Sécurité Informatique
Interrogation 1

Exercice

I. Chiffrement par décalage :

1. Trouver la clé de chiffrement correspondant aux données du tableau ci-dessous, puis remplir le tableau (trouver le reste du texte en clair et le texte chiffré).

A = (T + K) mod 26 === 0 = (19 + K) mod 26 ==== K = 7 (1 pts)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Texte en clair	I	N	T	E	R	R	O	G	A	T	I	O	N	(0.5 pts)
Texte chiffré	P	U	A	L	Y	Y	V	N	H	A	P	V	U	(0.5 pts)

2. En utilisant la méthode d'analyse de fréquences, est-il plus facile de déchiffrer un texte long ou un texte court chiffré par un décalage ?
   Il est plus facile de déchiffrer un texte long. (0.5 pts)

II. Chiffre de Vigenère :

3. Soit le couple texte en clair / texte chiffré suivant : « **ARCHIMEDE** » / « **ELTLSMIXV** », trouver la clé de chiffrement de Vigenère utilisée.
   K = EUREKA (1.5 pts)
4. Dans la cryptanalyse du chiffre de Vigenère, quel est le nom de méthode utilisée pour trouver la taille de la clé de chiffrement ?
   KASISKI (0.5 pts)

III.

5. Parmi ces deux algorithmes de chiffrement (César et Vigenère), lequel est un algorithme de chiffrement **monoalphabétique** et lequel est **polyalphabétique** ? Expliquer votre réponse en se basant sur les deux exemples (questions 1 et 3).
   César == monoalphabetique == exemple C (R) = Y et C (R) = Y Qst 1
   Vigenère == polyalphabetique == exemple C (E) = I et C (E) = V Qst 3

(Réponse : 0.5 pts + explication 1 pts)