

**Sécurité Informatique**

**1CS**

Examen de remplacement

***Partie Exercices***

Exercice1 *(2.5 points)*

Je désire casser le DES et je dispose d’une machine avec laquelle je peux tester deux mégas clés par second. En combien de temps exactement *(Années, mois, jours, heures, minutes, secondes)* puis-je le faire.

Exercice 2 *(4 points)*

On désire chiffrer le message suivant « Je suis esiste » par le protocole de Hill dont la clé est la matrice suivante :

3 5 7

6 15 4

8 11 2

* Donner le cryptogramme (en lettres)

Exercice 3 *(2 points)*

Soit les matrices **State** et **RoundKey** suivantes.

A3 05 07 4D

16 15 4B FF

28 B1 2C EE

1B A7 F0 4F

A3 05 07 4D

15 4B FF 16

2C EE 28 B1

4F 1B A7 F0

State RoundKey

Donnez la matrice state résultat après les deux transformations : **ShiftRows** suivie de **AddRoundKey.**