TD 6

Exercice 1 : Cypher Block Chaining

2. Non, car la redondance statistique sera éliminée par le XOR. EN revanche, on peut plus facilement retrouver la clé.
3. Le key Scheduling est un algorithme qui permet de générer une suite de clés à partir d'une clé de départ. Il est utilisé pour le chiffrement et le déchiffrement.
4. En voyant des mots similaires, on peut trouver une redondance.
5. Si $m_2 = m_3$, alors $c_3 = c_1$ car
   $c2 = Fk(m2)$ XOR $c1$
   $c3 = Fk(m3)$ XOR $Fk(m2) XOR c1 = c1$

Exercice 2 : RSA

1. 15^3 mod 187 = 9
2. $X^2 - (p+q)X + pq = 0$
   $(p-1)(q-1) = 160$ donc $p + q = 28$
   Donc $X = (p+q)/2 \pm sqrt((p+q)^2/4 - pq)$
   $p = 11$ et $q = 17$