

# Le fonctionnement d'iPod et d'iTunes

Projet proposé par Céline Chevalier

`celine.chevalier@ens.fr`

L'objet de ce projet est de comprendre le fonctionnement des deux logiciels phares d'Apple, et en particulier l'encodage de la musique au format AAC, ainsi que la protection cryptographique par les DRM FairPlay.

La possibilité est offerte de se concentrer sur le format MP3 plutôt que l'AAC, mieux décrit dans la littérature. Le principe de l'encodage MP3 repose sur l'utilisation de la transformée de Fourier discrète, ainsi que sur le codage de Huffman. Ces deux éléments seront étudiés, et pourront ensuite faire l'objet d'une implémentation. Vous pouvez consulter à ce sujet les pages :

[en.wikipedia.org/wiki/Advanced\\_Audio\\_Coding](http://en.wikipedia.org/wiki/Advanced_Audio_Coding)  
[www.commentcamarche.net/audio/mp3.php3](http://www.commentcamarche.net/audio/mp3.php3)  
[www.sebsauvage.net/comprendre/mp3](http://www.sebsauvage.net/comprendre/mp3)  
[computer.howstuffworks.com/mp3.htm](http://computer.howstuffworks.com/mp3.htm)  
[en.wikipedia.org/wiki/Mp3](http://en.wikipedia.org/wiki/Mp3)  
[en.wikipedia.org/wiki/Huffman\\_coding](http://en.wikipedia.org/wiki/Huffman_coding)

En ce qui concerne les DRM d'Apple, de nombreuses explications peuvent être trouvées à partir de l'adresse :

[en.wikipedia.org/wiki/FairPlay](http://en.wikipedia.org/wiki/FairPlay)

Il s'agit de bien comprendre le mode de fonctionnement, par exemple à l'aide d'un schéma récapitulatif, et d'étudier les schémas cryptographiques sous-jacents (la distribution de clés, le chiffrement AES ainsi que la fonction de hachage MD5).