Université de Batna 2 **1ère Master CS**
Faculté des Mathématiques et de l'Informatique
Département d'informatique 2019/2020

Nom : **Prénom :**

Durée : 30 min Le 24/06/2020

INTERROGATION
CHIFFREMENT AUDIO

1. Dans l'entête d'un fichier wav (header) on trouve le paramètre NumChannels sur deux octets (22 et 23ème octets). Expliquer comment peut-on placer ces deux octets dans une variable de type (short int) en C++.

2. Dans la première série du TP nous avons utilisé cette instruction :
   fread(tab, 1, 44, myFile);
   Expliquer ce qu'elle fait.

3. Pourquoi nous avons utilisé la compression des fichiers audio ?

4. Dans la compression MP3 vue dans le cours, nous avons défini le filtre d'analyse MDCT comme suit :

$$h_k(n) = w(n) \times \sqrt{\frac{2}{M}} \times \cos\left[\frac{(2 \cdot n + M + 1) \times (2 \cdot k + 1) \times \pi}{4 \cdot M}\right]$$

   Que représente M ?

5. Dans l'algorithme de chiffrement DES on utilise une clé de 64 bits. Un certain nombre de bits de cette clé sont générés aléatoirement, quel est leur nombre ?

6. A quoi sert la fonction de planification KS (Key Schedule) ?

CORRIGER DE L'INTERROGATION
CHIFFREMENT AUDIO

1. Dans l'entête d'un fichier wav (header) on trouve le paramètre NumChannels sur deux octets (22 et 23ème octets). Expliquer comment peut-on placer ces deux octets dans une variable de type (short int) en C++.

Pour placer les deux octets dans un (short int) on utiliser le SHIFT et le OR comme suit :

```
NumChannels = (header[23] << 8) | (header[22]);
```

2. Dans la première série du TP nous avons utilisé cette instruction :
   fread(tab, 1, 44, myFile);
   Expliquer ce qu'elle fait.

Cette instruction permet de lire **l'entête** du fichier wav, de taille 44 octets, à partir de **myFile** et le placer dans le buffer **tab**.

3. Pourquoi nous avons utilisé la compression des fichiers audio ?

Pour accélérer la transmission des fichiers audio.

4. Dans la compression MP3 vue dans le cours, nous avons défini le filtre d'analyse MDCT comme suit :

$$h_k(n) = w(n) \times \sqrt{\frac{2}{M}} \times \cos\left[\frac{(2 \cdot n + M + 1) \times (2 \cdot k + 1) \times \pi}{4 \cdot M}\right]$$

   Que représente M ?

M est la moitié du bloc à traiter (La taille du bloc et 2M).

5. Dans l'algorithme de chiffrement DES on utilise une clé de 64 bits. Un certain nombre de bits de cette clé sont générés aléatoirement, quel est leur nombre ?

Parmi les 64 bits de la clé, **56 bits sont générés aléatoirement**, les 8 bits qui restent sont utilisés pour la détection des erreurs en vérifiant la parité (1 bit pour les 7 bits de chaque octet).

6. A quoi sert la fonction de planification KS (Key Schedule) ?

La fonction de planification KS permet de choisir 48 bits à partir de la clé de chiffrement pour générer **les 16 clés** qu'on utilise dans les 16 itérations de l'algorithme DES.