Université d'Alger1
Faculté Des Sciences
Département Mathématiques – Informatique
Module : Sécurité des systèmes d'informatic

Durée : 1h
Licence ISIL - 2020/2021

Test

Exercice 1 (12pts)

1. Quel est le nombre de clés possibles pour un chiffrement de césar ? **26**
2. Quel est le nombre de clés possibles pour un chiffrement de Vigenère (de clé de longueur k) ? **26^k**
3. Le chiffrement de César se formalise mathématiquement, par :

   Lettre codée = (Lettre en clair + Clé) modulo 26

   Où : les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1 ...).

   Quelle est l'équation de déchiffrement ?

   Lettre codée = (Lettre en clair - Clé) modulo 26

4. Chiffrer le message MATH avec l'algorithme de César en utilisant la clé k=E

   Solution : QEXL

5. Chiffrer le message CRYPTO avec l'algorithme de César en utilisant la clé k=G

   Solution : IXEVZU

6. Le message QIIXPEXIV est crypté avec l'algorithme de César en utilisant la clé k=E.
   Déchiffrer ce message.
   Solution : MEET LATER
7. Un message m est chiffré par le chiffrement de Vigenère avec une clé K_0
   Cette clé est à son tour chiffrée par Vigenère avec la clé K_1: **OR**
   On donne
   - le chiffré de m : **KOADOLP**
   - et le chiffré de la clé K_0 : **XRBLOIM**

   Déchiffrer m.

   Solution :
   Déchiffrer la clé K_0 avec l'algorithme de Vigenère : JANUARY
   Déchiffrer le message m avec la clé K_0 déchiffré : BONJOUR

8. Notons $m_1, m_2, \cdots m_n$ les lettre d'un message M. Le message chiffré est donné par les lettres $c_1, c_2, \cdots, c_n$ avec **$c_1 = m_1 + k \bmod 26$ et pour $i \geq 2$ $c_i = m_i + c_{i-1} \bmod 26$**
   k est la clé de chiffrement.
   Chiffrer le message « MESSAGE » avec la clé k= C
   Trouvez la fonction de déchiffrement.
   NB. Les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1 …))

   Solution :
   Le message chiffré = OSKCCIM
   La fonction de déchiffrement : $m_1 = c_1 - k \bmod 26$ et pour $i \geq 2$ $m_i = c_i - c_{i-1} \bmod 26$

Exercice 2 (8pts) :

Un enseignant envoie ses notes au secrétariat de l'école par mail. L'algorithme RSA est utilisé pour le chiffrement des messages échangés. La clé publique de l'enseignant est la paire (3, 55), celle du secrétariat la paire (3, 33).

1. devinez les valeurs p, q, $\varphi(n)$ pour chacune des paires de clé publiques

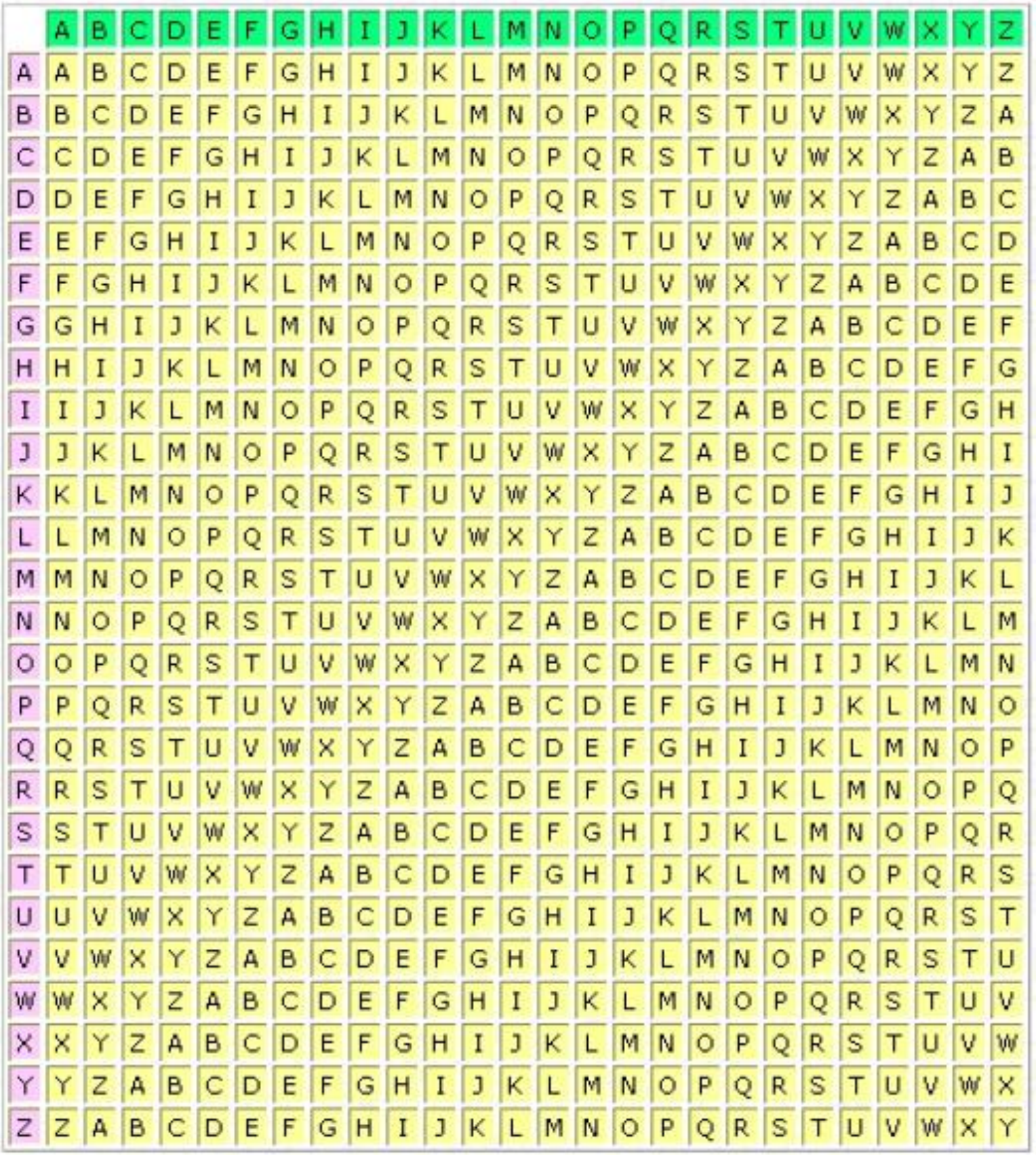
Pour la clé (3,55) :	Pour la clé (3,33) :
e= 3	**e= 3**
n= 55	**n= 33**
P = 11	**p =11**
q = 5	**q =3**
φ(n) = 40	**φ(n) =20**

Déterminer la clé privée de l'enseignant et du secrétariat de l'école

d=7 mod 20

2. Pour assurer la confidentialité de ces messages, l'enseignant chiffre les notes avec la clé RSA du secrétariat. Quel message chiffré correspond à la note 12 ?

12^3 mod 33 = 1728 mod 33 = 12 mod 33



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