Université Abdelmalek Essaâdi
Faculté des Sciences de Tétouan

Année *2021-2022*
CC – 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 *Code de Hill (5 pts)*

Décrypter le message "F_FHSAYYVBIOGNKQEAMXDQBB" crypté avec l'algorithme de Hill.

L'alphabet intègre l'espace et la clé utilisée étant $\begin{pmatrix} 1 & 3 & 2 \\ 1 & 0 & 3 \\ 2 & 1 & 1 \end{pmatrix}$

Exercice 2 *Décryptage asymétrique RSA (5 pts)*

On considère les valeurs $p = 3$ et $q = 13$.

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 deuxième 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 :

   { 4, 1, 14, 7, 0, 12, 8, 0, 4, 24, 18, 32, 8, 0, 1, 11, 7, 32, 9, 8, 14, 7, 0, 32, 24, 9}

Exercice 3 *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.

Exemple en Java :

```
$ > java vigenere "MOON"  "PRACTIC_MAKES_PERFECT"
   Le crypté du message original avec la clé "MOON" étant :
                BFPQFXRSMAPYRGOCRFUSPH
```

Exercice 4 *Sécurité Informatique (6 pts)*

1. Quels sont les services et les principaux objectifs de la sécurité informatique ?
2. Quel est le principe de chacune des attaques ci-dessous :
   - Ingénierie sociale
   - Attaque par dictionnaire
   - Denis de service.
3. Comment lutter contre ces attaques ?
4. Qu'est ce qu'un pare-feu (*fircwall*) ?
5. Expliquer les commandes iptables ci-dessous :
   - iptables -t filter -P INPUT DROP
   - iptables -t filter -A INPUT -p tcp –dport 80 -j ACCEPT