau - Proxy

Serveur proxy

Serveur utilisé comme intermédiaire pour accéder au web (appelé serveur mandataire)

Intérêt

- ▶ Mise en cache (diminution de l'utilisation de la connexion vers l'extérieur)
- ▶ Partage d'identité (pour l'accès à des ressources réservées)

Plan

7 Réseaux Informatiques

- Structure des réseaux

- Protocoles de communication : la base des réseaux

- Organisation des communications sur les réseaux

- Exemple du chargement d'une page web

- Proxy

- Réseaux privés virtuels

Compléments réseau - V.P.N.

Réseau privé virtuel (RPV, VPN)

Réseau privé construit sur une infrastructure publique (internet) à l'aide de moyen cryptographiques.

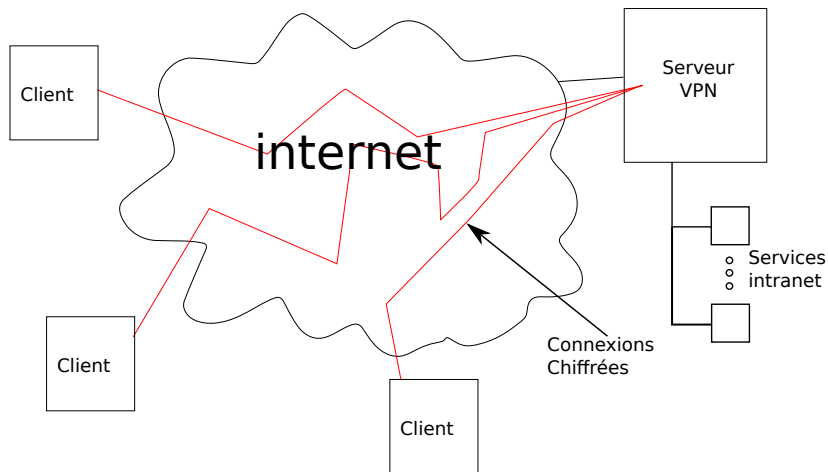
Fonctionnement

- ▶ Connexion à internet
- ▶ Mise en place d'une connexion sécurisée avec un serveur VPN
- ▶ Redirection du trafic réseau vers le serveur VPN

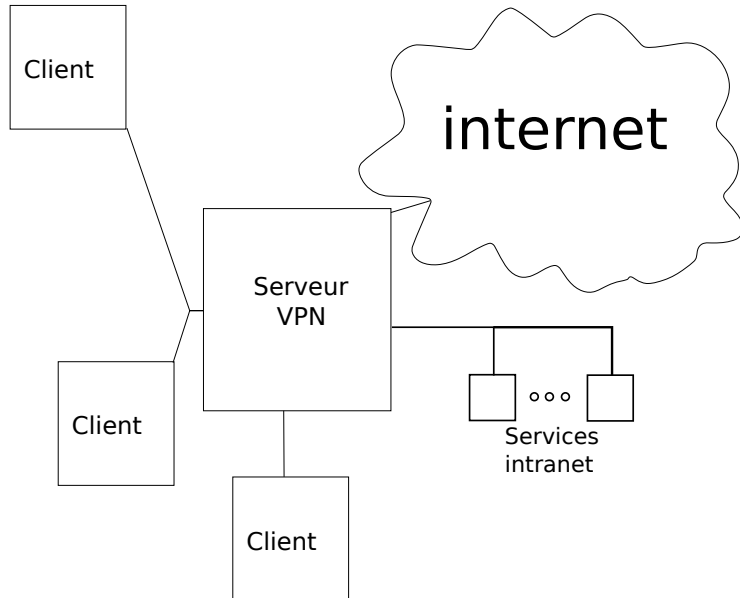
Outils

- ▶ Logiciel (Openvpn, PPTP)
- ▶ Matériel (Modem/routeur spécialisé)

V.P.N. - Connexions réelles



V.P.N. - réseaux virtuel



Plan

⑧ Sécurité

- Sécurisation de votre environnement de travail

- Menaces intérieures et parades

- Menaces extérieures

- Protections

Plan

⑧ Sécurité

Sécurisation de votre environnement de travail

Menaces intérieures et parades

Menaces extérieures

Protections

Sécurisation de votre environnement de travail

Votre machine

- + votre système d'exploitation
- + les applications que vous utilisez

Mais aussi des services en ligne :

- ▶ E-commerce
- ▶ Stockage en ligne
- ▶ Applications en ligne
- ▶ Environnements Numériques de Travail
- ▶ progiciel de gestion intégré (Enterprise Resource Planning ou ERP)
- ▶ Courriels, Réseaux sociaux, Services de discussion instantanée

Sécurisation de votre environnement de travail

- ▶ Sécurisation de vos données
 - ▶ Intégrité
 - ▶ Disponibilité
 - ▶ Confidentialité

Sécurisation de votre environnement de travail

- ▶ Sécurisation de vos données
 - ▶ Intégrité
 - ▶ Disponibilité
 - ▶ Confidentialité
- ▶ Sécurisation de l'accès à vos ressources
(Processeur, Accès internet, Comptes liés à des services)

Plan

⑧ Sécurité

Sécurisation de votre environnement de travail

Menaces intérieures et parades

Menaces extérieures

Protections

Menaces intérieures

perte de données

- ▶ Suppression involontaire
- ▶ Défaillance matérielle ou logicielle

Indisponibilité

- ▶ Panne matérielle
- ▶ Perte de connexion

Divulgaration d'informations confidentielles

- ▶ Fichiers contenant des versions antérieures
- ▶ Méconnaissance des informations contenues dans un fichier
- ▶ Outils de partage en ligne mal maîtrisés

Assurer l'intégrité et la disponibilité de vos données

- ▶ Sauvegardez

Assurer l'intégrité et la disponibilité de vos données

- ▶ Sauvegardez

- ▶ Sauvegardez

Assurer l'intégrité et la disponibilité de vos données

- ▶ Sauvegardez
- ▶ Sauvegardez
- ▶ Sauvegardez

Assurer l'intégrité et la disponibilité de vos données

- ▶ Sauvegardez
- ▶ Sauvegardez
- ▶ Sauvegardez

Sur des **supports différents**, stockés à des **endroits différents**

Préservation de la confidentialité

- ▶ Maîtriser les formats de fichiers utilisés
- ▶ Utilisation vigilante des outils de partage en ligne
 - ▶ Réflexion en amont de la mise en ligne
 - ▶ Maîtrise de réglages de confidentialité
 - ▶ Test des réglages

Plan

⑧ Sécurité

Sécurisation de votre environnement de travail

Menaces intérieures et parades

Menaces extérieures

Protections

Sécurisation de vos ressources

Quelques raisons de prendre le contrôle de votre machine

- ▶ Obtention d'informations confidentielles
- ▶ Usurpation d'identité (pour tromper vos contacts)
- ▶ Destruction d'informations
- ▶ Construction d'un *botnet*

Interception d'informations

But

- ▶ numéros de carte bleue
- ▶ identifiants / mots de passe
- ▶ informations stratégiques

Moyens

- ▶ redirection/copie du trafic réseau
- ▶ enregistrement des saisies clavier
- ▶ transmission des fichiers de la machine

Bestiaire

Cheval de troie

Application apparemment anodine comportant une fonctionnalité cachée permettant l'ouverture d'une brèche dans la sécurité de votre système.

Virus

Application malveillante (destructrice, ou ouvrant la porte à une prise de contrôle extérieur) pouvant se dupliquer et se *caler* dans d'autres applications de façon à passer inaperçue sur votre système,

Ver

Virus capable de s'installer sur une machine sans action de l'utilisateur, via une faille de sécurité du système d'exploitation.

Botnet

Botnet (Réseau de robots, de machines zombies)

Grands ensembles de machines infectées, contrôlables à distance, permettant divers usages malhonnêtes du réseau.

- ▶ Envoi de *spam* (courriers électroniques indésirables)
- ▶ Fonctionnement concerté de toutes les machines zombies pour
 - ▶ prendre le contrôle d'une machine spécifique
 - ▶ faire dysfonctionner des éléments d'internet
 - ▶ casser des chiffrements

Intérêt

- ▶ Accès à de grandes ressources (calcul, réseau)
Réseaux comportant jusqu'à 2 000 000 de machines
- ▶ Moyen d'anonymisation
- ▶ Economique (vente de campagne d'envoi de courriers, de moyens d'anonymisation)

Botnet : illustration



Usurpation d'identité

But

- ▶ Pousser vos contacts à transmettre des informations confidentielles
- ▶ Inciter vos contacts à effectuer des actions permettant la prise de contrôle de leur machine
- ▶ Orienter vos contacts vers des commerces peu scrupuleux
- ▶ Revente de vos informations personnelles

Plan

⑧ Sécurité

- Sécurisation de votre environnement de travail

- Menaces intérieures et parades

- Menaces extérieures

- Protections

Assurer la confidentialité de vos données

- ▶ Restreignez l'accès à votre machine à l'aide d'un mot de passe.
- ▶ Fermez votre session ou utilisez un économiseur d'écran avec mot de passe lorsque vous quittez votre machine.
- ▶ Fermez votre session lorsque vous quittez un service web.
- ▶ Lorsque vous transmettez des informations confidentielles via internet, utilisez un protocole sécurisé

Confidentialité - Utilisation de protocole sécurisé

Courriel via client de messagerie

- ▶ Courrier sortant : SMTP + StartTLS ou SMTPS
- ▶ Courrier entrant :
POP3 + StartTLS
- ▶ Courrier entrant (Avec gestion de dossiers) :
IMAP + StartTLS ou IMAPS

Toutes ces extensions des protocoles utilisent une connexion sécurisée par TLS

Confidentialité - Utilisation de protocole sécurisé

Web

Pour simplifier

- ▶ http = information publique
- ▶ https = communication chiffrée

Les communications chiffrées ne sont utiles que si vous avez confiance en votre interlocuteur

Confidentialité - https

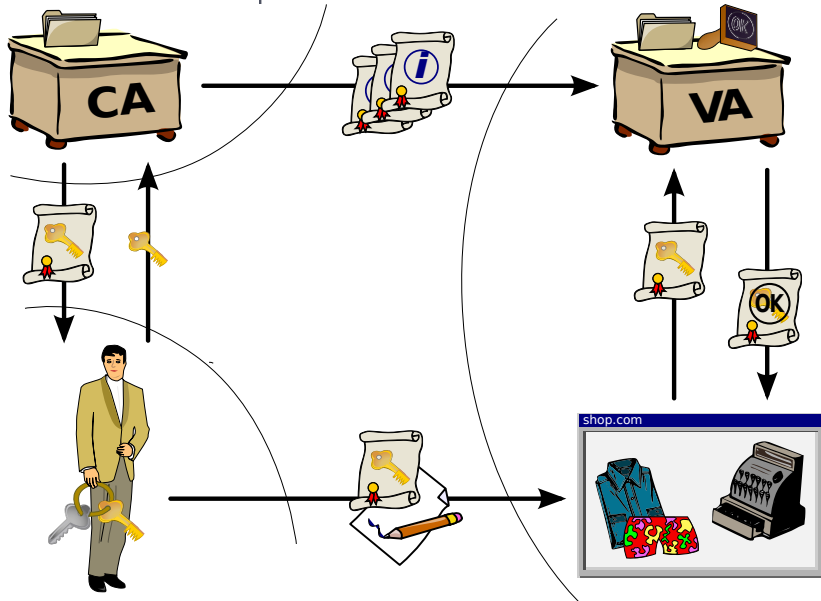
- ▶ Vérification de l'orthographe de l'adresse
www.mabanque.fr www.mabanque.fr www.mabanque.fl
- ▶ Authentification du serveur grâce à un certificat

Confidentialité - https - Certificats

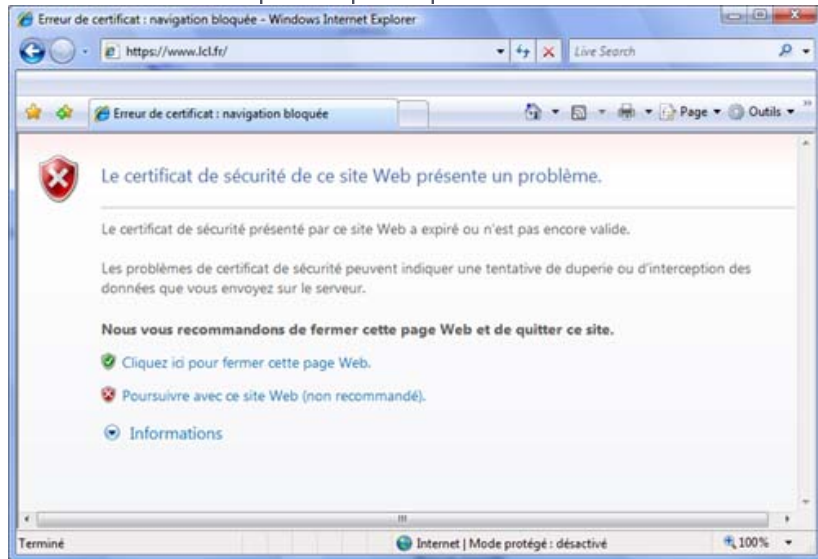
3 acteurs

- ▶ Client
- ▶ Serveur
- ▶ Autorité de certification

Confidentialité - https - Certificats



Confidentialité - https en pratique



Confidentialité - https en pratique



Cette connexion n'est pas certifiée

Vous avez demandé à Firefox de se connecter de manière sécurisée à **master.support.mozilla.com**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

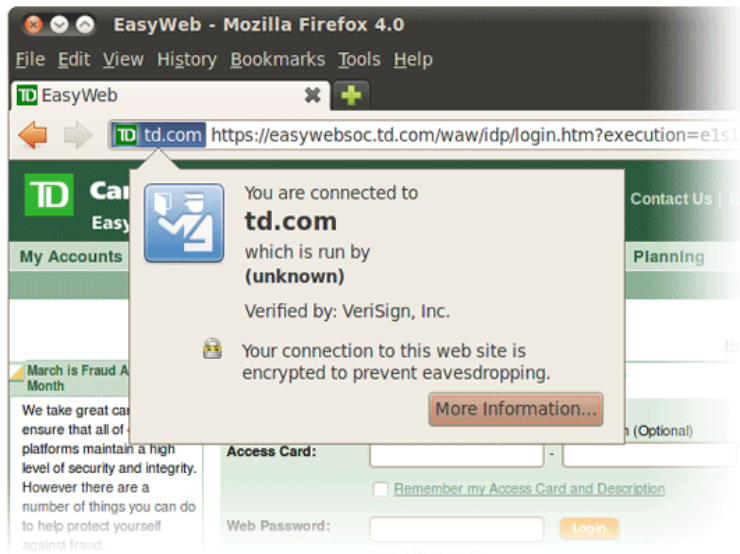
Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

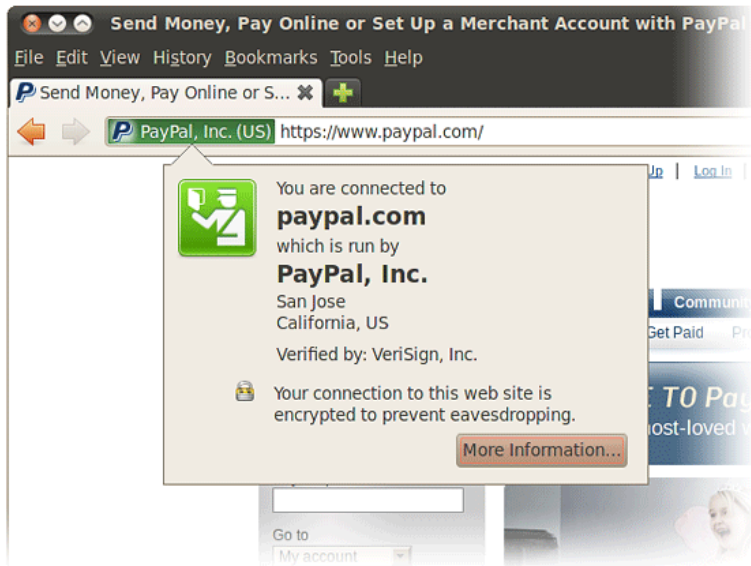
Sortir d'ici !

- ▶ **Détails techniques**
- ▶ **Je comprends les risques**

Confidentialité - https en pratique



Confidentialité - https en pratique



Confidentialité - https

Sur les machine publiques, Attention

Possibilité de réglage du navigateur pour qu'il accepte des certificats signés localement



Possibilité d'un enregistrement des communications par un intermédiaire

Comment protéger votre ordinateur

- ▶ Mettre à jour votre système d'exploitation et vos applications
- ▶ N'exécutez jamais un programme dont la source n'est pas sûre
- ▶ Utilisez un anti-virus
- ▶ Utilisez un pare-feu

Récapitulatif des conseils de base

« La plus importante faille des systèmes informatiques se trouve entre la chaise et le clavier. »

- ▶ Ne donnez **JAMAIS** vos mots de passe à quiconque
- ▶ N'utilisez pas le même mot de passe partout
- ▶ N'utilisez pas de mot existant ou de date de naissance pour vos mots de passe. (attaque par dictionnaire)
- ▶ Fermez votre session lorsque vous quittez un site web
- ▶ Fermez votre session ou utilisez un économiseur d'écran avec mot de passe lorsque vous laissez votre machine

Récapitulatif des conseils de base

« La plus importante faille des systèmes informatiques se trouve entre la chaise et le clavier. »

- ▶ N'exécutez jamais un programme dont la source n'est pas sûre
- ▶ N'ouvrez pas de fichier joint à un mail si vous n'avez pas confiance en l'expéditeur
- ▶ Mettez votre système à jour
- ▶ Utilisez des logiciels dont la fiabilité est reconnue
- ▶ Tenez vous informé sur les failles de sécurité que peuvent présenter vos logiciels

Plan

- ⑨ Internet et vie privée
 - Aspect juridique

Informations transmises lors d'une connexion à un site web

- ▶ Adresse IP
- ▶ Système d'exploitation
- ▶ Navigateur
- ▶ Page précédemment visitée
- ▶ Cookies

Cookie

Informations envoyée par un serveur http à un client http, que ce dernier retourne lors de chaque interrogation du même serveur.

Informations transmises lors d'une connexion à un site web

- ▶ Adresse IP $\Rightarrow$ FAI, **géolocalisation**
- ▶ Système d'exploitation
- ▶ Navigateur
- ▶ Page précédemment visitée
- ▶ Cookies $\Rightarrow$ **historique de navigation** sur tout le site du domaine et sur les sites importants des éléments du domaine.
Exemples : boutons google +, ou j'aime facebook

Cookie

Informations envoyée par un serveur http à un client http, que ce dernier retourne lors de chaque interrogation du même serveur.

Les géants d'internet

« *Facebook sait si vous êtes gay, Google que vous êtes enceinte.* »

Jean-Marc Manach

<http://bugbrother.blog.lemonde.fr/>

Pourquoi ?

Publicité ciblée :

Il est plus intéressant de présenter une publicité de vêtements pour femme enceinte à une femme enceinte qu'à 100 personnes au hasard.

Les géants d'internet

« *Facebook sait si vous êtes gay, Google que vous êtes enceinte.* »

Jean-Marc Manach

<http://bugbrother.blog.lemonde.fr/>

Comment ?

- ▶ En vous incitant à donner des informations sur vous
- ▶ En incitant vos contacts à donner des informations sur vous
- ▶ En suivant votre navigation
- ▶ En analysant vos conversations

Les géants d'internet

Si c'est gratuit, c'est que vous êtes le produit

Plan

- ⑨ Internet et vie privée
 - Aspect juridique

Que dit la loi ?

Loi relative à l'informatique, aux fichiers et aux libertés - Loi 78-17 du 6 janvier 1978

L'informatique doit être au service de chaque citoyen.

Son développement doit s'opérer dans le cadre de la coopération internationale.

Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

CNIL - Commission Nationale de l'Informatique et des Libertés

- ▶ Informe sur les droits et obligations de chacun
- ▶ Délivre des autorisations de constitution de fichiers
- ▶ Donne un avis sur les fichiers constitué par l'état
- ▶ Effectue une veille technologique
- ▶ Reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**
- ▶ **Le droit d'accès**
- ▶ **Le droit de rectification**
- ▶ **Le droit d'opposition**
- ▶ **Le droit d'accès indirect (via la CNIL)**

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**

Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée.

- ▶ **Le droit d'accès**

- ▶ **Le droit de rectification**

- ▶ **Le droit d'opposition**

- ▶ **Le droit d'accès indirect (via la CNIL)**

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**

- ▶ **Le droit d'accès**

Toute personne a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle.

- ▶ **Le droit de rectification**

- ▶ **Le droit d'opposition**

- ▶ **Le droit d'accès indirect (via la CNIL)**

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**

- ▶ **Le droit d'accès**

- ▶ **Le droit de rectification**

Toute personne peut faire rectifier des informations qui la concernent :

correction d'erreurs, suppression de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

- ▶ **Le droit d'opposition**

- ▶ **Le droit d'accès indirect (via la CNIL)**

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**
- ▶ **Le droit d'accès**
- ▶ **Le droit de rectification**
- ▶ **Le droit d'opposition**
Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier.
- ▶ **Le droit d'accès indirect (via la CNIL)**

Que dis la loi ? - Vos droits

- ▶ **Le droit à l'information**
- ▶ **Le droit d'accès**
- ▶ **Le droit de rectification**
- ▶ **Le droit d'opposition**
- ▶ **Le droit d'accès indirect** (via la CNIL), pour un certain nombre de fichiers constitués par l'état.

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier**
- ▶ **La confidentialité des données**
- ▶ **La durée de conservation des informations**
- ▶ **L'information des personnes**
- ▶ **L'autorisation de la CNIL**

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier :**
mesures de sécurité
 - ▶ physiques (sécurité des locaux)
 - ▶ logiques (sécurité des systèmes d'information)
- ▶ **La confidentialité des données**
- ▶ **La durée de conservation des informations**
- ▶ **L'information des personnes**
- ▶ **L'autorisation de la CNIL**

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier**
- ▶ **La confidentialité des données**
Seules des personnes autorisées, explicitement désignées, peuvent accéder aux données personnelles contenues dans un fichier.
- ▶ **La durée de conservation des informations**
- ▶ **L'information des personnes**
- ▶ **L'autorisation de la CNIL**

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier**
- ▶ **La confidentialité des données**
- ▶ **La durée de conservation des informations**
Les données personnelles ont une date de péremption.
Le responsable d'un fichier fixe une durée de conservation raisonnable en **fonction de l'objectif du fichier**.
- ▶ **L'information des personnes**
- ▶ **L'autorisation de la CNIL**

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier**
- ▶ **La confidentialité des données**
- ▶ **La durée de conservation des informations**
- ▶ **L'information des personnes sur :**
 - ▶ L'identité du responsable du fichier
 - ▶ La finalité de son traitement
 - ▶ Le caractère obligatoire ou facultatif des réponses
 - ▶ Les destinataires des informations
 - ▶ L'existence de droits
 - ▶ Les transmissions envisagées.
- ▶ **L'autorisation de la CNIL**

Que dis la loi ? - Obligation du détenteur d'un fichier

- ▶ **La sécurité du fichier**
- ▶ **La confidentialité des données**
- ▶ **La durée de conservation des informations**
- ▶ **L'information des personnes**
- ▶ **L'autorisation de la CNIL**
Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en oeuvre, être soumis à l'autorisation de la CNIL.

Plan

10 Cloud computing

Cloud computing

Définition

- ▶ Informatique en nuage / dans le nuage / dans les nuages
- ▶ Infonuagique
- ▶ Informatique dématérialisé

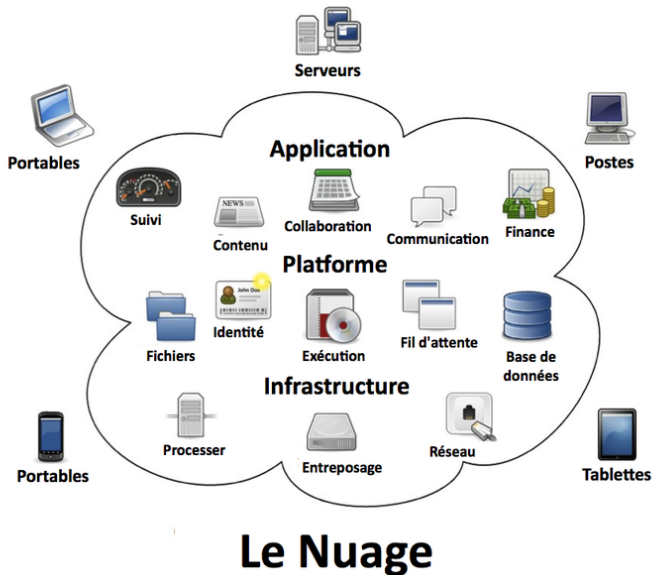
Concept consistant à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur.

Cloud computing

Principes directeurs

- ▶ mutualisation des infrastructures matérielles
- ▶ paiement à l'usage

Cloud computing



Cloud computing - coté utilisateur

Stockage en ligne (Dropbox, Google Drive, Microsoft Skydrive)

Avantages :

- ▶ Accessible depuis n'importe quel terminal connecté au web
- ▶ Serveurs plus sûrs
 - ▶ copies multiples
 - ▶ multi-sites
 - ▶ alimentations redondantes
- ▶ Partage simplifié

Inconvénients :

- ▶ Règles de confidentialité souvent floues
- ▶ Localisation physique des données souvent impossible :
Quel loi s'applique à mes données ?
- ▶ Forte dépendance au fournisseur de service
- ▶ Nécessite une connexion

Cloud computing - coté utilisateur

Applications en ligne

(Google docs, Microsoft Office Web Apps, IBM SmartCloud)

Avantages :

- ▶ idem stockage
- + Édition collaborative de documents
- + Montée en charge plus facile pour le calcul

Inconvénients :

- ▶ idem stockage
- + Fonctionnalité réduite pour le moment

Plan

- 11 Recherche documentaire & Veille informationnelle

Moteurs de recherche

Définition

Outil automatisé de recherche de documents à partir d'une description (généralement textuelle)

Moteurs de recherche web généralistes

Google (web, images, x vidéos), Yahoo, Baidu, Yandex, Bing, Exalead, Duckduckgo

Moteurs de recherche spécialisés

- ▶ Définition, synonymie, étymologie : www.cnrtl.fr
- ▶ Droit français : www.legifrance.gouv.fr

Moteurs de recherche web - fonctionnement

Exploration - Crawler

Programme robot parcourant le web, suivant chaque lien qu'ils rencontrent lorsqu'ils *lisent* une page.

Indexation

Recherche

PageRank

Moteurs de recherche web - fonctionnement

Exploration - Crawler

Indexation

Pour chaque page :

- ▶ Éventuellement mise en cache
- ▶ Extraction des mots *significatifs*
- ▶ Calcul de pertinence pour chaque mot
- ▶ Ajout du lien dans un dictionnaire

Recherche

PageRank

Moteurs de recherche web - fonctionnement

Exploration - Crawler

Indexation

Recherche

- ▶ Analyse de la requête
- ▶ Correction, sélection de synonymes
- ▶ Calcul des PageRank
- ▶ affichage du resultat

PageRank

Moteurs de recherche web - fonctionnement

Exploration - Crawler

Indexation

Recherche

PageRank

Score de pertinence d'une page, calculé à partir

- ▶ du nombre de liens vers cette page
- ▶ des choix précédents des utilisateurs du moteur de recherche
- ▶ du nom de domaine
- ▶ ...
- ▶ de vos centres d'intérêts

Moteurs de recherche - Personnalisation

Intérêt

Réponses généralement plus pertinentes, puisque proche de vos centres d'intérêts supposés

Risque

Exclusion de réponses contradictoires, enfermement dans un sous-web

Moteurs de recherche - requête

Contrôles

- ▶ Texte exact "Usage du logiciel libre dans l'administration"
- ▶ Texte presque exact : "Usage * libre * administration"
- ▶ exclusion de terme : téléphone portable -forfait
- ▶ inclusion de terme : +le parrain
- ▶ recherche dans les liens : vie étudiante link:u-pec.fr
- ▶ recherche dans le titre : intitle:"vie étudiante"
- ▶ recherche sur un site particulier : site:"u-pec.fr"

Connecteurs logiques

- ▶ AND "logiciel libre" AND "open source"
- ▶ OR "logiciel libre" OR "open source"

Veille informationnelle

Définition

Activité continue ayant pour but la surveillance active de l'évolution d'un domaine défini.

En droit

- ▶ Évolutions de la législation
- ▶ Jurisprudence
- ▶ Commentaires

Sur Internet

- ▶ Grande quantité d'informations
- ▶ Nécessité de filtrer
 - ▶ Définir des objectifs de veille clairs
 - ▶ Identifier les sources pertinentes

Veille informationnelle

Outils

- ▶ Mémorisation d'une recherche
- ▶ E-mail
 - ▶ Listes de discussion
 - ▶ Newsletters
 - ▶ Alertes
- ▶ Flux de syndication
- ▶ Réseaux sociaux

Veille informationnelle - Mémorisation d'une recherche

Moyens

- ▶ marque-pages/favoris du navigateur
- ▶ marque-pages en ligne (delicious.com, google bookmark)

Attention

vérifier la pérennité du lien enregistré

Veille informationnelle - Email

Newsletter (lettre d'information)

Système permettant à un groupe de personnes intéressées par un même sujet de recevoir un document d'information envoyé de manière périodique par courrier électronique.

Veille informationnelle - Email

Listes de discussion et de diffusion

Système permettant à un groupe de personnes intéressées par un même sujet d'échanger des e-mails avec l'ensemble du groupe

- ▶ Inscription pour recevoir les mails échangés
- ▶ Un mail envoyé à l'adresse de la liste est transmis à l'ensemble des personnes inscrite à cette liste

Les réponses à un mail de la liste sont généralement dirigée vers l'intégralité de la liste, attention à l'adresse du destinataire si vous voulez faire une réponse privée.

Veille informationnelle - Email

Alerte e-mail

Système permettant à une personnes d'être informée par E-mail lorsqu'une recherche produit de nouveaux résultats

Services d'alertes généralistes ([google alerts](#), [yahoo alerts](#)) ou spécialisés (alertes sur [senat.fr](#), ...)

Flux de syndication (RSS/Atom)

Définition

Système permettant de publier périodiquement une partie du contenu d'un site sur d'autres sites ou d'autres supports

Aggrégateurs de Flux

- ▶ En ligne : Google Reader, Netvibes, My Yahoo
- ▶ Sur votre machine : Widgets, Firefox, Thunderbird

Flux de syndication - fonctionnement

À chaque mise à jours du site, ajout d'article, etc, un résumé est inséré dans le flux, avec la date de modification et un lien vers la page créée.

flux de syndication

Démo

Créateur de flux de syndication

Pour les site ne proposant pas de flux de syndication, il existe des sites capables de les construire([page2rss](#), [Feed43](#), ...)

Réseaux sociaux

- ▶ Suivi d'organisations, de personnes d'autorité dans un domaine
- ▶ Partage d'information au travers de groupes d'intérêts
- ▶ Attention à bien séparer vie public - vie privée

Quelques conseils

- ▶ Structurez le résultat de vos recherches en fonction de la fiabilité de la source
- ▶ Gardez des liens (permanents) vers vos sources
- ▶ Gardez une copie des documents les plus importants
- ▶ Citez vos sources quand vous produisez un document

Plan

12 Web passé, présent et futur

Web 1.0, la base

- HTML - HyperText Markup Language

Web 2.0, le web collaboratif

- Blog

- Réseaux sociaux

- Wiki

- Content management System (CMS)

Web 3.0

- Le web sémantique

- L'internet des objets

- Un web contextualisé

- Enjeux

Plan

12 Web passé, présent et futur

Web 1.0, la base

HTML - HyperText Markup Language

Web 2.0, le web collaboratif

Blog

Réseaux sociaux

Wiki

Content management System (CMS)

Web 3.0

Le web sémantique

L'internet des objets

Un web contextualisé

Enjeux

Le Web, la toile

La toile

Ensemble des documents accessibles sur internet inter-connectés par des *liens hypertextes*

- ▶ Web 1.0, l'origine, la structure de base
- ▶ Web 2.0, le web participatif
- ▶ Web 3.0, le web du futur

Web 1.0, la base

Site web

- ▶ Ensemble de pages web
- ▶ Page : un fichier au format HTML + d'autres documents (image, son,...)
- ▶ Reliées entre elles par des liens hypertextes

Publication

- ▶ Réalisé par un concepteur
- ▶ Hébergé sur un serveur
- ▶ Consulté par des utilisateurs

HTML - structure

`<html>`

`</html>`

HTML - structure

```
<html>  
  <head>  
  
    </head>  
    <body>  
  
      </body>  
</html>
```

HTML - structure

```
<html>
  <head>
    <title> Titre de la Page </title>
    <meta name="Keywords" content="mot-clefs ..." />
    <link rel="stylesheet" href="style.css" title="style-1" />
  </head>
  <body>
    <h1> Titre partie </h1>
    <p> Un paragraphe se termine par un saut de paragraphe </p>
    <h2> Titre sous partie </h2>
    <p> On peut aussi trouver un saut de ligne <br/>
    mais c'est à éviter </p>
  </body>
</html>
```

HTML

<h1> formatage de texte </h1>

<p> le texte peut être mis en gras, en <i>italic</i>
mais surtout, on peut créer des liens hypertextes

 vers d'autres pages
</p>

Titre partie

Un paragraphe se termine par un saut de paragraphe

Titre sous partie

On peut aussi trouver un saut de ligne
mais c'est à éviter

formatage de texte

Le texte peut être mis en **gras**, **agrandi** mais surtout, on peut créer des liens hypertextes **vers d'autres pages**

Feuille de style

Idée principale

Séparer la mise en forme du contenu.

HTML + CSS

Les balises structurent le document d'un point de vue sémantique, la feuille de style décrit l'apparence des différents éléments.

Démo

Vers plus d'interactivité

Coté serveur

Utilisation de programme et de base de données, page générée au moment de la requête.

- ▶ Enregistrement d'informations envoyées par l'utilisateur
- ▶ Pages personnalisées
- ▶ Affichage d'informations provenant d'une base de données (stock, utilisateurs, ...)

Coté client - javascript

- ▶ Code dans la page
- ▶ Interprété par le navigateur
- ▶ Modification de la page sans interaction avec le serveur

Plan

12 Web passé, présent et futur

Web 1.0, la base

HTML - HyperText Markup Language

Web 2.0, le web collaboratif

Blog

Réseaux sociaux

Wiki

Content management System (CMS)

Web 3.0

Le web sémantique

L'internet des objets

Un web contextualisé

Enjeux

Web 2.0, le web collaboratif

- ▶ Blogs
- ▶ Site de réseaux sociaux
- ▶ Site web collaboratifs (Wiki)
- ▶ CMS
(Content Management System, Système de Gestion de contenu)

Fonctionnement

- ▶ 1 auteur, écriture de contenus facile, via une page du site, pas de html
- ▶ Possibilité pour les lecteurs de laisser des commentaires

Création

- ▶ Compte sur une plateforme de blog

ou

- ▶ Installation sur un site de page perso
(nécessite un support PHP+base de données)

Réseaux sociaux - micro-blogging

Fonctionnement

Interconnexion de micro-blogs

Création

Compte sur une plateforme

Wiki

Fonctionnement

- ▶ Multiples auteurs
- ▶ Possibilité pour tous de modifier toutes les pages
- ▶ Syntaxe simple pour structurer le document
- ▶ Gestion de droit d'accès possible
- ▶ Gestion de version des pages (possibilité de revenir en arrière)

Création

- ▶ Compte sur une plateforme de wiki

ou

- ▶ Installation sur un site de page perso
(nécessite un support PHP+base de données)

Syntaxe wiki

- ▶ titres

```
= titre 1 =  
== titre 2 ==  
=== titre 3 ===
```

- ▶ liens externes/internes

```
[[lien interne]]  
les [[lien interne | liens internes]] ...
```

```
http://lien_externe.com/  
ce [http://lien_externe.com/ site externe] ...
```

Syntaxe wiki

► listes à puce

```
* text niveau 1
** niveau 2
** niveau 2
* niveau 1
```

► text niveau 1

- text niveau 2
- text niveau 2

► niveau 1

► tableau

```
{|
| col 1 || col 2 || col 3|
|-
| d 1 || d 2 || d 3|
| d 1 || d 2 || d 3|
|}

```

col 1	col 2	col 3
d 1	d 2	d 3
d 1	d 2	d 3

Fonctionnement

- ▶ Sorte de bureau virtuel en ligne
- ▶ Publication de contenu à l'aide de wikis
- ▶ Mise en ligne de documents avec commentaires (+ éventuellement gestion de versions)
- ▶ Possibilité de gestion fine du partage de contenus et documents (lecture et/ou écriture)

Création

Nécessite souvent un serveur dédié (plus difficile à installer)

Plan

12 Web passé, présent et futur

Web 1.0, la base

HTML - HyperText Markup Language

Web 2.0, le web collaboratif

Blog

Réseaux sociaux

Wiki

Content management System (CMS)

Web 3.0

Le web sémantique

L'internet des objets

Un web contextualisé

Enjeux

Futurologie, un exercice difficile

Quelques pistes

- ▶ Le web sémantique
- ▶ L'internet des objets
- ▶ Le web contextualisé (géolocalisation, ...)

Web sémantique

- ▶ Interaction en langage naturel.
- ▶ Structuration des informations du web,
- ▶ pour l'interrogation automatique, comme une grande base de connaissance
- ▶ et restitution sous forme de résumé généré automatiquement.

L'internet des objets

- ▶ Domotique
- ▶ Objets *interagissant* avec d'autres,
- ▶ portant de l'information (RFID, QRcode,)
- ▶ ou générant de l'information (capteurs divers)

Le web contextualisé

- ▶ Géolocalisation
- ▶ Profilage de l'utilisateur
- ▶ Détection des personnes présentes
- ▶ Détection de l'humeur
- ▶ Réalité augmentée (capture d'image/son + interprétation + enrichissement)

Les enjeux

Enjeux de l'omni-présence de l'information

- ▶ Un internet libre de la censure ?
- ▶ Un internet où nous pouvons contrôler l'accès à nos données ?
- ▶ Des programmes sûrs !

Plan

- 13 Production de documents
 - Éléments divers
 - Structure d'un document

Documents numériques

Principes Généraux

- ▶ Séparation du contenu et de la mise en forme
- ▶ Structure hiérarchique
- ▶ Navigation

What You See Is What You Get

Logiciels de traitement de texte

W Y S I W Y G

Microsoft Word, LibreOffice, Lotus Note, ...

Règles Typographiques françaises

Espace et Ponctuation

,. pas d'espace avant, une espace après
; : ! ? une espace insécable avant ; une espace après
([« »]) une espace à l'extérieur (pas d'espace à l'intérieur)

Espace insécable

- ▶ Obtenue par ctrl+maj+espace dans la plupart des logiciels.
- ▶ Empêche le retour à la ligne entre les deux entités qu'elle sépare.

En cas de doute sur la règle à suivre :

*Lexique des règles typographiques en usage à
l'imprimerie nationale*



Plan

- 13 Production de documents
 - Éléments divers
 - Structure d'un document

Production de documents - Démo

Sauts

- ▶ de paragraphe - entrée
- ▶ de ligne - maj+entrée
- ▶ de page - ctrl+entrée

Caractères invisibles

- | | |
|------------------------|----------------|
| ▶ saut de paragraphe ¶ | ▶ espace · |
| ▶ saut de ligne ↵ | ▶ tabulation → |

Plan

- 13 Production de documents
 - Éléments divers
 - Structure d'un document

Production de documents structurés - Démo

Catégorisation des différents éléments du texte

- ▶ Tabulation
- ▶ Liste à puce
- ▶ Utilisation des styles
- ▶ Numérotation des parties
- ▶ Déplacement des parties
- ▶ En-tête/ pieds de page
- ▶ Notes de bas de page
- ▶ Champs : n° de page, auteurs, dates, ...
- ▶ Renvois et repères de texte
- ▶ Références bibliographiques

Production de documents structurés - Démo

Structure et tables automatiques

- ▶ Hiérarchie de section
- ▶ Table des matières
- ▶ Index
- ▶ Bibliographie

Master Document

- ▶ Construction de gros documents
- ▶ Réutilisation de documents
- ▶ Travail Collaboratif