Université Abdelmalek Essaâdi
Faculté des Sciences de Tétouan

Année *2021-2022*
Rattrapage – SMI-S6

SÉCURITÉ & CRYPTOGRAPHIE

Remarques :
- Durée $01^h : 30^{min}$; aucun document n'est autorisé.
- Usage de tout appareil électronique connecté est interdit.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
_	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
19.3	6.7	0.6	2.4	2.9	13.9	0.9	0.8	0.8	6.1	0.3	0	4.7	2.1	5.6	4.1	2.5	1.3	5.3	6.3	6.3	5.2	1.3	0	0.4	0.3	0.1

Exercice 1 *Déchiffrement de Cesar (3 pts)*
Soit "JYVQVRHBOQSZHUQTRJTYVIQJYVQMEHC" un message chiffré par l'algorithme de Cesar. En utilisant une attaque statistique, trouver le décalage utilisé et déchiffrer le message.

Exercice 2 *Implémentation du code de Vigenère (4 pts)*
Écrire un programme (en Java ou en C) qui code uniquement l'algorithme de chiffrement de Vigenère. Votre programme devra pendre en ligne de commande la clé utilisée et message à chiffrer et produit en sortie le massage chiffré.

Exercice 3 *Code de Hill (4 pts)*
Décrypter le message "WGEAXFCVKFSJHTVE_XEEASWUFBAW_USSK" crypté avec l'algorithme de Hill, sachant que l'alphabet intègre l'espace et la clé utilisée étant

$$\begin{pmatrix} 1 & 1 & 2 \\ 3 & 0 & 1 \\ 2 & 3 & 0 \end{pmatrix}$$

Exercice 4 *Décryptage asymétrique RSA (4 pts)*
On considère les valeurs $p = 7$ et $q = 5$.

1. Calculer la valeur publique n et la fonction d'Euler $\varphi(n)$.
2. Calculer au moins *3* premiers exposants valides.
3. En utilisant le premier exposant valide trouvé et l'algorithme étendu d'Euclid, calculer la valeur d de la clé privée.
4. Déchiffrer le message ci-dessous avec la clé privée calculée :

{ 33, 17, 10, 1, 14, 17, 4, 14, 10, 24, 24, 0, 4, 24, 0, 14, 10, 19, 20, 0, 20, 15, 0, 7, 15, 9, 4, 14, 10, 24,24 }

Exercice 5 *Sécurité Informatique (5 pts)*

1. Quel est le principe de chacune des attaques ci-dessous et comment lutter contre elles.
   - Usurpation d'identité
   - Cheval de Troie
   - Rançongiciel (*ransomware*)
2. L'organisme OWASP publie des rapports sur les 10 principaux risques de sécurité des applications Web, selon vous, quelles sont les actions à entreprendre pour sécuriser une application Web ?

LaTeX