1 Le chiffrement de Vernam.

Cet algorithme, inventé en 1917 par Gilbert Vernam, s'appelle également algorithme du masque jetable ou « one time pad ». La clef k consiste en une suite de bits aléatoires, de même longueur que le texte en clair x. Le texte chiffré y est simplement la somme modulo 2, bit à bit, de x et k.

$$y = x \oplus k$$

On voit facilement que

$$x = y \oplus k$$

car $k \oplus k = 0$ et donc $y \oplus k = x \oplus k \oplus k = x$

En 1946, Shannon a démontré que ce système était le seul algorithme cryptographique à confidentialité parfaite et le seul qui soit donc rigoureusement incassable, mais à condition, comme l'indique le théorème, que chaque clef ne soit utilisée qu'une unique fois. Si tel n'est pas le cas, la cryptanalyse est possible. Par ailleurs, la clef doit avoir la même longueur que le texte chiffré et ne doit jamais être utilisée deux fois, ce qui provoque de très gros problèmes de gestion de clefs. C'est pour cette raison que ce protocole n'est pas tellement utilisé (il servit durant la guerre froide aux communications utilisant le téléphone rouge entre Washington et Moscou et est encore utilisé en diplomatie et dans l'armée).

1°. Ecrire un programme permettant de taper un texte au clavier (ou de le lire depuis un fichier texte), de générer une clef aléatoire, ainsi que le texte chiffré par la méthode du masque jetable.

2°. Effectuer l'opération inverse pour retrouver le message initial.

2 La méthode de chiffrement AES.

On se propose de mettre en œuvre l'algorithme de cryptographie à clef secrète AES.

AES (Advance Encryption Standard) est le nom générique de l'algorithme Rijndael inventé par Joan Daemen et Vincent Rijmen et qui remplace officiellement le DES depuis 2000. C'est le système de chiffrement à clef secrète le plus utilisé au monde aujourd'hui. Nous n'en rappelons pas tous les détails qui sont expliqués dans le diaporama et également dans le document « AES proposal : Rijndael ».

Le répertoire `TP2-AES` contient un fichier appelé `AES.c` dans lequel se trouve l'ensemble des fonctions et routines nécessaires au fonctionnement de l'algorithme AES. Il n'y a pas besoin de bibliothèque annexe et le programme est en mesure de compiler en l'état.

L'objectif de ce paragraphe est d'entrer une phrase tapée au clavier (ou de la lire depuis un fichier texte), de la chiffrer, puis de la déchiffrer selon l'algorithme AES. Votre travail consiste donc à modifier le programme principal pour y intégrer l'algorithme suivant :

```
saisie du texte en clair
choix de la taille de la clef
creation des clefs de rondes par expansion de la clef initiale
ajout initial de la clef secrète
pour i variant de 1 au nombre de rondes - 1
    brouillage par la S-boite
    décalage des lignes
    mélange des colonnes
    ajout de la clef de ronde
refaire
dernière ronde :
brouillage par la S-boite
décalage des lignes
ajout de la clef de ronde
affichage du bloc chiffré
```

Pour le déchiffrement, les opérations sont à faire en sens inverse, mais avec quelques petites différences. Voici l'algorithme :

```
ajout initial de la dernière clef de ronde
pour i variant du nombre de rondes - 1 à 1
    décalage inverse des lignes
    brouillage par la S-boite inverse
    ajout de la clef de ronde
    mélange inverse des colonnes
refaire
dernière ronde :
décalage inverse des lignes
brouillage par la S-boite inverse
ajout de la clef de ronde
affichage du bloc déchiffré
```

afin de simplifier le problème, nous considèrerons que le bloc chiffré et le bloc déchiffré ont une taille de 128 bits (l'algorithme originel propose 128, 192 ou 256 bits). On supposera également que la clef secrète initiale est donnée dans le programme (mais vous pourrez ensuite la générer de façon aléatoire, si vous le souhaitez).