TD 1 — Codage de l'information

Exercice 1 — Changement de base

Q. 1.1 Convertir en nombres décimaux les nombres binaires suivants : 11, 1101, 100101110.
Q. 1.2 Convertir en nombres binaires les nombres décimaux suivants : 7, 51, 128, 131, 234.
Q. 1.3 Convertir en nombres binaires puis en nombres décimaux les nombres hexadécimaux suivants : 12, *DADA* et $5F3$.

Exercice 2 — Opérations binaires

On travaille dans cet exercice sur des entiers naturels codés sur un octet.

Q. 2.1 Quels sont les entiers naturels que l'on peut représenter sur un octet ?
Q. 2.2 Donner le résultat des opérations suivantes en binaire puis en décimal.
(a) $0001\ 0101_2 + 1011\ 0111_2$
(b) $0100\ 0111_2 + 1101\ 1001_2$
(c) 134_{10} **ET** 244_{10}
(d) 17_{10} **OU** 123_{10}
(e) **NON** 27_{10}
(f) 44_{10} **XOR** 157_{10}
Q. 2.3 Soit x un octet quelconque. Que vaut le résultat (en binaire ou en décimal) des opérations suivantes :
(a) x **OU** 255_{10}
(b) x **ET** 255_{10}
(c) **NON** x

Exercice 3 — Décalage binaire

Coder en binaire les nombres 26 et 52. Que remarque-t-on ? En déduire une méthode rapide pour multiplier ou diviser par 2^k un nombre binaire. Généraliser à une base B quelconque.

Exercice 4 — Jeu de cartes

On s'intéresse à des jeux de 52 cartes réparties en 4 couleurs (pique, cœur, carreau et trèfle) de 13 cartes désignées par leurs rangs (As, 2, 3, . . . , 10, Valet, Dame et Roi).

Q. 4.1 Proposer un schéma de codage binaire des cartes du jeu.
Q. 4.2 Donner, dans ce schéma, la représentation binaire du valet de trèfle.
Q. 4.3 On considère deux cartes dont les représentations binaires sont C_1 et C_2. Sous quelles conditions, ces deux cartes ont-elle la même couleur ? le même rang ? On utilisera l'opérateur binaire ET pour déterminer ces conditions.

Exercice 5 — Cryptage

Lorsque l'on envoie un message sur Internet et qu'on ne veut pas que ce message puisse être intercepté et compris par une personne autre que le destinataire on doit utiliser une méthode (ou un algorithme) de *cryptage*. Le principe général est d'altérer le message selon une méthode connue de l'émetteur et du récepteur et d'envoyer sur le réseau le message ainsi modifié. Bien entendu, seul le récepteur doit être en mesure de décrypter le message reçu pour retrouver le message initial, c'est-à-dire avant sa transformation par l'opération de cryptage.

Certains algorithmes de cryptage reposent sur l'utilisation d'une *clé* qui est une séquence de bits quelconque connue uniquement de l'émetteur et du destinataire du message. Le message crypté envoyé sur le réseau est obtenu en transformant le message initial à l'aide de cette clé (selon une méthode connue de l'émetteur et du récepteur) de même que le décryptage par le destinataire est obtenu en transformant le message crypté à l'aide de cette clé.

Un algorithme de cryptage très simple consiste à crypter le messsage en utilisant une clé c de 8 bits et en transformant chaque octet m du message par l'octet m **XOR** c. Le destinataire effectue la même opération : il transforme chaque octet m' qu'il a reçu par l'octet m' **XOR** c pour retrouver l'octet du message initial.

Cette méthode peut naturellement être généralisée pour une longueur de clé quelconque, et pas uniquement de 8 bits. Dans cet exercice, on s'intéresse au cryptage d'un texte codé en ASCII (donc avec des caractères codés sur 7 bits) à l'aide

d'une clé de 7 bits.

Q. 5.1 On veut envoyer le mot `yop`. Donner, à l'aide de la table ASCII donnée dans le cours, la séquence binaire correspondant à ce mot.

Q. 5.2 On utilise la clé 55. Quel sera alors le message envoyé après cryptage (en binaire et en texte) ?

Q. 5.3 Vérifier qu'après décryptage, le destinataire retrouve bien le message initial.

Q. 5.4 Prouver à l'aide d'une table de vérité que le destinataire peut toujours retrouver le message initial à partir de la clé et du message crypté.

Q. 5.5 En pratique, une longueur de clé de 7 bits est insuffisante. On utilise des clés d'au moins 32 ou 64 bits. Pourquoi ?