Exercice 1. On considère le cryptogramme de César récursif. La procédure de chiffrement est la suivante : notons $m_1, m_2, \cdots, m_n, \cdots$ les lettres du message avec la correspondance usuelle entre lettres et entiers modulo 26 : $A = 0, B = 1, \cdots, Z = 25$. La clé est une lettre K. Le message chiffré est alors donné par les lettres $c_1, c_2, \cdots, c_n, \cdots$ avec $c_1 = m_1 + K$ et pour $i \geq 2, c_i = m_i + c_{i-1}$.
1. Chiffrer le message "MESSAGE" avec la clé "C".
2. Déchiffrer le message "PNAAMUKEI" chiffré avec la clé "M".
3. Que peut-on dire de la sécurité de ce cryptogramme ? Le comparer au cryptogramme de César.
4. Proposer une attaque de ce cryptogramme.

Exercice 2. Effectuer les opérations suivantes dans le corps A.E.S.
1. $EF + 39$.
2. $C1 \times 12$.
3. Calculer l'inverse multiplicatif de l'octet 11110110 et de 00110001.
4. Appliquer SubBytes à l'octet (00001001).

Exercice 3. Exécuter à la main le chiffrement DES pour le texte clair en hexadécimal suivant : 0123456789ABCDEF, la clé K est identique au texte clair.
1. Donner le texte après la permutation initiale
2. Donner la valeur de K_1
3. Donner le bloc gauche G_0 et droite D_0
4. Donner le bloc D_0 après expansion
5. Donner le bloc G_1
6. Donner le bloc D_1.

Exercice 4. On suppose que les 56 sous-clés de I.D.E.A. soient toutes les mêmes. Montrer que tous les bits de la première sous-clé ont la même valeur. En déduire que tous les bits de la clé ont la même valeur.