

1. a)  $0x80$  (hex)  $\approx 128$  (decimal)  
bits est une chaîne, on a besoin de trouver la valeur de bit à pos-ème.  
fonction  
retourne la valeur de bit qui est dans la pos-ème.  
ex:  
 $01001000$ ,  
**Ex:**  
 $00001000$  → begin de Récupérer  
« est l'opération décalage à droite  
**pos :**  $\approx$  pos-ème bit  
value 0 et 1, est - à - dire si la valeur qu'on récupère.  
2. a) cette fonction mettre la valeur "et" (1 ou 0) à la position  
pos-ème dans le char bit  
bit : le caractère  
pos : la position pos-ème  
est l'opération pos-ème dans le char bit  
return une chaîne avec la pos-ème valeur qui est change  
est l'opération à nouveau  
pos : la nouvelle effet  
return une chaîne avec la pos-ème valeur qui est change  
3. a) ~~non~~ Effectuer le XOR bit  $\oplus$  bit des deux températures  
bit : la valeur de bit dans les deux températures  
bit & 1 : même première température  
bit & 2 : dernière température  
bit & 1 = bit & 1  $\oplus$  bit & 2 (le résultat d'opération)  
4. a) Rétention du tempér avec le nom de fois très peu de goutte.  
bit : la quantité de bit dans deux températures  
bit & 1 : fois  $\approx 2 \rightarrow 0001$ .  
b) faire : • quantité de bit

Chiffre à crypter

Chiffre

TL2

exo 1

2. Le code suivant est de décataloger le marchandise gauche à partir d'un  
poids réel et la valeur unitaire pour une quantité de 40000000.
- Le code applique ce code, la position de 811 est décatalogue vers la position finale
- ce qui aide à récupérer la valeur de bit ~~de~~ de bits.
1. Des - transform : La matrice dans la première étape consiste en une permutation
- (CQ - L) afin d'obtenir une clé d'une longueur de 56 bits.
- Des - transform : Des - transforme dans la première étape consiste en une permutation
- qui correspond à une permutation de deux positions qui coïncident
- Des - rotation [16] : décalage à gauche de une ou deux positions qui coïncident
- Des - transform [64] : chaque sonde (Fst sonde) → (1ère sonde) → (2ème sonde) → ... → (64ème sonde)
- Des - initial [64] : à la permutation initiale
- Des - expansion [32] : sur un bloc de 32 bits, dans l'étape de permutation, on a 32 bits du bloc en tête et renvoie un bloc soit de 48 bits, dans l'étape de permutation, il faut remplacer les 48 bits tout simplement par 32 bits eux-mêmes avec des décalages et des décalages eux-mêmes.
- Des - Sbox : apporte puissance des - Sbox, le bloc de 32 bits obtenu est décalé à une permutation P.
- Des - Mix : A la fin de 16 rondes, les 2 blocs L16 et R16 sont soumis à la permutation ~~mix~~ initiale inverse
- Des - Final : A la fin de 16 rondes, les 2 blocs L16 et R16 sont soumis à la permutation P.