Corrigé CI_SEC

Partie QCM (sujet 1)

1. Rijndael est : **A**,
2. **A, B**.
3. **D**.
4. **A**.
5. **C**.
6. **A**.
7. **B**
8. **B.**
9. **B**
10. **B, C**.
11. A
12. C
13. B
14. A, D

Partie QCMt(sujet 2)

1. Quel est : **C**,
2. **C**.
3. **A, B**.
4. **B**.
5. **A, D**.
6. **A**.
7. **A**
8. **B.**
9. **D**
10. **B**.
11. **A**
12. **B, C**
13. **B**
14. **A.**

Questions

1. **L'ingénierie sociale** est une technique utilisée par les cybercriminels qui consiste à inciter les gens à partager leurs informations confidentiels. Une pratique de manipulation psychologique à des fins d'escroquerie. (phishing)
   - *92 % des logiciels malveillants sont transmis par e-mail* ?

2.1. Alan Turing : Mathématicien britannique considéré comme le père de l'ordinateur et Pionnier de l'intelligence artificielle. Il a joué un rôle important dans la victoire des alliés sur les allemands durant la deuxième guerre mondiale, il a conçu la machine Kolossus qui déchiffra les codes d'ENIGMA.

2.2. Feistel : Horst Feistel a conçu en 1971 l'algorithme de chiffrement **Lucifer** qui est devenu par la suite DES après quelque modifications du NSA.

2.3. Serpent : Un des cinq finalistes de l'appel d'offre du NIST pour l'AES.

2.4. ENIGMA : Machine pour crypter l'information conçue par les allemands durant la deuxième guerre mondiale. Cette machine a permis aux allemands plusieurs victoires jusqu'à l'arrivée du KOLOSSUS de Turing

Exercice Multiplication dans GF (2^8) de {57}*{83}

57 = 01010111 $P(x)_{57} = x^6 + x^4 + x^2 + x + 1$

83 = 10000011 $P(x)_{83} = x^7 + x + 1$

$$\begin{array}{rr} & x^6 + x^4 + x^2 + x + 1 \\ \times & x^7 + x + 1 \\ \hline & x^6 + x^4 + x^2 + x + 1 \\ & x^7 + x^5 + x^3 + x^2 + x \\ x^{13} + x^{11} + x^9 + x^8 + x^7 & \\ \hline = & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{array}$$

On doit réduire par

$x^{(13-8)} \times (x^8 + x^4 + x^3 + x + 1) = x^{13} + x^9 + x^8 + x^6 + x^5$

$$\begin{array}{rr} & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ + & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline = & x^{11} + x^4 + x^3 + 1 \end{array}$$

Une autre réduction

$x^{(11-8)} \times (x^8 + x^4 + x^3 + x + 1) = x^{11} + x^7 + x^6 + x^4 + x^3$

$$\begin{array}{rr} & x^{11} + x^4 + x^3 + 1 \\ + & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \hline = & x^7 + x^6 + 1 \end{array}$$

Le polynôme résultat $x^7 + x^6 + 1$ représente l'octet 11000001 = C1