A toutes fins utiles, petite introduction à des concepts d'informatique

Orena GAPUISSI

Table des matières

La cryptographie, qu'est-ce que c'est ?

La **cryptographie** est une des disciplines de la cryptologie s'attachant à **protéger des messages** (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de *secrets* ou *clés*. Elle se distingue de la sténographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un **message inintelligible** à autre que qui-de-droit.

Elle est utilisée depuis l'Antiquité, mais certaines de ces méthodes les plus importantes, comme la cryptographie asymétrique, datent de la fin du XXe siècle.

(Source : Wikipédia)

Un exemple de cryptographie symétrique : le chiffre de Vigenère

Le **chiffre de Vigenère** est un système de chiffrement par substitution, où une même lettre du message à transmettre (**message clair**) peut, suivant sa position dans celui-ci, être remplacé par des lettres différentes dans le **message chiffré**.

Le chiffre de Vigenère a été percé par le major prussien Friedrich Kasiski qui a publié sa méthode en 1863. Depuis cette époque, il n'offre plus aucune sécurité, mais sa méthodologie reste à la base des techniques de chiffrement modernes à base de clés.

Le **chiffrement à clé** utilise une chaine de chiffres ou de caractères (**la clé**) pour indiquer par quelle lettre doit être substitué chaque lettre du message en clair. Dans les méthodes modernes, la clé est alphanumérique, unique et aléatoire.

Dans le **chiffre de Vigenère**, la clé est un mot qui est répété plusieurs fois (ce qui est sa faiblesse et a permis d'en produire une méthode de décodage). A chaque lettre du message clair correspond alors une lettre de la clé, qui définit la substitution. Le codage se fait alors à partir d'**une table** indiquant, dans un tableau croisé, la lettre qui servira à coder.

(Adapté de Wikipédia)

Blaise de Vigenère
Wikimedia commons

Le binaire, des 0 et des 1, pourquoi ?

L'arithmétique binaire (plus simplement le calcul binaire) est utilisée par les systèmes électroniques les plus courants (calculatrices, ordinateurs, etc.) car les deux chiffres 0 et 1 s'y traduisent par le **passage ou l'absence d'un courant électrique** (ou par une différence de **tension**).

Le 1 représente généralement le passage d'un courant alors que le 0 représente l'absence de courant.

En **logique**, le 1 représente le « vrai » et le 0 le « faux ».

Pour ma culture personnelle, les débuts du binaire :

Décembre 1937, John Atanasoff, physicien de son métier, las de passer son temps à faire des calculs, prend sa voiture et fonce vers Des Moines (ville des Etats-Unis, capitale de l'Etat de l'Iowa). En début d'après-midi, il

*s'arrête dans un bar au bord du Mississipi, avale quelques Scotch et là l'illumination : « **1 et 0**, le **binaire**, c'est la solution ». Et là sur la nappe devant lui, il écrit les bases des grandes caractéristiques des ordinateurs numériques et non plus mécaniques qui seront construits dans les décennies qui suivront : « ils travailleront avec des 0 et des 1. Ils disposeront d'une mémoire et feront des opérations logiques. » Avec son assistant Clifford Berry, il construisit le premier ordinateur numérique de l'histoire.*

John Atanasoff avait été un calculateur humain (un computer comme on disait alors en anglais). Il appela sa machine « computer » et à la fin de 1939 l'ABC (Atanasoff Berry Computer) entra en service : il effectuait un calcul toutes les 15s et pesait plus de 300 kilos.

(Librement adapté de owni.fr)

Images et encodage :

Qu'est-ce qu'un bit ?

Le **bit** (**bi**nary digi**t** ou chiffre binaire) est l'**unité** la plus simple dans un système de numération ne pouvant prendre que deux valeurs 0 ou 1.

Qu'est-ce qu'une image numérique ?

L'appellation « **image numérique** » désigne toute image (dessin, icône, photographie…) *acquise*, *créée*, *traitée* et *stockée* sous forme binaire.

(Wikipédia)

Visuellement, l'image numérique apparait comme un tableau de pixels, d'une certaine **largeur l** et d'une **hauteur h** : **l x h**

Bien que toujours stockée sous forme binaire, il existe **différents encodages** pour stocker une image numérique. Les différents encodages prennent plus ou moins de place et conservent plus ou moins la qualité de l'image de base.

Qu'est-ce qu'un pixel ?

Le **pixel** est l'unité de base permettant de mesurer la définition d'une image numérique. Son nom provient de la locution anglaise *picture element*, qui signifie « élément d'image ».

La **définition** d'une image numérique correspond au nombre de pixels la composant sur l'axe horizontal et sur l'axe vertical.

La **résolution** correspond au nombre de pixels par pouce (=2,54cm) et est exprimée en ppp (points par pouce) ou dpi (dots per inch). Plus la résolution est importante, moins les pixels de l'image sont visibles.

Et mon écran ?

En informatique, un pixel est codé sur un ou plusieurs bits :

Pour une image en noir et blanc, chaque pixel est soit noir, soit blanc, c'est-à-dire codé sur un bit (0 ou 1).

<u>Pour ma culture personnelle :</u>

Pour une image en nuances de gris avec seulement 4 possibilités : noir, gris foncé, gris clair et blanc, on code alors un pixel sur deux bits.

En général, pour une image en nuances de gris variées, chaque pixel est codé sur 8 bits (1 octet) donc 2^8 = 256 niveaux de gris.

Pour une image en couleurs, chaque pixel est composé de trois sous-pixel (RVB : rouge-vert-bleu) qui peuvent chacun être codé sur 8 bits donc 256^3 soit plus de 16 millions de couleurs.

Sous-pixels dans le système RVB
Wikimedia commons

Qu'est-ce qui compose un ordinateur ?

- **Processeur** : c'est la **tête pensante** de l'ordinateur. Il est chargé de traiter et d'exécuter les instructions. Plus il est puissant, plus les **calculs** se font rapidement.

- **RAM** (ou **mémoire vive**) : c'est un espace de stockage de l'ordinateur qui sert à **stocker les données temporairement** pendant que l'on travaille. C'est la **mémoire à court terme**. Plus la RAM est importante, plus l'ordinateur est performant. La capacité de stockage s'exprime en octet.

- **Disque Dur** : le disque dur est un **espace de stockage** et l'un des composants principaux de l'ordinateur. C'est la **mémoire à long terme** qui permet de stocker vos programmes, vos photos et vidéos ainsi que d'autres sortes de données informatiques. Il est possible d'utiliser un disque dur externe sur un ordinateur, en plus de celui qui lui est déjà interne.

- **Carte mère** : c'est l'élément sur lequel sont **connectés tous les éléments** de l'ordinateur (processeur, mémoires, périphériques d'entrée et sortie…) et qui leur permet de **communiquer** entre eux.

- **Nappes** : elles **relient** les différents **composants** à la **carte mère** et assurent donc une bonne et rapide **communication** au sein de l'ordinateur.

- **Carte graphique** : c'est grâce à elle que s'affichent tous les **éléments graphiques** : photos, vidéos, jeux… car elle permet de produire une **image sur un écran**.

- **Carte son** : elle permet de **restituer des sons** venant de l'ordinateur ou d'**acquérir des sons** venant de l'extérieur.

- **Carte réseau** : c'est un ensemble de composants intégrés généralement sur la carte mère, elle permet à l'ordinateur de **se connecter sur un réseau** afin de **partager des données**.

- **Bloc d'alimentation** : il fournit du **courant électrique** à l'ensemble des **composants** de l'ordinateur.

- Exemples de **périphériques d'entrée** :

  -le **clavier** : il permet d'écrire

  -la **souris** : elle permet de déplacer un curseur sur l'écran

  -le **micro** : il permet de capter une source sonore

  -la **webcam** : elle permet de capter une source animée

- Exemples de **périphériques de sortie** :

  -l'**écran** : il permet de visualiser les informations venant de l'ordinateur

  -l'**imprimante** : elle permet de mettre sur différents supports des textes, des images… provenant de l'ordinateur

  -les **haut-parleurs** : ils permettent d'émettre des sons venant de l'ordinateur

- Exemples de **périphériques d'entrée-sortie** :

  -**lecteur de disque** : il permet de **lire** (et de graver pour certains donc d'**écrire**) des **données numériques** sur un disque optique (CD, DVD…). Même sur un ordinateur éteint, il peut être **ouvert mécaniquement** en insérant un **trombone** dans un trou non loin prévu à cet effet.

  -**lecteur disquette** : tout comme le lecteur de disque, le lecteur disquette permet de **lire** et d'**écrire** des **données numériques** sur des disquettes

  -**clé USB** (ou disque dur externe) : elle permet d'**enregistrer** et de **lire** des **données numériques**

- **Connexions** à l'ordinateur :

  -**ports USB** : ils permettent de **connecter** facilement des **périphériques** à l'ordinateur

  -**port VGA** : il permet de **connecter** un **écran** à l'ordinateur via la **carte graphique**

  -**prise micro** : elle permet de **connecter** un **microphone** à l'ordinateur via la **carte son**

  -**prise audio** : elle permet de **connecter** des **haut-parleurs**, des **écouteurs** ou un **casque** à l'ordinateur via la **carte son**

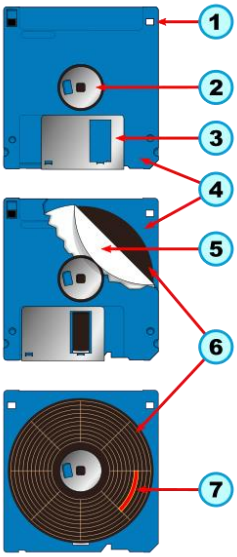
(*Librement adapté de pratique.leparisien.fr)*

<u>*Pour ma culture personnelle :*</u>

Voici à quoi ressemble une disquette, et si, si, je vous assure, ça a existé !

Légende :

1. *Indication de la taille de la disquette (ici, grande)*
2. *Hub (disque d'entrainement)*
3. *Cache (volet de protection amovible)*
4. *Coque en plastique*
5. *Disque de papier/tissus doux*
6. *Disque magnétique*
7. *Secteur d'une piste du disque*



Vue schématique d'une disquette

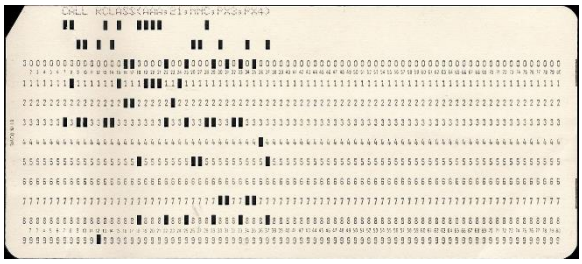
Wikimedia commons

Bases de données :

Une **base de données** (en anglais database), permet de stocker et de retrouver l'intégralité de **données** brutes ou d'informations en rapport avec un thème ou une activité ; celles-ci peuvent être de natures différentes et plus ou moins reliées entre elles.

Les premières bases de données étaient calquées sur la présentation **des cartes perforées** : réparties en lignes et colonnes de largeur fixe.

Une **carte perforée** est un morceau de papier rigide qui contient des informations représentées par la présence ou l'absence de trou dans une position donnée.



Carte perforée à 80 colonnes et 10 lignes
Wikimedia commons

Au début, le **mécanisme de lecture** des cartes perforées était très particulier. En effet, une aiguille passait en revue les lignes et colonnes de la carte. De l'autre côté de la carte, se trouvait un baquet rempli de mercure. Si l'aiguille touchait le mercure, un courant électrique transmis dans l'aiguille passait et fermait le circuit, ce qui indiquait la présence d'un trou.

Pour ma culture personnelle :

Les cartes étaient perforées par des opératrices spécialisées travaillant à partir de « bordereaux de saisie ». Les cartes étaient susceptibles d'être triées sur des machines appelées trieuses et interclasseuses. Les machines mécanographiques ont utilisé ces cartes jusqu'au remplacement des dernières de ces machines par des ordinateurs vers 1970. Les ordinateurs ont été équipés d'unités périphériques capables de lire et de perforer ces cartes jusqu'au début des années 1980.

Cartes perforées ? Simplification !

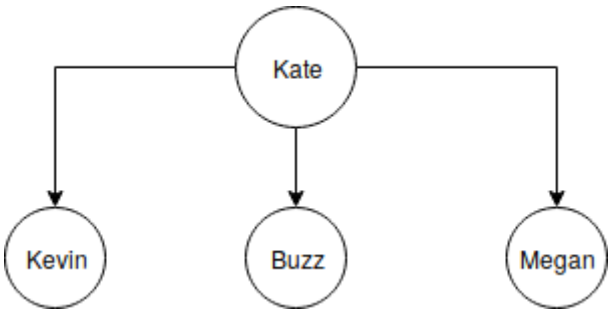
De manière simplifiée, nous pourrions imaginer un système où **chaque carte** représente **un élément** et toutes les cartes sont **perforées** pour chaque **propriété** possible. Cependant, le trou ne serait pas le même selon la **valeur** propre à l'élément pour chaque **propriété**. Si l'élément possède la propriété souhaitée, le trou est « **ouvert** », c'est-à-dire relié au bord de la carte, si ce n'est pas le cas, le trou est alors « **fermé** ». On pourrait ainsi utiliser des **aiguilles** pour faire une certaine **requête** : si l'on passe une aiguille dans le trou correspondant à la propriété testée pour le paquet de fiches en le soulevant, alors seules les fiches où l'élément possède la propriété sélectionnée tomberont (les autres resteront accrochées).

Exemple d'application de ce système par Marie Duflot-Kremer : pour trouver un plat à cuisiner lors d'une réception, chaque carte est un ami et chaque propriété est un plat que l'ami en question aime (trou ouvert) ou n'aime pas (trou fermé)

Les arbres

Un arbre est une **structure de données** qui permet de **hiérarchiser** les données. Par exemple, sur l'arbre ci-contre, Kate est la mère de Kevin, Buzz et Megan.

*Les **structures de données** sont un moyen de stocker et d'organiser des données pour faciliter leur stockage, leur utilisation et leur modification.*



Dans "Maman, j'ai raté l'avion", Kate est la mère de Kevin, Buzz et Megan

Propriétés des arbres :

-un **nœud** est un élément de l'arbre. Ci-contre, "Kate", "Kevin", "Buzz" et "Megan" sont des nœuds. Chaque nœud a un seul **parent**, sauf pour la racine ("Kate" ici)

-la **racine** est un nœud qui n'a pas de parent

-si le nœud P est le parent du nœud E, nous dirons alors que E est l'**enfant** de P

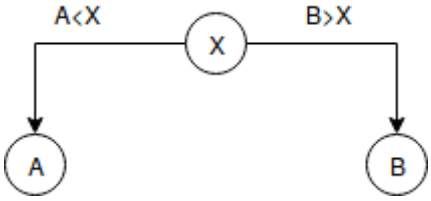
-une **feuille** est un élément de l'arbre qui n'a pas d'enfant. Dans notre exemple "Kevin", "Buzz" et "Megan" sont des feuilles.

-un **sous-arbre** est une partie d'un arbre. Sa racine est n'importe quel nœud autre que la racine de l'arbre.

Un arbre binaire de recherche ? Qu'est-ce que c'est ?

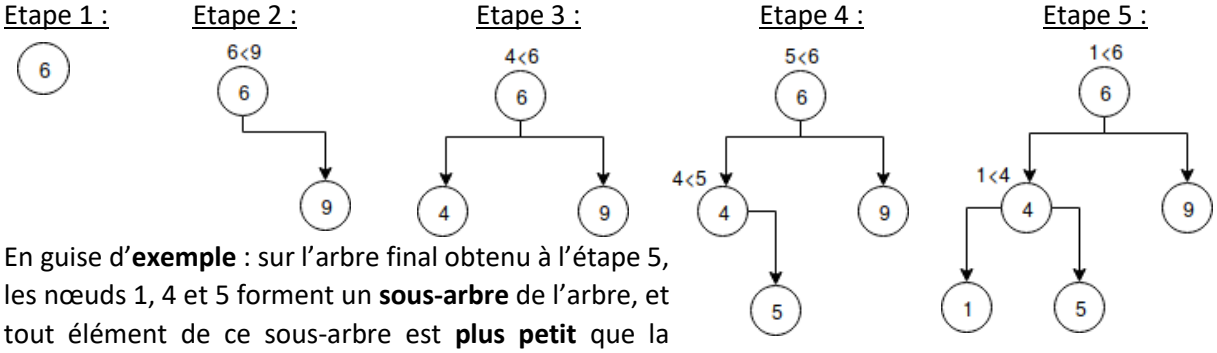
Dans un arbre binaire, **chaque nœud** a, **au plus**, **deux enfants** : un enfant à gauche et un enfant à droite.

Dans un arbre binaire de recherche, l'enfant à **gauche** d'un nœud (et tout élément d'un sous-arbre à gauche) est **plus petit** que ce nœud. L'enfant à **droite** d'un nœud (et tout élément d'un sous-arbre à droite) est **plus grand** que ce nœud.



Principe d'un arbre binaire de recherche

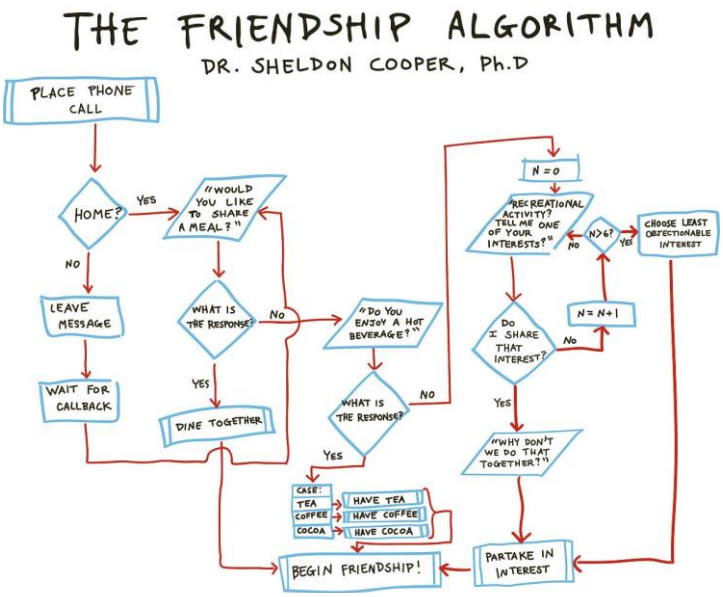
Exemple de construction d'un arbre binaire de recherche à partir de la liste ordonnée de nombres 6, 9, 4, 5, 1 :



En guise d'**exemple** : sur l'arbre final obtenu à l'étape 5, les nœuds 1, 4 et 5 forment un **sous-arbre** de l'arbre, et tout élément de ce sous-arbre est **plus petit** que la **racine** de l'arbre (6 ici) puisque le sous-arbre est à gauche de la racine.

L'algorithmique

Un algorithme est une **suite finie d'instructions** rédigée de manière **non-ambiguë** qui a pour but de **résoudre un problème**. Le processeur, par exemple, prend en entrée des instructions et les exécute, c'est ainsi que l'ordinateur fonctionne. C'est la **programmation** qui permet de passer d'un **algorithme** en pseudo-code à une **suite d'instructions** rédigée dans un langage que l'ordinateur peut **interpréter** après compilation, et donc, exécuter. Le mot algorithme vient du nom du mathématicien Al Khwarizmi (780-850 environ) qui a introduit la numérotation décimale et les calculs s'y rapportant. Les algorithmes sont étudiés afin de **réduire** leur **complexité en temps et en espace**, c'est-à-dire pour les **optimiser**.



Algorithme utilisant des conditions et des boucles
The Big Bang Theory

Une boucle est une **structure logique** qui permet d'**exécuter** une instruction ou un bloc d'instructions **de manière répétitive**. Il existe **deux types** de boucles, la boucle « **pour** » qui permet de répéter une instruction **un certain nombre de fois** et la boucle « **tant que** » qui permet de répéter une instruction tant qu'une **condition** est **vérifiée**, par exemple « tant que X<10 ». Un passage dans une boucle est appelé **itération**.

Une condition est une **structure de contrôle** qui **exécute** une instruction ou un bloc d'instructions **uniquement si** une certaine **condition** est **vérifiée**.

Pour ma culture personnelle, quelques notions en algorithmique :

Le pseudo code *est une manière informelle d'écrire un algorithme. Avec une structure algorithmique et un langage proche du langage courant, il permet d'écrire l'essentiel des instructions utiles à la résolution du problème.*

La compilation *est la transformation d'un programme écrit dans un langage de programmation lisible par un humain en un code binaire interprétable et exécutable par une machine.*

Algorithme récursif *: un algorithme est dit récursif s'il s'appelle lui-même. Le principe de la récursivité consiste à décrire les étapes nécessaires à la résolution d'un problème en utilisant la résolution du même problème sur des entrées plus petites.*

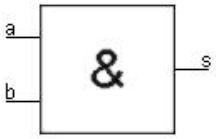
Le paradigme divisé pour régner *est une technique qui consiste en premier lieu à diviser le problème en plusieurs sous-problèmes puis à résoudre chaque sous-problème de manière individuelle et finalement à les combiner, c'est-à-dire calculer une solution au problème initial. Cette technique fournit des algorithmes très efficaces. On l'utilise dans le problème du tri d'éléments, dans la recherche dichotomique et elle convient généralement pour des problèmes à très grande complexité en temps et en espace.*

(Source : https://www.lamsade.dauphine.fr/~mayag/Chapitre_1_Introduction_Algorithmique.pdf)

Portes logiques

Un des fondamentaux de l'électronique numérique est ce qu'on appelle les « **portes logiques** ». Il s'agit d'**éléments électroniques simples**, prenant une ou plusieurs entrées en compte, et réalisant un calcul à partir de ces entrées. Le résultat est envoyé sur l'unique sortie. Ces calculs reposent sur la **logique dite booléenne**, du nom de son créateur Georges Boole.

La version schématique de ces portes logiques prend la forme suivante :



- Les lettres **a et b sont les variables d'entrée**, mais il peut y avoir une seule ou plusieurs entrées. Les entrées auront une valeur de 0 (aucun signal électrique) ou 1 (un courant électrique passe).
- Le **carré** représente le **composant électronique.** Au centre du carré, on va trouver un **symbole** correspondant au calcul fait par le composant. Ici, il s'agit du calcul nommé « ET » : s prend la valeur 1 uniquement si a = 1 ET b = 1.
- La lettre **s est le résultat** en sortie, d'une valeur 0 ou 1.
- Sur le trait de la sortie, il peut y avoir un **petit cercle collé au carré** : cela signifie qu'on inverse la valeur de sortie (nommé NON + le nom du calcul). Si pour un ET on a a = 1 et b = 1, s sera égal à 1 ; pour NON ET, s est inversé et prend la valeur 0.

On utilise généralement des **tables de vérités** qui indiquent pour chaque ensemble de valeurs en entrées les valeurs de sorties correspondantes.

Pour ma culture personnelle :

*Prenons un **exemple concret** : l'interrupteur d'une lampe. Si le courant passe, la lampe s'allume, s'il ne passe pas, elle reste éteinte. Imaginons que l'allumage de la lampe est géré par un système électronique et qu'il y a deux boutons qui doivent être activés en même temps pour allumer la lampe. Ces deux boutons sont reliés à une porte logique « ET » et cette porte ne laissera du courant passer (c'est-à-dire une valeur de 1) vers la lampe que si on appuie simultanément sur les deux boutons. Si un seul bouton est activé, la porte logique « ET » gardera comme valeur de sortie 0, c'est-à-dire qu'il n'y aura pas de courant, et la lampe restera éteinte.*

Adresses IP et routage

Sur un réseau local (par exemple celui de mon collège) ou sur le **réseau internet**, mon ordinateur (ainsi que les autres outils numériques comme mon téléphone) est **identifié** auprès des autres par **une adresse dite IP** (*Internet Protocol*), tout comme mon lieu d'habitation qui lui a une adresse postale. Cette adresse IP se présente **sous la forme de 4 nombres allant de 0 à 255**, séparés par des points : « X.Y.Z.W ». (Par exemple : 190.170.10.254)

Quand je vais sur Internet, mon ordinateur doit **se connecter à des serveurs,** qui vont héberger mon site Internet préféré par exemple, ou stocker mes mails. Ceux-ci ont également des adresses IP. Pour se connecter, **des « paquets » d'informations vont donc être envoyés vers une destination** (le serveur d'un site). Pour atteindre la destination, **les paquets vont être transférés au fur et à mesure, d'un élément informatique au suivant, par ce que l'on appelle des routeurs**, qui ont également une adresse IP.

Chaque routeur possède une **table de routage**, qui **répertorie** pour chaque adresse qu'il connaît

l'**adresse du prochain routeur** auquel transférer le message. Ainsi, le paquet ne passe pas toujours par le chemin le plus court ou le plus rapide, mais est redirigé au fur et à mesure suivant ce que chaque table de routage va lui indiquer.

Pour ma culture personnelle :

*Un **serveur** est un dispositif qui offre des services, comme par exemple l'utilisation d'une boîte mail, l'accès à un site internet. C'est à lui que l'ordinateur va se connecter pour accéder à ces services.*
*Quand une information est envoyée sur un réseau, elle est divisée en plusieurs **paquets**, qui seront de nouveau assemblés une fois arrivés au destinataire.*
*Un **routeur** est un équipement informatique qui va permettre de transmettre les informations pour qu'elles arrivent jusqu'à l'adresse de destination. Il va recevoir le paquet d'informations et l'envoyer à une autre adresse, d'un autre routeur par exemple, qui va à son tour envoyer l'information à une autre adresse, et ainsi de suite jusqu'au destinataire.*
*Pour savoir quelle est la prochaine adresse à laquelle le routeur doit envoyer l'information, il utilise ce que l'on appelle une **table de routage**. Dans celle-ci, pour chaque adresse de destination connue, il est indiqué l'adresse du prochain élément à qui envoyer l'information afin que celle-ci puisse arriver à destination.*