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

**1.Qu’est -e que la cryptanalyse ?**

**2.Dans le jargon de la cryptographie, que signifie une attaque ?**

**3.Que signifie une attaque par force brute (i.e recherche exhaustive) ? Quand peut-on utiliser cette attaque ?**

1. Science de la reconstitution du texte en clair sans la connaissance de la clé utilisée lors du chiffrement
2. On appelle « attaque », toutes tentatives de cryptanalyse
3. La stratégie de cette attaque est simple, elle consiste à vérifier systématiquement toutes les clés possibles jusqu’à que la clé originale soit trouvée. En Théorie cette attaque peut être utilisée tout le temps et contre n’importe quel crypto système. Elle est surtout utilisée quand il n’est pas facile de détecter des faiblesses dans l’algorithme permettant de faciliter la cryptanalyse.

B.3.La clé utilisée lors du chiffrement est [plus grande fréquence] – [e]. En effet |e| est la lettre la plus utilisée en français.