FICHE DE REVISION
Sécurisation des communications

Ce qu'il faut savoir

- connaître le principe du chiffrement symétrique => utilisation d'une clé de chiffrement privé partagée par les 2 interlocuteurs. Utilisation de la fonction XOR bit à bit pour chiffrer (et déchiffrer un message) à l'aide d'une clé (voir le cours).
- connaître le principe du chiffrement asymétrique => utilisation d'une clé publique et d'une clé privée. Seule la clé publique est diffusée (voir le cours). A chiffre un message à l'aide de la clé publique de B puis envoie ce message chiffré à B, B utilise sa clé privée pour déchiffrer le message envoyé par A (voir le cours).
- connaître le principe du protocole HTTPS => utilisation du chiffrement asymétrique pour partager une clé K puis utilisation du chiffrement symétrique (utilisation de la clé K) afin de chiffrer les données qui transitent sur le réseau (voir le cours)

Ce qu'il faut savoir faire

Dans le cadre du chiffrement symétrique, vous devez être capable de chiffrer et déchiffrer un message à l'aide d'une clé => utilisation de la fonction XOR bit à bit (voir le "À faire vous-même 1")

ATTENTION : La lecture de cette fiche de révision ne remplace en rien l'étude approfondie du cours (lecture attentive + résolution des exercices proposés). Cette fiche a uniquement pour but de vous donner des points de repère lors de vos révisions.