TP n°2 – feuilles de style, sécurisation des documents

Partie 1 – feuilles de style

Source : http://lemoigno.fr

Objectif : apprendre à utiliser les feuilles de style : la syntaxe de base, les styles contextuels, les classes de style, les divisions.

1. Les feuilles de style

Lorsque l'on réalise un ensemble de pages web, par exemple si on construit un site Internet, il est bien plus judicieux de séparer le contenu de la forme. La façon la plus « économique » de le faire est fournie par les **feuilles de style en cascade** (ou **CSS** pour Cascading Style Sheet). Ces feuilles CSS sont des fichiers munis de l'extension .css qui vont contenir toutes les indications de style (fond d'écran, fontes, couleurs, etc) tandis que le fond sera cantonné aux fichiers .html. En général, un fichier de style unique est utilisé pour toutes les pages d'un style: quand on veut changer celui-ci, il suffit de changer quelques lignes dans le fichier .css, sans toucher à tous les fichiers .html.

1.1. Principe

Pour indiquer à un navigateur que le style d'une page html sera donné dans une feuille css externe, il faut ajouter un lien vers cette dernière dans l'en-tête de la page html :

```
<head>
...
<link rel=stylesheet href=url du fichier de style type=text/css>
...
</head>
```

Il n'est pas nécessaire que la feuille de style soit dans le même répertoire que les pages html puisque son adresse est indiquée. On peut même en indiquer plusieurs, sous réserve qu'elles portent des noms différents (ceci peut être utile si l'on veut distinguer des styles différents pour l'affichage à l'écran, pour les mobiles, pour l'impression,...).

1.2. Syntaxe

La syntaxe CSS est assez simple :

```
nom_balise {
  propriété1: valeur;
  propriété2: valeur;
  ....
  propriétén: valeur;
}
```

Chaque bloc de style commence par le nom d'une balise HTML (body, h2, ul,...) suivie des propriétés de style qu'on veut donner au contenu de cette balise. Ces propriétés sont contenues entre deux accolades et se terminent par un point virgule (y compris s'il s'agit d'une propriété unique).

Remarque : même si ce n'est pas obligatoire, il est très recommandé de présenter les feuilles de style selon le modèle donné ci-dessus, en présentant une propriété par ligne: cela fait beaucoup pour la clareté de votre feuille de style...

1.3. Les principales propriétés

Ceci n'est qu'une liste partielle, qui permet tout de même d'obtenir une grande variété de styles. Les valeurs soulignées sont celles utilisées par défaut.

Attention, les noms de certaines propriétés sont proches du HTML mais pas identiques: par exemple background-image (css) est différent de background (HTML).

background-image : url du fichier image permet de spécifier une image de fond.
background-color : couleur permet de définir une couleur de fond.
border-style : dashed, dotted, double,groove, inset, outset, ridge, solid, none spécifie le style des bordures d'un élément. Attention: par défaut, cette propriété a la valeur none, c'est à dire qu'il n'y a pas de bordure.
border-width : largeur en pixel définit la bordure d'un élément.
border-color : couleur définit la couleur de la bordure.
color : permet de définir la couleur d'écriture du texte
float : right, left, none détermine si un élément (en particulier une image) flottera à gauche ou à droite du texte environnant.
font-family : permet de changer la police d'un texte
font-size : xx-small, x-small, small, medium, large, x-large, xx-large ou taille en pixels définit la taille de la police utilisée.
font-style : normal, italic permet de demander l'affichage du texte en italique.
font-weight : normal, bold permet de demander l'affichage du texte en gras.
height : hauteur en pixel, en pourcent, auto hauteur d'un élément.
liste-style-position : inside, outside dans un élément de liste qui s'étend sur plusieurs lignes, permet de garder l'indentation de la première ligne (valeur outside par défaut) pour les lignes suivantes ou limite l'indentation à la première ligne.
list-style-type : disc, circle, square, decimal, lower-alpha, lower-roman, none, upper-alpha, upper-roman définit les marqueurs ou puces des éléments des listes non ordonnées (circle, disc, square) ou ordonnées (decimal=chiffres, roman=chiffres romains ou alpha=lettres).
margin-left : largeur en pixel ou en % de la marge à gauche.
margin-right : largeur en pixel ou en % de la marge à droite.
margin-top : largeur en pixel ou en % de la marge en haut.
margin-bottom : largeur en pixel ou en % de la marge en bas.
padding(-left, -right, -bottom, -top) : cette propriété est analogue à la propriété margin mais indique l'écart entre un élément et son contenu. Les unités sont les mêmes que pour la propriété margin.
text-align : center, right, left, justify définit l'alignement horizontal du texte dans un élément.
text-decoration : line-through, none, overline, underline définit certains effets de caractères et permet d'obtenir du texte barré (line-through), souligné (underline) ou surligné (overline).
width : largeur en pixel, en pourcent, auto largeur d'un élément (exemple une image).

a:link : couleur du lien hypertexte à visiter (definir dans le css)
a:hover : couleur du lien hypertexte lorsqu'on passe la souris dessus (definir dans le css)
a:visited : couleur du lien hypertexte lorsque celui-ci a été visité (definir dans le css)
a:active : couleur du lien hypertexte au moment du clic souris sur le lien (definir dans le css)

Pour étudier l'effet de la propriété "float", ouvrez le fichier cassoulet.html que vous aurez copié dans votre arborescence. Ouvrir ce fichier avec Gedit et firefox. Complétez ce fichier en insérant l'image cassoulet.jpg au début du paragraphe, juste après la liste des ingrédients. Modifiez le fichier ouvert en Gedit (language html), sauvegarder et visualiser sur firefaox en actualisant la page.

Liez ce fichier à une feuille de style cassoulet.css que vous créerez (fichier Gedit) et dans laquelle vous définirez le style de l'image, en essayant en particulier les trois valeurs de "float".

Placez à présent l'image après le texte de ce premier paragraphe et testez à nouveau l'effet des différentes valeurs de float dans la feuille de style associée.

Complétez la feuille de style de façon à obtenir un aspect qui ressemble à l'image Cassoulet.jpg.

La spécification de la largeur d'un élément associée à des valeurs des marges particulières permet de centrer un élément: modifiez la feuille de style du document précédent pour centrer le tableau.

N'oubliez pas de sauvegarder votre fichier dans votre dossier TP2

1.4. Les styles contextuels

Il est également possible de définir le style d'un marqueur en fonction du contexte dans lequel ce marqueur apparaît. Par exemple, pour définir le style associé à un élément d'une liste non ordonnée (une puce en forme de cercle), on emploiera

```
ul li {
  list-style:circle;
}
```

si cette liste est elle-même un élément d'une liste non ordonnée, on souhaitera que la puce soit un carré et on ajoutera dans la feuille de style

```
ul ul li {
  list-style:square;
}
```

La suite ul ul li indique que le style est celui d'un élément de liste (li) d'une liste non ordonnée (ul) elle même élément d'une liste non ordonnée (ul).

Modifier la feuille de style liée au document précédent pour que les liens hypertextes apparaissent en vert foncé (darkgreen) si ils sont situés dans un élément de liste (li).

1.5. Les classes de style

Il est très souvent pratique de définir plusieurs styles pour un même marqueur (X)HTML, par

exemple de définir plusieurs style d'image (marqueur <img>) ou de paragraphe (marqueur <p>).
On différencie alors les marqueurs du document HTML par l'attribut class=nom où nom est choisi pour identifier une des classes associée à ce marqueur (ne pas mettre un chiffre ou nombre). Dans la feuille de style, on écrira alors :

```
nom_marqueur.nom_classe {
 ....
 style
 ....
}
```

On pourra par exemple dans son document HTML définir pour les paragraphes une classe résumé, une classe introduction, etc dont les styles seront indiqués dans la feuille de style par la succession :

```
p.résumé {
 ....
 style
 ....
}
p.introduction {
 ....
 style
 ....
}
```

Modifiez la feuille de style cassoulet.css et le document cassoulet.html pour définir un nouveau type de paragraphe : le paragraphe de type *note* devra être écrit sur fond jaune (background-color) avec une fonte x-small (font-size)et des marges à droite et à gauche de 60 pixels (margin). Appliquez ce style pour le dernier paragraphe commencant par « poser le plat... » de cassoulet.html.

2. Les divisions

2.1. Description

La balise HTML **div** permet de séparer un document en sections logiques, appelées **divisions**.
Une division est un conteneur, c'est à dire un élément qui peut en contenir d'autres.

Vous allez apprendre à utiliser cet élément, en conjonction avec les feuilles de style.

Remarque : la balise body est également un conteneur puisqu'elle peut contenir d'autres éléments comme des paragraphes, des titres... ou des div.

2.2. Bases

Copiez le fichier base.html dans le répertoire TP2. Ouvrez-le avec Gedit et avec votre navigateur firefox pour le visualiser.

Quatre sections DIV ont été faites dans le fichier, chacune contenant le même texte. Dans la fenêtre d'affichage du navigateur, les quatre paragraphes (identiques) apparaissent juxtaposés, sans distinction : les divisions n'ont pour l'instant, aucun aspect particulier.
Pour appliquer des styles de mise en forme aux divisions, vous allez utiliser une feuille de style dont vous connaissez à présent le maniement.

Pour cela, liez le fichier base.html à une nouvelle feuille de style base.css que vous créerez avec Gedit.

Pour visualiser les quatre divisions, identifiez chacune d'entre elle par un nom de classe particulier (un, deux, trois et quatre respectivement) puis, dans la feuille de style, donnez-leur une couleur particulière. Vous donnerez également la couleur « dimgray » au corps de la page html (grâce à la feuille de style).

Quelle est la taille (largeur, hauteur) par défaut d'une division ?

Comment les divisions évoluent-elles quand on module la taille de la fenêtre du navigateur?

En utilisant des valeurs négatives pour les marges à droite et à gauche sur une des quatre divisions, trouvez la largeur par défaut (à gauche et à droite) de la marge en pixels.

Par défaut, le contenu du DIV est collé à ses bords: la propriété **padding** permet d'espacer le contenu avec les bordures d'un DIV, mais aussi d'autres conteneurs (comme body).

Faîtes apparaître un écart du contenu avec les bords de divisions de 5 pixels à gauche et à droite et de 3 pixels en haut et en bas.

Autour de la troisième division (celle identifiée par class=trois), créez une bordure solide, noire, de largeur 2px. Que constatez-vous?

Dans chaque DIV, mettez le texte entre les balises et : quel est l'effet produit lorsque vous visualisez la page Web ? Conclusions ?

Après vos modifications vous devez avoir un aspect qui ressemble à l'image base.jpg

N'oubliez pas de sauvegarder votre fichier dans votre dossier TP2

3. À retenir

Les feuilles de style servent à séparer le contenu (inscrit dans le fichier (X)HTML) et la forme, qui est contenue dans le fichier de style.
Elles sont particulièrement utiles pour homogénéiser le style donné à plusieurs pages HTML. Elles facilitent également la maintenance de ces pages (par exemple, celles qui forment un site Web) car il suffit de la modifier pour modifier instantanément le style de toutes les pages liées à la feuille de style.
Les divisions permettent de définir des conteneurs flottants, dont l'agencement souple permet d'améliorer le rendu des sites Web.

Partie 2 : site web et contrôle continu n°1

Le premier contrôle continu de cette unité d'enseignement consiste à réaliser un site web mettant en œuvre les techniques vues lors des TP 1 et 2 (sans vous y limiter !) et présentant les travaux que vous avez produits lors des différents TP. Il sera déposé sur le dossier public_html de votre répertoire personnel (voir TP n°1) et sera rendu lors de la dernière séance de TP.

Vous pouvez commencer dès maintenant !

Partie 3 : sécurisation des informations (à lire uniquement)

Les fichiers informatiques sont duplicables, modifiables, altérables par un individu ou un système informatique, soumis à la fragilité de leur support et souvent accessibles par un réseau. Il est nécessaire de sécuriser les informations numériques en les sauvegardant, en protégeant leur accès et en les communiquant de manière sécurisée.

Créer un fichier texte intitulé « reponses_tp_2_partie_3 » que vous remplirez avec les réponses aux questions de cette partie.

1. Sauvegarder

1.1. Archivage électronique et compression

L'**archivage électronique** est synonyme de stockage ou de sauvegarde. Trois critères principaux caractérisent un bon archivage :
- la **fidélité** des données sauvegardées par rapport aux données initiales ;
- la **robustesse** du dispositif de sauvegarde : quelle est la durée de vie du support matériel ? Des sauvegardes ont-elles été faites sur plusieurs dispositifs ?
- la **sécurisation** des fichiers archivés face aux tentatives d'accès extérieures

Rechercher sur Internet la durée de vie moyenne d'un DVD, d'une clé USB, d'un disque dur. Selon vos recherches, quel est le support le plus fiable ?

La plupart des logiciels d'archivage offrent une fonctionnalité de **compression** , qui permet d'obtenir une archive d'une taille inférieure aux documents initiaux. Certains logiciels permettent en plus de protéger l'accès au contenu de l'archive par un **mot de passe**.

Parmi les formats suivants, lesquels sont des formats compressés ? .txt .doc .odt .raw .png .jpg (effectuer une recherche sur Internet).

Ouvrir un gestionnaire de fichiers puis lancer le logiciel d'archivage par défaut en effectuant un clic droit sur l'icône d'un dossier. Afficher toutes les options d'archivage.

Parmi les formats d'archivage proposés, lesquels sont propriétaires ? Lesquels vous permettent de protéger votre archive par un mot de passe ? De protéger aussi la liste des fichiers archivés ? Selon vous, à quoi sert-il de « découper » l'archive en plusieurs fichiers de même taille comme certains formats le proposent ?

Réaliser une archive compressée de votre dossier en la protégeant par un mot de passe, puis la décompresser dans un autre dossier.

1.2. Espace personnel de l'ENT

Votre ENT présente un outil de stockage vous permettant d'accéder à vos documents depuis tout ordinateur connecté à Internet (Onglet espace personnel, Espace de stockage).

Dans cet espace, créer un dossier HLSE305 dans lequel vous placerez vos fichiers de travail.

1.3. Logiciels de sauvegarde

Parmi les supports permettant la sauvegarde d'informations numériques, on citera :
- les supports **locaux** : clés USB, disque-dur externe, carte SD notamment ;
- les supports **distants**, sur Internet (« clouds ») ou un autre espace accessible par le réseau.

La sauvegarde s'effectue soit par le biais de l'utilisateur, soit par un **logiciel de sauvegarde automatique**, qui effectue des sauvegardes régulières de fichiers et dossiers choisis par l'utilisateur sur un support donné. Certains de ces logiciels utilisent la **sauvegarde incrémentale**, d'autres la **synchronisation des supports** ou le **versioning**.

Rechercher sur Internet la signification de sauvegarde incrémentale, synchronisation de supports et versioning, puis citer des logiciels sous licence libre proposant ces fonctionnalités.

Rechercher sur Internet un exemple récent de piratage d'informations depuis un espace de stockage sur Internet (« cloud »).

2. Protéger l'accès à ses informations

2.1. Gestion des droits d'accès

Source : http://lemoigno.fr

Un **système de protection sur les fichiers** permet d'en contrôler l'accès. On va apprendre à utiliser ce système sous Linux, principalement par l'interface graphique.

Interface graphique :

Créez un fichier Test.txt sur votre bureau, faites un clic droit dessus et choisissez Propriétés dans le menu déroulant. Enfin, sélectionnez l'onglet Droits d'accès dans la boîte de dialogue.

Plusieurs informations sur le fichier sont disponibles :
- Les **groupes** : Un utilisateur peut appartenir à un ou plusieurs groupes, par exemple un groupe qui contient seulement l'utilisateur, un groupe qui contient tous les utilisateurs de la même promotion, un groupe qui contient uniquement les utilisateurs pouvant accéder à la carte son des machines...
- Le **groupe d'un fichier** est un des groupe des son propriétaire (par défaut, celui que le propriétaire avait au moment de sa création). On peut toutefois changer le groupe d'un fichier en un autre groupe auquel appartient son propriétaire. Cela sera détaillé dans la partie suivante.
- Dans le cadre **Appartenance**, le nom du propriétaire du fichier, normalement vous-même, ainsi que le nom du groupe auquel appartient le fichier, qui est par défaut le groupe de son propriétaire au moment de la création.
- Dans le cadre **Droits d'accès**, les droits accordés au propriétaire, aux utilisateurs de même groupe que celui du fichier, et à tous les autres utilisateurs. Ces droits sont modifiables par l'intermédiaire de menus déroulants.

De façon générale, les droits accordés aux utilisateurs sont de trois types :

Lecture : pour un fichier, pouvoir le lire, et pour un répertoire, pouvoir voir et lister son contenu.
Écriture : pour un fichier, pouvoir écrire dedans, et pour un répertoire, pouvoir effacer ou créer des fichier ou sous-répertoire dans ce répertoire.
Exécution : pour un fichier, l'exécuter, si c'est un programme exécutable, et pour un répertoire, pouvoir le traverser pour accéder à des sous-répertoires.

Pour approfondir : Il existe trois autres types de droits : les droits spéciaux qui permettent, sommairement, deux types de permissions supplémentaires : pouvoir accorder des droits particuliers à un fichier exécutable le temps de son exécution (droits SUID et SGID) et n'autoriser la suppression d'un fichier qu'au propriétaire de celui-ci (droit 'sticky'), alors qu'habituellement ce droit appartient au propriétaire du répertoire contenant le fichier à effacer.

À l'aide de la souris, on peut modifier une partie de ces droits. Un contrôle plus précis peut se faire en mode ligne de commande.

Les 5 questions suivantes sont à faire en changeant les droits du Propriétaire des fichiers et répertoires considérés.

Supprimez le droit d'écriture du fichier Test.txt. Ouvrez celui-ci avec un éditeur de texte et essayez d'écrire quelque chose dans le fichier et de sauvegarder.

Rétablissez les droits d'écriture de Test.txt et écrivez quelques lignes dans ce fichier. Supprimez ensuite le droit de lecture (Interdit dans le menu déroulant) et essayez d'ouvrir le fichier.

Dans votre répertoire personnel, créez un répertoire Photos, dans ce répertoire, créez un fichier texte Paysage et un sous-répertoire Vacances.

Supprimez le droit d'écriture (modifier le contenu) sur le répertoire Photos. Essayez de supprimer le fichier Paysage. Essayez de créer un fichier Montagnes dans le répertoire Photos. Rétablissez le droit d'écriture sur le répertoire Photos.

Supprimez le droit de lecture (voir le contenu) du répertoire Photos et essayez d'accéder à son contenu. Rétablissez le droit de lecture ; en cas d'impossibilité, vous pouvez le faire en ligne de commande : chmod u+r Photos

Un bref aperçu de la ligne de commande

En utilisant des instructions en ligne de commande, il est possible de gérer plus finement les droits que précédemment. On peut alors utiliser les droits pour sécuriser certaines parties d'un répertoire personnel et en laisser d'autres accessibles aux autres utilisateurs. Voici un survol des commandes permettant de gérer les droits d'accès.

id : donne des renseignements sur votre identifiant et le numéro d'utilisateur associé, sur votre groupe et le numéro de groupe associé ainsi que la liste des groupes auxquels vous appartenez (possiblement qu'un seul pour l'instant...) : essayez-la !
ls -l (deux fois la lettre L) : affiche la liste des fichiers et des dossiers du répertoire courant, accompagnés de leurs droits d'accès. Un droit d'accès est représenté par dix caractères, correspondant au type de fichier (principalement - pour un fichier 'normal', d pour un répertoire), les droits de l'utilisateur : r ("read") pour la lecture, w ("write") pour l'écriture et x ("execute") pour l'exécution, les droits du group et les droits des autres utilisateurs. Essayez-la !

```
[bessy@maloya ~/Photos]$ ls -l
total 2
-rw-r--r--+ 1 bessy info 0 aoû 28 14:52 Paysage
drwxr-xr-x  2 bessy info 3 aoû 28 12:05 Vacances
 u g o
```

chown : change le propriétaire d'un fichier
chgrp : change le groupe d'appartenance d'un fichier
chmod : change les droits d'accès d'un fichier
umask : change les droits d'accès donnés à un fichier lors de sa création

Remarques :
- pour plus de détail et d'expérimentation sur ces commandes, vous pouvez consulter le TP n°3 du site http://lemoigno.fr .
- dans un site web, les règles d'accès aux sous-dossiers du site sont gérées par un fichier nommé « .htaccess », placé à la racine du site sur le serveur.

2.2. Chiffrage

« Je n'ai rien à cacher » : Si on vous parle de chiffrer vos mails ou vos données, comme beaucoup de gens vous répondrez « je n'ai rien à cacher » ou « il serait étonnant que la NSA s'intéresse au contenu de mon ordinateur ». Vous avez raison, vous ne risquez probablement pas grand-chose, du moins dans l'état actuel des lois. Mais êtes-vous certains que vos contacts (famille, amis, relations, …) ne soient pas « intéressants » pour des services de renseignements publics ou privés ? Le copain de lycée qui travaille maintenant pour une entreprise sensible, votre cousin journaliste qui enquête sur une affaire de corruption, par exemple ? Ils ont beau de leur côté prendre beaucoup de précautions, si vous leur envoyez des mails en clair ou des documents non cryptés, ceux qui le souhaitent pourront y avoir accès, les lire et éventuellement localiser votre interlocuteur. En clair, en vous protégeant, c'est en fait les autres que vous protégez.

Panneau à l'entrée d'une réserve africaine : il demande aux visiteurs de désactiver le GPS de leur appareil photo ou téléphone car l'exploitation des méta-données des photos permet aux braconniers de repérer les lieux où se trouvent les rhinocéros.

Il existe plusieurs façon de chiffrer ou de signer ses données : nous utiliserons ici exclusivement le **chiffrement par clefs asymétriques**. Cette méthode utilise une paire de clefs, c'est à dire deux très grands nombres, aux rôles différents :

- la **clef publique**, distribuée largement, permet de passer du message en clair au message chiffré (mais pas l'inverse)
- la **clef privée**, qui doit rester secrète, permet de retrouver, à partir du message chiffré, le message en clair.

Comment fonctionne le chiffrement/ la signature par clés asymétriques ?

Jean-Claude a généré une paire de clefs (publique/privée) au moyen du logiciel gpg. Il met sa clé publique à disposition de ses correspondants : sur son site web, en signature de ses mails ou sur un serveur de clés publiques. Les correspondants peuvent alors chiffrer les messages ou les fichiers confidentiels destinés à Jean-Claude à l'aide de la clef publique : seul Jean-Claude pourra déchiffrer le mail ou le fichier grâce à sa clef privée (qu'il est le seul à détenir).

Comment générer une paire de clef ? **(uniquement pour les étudiants motivés)**

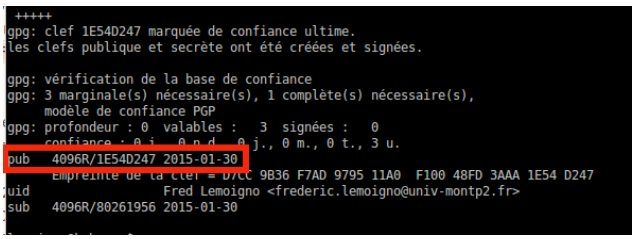
On utilisera le logiciel libre gpg (pour GnuPG) qui est une implémentation du standard OpenPGP.

Ouvrez un terminal et tapez : `gpg --gen-key`

Le programme vous demande d'abord quel type de clef vous souhaitez créer : choisissez une paire de clefs RSA (choix par défaut). Vous devez choisir la longueur de votre clef, entre 1024 et 4096 bits. Une clef longue est plus difficile à casser mais aussi plus longue à créer (plusieurs minutes). Vous pouvez vous contenter de 1024 bits. Après avoir renseigné le nom, l'adresse mail et le commentaire attachés à ces clés puis vérifié votre saisie, vous devez saisir une phrase de passe. C'est ce qui vous permettra d'autoriser l'utilisation de votre clef puis, plus tard, de la modifier ou la révoquer. Choisissez une phrase simple facile à mémoriser. Attention, pour des raisons de sécurité, aucun caractère n'apparaît quand vous tapez votre phrase.

Maintenant, le système va créer votre clef. Vous allez voir un message apparaître, indiquant qu'il cherche à « obtenir suffisamment d'entropie » pour générer des nombres aléatoires. Il vous invite donc à taper (n'importe quoi) sur le clavier ou à bouger la souris… Si vous ne touchez à rien, le système vous rappellera à l'ordre !

La génération d'une clef peut prendre plusieurs minutes. À la fin, l'écran va afficher les identifiants de la paire de clefs créée. Vous trouvez entre autres (cadre rouge) le type de la clef et sa longueur (4096R) ainsi que son identifiant (1E54D247) et sa date de création (30 janvier 2015).



> **Remarque :** Toutes les informations relatives à la paire de clefs créée sont à présent stockés dans les fichiers du répertoire (caché) .gnupg.

A présent, vous devez exporter votre clé publique en format texte pour la diffuser :

```
gpg --output maclef.asc --armor --export identifiant_clef
```

et vous obtiendrez un fichier lisible nommé maclef.asc.

Chiffrer un fichier

Commencez par noter l'identifiant de votre clef publique en listant celles qui sont présentes sur votre système (« anneau ») : `gpg --list-keys`

Tapez ensuite `gpg --encrypt xxx.pdf` : le programme vous demande l'identité de la clef publique à utiliser.

Listez ensuite le répertoire courant contient un fichier xxx.pdf.gpg. C'est le fichier chiffré. Le fichier ne sera lisible que si vous le déchiffrez avec la clé privée : `gpg --output --decrypt xxx.pdf.gpg` Cette commande va vous demander votre phrase passe et créer un fichier xxx-decrypt.pdf .

Vérifiez que ce nouveau fichier est parfaitement lisible.

Exercice récapitulatif : en utilisant la clef publique d'un de vos voisins, crypter le fichier xxx.pdf et envoyez le lui. En retour,il vous enverra le même fichier crypté en utilisant votre clef publique. Vérifiez que ce fichier est illisible en l'état puis déchiffrez-le et essayer à nouveau de le lire.

> **Remarque :** C'est le même principe qui sera utilisé au SIF pour accéder à d'autres types d'infirmation (Git, espace projet, etc). Il suffit de taper à la racine de son autohome : `ssh-keygen -t rsa`

3. Communiquer de manière sécurisée

3.1. Échanges sur le web : norme https

Les adresses web sont précédées d'un préfixe :
http pour les sites web non sécurisés,
https pour les sites web sécurisés (en général, un élément sur le navigateur indique si le site est sécurisé : icône de cadenas, ou bien coloration de la barre d'adresse) ; ce système de sécurité permet d'encoder les données transmises avant transmission, et de décoder les données reçues. Ainsi, les données ne circulent pas en clair entre votre ordinateur et le serveur du site web sécurisé.

Si vous devez saisir des données sensibles, vérifiez que le site web est sécurisé.

Attaque de l'homme du milieu : (source : Wikipédia) partant du principe que les internautes précisent rarement le type de protocole dans les URL (le protocole HTTP étant sélectionné par défaut) et se contentent de suivre des liens, un chercheur en sécurité informatique, connu sous le pseudonyme de Moxie Marlinspike, a développé une attaque du type Attaque de l'homme du milieu (« Man in the middle » en anglais), afin de contourner le chiffrement de HTTPS. Le pirate se positionne entre le client et le serveur et change les liens https: en http:, ainsi le client envoie ses informations en clair via le protocole HTTP et non HTTPS. Ce type d'attaque a été présenté par Marlinspike à la Blackhat Conference 2009. Durant cette conférence, Marlinspike a non seulement présenté le fonctionnement de l'attaque, mais également quelques statistiques d'utilisation. Il a réussi à récupérer plusieurs centaines d'identifiants, informations personnelles et numéros de cartes bancaires en 24 heures, aucune personne ne se doutant de l'attaque en cours.

3.2. Chiffrement des messages électroniques

Le chiffrement des messages électroniques utilise le système de clefs asymétriques présenté au paragraphe 2.2. Une fois le logiciel de messagerie configuré avec la paire de clefs, le chiffrement et déchiffrement de messages est transparent pour l'utilisateur. Il est à noter qu'un nombre croissant de fournisseurs de messagerie proposent un chiffrement des échanges de mail par le protocole sécurisé SSL ou TLS.

3.3. Un outil sécurisé de partage de texte : framabin

Il peut arriver que vous ayez besoin de partager des informations sensibles sans vouloir passer par la voie du courrier électronique. Framabin est un service en ligne sous licence libre qui permet de partager des textes de manière sécurisée. La différence par rapport à d'autres éditeurs collaboratifs est que le document est chiffré sur le serveur et que seuls les utilisateurs possèdent une clé de déchiffrement.

Essayez-le !