

**Sécurité Informatique**

**1CS**

Contrôle Final

***Partie Exercices***

Exercice1 *(5 points)*

Soit le message à chiffrer avec le crypto système RSA défini avec la clé publique . Donner le chiffré de .

Sachant que , avec Déchiffrer

Exercice 2 *(2 points)*

On désire chiffrer le texte suivant par la méthode de Vigenère.

«

»

Dont la clé est la suivante : « **Faille de sécurité sur internet** »

1. Donner le chiffré de «  ».
2. On voudrait chiffrer le message en entier, que proposez-vous, comme méthode, pour le faire rapidement ?

Exercice 3 *(4 points)*

Une des opérations utilisée dans la MixCulumn de l’AES est la multiplication dans GF(28). Soit une donnée A sur 8 bits (on désire réaliser un circuit permettant de faire la multiplication, dans le corps le Galois GF(28), par la valeur 05.

- Proposer un circuit (à base de portes Xor) permettant de faire cette opération.

Expliquer la conception de ce circuit.

- Donner le nombre de portes et la latence de ce circuit.

- Calculer la multiplication de 8F par 05.

On donne le polynome irréductible P(x)= (x8+ x4+ x3+ x +1).