**Cryptographie : TD1\_2 Chiffrement de Jules César 29/01/2019**

**1.Expliquer comment fonctionne le chiffrement de Jules César et donner une modélisation algébrique.**

**2.En utilisant la correspondance suivante : Alphabet -> Z26 = {0,1 ..., 25}, Numériser le texte : « le monde appartient a ceux qui se levent tot ».**

**3.Chiffrer le message précédent en utilisant la méthode de Jules César avec un décalage de 7.**

**4.Quelles sont les faiblesses de cette méthode de chiffrement ?**

**5.que signifie l’intégrité des données en cryptographie ?**

1. Chiffrement de jules césar est un chiffrement par substitution où chaque caractère du texte clair est décalé vers 4 rangs vers la droite.
2. Ek(x) = x + k mod 26

Dk(y) = y – k mod 26

1. 11 4 12 14 13 3 4 ...

18 11 19 21 20 10 11 (+7)

1. Chaque caractère du texte clair est chiffré par le même caractère dans le texte chiffré ce qui ne change pas l’entropie du message. L’espace des clés n’est que de 26, donc il est facile de tester toutes les clés afin de casser ce système.
2. Les données reçues ne doivent pas subir de modifications ou d’altérations pendant leur transmission. L’information à l’arrivée doit être similaire à l’information originale.