Exercice 2 : chiffrement symétrique

Remarques :

- Les exercices sont attribués en fonction de l'ordre alphabétique de votre nom de famille
- Tous doivent être résolus « à la main » et les détails doivent apparaître lors de la remise de la solution

Enoncé :

Soit la clé K : (notation hexadécimale) `0 1 2 3 4 5 6 7 8 9 A B C D E F`
Soit le texte clair suivant (notation hexadécimale) :

```
[A-C] 0 1 2 3 4 5 6 7 8 9 A B C D E F
[D-F] 1 2 3 4 5 6 7 8 9 A B C D E F 0
[G-J] 2 3 4 5 6 7 8 9 A B C D E F 0 1
[K-N] 3 4 5 6 7 8 9 A B C D E F 0 1 2
[O-R] 4 5 6 7 8 9 A B C D E F 0 1 2 3
[S-Y] 5 6 7 8 9 A B C D E F 0 1 2 3 4
```

En utilisant l'algorithme du DES, il est demandé de:

1. dériver K_1 la première sous-clé
2. calculer L_0 et R_0
3. appliquer l'expansion sur R_0 pour obtenir $E[R_0]$
4. calculer $A = E[R_0]$ XOR K_1
5. grouper le résultat de 4. en ensemble de 6 bits pour évaluer les valeurs dans les S-Box correspondantes
6. concaténer les résultats obtenu en 5. pour obtenir B (sur 32 bits)
7. appliquer la permutation pour obtenir P(B)
8. calculer $R_1 = P(B)$ XOR L_0
9. écrire le texte chiffré obtenu (en hexadécimal)

Evaluation du temps nécessaire : +/- 1 heure