CESAR

Exercice 1

Crypter le mot *MATHEMATIQUES* par la méthode de César par paquet de 1 avec 19 comme clef.

Correction
FTMAXFTMBJNXL

Exercice 2

Crypter le mot *ZEBRE* par la méthode de César par paquet de 2 avec 25 comme clef.

Correction
3-142-425

Exercice 3

Crypter le message *VIVELACRYPTO* par la méthode de César par paquet de 3 avec 190091 comme clef.

Correction
148386-231191-211815-89479

Exercice 4

On a utilisé la méthode de César par paquet de 1 avec 25 comme clef pour obtenir *BDRSBGZTCBZAQTKD*. Quel était le message original ?

Correction
CESTCHAUDCABRULE

Exercice 5

On a utilisé la méthode de César par paquet de 3 avec 250025 comme clef pour obtenir *208907-107501-39318-48312-77499*. Quel était le message original ?

Correction
VOILACESTFINI

Exercice 6

Ce message a été codé par la méthode de César : *2138-523-1651-1650-712-1434-1834-2338-412-721-212-708*. Quel était le message original ?

Correction
JESPEREQUECAGALEREUNPEU

AFFINE

Exercice 7

Dans chacun des cas suivant, appliquer l'algorithme d'Euclide pour déterminer le PGCD de A et B.

1. $A = 540$, $B = 256$
2. $A = 561$, $B = 187$
3. $A = 982$, $B = 1000$

Correction

1.

a	b	r	q
540	256	28	2
256	28	4	9
28	4	0	7

$\text{PGCD}(540, 256) = 4$

2.

a	b	r	q
561	187	0	3

$\text{PGCD}(561, 187) = 187$

3.

a	b	r	q
982	1000	982	0
1000	982	18	1
982	18	10	54
18	10	8	1
10	8	2	1
8	2	0	4

$\text{PGCD}(982, 1000) = 2$

Exercice 8

Dans chacun des cas, donner l'inverse de a modulo n lorsque cela est possible.

1. $a = 13$, $n = 7$
2. $a = 4$, $n = 17$
3. $a = 2$, $n = 8$
4. $a = 54$, $n = 17$

Correction

1.

a	b	r	q	u	v
13	7	6	1	−1	2
7	6	1	1	1	−1
6	1	0	6	0	1

$13^{-1} \equiv_7 -1$

2.

a	b	r	q	u	v
4	17	4	0	−4	1
17	4	1	4	1	−4
4	1	0	4	0	1

$4^{-1} \equiv_{17} -4$

3.

a	b	r	q	u	v
2	8	2	0	1	0
8	2	0	4	0	1

Puisque $\text{PGCD}(2, 8) = 2 \neq 1$ alors 2 n'est pas inversible modulo 8

4.

a	b	r	q	u	v
54	17	3	3	6	−19
17	3	2	5	−1	6
3	2	1	1	1	−1
2	1	0	2	0	1

$54^{-1} \equiv_{17} 6$

Exercice 9

Les couples suivants définissent-ils des clefs de cryptage affine par paquet de N

1. Pour $N = 1$: $(3, 2)$, $(13, 8)$, $(9, 0)$.
2. pour $N = 2$: $(7, 421)$, $(25, 11)$, $(421, 801)$
3. pour $N = 3$: $(2015, 1998)$, $(4567, 9002)$, $(4073, 88)$

Correction
Pour que les clefs soient valident, il faut et il suffit que le a soit inversible le modulo de base.

1. Le modulo de base est 26.

$(3,2)$:

a	b	r	q
3	26	3	0
26	3	2	8
3	2	1	1
2	1	0	2

Donc PGCD$(3,26) = 1$ et $(3,2)$ est une clef valide.

$(13,8)$:

a	b	r	q
13	26	13	0
26	13	0	2

Donc PGCD$(13,26) = 13$ et $(13,8)$ n'est pas une clef valide.

$(9,0)$:

a	b	r	q
9	26	9	0
26	9	8	2
9	8	1	1
8	1	0	8

Donc PGCD$(9,26) = 1$ et $(9,0)$ est une clef valide.

2. Le modulo de base est 2526.

$(7,421)$:

a	b	r	q
7	2526	7	0
2526	7	6	360
7	6	1	1
6	1	0	6

Donc PGCD$(7,2526) = 1$ et $(7,421)$ est une clef valide.

$(25,11)$:

a	b	r	q
25	2526	25	0
2526	25	1	101
25	1	0	25

Donc PGCD$(25,2526) = 1$ et $(25,11)$ est une clef valide.

$(421,801)$:

a	b	r	q
421	2526	421	0
2526	421	0	6

Donc PGCD$(421,2526) = 421$ et $(421,801)$ n'est pas une clef valide.

3. Le modulo de base est 252526.

$(2015,1998)$:

a	b	r	q
2015	252526	2015	0
252526	2015	651	125
2015	651	62	3
651	62	31	10
62	31	0	2

Donc PGCD$(2015,252526) = 31$ et $(2015,1998)$ n'est pas une clef valide.

$(4567,9002)$:

a	b	r	q
4567	252526	4567	0
252526	4567	1341	55
4567	1341	544	3
1341	544	253	2
544	253	38	2
253	38	25	6
38	25	13	1
25	13	12	1
13	12	1	1
12	1	0	12

Donc PGCD$(4567,252526) = 1$ et $(4567,9002)$ est une clef valide.

$(4073,88)$:

a	b	r	q
4073	252526	4073	0
252526	4073	0	62

Donc PGCD$(4073,252526) = 4073$ et $(4073,88)$ n'est pas une clef valide.

Exercice 10

Pour chacune des clefs valides de l'exercice précédent, déterminer la fonction de déchiffrement.

Correction
D'après le cours, si (a,b) est une clef du chiffrement affine alors $D(x) \equiv_n a^{-1}(x-b)$ est la fonction de déchiffrement.

1. Le modulo de base est 26.

$(3,2)$:

a	b	r	q	u	v
3	26	3	0	9	−1
26	3	2	8	−1	9
3	2	1	1	1	−1
2	1	0	2	0	1

Donc $D(x) \equiv_{26} 9(x-2)$.

$(9,0)$:

a	b	r	q	u	v
9	26	9	0	3	−1
26	9	8	2	−1	3
9	8	1	1	1	−1
8	1	0	8	0	1

Donc $D(x) \equiv_{26} 3x$.

2. Le modulo de base est 2526.

$(7,421)$:

a	b	r	q	u	v
7	2526	7	0	361	−1
2526	7	6	360	−1	361
7	6	1	1	1	−1
6	1	0	6	0	1

Donc $D(x) \equiv_{2526} 361(x-421)$.

$(25,11)$:

a	b	r	q	u	v
25	2526	25	0	−101	1
2526	25	1	101	1	−101
25	1	0	25	0	1

Donc $D(x) \equiv_{2526} -101(x-11)$.

3. Le modulo de base est 252526.

$(4567,9002)$:

a	b	r	q	u	v
4567	252526	4567	0	19961	−361
252526	4567	1341	55	−361	19961
4567	1341	544	3	106	−361
1341	544	253	2	−43	106
544	253	38	2	20	−43
253	38	25	6	−3	20
38	25	13	1	2	−3
25	13	12	1	−1	2
13	12	1	1	1	−1
12	1	0	12	0	1

Donc $D(x) \equiv_{252526} 19961(x-9002)$.

Exercice 11

Crypter le message *CHOCOBO* par la méthode affine par paquet de 1 avec $(7,7)$ comme clef.

Correction

Le message chiffré est VEBVBOB.

	C	H	O	C	O	B	O
x	2	7	14	2	14	1	14
7x	14	49	98	14	98	7	98
7x + 7	21	56	105	21	105	14	105
$\equiv_{26}$	21	4	1	21	1	14	1
	V	E	B	V	B	O	B

Exercice 12

Crypter le message *VACANCES* par la méthode affine par paquet de 2 avec $(1999, 999)$ comme clef.

Correction

Le message chiffré est $687 - 1691 - 1917 - 475$.

	VA	CA	NC	ES
x	2100	200	1302	418
$1999x$	4197900	399800	2602698	835582
$1999x + 999$	4198899	400799	2603697	836581
$\equiv_{2526}$	687	1691	1917	475

Exercice 13

Déchiffrer le message *CBLXD* obtenue par le cryptosystème affine par paquet de 1 avec $(7, 1)$ comme clef.

Correction

D'après l'algorithme d'Euclide étendue,

a	b	r	q	u	v
7	26	7	0	-11	3
26	7	5	3	3	-11
7	5	2	1	-2	3
5	2	1	2	1	-2
2	1	0	2	0	1

ce qui prouve d'une part que la clef indiqué est valide et d'autre part que la fonction de déchiffrement est $D(x) \equiv_{26} -11(x - 1)$.

	C	B	L	X	D
x	2	1	11	23	3
$x - 1$	1	0	10	22	2
$\equiv_{26}$	1	0	10	22	2
$\times -11$	-11	0	-110	-242	-22
$\equiv_{26}$	15	0	20	18	4
	P	A	U	S	E

Le message claire est PAUSE.

Exercice 14

Décrypter ce message sachant que l'on a utilisé un cryptage affine et que le texte claire commence par *TOUT*.

OLZOJFENAFKNZOWNDEFWLXDLAHZXUFJLZEFUFOFDRFZG UFOFDRFZGKFSODENJDLZ-PLANPFOSFPYEFFODFKLXONEFAKFSD

Correction

Soit (a, b) la clef de chiffrement. On sait que *TOUT* a été transformé en *OLZO*. Numériquement, par la transformation modulaire $ax + b$, la suite de chiffre $19 - 14 - 20 - 19$ est transformé en $14 - 11 - 25 - 14$. Cela se traduit par les équations suivantes :

$$\begin{cases} 19a + b & \equiv_{26} & 14 \\ 14a + b & \equiv_{26} & 11 \\ 20a + b & \equiv_{26} & 25 \end{cases}$$

(la dernière étant une redondance de la première nous ne l'avons pas fait apparaitre dans le système).

En soustrayant la première à la seconde on trouve l'équation $5a \equiv_{26} 3$ de sorte que $a \equiv_{26} 5^{-1}3$. Naturellement 5 est inversible modulo 25 puisque l'on peut par exemple rapidement remarquer que $5(-5) = -25 \equiv_{26} 1$ de sorte que l'on observe de plus que $5^{-1} \equiv_{26} -5 (\equiv_{26} 21)$. Ainsi $a \equiv_{26} -5 \times 3 = -15 \equiv_{26} 11$. En substituant cette valeur

dans n'importe laquelle des équations modulaires suivantes, on trouve $b \equiv_{26} 13$.

Finalement la clef de chiffrement est $(a, b) = (11, 13)$ ce qui nous permet de déchiffrer le message et observer qu'il s'agit de quelques vers du *poison* de Baudelaire :

	O	L	Z	O	J	F	E	N	A	F	K	N	Z	O	W	N	D
x	14	11	25	14	9	5	4	13	0	5	10	13	25	14	22	13	3
$x-13$	1	−2	12	1	−4	−8	−9	0	−13	−8	−3	0	12	1	9	0	−10
$\equiv_{26}$	1	24	12	1	22	18	17	0	13	18	23	0	12	1	9	0	16
$\times -7$	−7	−168	−84	−7	−154	−126	−119	0	−91	−126	−161	0	−84	−7	−63	0	−112
$\equiv_{26}$	19	14	20	19	2	4	11	0	13	4	21	0	20	19	15	0	18
	T	O	U	T	C	E	L	A	N	E	V	A	U	T	P	A	S

	E	F	W	L	X	D	L	A	H	Z	X	U	F	J	L	Z	E
x	4	5	22	11	23	3	11	0	7	25	23	20	5	9	11	25	4
$x-13$	−9	−8	9	−2	10	−10	−2	−13	−6	12	10	7	−8	−4	−2	12	−9
$\equiv_{26}$	17	18	9	24	10	16	24	13	20	12	10	7	18	22	24	12	17
$\times -7$	−119	−126	−63	−168	−70	−112	−168	−91	−140	−84	−70	−49	−126	−154	−168	−84	−119
$\equiv_{26}$	11	4	15	14	8	18	14	13	16	20	8	3	4	2	14	20	11
	L	E	P	O	I	S	O	N	Q	U	I	D	E	C	O	U	L

	F	U	F	O	F	D	R	F	Z	G	U	F	O	F	D	R	F
x	5	20	5	14	5	3	17	5	25	6	20	5	14	5	3	17	5
$x-13$	−8	7	−8	1	−8	−10	4	−8	12	−7	7	−8	1	−8	−10	4	−8
$\equiv_{26}$	18	7	18	1	18	16	4	18	12	19	7	18	1	18	16	4	18
$\times -7$	−126	−49	−126	−7	−126	−112	−28	−126	−84	−133	−49	−126	−7	−126	−112	−28	−126
$\equiv_{26}$	4	3	4	19	4	18	24	4	20	23	3	4	19	4	18	24	4
	E	D	E	T	E	S	Y	E	U	X	D	E	T	E	S	Y	E

	Z	G	K	F	S	O	D	E	N	J	D	L	Z	P	L	A	N
x	25	6	10	5	18	14	3	4	13	9	3	11	25	15	11	0	13
$x-13$	12	−7	−3	−8	5	1	−10	−9	0	−4	−10	−2	12	2	−2	−13	0
$\equiv_{26}$	12	19	23	18	5	1	16	17	0	22	16	24	12	2	24	13	0
$\times -7$	−84	−133	−161	−126	−35	−7	−112	−119	0	−154	−112	−168	−84	−14	−168	−91	0
$\equiv_{26}$	20	23	21	4	17	19	18	11	0	2	18	14	20	12	14	13	0
	U	X	V	E	R	T	S	L	A	C	S	O	U	M	O	N	A

	P	F	O	S	F	P	Y	E	F	F	O	D	F	K	L	X	O
x	15	5	14	18	5	15	24	4	5	5	14	3	5	10	11	23	14
$x-13$	2	−8	1	5	−8	2	11	−9	−8	−8	1	−10	−8	−3	−2	10	1
$\equiv_{26}$	2	18	1	5	18	2	11	17	18	18	1	16	18	23	24	10	1
$\times -7$	−14	−126	−7	−35	−126	−14	−77	−119	−126	−126	−7	−112	−126	−161	−168	−70	−7
$\equiv_{26}$	12	4	19	17	4	12	1	11	4	4	19	18	4	21	14	8	19
	M	E	T	R	E	M	B	L	E	E	T	S	E	V	O	I	T

	N	E	F	A	K	F	S	D
x	13	4	5	0	10	5	18	3
$x-13$	0	−9	−8	−13	−3	−8	5	−10
$\equiv_{26}$	0	17	18	13	23	18	5	16
$\times -7$	0	−119	−126	−91	−161	−126	−35	−112
$\equiv_{26}$	0	11	4	13	21	4	17	18
	A	L	E	N	V	E	R	S

Exercice 15

On a utilisé le cryptosystème affine pour obtenir *50029-125229-237773-194389-55281-50645*. Retrouver le message original.

Correction
Cet exercice se résout à l'aide de l'ordinateur ; le TP2 donne tous les outils pour appliquer la bonne fonction. En première observation, il s'agit d'un texte par paquet de 3. Il faut lancer l'attaque avant d'aller dormir, se coucher très tôt et se lever très tard... Peut-être que vous saurez ce que cache ce terrible message !

VIGENERE

Exercice 16

Chiffrer ce message par la méthode de vigénère de clef **ASSIEGIONS** :

QUIMAIMEMESUIVE

Correction

On applique le processus pour obtenir

QMAUEOUSZWSMADI

Message	Q	U	I	M	A	I	M	E	M	E	S	U	I	V	E
Codex	16	20	8	12	0	8	12	4	12	4	18	20	8	21	4
+clef	A 0	S 18	S 18	I 8	E 4	G 6	I 8	O 14	N 13	S 18	A 0	S 18	S 18	I 8	E 4
=	16	38	26	20	4	14	20	18	25	22	18	38	26	29	8
$\equiv_{26}$	16	12	0	20	4	14	20	18	25	22	18	12	0	3	8
Crypte	Q	M	A	U	E	O	U	S	Z	W	S	M	A	D	I

Exercice 17

Chiffrer ce message par la méthode de vigénère de clef **RASSASIONS** :

LANEFROTTELANE

Correction

On applique le processus pour obtenir

CAFWFJWHGWCAFW

Message	L	A	N	E	F	R	O	T	T	E	L	A	N	E
Codex	11	0	13	4	5	17	14	19	19	4	11	0	13	4
+clef	R 17	A 0	S 18	S 18	A 0	S 18	I 8	O 14	N 13	S 18	R 17	A 0	S 18	S 18
=	28	0	31	22	5	35	22	33	32	22	28	0	31	22
$\equiv_{26}$	2	0	5	22	5	9	22	7	6	22	2	0	5	22
Crypte	C	A	F	W	F	J	W	H	G	W	C	A	F	W

Exercice 18

Déchiffrer ce message par la méthode de vigénère de clef **CHIPES** :

EOIGMLGIQTRGTKWCRWGJWBQWPJMEEJUVQBIEG

Correction

On applique le processus pour obtenir

CHARITEBIENORDONNEECOMMENCEPARSOIMEME

Message	E	O	I	G	M	L	G	I	Q	T	R	G	T	K	W	C	R	W	G
Codex	4	14	8	6	12	11	6	8	16	19	17	6	19	10	22	2	17	22	6
-clef	C 2	H 7	I 8	P 15	E 4	S 18	C 2	H 7	I 8	P 15	E 4	S 18	C 2	H 7	I 8	P 15	E 4	S 18	C 2
$=$	2	7	0	−9	8	−7	4	1	8	4	13	−12	17	3	14	−13	13	4	4
$\equiv_{26}$	2	7	0	17	8	19	4	1	8	4	13	14	17	3	14	13	13	4	4
Crypte	C	H	A	R	I	T	E	B	I	E	N	O	R	D	O	N	N	E	E

Message	J	W	B	Q	W	P	J	M	E	E	J	U	V	Q	B	I	E	G
Codex	9	22	1	16	22	15	9	12	4	4	9	20	21	16	1	8	4	6
-clef	H 7	I 8	P 15	E 4	S 18	C 2	H 7	I 8	P 15	E 4	S 18	C 2	H 7	I 8	P 15	E 4	S 18	C 2
$=$	2	14	−14	12	4	13	2	4	−11	0	−9	18	14	8	−14	4	−14	4
$\equiv_{26}$	2	14	12	12	4	13	2	4	15	0	17	18	14	8	12	4	12	4
Crypte	C	O	M	M	E	N	C	E	P	A	R	S	O	I	M	E	M	E

Exercice 19

Déchiffrer ce message par la méthode de vigénère de clef **CRYPTASSE** :

NRAPEOEFMGVQIEAJEIWCRXFEVWPKDNJBSKSRV

Correction

On applique le processus pour obtenir

LACALOMNIEESTLARMEULTIMEDELIMPUISSANT

Message	N	R	A	P	E	O	E	F	M	G	V	Q	I	E	A	J	E	I	W
Codex	13	17	0	15	4	14	4	5	12	6	21	16	8	4	0	9	4	8	22
-clef	C 2	R 17	Y 24	P 15	T 19	A 0	S 18	S 18	E 4	C 2	R 17	Y 24	P 15	T 19	A 0	S 18	S 18	E 4	C 2
$=$	11	0	−24	0	−15	14	−14	−13	8	4	4	−8	−7	−15	0	−9	−14	4	20
$\equiv_{26}$	11	0	2	0	11	14	12	13	8	4	4	18	19	11	0	17	12	4	20
Crypte	L	A	C	A	L	O	M	N	I	E	E	S	T	L	A	R	M	E	U

Message	C	R	X	F	E	V	W	P	K	D	N	J	B	S	K	S	R	V
Codex	2	17	23	5	4	21	22	15	10	3	13	9	1	18	10	18	17	21
-clef	R 17	Y 24	P 15	T 19	A 0	S 18	S 18	E 4	C 2	R 17	Y 24	P 15	T 19	A 0	S 18	S 18	E 4	C 2
$=$	−15	−7	8	−14	4	3	4	11	8	−14	−11	−6	−18	18	−8	0	13	19
$\equiv_{26}$	11	19	8	12	4	3	4	11	8	12	15	20	8	18	18	0	13	19
Crypte	L	T	I	M	E	D	E	L	I	M	P	U	I	S	S	A	N	T

Exercice 20

Vous trouverez un message chiffré par la méthode de vigénère. Vous ne connaissez pas la clef mais vous savez que le texte est en français et que, dans cette langue, la lettre la plus fréquente est le *E*.

Déterminer la clef de chiffrement utilisée.

Vous trouverez en annexe différentes analyses statistiques sur le cryptogramme. Lorsqu'une ligne indique Freq $x\%n+i$ cela signifie que sur la ligne concernée la fréquence d'apparition des lettres est donnée tout les n caractères décalés de i.

0	U	G	A	T	X	S	J	W	V	E	A	W	J	K	M	D	M	U	G	K	V	C	Q	V	W
25	P	K	E	A	I	M	G	R	A	Q	W	E	D	Z	A	A	K	W	N	I	**P**	**Z**	**G**	**X**	**G**
50	**A**	**S**	**Q**	**G**	**F**	F	M	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	W	M	T	W	F	N	A	U	K	M
75	L	T	W	E	G	V	T	T	W	H	T	M	M	Q	W	J	O	I	T	Q	F	V	W	X	R
100	Q	F	L	G	U	P	A	V	W	G	B	P	W	M	J	C	C	T	I	F	L	S	C	E	R
125	S	A	G	X	U	K	Z	W	T	K	H	M	J	B	G	N	U	A	D	W	R	Z	E	U	A
150	W	T	P	O	T	D	S	P	L	A	Q	K	S	N	M	F	I	A	J	G	L	A	V	K	E
175	Q	V	P	I	Q	K	T	M	T	Z	G	**K**	**R**	**M**	**C**	**B**	A	N	**G**	**U**	**E**	**V**	**L**	D	C
200	K	H	W	K	W	N	I	P	T	M	K	G	B	O	V	F	S	P	B	E	N	M	L	N	I
225	L	M	F	L	G	C	R	I	N	W	E	T	A	Y	M	W	N	T	E	**T**	**S**	**H**	**T**	**W**	F
250	M	K	K	K	W	N	L	W	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	W	E	G	Z	G	M
275	S	V	W	U	O	Q	F	K	F	I	N	A	E	S	T	M	G	Q	G	F	F	C	M	W	F
300	V	G	C	N	M	D	W	P	B	E	C	J	I	W	Q	E	A	L	E	C	Q	N	B	W	F
325	C	V	T	L	A	X	H	Q	C	Q	D	W	C	K	R	W	A	J	G	U	A	Q	K	B	C
350	Q	D	M	M	P	U	W	U	D	W	F	K	Z	S	B	J	W	U	V	E	B	K	V	G	K
375	E	B	L	W	R	M	R	Q	G	V	G	Y	U	Q	U	G	P	N	I	Z	E	W	P	B	C
400	M	L	L	G	T	E	V	L	W	W	Z	S	I	F	K	C	C	C	C	F	V	Q	C	T	M
425	S	H	T	M	S	I	N	G	K	Z	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	W	H	G	V	D	I	F
450	L	V	Z	O	Q	K	S	P	A	J	M	M	K	W	V	E	L	A	K	E	C	S	A	A	G
475	P	I	V	M	U	S	X	I	N	E	A	B	P	O	A	I	J	V	G	V	Q	C	A	**W**	**V**
500	**I**	**I**	**B**	S	D	Q	Z	S	U	G	F	R	I	T	Z	G	F	C	C	C	M	F	L	T	M
525	D	M	E	S	V	P	E	U	S	L	K	Y	U	M	K	V	C	U	S	B	W	J	F	I	M
550	C	F	W	F	Q	S	K	M	K	U	Q	O	V	H	G	W	Z	L	I	I	M	G	T	L	M
575	B	W	N	C	I	Z	W	K	V	M	R	I	A	K	C	R	A	U	S	A	U	Z	E	K	G
600	F	P	I	I	A	K	S	P	B	L	I	I	M	G	A	T	Q	G	F	G	B	A	Q	L	I
625	W	M	E	B	S	F	V	A	I	U	M	D	V	I	N	M	E	W	P	B	S	C	H	H	Q
650	A	E	M	L	M	F	Q	E	Z	D	S	R	P	Y	A	A	I	W	M	T	P	W	G	T	Q
675	Q	C	W	S	N	C	N	Q	N	W	T	A	I	B	W	V	G	T	E	Q	V	W	P	M	T
700	B	J	G	W	D	A	V	L	D	G	A	D	M	M	P	C	K	T	Q	N	A	V	M	S	L
725	W	H	N	C	S	M	F	H	N	C	S	L	A	X	H	Q	C	Q	D	W	U	I	C	W	F
750	U	K	T	I	M	J	B	G	L	E	D	S	A	U	U	E	L	W	U	K	L	E	Z	K	G
775	K	B	A	I	J	J	G	B	E	Z	V	W	R	Z	O	O	J	S	O	U	E	Z	W	L	C
800	L	E	D	W	F	K	Z	U	V	N	W	T	Q	T	I	T	D	G	C	N	Z	W	**K**	**R**	**M**
825	**C**	**B**	S	T	N	M	T	P	W	G	T	Q	C	Q	W	F	F	M	L	I	H	Z	A	A	I
850	Y	M	W	U	W	I	B	S	S	E	P	E	D	W	J	O	M	S	M	L	M	F	M	S	L
875	W	H	J	G	S	Q	I	M	G	A	A	D	W	U	N	M	M	Q	F	A	O	C	M	L	W
900	X	H	W	R	B	W	L	C	L	E	D	W	F	K	Z	O	C	A	I	W	W	I	C	F	**H**
925	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	E	S	K	A	**E**	**B**	**S**	**A**	**V**	K	E	C	F	W	R
950	Z	O	N	W	K	U	Q	O	V	J	W	U	X	E	K	L	S	D	T	E	K	S	J	C	X
975	R	M	K	L	Q	C	T	Y	M	**W**	**V**	**I**	**I**	**B**	U	W	S	C	E	**T**	**S**	**H**	**T**	**W**	**G**
1000	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	Q	C	**E**	**B**	**S**	**A**	**V**	T	E	A	G	D	K	L	E	K
1025	Z	S	O	X	D	M	U	G	P	V	A	Q	K	K	C	V	C	M	K	I	W	Q	P	W	M
1050	N	C	Q	T	T	S	K	Q	C	T	M	F	A	T	K	O	U	E	W	W	V	E	L	A	K
1075	E	Q	P	T	A	F	G	Q	N	B	W	D	N	M	C	B	M	W	N	**T**	**E**	**U**	**W**	**F**	**V**
1100	Z	E	A	H	W	E	B	A	J	D	W	L	M	M	M	J	S	R	X	E	T	D	W	V	Z
1125	E	A	N	A	X	**M**	**M**	**M**	**F**	**L**	E	W	M	U	W	B	G	V	V	Q	S	A	O	M	S
1150	K	G	D	N	M	G	C	W	K	V	Z	A	D	S	A	N	T	A	V	L	K	W	Z	L	M
1175	E	S	V	M	R	Q	W	D	S	C	I	Q	F	L	G	Z	R	W	Y	W	U	A	U	Z	D
1200	W	W	Z	S	K	G	E	R	M	T	M	F	U	G	A	**P**	**Z**	**G**	**X**	**G**	**A**	**S**	**Q**	**G**	**F**
1225	P	M	L	T	W	K	R	W	U	D	S	A	G	V	T	I	M	E	Q	Q	N	A	E	W	V
1250	B	R	M	W	F	C	D	A	V	L	D	G	C	R	X	D	W	K	V	E	K	G	F	P	I

1275	I	A	K	S	P	K	E	L	W	K	V	C	B	M	K	S	X	Q	D	M	V	W	U	I	M
1300	X	D	A	H	Q	C	I	L	W	W	Z	S	M	L	L	Q	C	T	T	W	J	G	A	T	M
1325	S	D	Q	Z	S	Y	M	W	L	I	V	I	A	K	N	Q	M	X	J	W	U	A	I	W	F
1350	I	W	M	C	W	F	X	T	W	N	B	W	S	E	M	T	B	W	I	W	M	S	B	A	G
1375	P	R	E	V	S	M	T	I	I	A	J	A	G	V	E	C	S	J	G	X	O	V	V	J	G
1400	M	M	X	D	A	F	M	D	W	M	L	G	A	J	M	X	J	C	X	P	I	A	K	C	T
1425	A	X	G	J	V	M	D	C	T	M	T	M	A	C	V	W	Y	Q	J	V	Y	S	C	Z	D
1450	M	F	W	V	T	U	Q	V	W	O	I	N	L	S	A	U	A	I	R	W	H	Q	C	V	I
1475	A	K	N	C	I	X	S	J	N	M	R	Y	M	W	N	Y	U	M	K	A	P	A	T	I	F
1500	L	U	Y	U	I	F	V	L	M	Q	C	A	L	V	I	I	A	K	G	P	J	U	Z	W	S
1525	W	X	L	C	K	A	G	C	R	A	Z	W	W	Z	**E**	**A**	**H**	**D**	**W**	**A**	T	I	J	V	L
1550	M	T	I	A	K	W	V	E	I	M	L	T	M	P	M	J	K	Q	V	N	M	U	S	T	I
1575	P	Z	W	K	C	D	O	Q	J	H	C	B	I	M	E	E	G	V	T	M	U	G	W	B	E
1600	U	W	K	R	Z	O	J	D	W	O	M	S	M	L	V	K	B	D	I	U	U	Q	Z	D	I
1625	N	W	E	U	O	Q	I	M	K	T	N	G	S	N	C	Q	T	X	S	K	X	Z	A	Q	E
1650	**W**	**P**	**B**	**D**	**M**	V	A	U	K	I	X	D	A	P	M	D	M	D	S	R	Z	O	O	J	S
1675	O	U	A	B	A	G	P	Q	L	A	W	E	K	B	A	M	P	H	N	Q	Q	C	W	J	R
1700	W	S	M	E	W	P	B	Q	C	W	D	G	A	O	Z	V	A	P	I	T	M	M	J	U	I
1725	U	B	G	E	C	B	I	Y	M	W	U	M	T	**I**	**A**	**W**	**P**	**B**	L	I	H	G	W	Z	D
1750	C	J	W	T	Y	U	**M**	**F**	**G**	**W**	**A**	N	M	F	W	V	Q	O	V	K	I	W	I	U	L
1775	W	T	W	B	E	B	I	M	G	X	E	C	L	W	V	Z	E	R	W	K	G	Z	A	Q	K
1800	M	P	M	D	M	K	H	G	Z	S	W	F	F	G	A	A	X	H	W	N	M	E	A	S	X
1825	C	Q	R	M	V	W	N	I	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	S	L	K	W	N	C	F	W	F
1850	Q	S	K	A	H	N	Q	N	M	J	W	U	X	E	K	L	S	D	T	E	L	S	F	U	T
1875	E	A	S	F	P	M	E	A	S	N	G	V	I	Z	U	W	H	C	T	C	F	L	Q	C	R
1900	V	S	F	V	L	E	U	S	N	K	M	E	B	B	W	O	M	D	M	T	S	T	Z	A	A
1925	K	S	K	A	D	M	E	W	U	M	T	C	V	W	U	L	E	X	Z	Q	U	Q	Q	C	W
1950	K	N	M	P	T	M	K	T	I	P	Q	V	W	O	M	N	B	H	G	U	A	I	J	D	W
1975	W	V	E	L	W	K	O	W	R	I	D	W	U	L	E	K	W	L	V	M	H	Q	K	L	Q
2000	Q	R	M	W	K	V	J	I	M	F	K	W	Z	Q	C	W	F	Q	C	S	L	W	N	Q	V
2025	S	N	S	A	T	M	T	Z	W	K	C	B	T	M	F	L	K	W	N	T	G	J	U	Y	U
2050	**M**	**F**	**G**	**W**	**A**	D	W	F	F	Q	V	S	L	W	K	E	W	N	A	W	A	N	A	A	V
2075	G	K	E	I	D	M	L	K	R	I	R	N	G	A	U	Q	L	A	D	W	U	A	U	Q	N
2100	**W**	**P**	**B**	**D**	**M**	M	P	C	V	S	X	D	M	U	B	A	Z	V	W	P	R	E	U	W	E
2125	C	Z	I	I	A	K	G	B	L	I	U	W	T	M	M	W	F	A	G	P	O	T	D	S	P
2150	L	A	Q	K	W	F	C	M	I	J	A	C	O	E	L	W	E	C	V	D	I	F	L	S	C
2175	E	D	G	M	U	L	E	K	D	S	T	Q	E	H	N	G	V	Z	E	X	J	G	H	M	S
2200	A	A	G	P	R	E	L	W	U	N	I	R	I	A	K	S	C	E	R	W	L	C	Q	S	**X**
2225	**J**	**G**	**I**	**Z**	**A**	**U**	**E**	W	W	Z	M	I	A	K	N	M	S	I	M	L	Q	Z	I	B	W
2250	K	O	C	N	Q	U	A	R	I	L	M	K	V	G	T	A	D	A	D	N	M	D	I	E	K
2275	V	M	R	L	S	E	P	M	L	I	U	U	G	X	T	M	J	W	P	B	P	I	K	U	Q
2300	V	S	Q	V	W	T	I	N	B	I	M	W	V	E	B	W	D	N	M	**P**	**Z**	**G**	**X**	**G**	**A**
2325	**S**	**Q**	**G**	**F**	P	M	X	Q	K	L	C	Q	T	X	S	K	G	B	C	Z	G	Q	G	H	L
2350	M	G	M	P	W	N	A	G	M	U	T	E	B	A	L	T	M	**P**	**Z**	**G**	**X**	**G**	**A**	**S**	**Q**
2375	**G**	**F**	O	W	N	I	U	L	G	L	E	U	S	J	K	I	G	M	H	G	T	B	E	T	S
2400	E	G	V	T	Q	G	F	T	Q	D	Q	U	M	N	M	D	M	H	Z	A	A	I	K	A	W
2425	P	B	H	M	G	J	K	Y	U	M	N	G	K	T	A	X	G	M	T	T	A	T	W	F	V
2450	M	U	Z	S	N	G	K	L	I	I	M	G	T	L	M	B	S	K	D	U	**T**	**S**	**H**	**T**	**W**
2475	F	M	K	K	K	W	N	L	W	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	W	E	G	Z	G
2500	M	J	V	C	V	S	U	G	F	R	Z	O	X	J	W	R	I	Y	A	V	W	R	C	I	A

2525	D	G	T	A	J	I	A	N	W	C	N	M	H	D	W	A	G	Z	S	F	F	M	P	I	J
2550	L	K	M	D	C	E	G	P	L	E	M	L	E	Q	V	I	U	H	J	G	A	S	Q	G	F
2575	I	M	N	M	J	S	N	M	E	A	L	I	W	M	D	I	F	K	N	M	S	I	M	L	T
2600	M	S	X	S	Q	U	I	V	M	U	I	W	M	L	Y	M	W	U	L	E	K	S	D	C	O
2625	E	A	V	W	F	I	T	M	K	D	G	U	O	L	W	D	G	L	E	K	J	G	K	A	S
2650	I	F	U	G	I	E	B	W	W	P	O	R	I	F	V	G	X	A	Z	L	A	G	T	E	U
2675	W	E	G	T	A	Q	K	K	G	H	M	W	A	W	U	A	A	G	W	J	F	M	D	M	U
2700	J	K	Z	E	T	S	K	K	B	U	I	L	A	Q	V	D	I	F	K	E	M	S	R	G	M
2725	T	A	A	V	U	A	G	V	S	I	N	W	E	C	N	X	W	M	R	T	U	A	V	W	F
2750	M	T	I	A	D	F	I	N	A	D	W	U	X	O	Q	J	I	W	M	C	M	D	S	P	W
2775	U	A	V	G	P	V	E	C	F	W	O	M	I	T	D	W	W	Z	E	K	G	E	R	Z	E
2800	P	W	F	U	Q	O	V	V	W	N	I	S	Q	L	M	C	B	I	W	F	S	W	R	O	C
2825	J	V	J	C	I	M	F	H	Q	C	R	A	M	A	X	I	N	B	F	G	V	Z	E	I	F
2850	S	N	G	S	M	F	G	W	A	V	M	J	J	Q	V	S	K	G	E	O	M	T	I	F	L
2875	F	M	M	I	D	W	P	B	E	V	V	M	U	I	P	Z	G	H	Q	A	D	M	D	S	X
2900	M	R	Q	L	S	D	T	E	V	S	L	W	Z	E	L	W	D	C	K	T	Q	N	A	V	M
2925	D	M	H	J	Q	O	R	I	E	E	C	B	I	W	F	H	G	C	V	M	F	L	T	M	M
2950	W	F	L	G	Z	A	K	W	H	C	A	S	M	E	S	K	V	T	M	F	S	P	B	L	W
2975	A	F	V	I	I	V	D	W	U	X	R	M	E	A	G	Z	S	W	J	V	K	V	A	B	W
3000	M	T	A	E	T	W	U	V	Z	O	V	A	I	W	M	S	I	M	L	Q	U	A	B	A	I
3025	W	M	S	M	L	S	K	M	N	B	L	G	W	A	D	M	K	E	C	K	H	Q	F	W	U
3050	C	N	Q	I	M	G	A	E	V	M	F	U	M	U	T	W	P	G	U	P	T	S	A	T	M
3075	E	B	A	D	U	M	T	I	A	W	P	B	T	W	M	K	U	Q	T	C	W	K	F	I	N
3100	A	M	F	G	V	V	Q	J	G	P	V	E	U	W	F	V	Q	M	X	J	W	I	V	E	L
3125	W	D	C	U	B	Q	S	F	E	M	E	V	L	Z	Q	C	S	Q	S	K	O	I	N	B	W
3150	V	W	V	L	I	T	G	T	I	T	W	A	J	G	M	X	X	W	J	K	U	E	V	L	S
3175	N	Y	U	I	F	V	N	Q	D	M	W	V	G	T	O	Z	V	A	P	I	T	M	M	J	C
3200	C	T	W	E	S	V	Q	Q	C	W	S	R	X	A	Z	M	L	U	I	R	M	S	D	K	A
3225	A	B	A	G	P	N	U	B	M	F	H	W	R	U	A	V	C	J	L	M	V	W	H	Q	P
3250	W	M	J	N	I	T	M	U	Z	P	W	L	W	Y	A	G	M	L	M	U	L	T	W	N	Q
3275	I	M	G	L	I	A	H	G	P	Q	B	T	W	S	N	M	P	W	I	M	G	M	T	C	F
3300	W	E	P	O	A	W	W	U	B	C	M	J	L	C	Q	N	M	F	G	W	A	N	M	H	G
3325	W	D	O	V	K	H	C	A	N	Q	W	J	N	M	C	W	M	J	C	O	E	L	W	K	G
3350	Y	U	Q	H	W	U	Y	U	Q	V	W	E	Q	D	M	J	W	P	B	D	M	K	W	N	I
3375	N	K	W	J	F	I	N	A	D	S	E	W	N	A	L	J	W	K	T	Q	G	F	F	C	N
3400	M	I	M	K	X	E	U	W	F	V	I	U	A	K	A	H	I	N	B	S	K	V	Q	Q	C
3425	W	U	C	Z	C	M	L	S	K	B	D	M	K	W	S	C	I	X	W	E	G	V	T	A	X
3450	S	P	B	A	A	L	A	S	C	E	A	J	W	V	Z	O	A	H	W	E	B	I	D	W	E
3475	G	V	T	W	F	H	G	C	T	A	W	M	N	M	M	M	F	L	U	M	M	M	J	N	G
3500	Q	L	T	W	J	S	C	E	K	W	K	R	Z	E	U	A	W	T	M	S	U	S	U	J	Q
3525	N	M	K	S	K	M	N	B	K	W	W	T	E	U	W	F	V	N	O	V	U	L	K	W	N
3550	V	W	V	W	U	O	Q	F	K	R	I	R	N	G	A	U	T	A	B	S	U	J	M	E	K
3575	J	S	U	I	N	B	W	W	V	I	I	B	V	W	O	M	T	B	J	W	G	B	D	M	U
3600	G	P	A	E	Z	N	W	T	K	E	A	E	S	E	P	I	V	W	K	G	V	E	B	S	L
3625	F	M	F	W	F	U	V	Q	O	V	F	W	O	M	N	B	D	S	R	Z	E	W	U	U	W
3650	X	A	B	A	G	P	M	N	D	W	J	U	T	E	A	S	K	R	M	C	B	K	E	C	B
3675	E	Z	A	W	N	A	D	C	U	S	N	K	U	T	S	M	V	W	M	I	L	A	S	C	E
3700	A	W	J	G	N	L	M	L	W	V	W	U	R	G	M	T	A	D	I	F	K	N	M	S	V
3725	G	E	U	L	E	A	H	D	W	A	V	Q	W	A	N	T	E	A	K	G	E	Q	E	B	W
3750	K	U	K	I	M	F	L	K	N	I	Y	M	W	U	L	U	A	W	U	V	M	U	Z	U	G

3775	O	U	E	T	S	K	U	W	C	Q	S	L	K	W	N	X	G	M	T	T	O	C	L	A	N
3800	T	A	O	W	A	P	N	O	Z	E	S	V	Q	Q	C	W	S	U	A	O	K	A	**S**	**V**	**Q**
3825	**O**	**V**	X	G	T	K	O	U	H	M	V	Q	N	O	**E**	**S**	**E**	**P**	**I**	**V**	**W**	J	A	I	C
3850	U	G	M	N	I	S	W	U	A	G	B	E	J	J	A	V	I	N	V	A	I	W	M	D	M
3875	D	G	T	L	I	V	S	L	G	C	R	J	J	A	V	Q	S	P	U	G	O	X	U	B	W
3900	J	U	W	C	Q	W	L	A	L	E	A	F	G	O	A	F	I	A	K	C	V	T	L	A	J
3925	G	K	T	M	E	W	P	B	R	M	X	W	T	M	N	K	W	S	N	M	Q	C	A	H	**G**
3950	**U**	**E**	**V**	**L**	E	C	B	E	Z	A	W	N	M	T	T	W	H	C	C	V	Z	W	**H**	**T**	**W**
3975	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	W	L	D	Q	E	V	S	D	C	D	E	Z	A	L	G	W	N
4000	T	W	J	G	U	A	Z	I	M	C	Q	T	I	H	W	K	V	E	L	S	T	Q	Z	D	T
4025	W	K	R	Z	E	U	A	W	T	M	S	**U**	**S**	**U**	**J**	**Q**	**N**	**M**	K	W	V	I	I	M	F
4050	L	U	Q	M	I	K	K	K	D	E	A	I	M	G	T	L	M	K	W	V	I	I	M	F	L
4075	R	Z	A	B	A	I	W	**M**	**M**	**M**	**F**	**L**	K	U	P	W	K	K	K	J	L	M	K	S	F
4100	M	P	T	S	U	G	Z	E	B	V	W	R	T	U	A	W	D	N	M	S	L	W	E	C	V
4125	D	**I**	**A**	**W**	**P**	**B**	U	V	W	E	C	Q	N	B	W	F	C	V	C	M	K	A	E	W	N
4150	A	A	V	G	Z	A	J	D	W	S	C	I	T	W	K	V	V	A	B	M	J	G	T	Q	C
4175	W	D	G	V	D	Z	G	A	V	W	U	T	W	K	I	M	N	A	W	K	U	I	Y	**I**	**A**
4200	**W**	**P**	**B**	**D**	**M**	D	W	U	C	T	Q	D	A	U	M	R	M	L	S	K	B	L	M	D	S
4225	D	W	R	I	L	G	K	Z	E	U	W	E	G	W	U	M	D	D	G	A	A	D	S	A	G
4250	V	T	M	L	W	O	Q	S	M	K	S	W	X	O	Q	F	L	F	M	U	F	A	W	O	**M**
4275	**M**	**M**	**F**	**L**	U	W	N	B	J	S	X	I	I	T	S	H	G	C	P	Z	W	K	K	V	V
4300	Q	K	A	D	T	E	M	L	S	K	B	S	I	F	K	R	Z	E	A	L	A	I	M	V	W
4325	M	K	R	W	U	D	A	W	B	U	O	V	L	J	G	Z	L	I	**E**	**S**	**E**	**P**	**I**	**V**	**W**
4350	S	W	F	V	Q	K	A	V	M	U	Z	K	W	V	K	**E**	**B**	**S**	**A**	**V**	X	L	C	K	**K**
4375	**R**	**M**	**C**	**B**	S	U	W	T	A	Q	J	W	F	M	P	T	M	K	K	M	U	Z	K	G	T
4400	L	R	M	K	V	G	O	R	I	F	V	G	C	R	Y	M	W	S	C	E	T	I	M	G	A
4425	F	M	M	A	N	T	E	A	V	W	N	Q	S	B	A	F	I	U	A	Q	K	D	G	X	L
4450	C	K	A	O	X	O	Z	L	S	P	B	D	M	L	G	W	B	**E**	**B**	**S**	**A**	**V**	Y	U	M
4475	D	W	R	Z	O	O	J	S	O	U	E	C	J	D	W	Q	M	M	E	W	C	D	A	Q	L
4500	M	P	M	O	X	A	F	K	W	N	B	J	W	U	U	O	L	W	K	V	M	D	M	K	G
4525	P	B	R	I	N	S	K	T	T	W	M	L	G	T	A	A	A	Y	P	Q	F	Q	U	**S**	**V**
4550	**Q**	**O**	**V**	V	W	U	W	N	B	J	S	X	I	I	T	N	W	P	I	I	B	V	W	N	M
4575	X	Q	K	L	G	V	C	M	V	W	E	M	T	B	W	H	T	W	D	Q	Y	A	G	C	S
4600	M	**E**	**S**	**E**	**P**	**I**	**V**	**W**	H	C	Z	C	M	I	M	G	K	E	B	L	W	O	I	C	P
4625	A	F	G	M	T	I	A	L	W	V	I	Y	M	W	K	T	N	M	K	S	X	**I**	**I**	**B**	**I**
4650	**M**	G	B	R	W	H	T	K	M	N	Y	M	W	U	M	S	**X**	**J**	**G**	**I**	**Z**	**A**	**U**	**E**	W
4675	U	V	A	D	S	A	G	V	T	Y	M	M	P	M	P	W	J	L	G	M	L	W	U	S	N
4700	M	E	B	S	M	U	A	I	X	M	A	U	Y	U	Q	D	**W**	**V**	**I**	**I**	**B**	T	A	G	V
4725	E	D	A	V	G	V	T	Y	M	W	E	M	T	B	W	E	C	K	H	Q	F	W	C	C	R
4750	I	A	L	W	V	E	L	M	J	G	M	D	M	N	A	G	T	I	U	A	L	G	M	I	T
4775	K	S	X	**I**	**I**	**B**	**I**	**M**	G	B	R	M	K	H	G	C	D	M	K	G	P	B	R	I	N
4800	S	K	T	A	C	J	S	K	B	U	V	W	N	C	T	E	C	J	V	W	Z	A	J	D	W
4825	H	Q	N	I	D	W	O	M	N	B	A	D	A	I	U	V	S	M	V	Z	E	I	K	H	G
4850	K	T	L	W	K	E	Q	R	K	G	F	U	B	A	V	U	W	U	Y	U	Q	S	N	C	Q
4875	T	C	F	W	K	V	F	T	M	W	P	K	E	X	J	G	H	W	N	L	W	K	W	Z	L
4900	I	L	L	K	B	U	L	W	V	W	X	R	W	Y	J	C	U	M	M	M	J	G	V	V	M
4925	J	K	U	W	N	B	J	S	X	I	I	T	V	M	P	K	O	B	W	W	P	X	L	C	K
4950	V	G	B	R	M	H	W	W	N	I	I	T	D	G	A	A	**U**	**S**	**U**	**J**	**Q**	**N**	**M**	W	L
4975	C	Q	T	P	S	T	K	B	U	M	D	D	**G**	**U**	**E**	**V**	**L**	L	T	W	P	T	W	F	V
5000	M	E	B	K	S	O	M	M	W	A	J	G	B	R	W	H	H	G	B	I	B	W	A	N	M

5025	T	I	A	L	C	T	E	B	J	G	K	B	A	T	G	J	U	Y	U	M	V	W	N	I	U
5050	B	J	W	U	W	N	K	G	V	G	L	I	V	K	L	T	C	C	B	A	G	P	M	N	O
5075	W	F	G	Z	A	T	H	D	W	B	O	B	K	A	P	O	U	T	A	W	T	T	A	Q	K
5100	K	C	Q	T	T	W	U	J	I	M	X	D	A	D	Z	E	I	M	P	E	W	N	A	L	J
5125	W	K	T	Q	G	F	U	T	**E**	**A**	**H**	**D**	**W**	**A**	I	V	S	L	V	M	N	L	M	W	U
5150	M	T	I	U	W	V	B	E	M	H	G	S	C	E	J	W	S	W	K	O	C	H	V	G	X
5175	R	W	Y	J	C	U	M	M	M	J	U	I	S	B	M	U	K	M	U	F	J	W	V	Q	R
5200	**I**	**A**	**W**	**P**	**B**	U	V	W	A	O	U	E	V	K	W	U	I	T	Q	K	X	C	K	T	Q
5225	G	F	K	V	T	M	D	D	G	K	T	C	W	D	N	M	D	M	K	S	U	B	U	K	W
5250	K	K	V	G	M	F	A	G	C	S	M	K	Y	T	I	C	M	S	M	Z	Y	U	M	D	D
5275	G	A	I	T	K	H	C	Z	V	M	F	S	K	M	N	B	S	X	C	Q	R	M	L	W	P
5300	Q	R	T	A	E	R	W	S	A	A	T	N	M	D	I	F	K	N	M	C	I	V	J	G	K
5325	O	V	L	J	C	Q	G	V	S	F	V	L	E	T	W	M	T	M	Q	C	A	H	**G**	**U**	**E**
5350	**V**	**L**	V	G	C	X	W	H	A	P	Q	O	V	K	U	Q	V	C	M	J	F	C	V	T	**T**
5375	**S**	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	F	I	T	M	F	L	F	M	C	M	L
5400	L	G	M	P	W	I	M	G	R	E	T	W	K	O	M	N	B	A	G	P	V	E	A	A	E
5425	R	**T**	**E**	**U**	**W**	**F**	**V**	R	Y	Z	W	N	K	M	N	L	J	S	K	A	T	W	M	L	C
5450	T	H	M	M	J	G	T	U	V	**W**	**W**	**V**	**I**	**I**	**B**	**I**	**M**	W	V	**P**	**Z**	**G**	**Y**	**T**	**I**
5475	**M**	**U**	W	M	T	D	R	I	A	E	G	V	T	K	G	E	R	M	T	M	F	L	F	M	V
5500	I	A	L	G	B	R	M	S	E	C	B	E	C	J	V	G	V	I	O	E	W	U	M	T	L
5525	S	K	V	C	C	M	K	D	C	C	T	Z	**W**	**W**	**V**	**I**	**I**	**B**	**I**	**M**	G	T	A	**X**	**J**
5550	**G**	**I**	**Z**	**A**	**U**	**E**	**S**	**V**	**Q**	**O**	**V**	F	**W**	**V**	**I**	**I**	**B**	J	A	G	V	D	M	H	D
5575	W	A	Q	C	W	D	Q	X	T	Q	E	A	U	**I**	**T**	**Q**	**G**	**F**	F	C	P	Z	G	U	G
5600	A	S	C	K	V	G	K	A	T	U	M	N	L	A	V	K	M	P	A	E	V	K	G	W	L
5625	A	V	K	D	C	C	T	Z	W	U	G	B	T	M	V	W	T	V	I	M	J	W	Q	X	I
5650	V	A	G	P	M	T	I	A	L	N	M	R	M	K	M	N	B	A	B	V	W	U	K	I	Z
5675	U	G	P	A	T	I	F	U	G	A	F	Z	W	I	W	M	N	B	W	K	Q	C	L	M	I
5700	M	K	X	**E**	**U**	**W**	**F**	**V**	L	I	A	H	G	P	Q	B	T	**W**	**W**	**V**	**I**	**I**	**B**	N	W
5725	T	Q	T	I	T	D	**G**	**U**	**E**	**V**	**L**	L	T	M	S	K	G	F	V	Z	A	Q	Y	F	C
5750	V	T	M	L	D	Q	V	R	M	F	U	Q	V	T	Z	S	A	V	A	O	C	N	W	P	B
5775	L	M	K	H	G	Z	A	V	U	W	P	I	I	D	W	I	W	C	N	M	X	G	K	A	Q
5800	C	W	V	G	A	M	I	U	Z	K	V	**E**	**A**	**H**	**D**	**W**	**A**	P	C	A	K	U	I	N	B
5825	W	K	U	M	R	**I**	**A**	**W**	**P**	**B**	D	Q	K	H	Q	V	I	J	D	W	U	T	A	**X**	**J**
5850	**G**	**I**	**Z**	**A**	**U**	**E**	**S**	**V**	**Q**	**O**	**V**	F	W	U	M	R	I	A	L	R	T	U	A	M	F
5875	R	Z	O	J	D	W	O	M	P	C	A	K	S	C	A	K	W	E	Q	U	E	V	L	D	C
5900	T	E	N	X	G	T	B	P	W	M	J	R	W	U	A	K	W	T	T	A	**U**	**S**	**U**	**J**	**Q**
5925	**N**	**M**	S	D	C	T	I	U	A	L	G	L	E	A	W	K	E	I	P	I	U	A	V	M	S
5950	V	W	K	G	Z	A	Q	L	H	N	C	S	V	W	U	G	A	S	I	A	J	G	M	T	K
5975	W	L	C	Q	T	J	A	W	P	T	A	B	G	M	V	K	E	M	F	I	W	W	I	**T**	**S**
6000	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	E	W	N	A	A	K	V	I	I	B	F	G
6025	P	U	A	Q	K	S	W	K	O	C	J	K	F	M	S	L	W	U	G	V	N	Q	W	K	U
6050	C	I	D	S	F	V	M	S	Y	M	W	N	Y	U	M	U	Z	Q	A	E	L	W	U	Q	U
6075	P	T	W	L	**G**	**U**	**E**	**V**	**L**	V	K	N	F	M	J	W	P	B	A	Z	J	A	X	I	D
6100	M	K	E	C	K	H	Q	F	W	U	X	L	C	K	H	W	Q	S	A	S	F	V	M	S	I
6125	H	H	C	Z	U	Z	W	F	V	X	A	A	K	W	W	**T**	**E**	**U**	**W**	**F**	**V**	X	L	C	K
6150	H	W	Q	S	A	S	F	V	M	S	L	M	F	Q	Z	D	Z	W	V	G	U	A	O	F	A
6175	V	C	D	M	E	S	K	A	P	T	M	K	R	C	I	A	K	S	P	B	E	A	V	W	R
6200	T	U	A	A	W	W	Z	S	W	J	V	T	M	S	L	W	E	C	O	N	Q	L	M	F	M
6225	M	I	A	K	C	C	L	Q	W	M	F	M	N	W	M	K	T	M	T	Z	G	M	X	M	R

Cara	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
Freq x%3 + 0	7.4	0.4	1.6	5	10	3.7	3.8	2.4	4.7	2.9	4.5	5.6	4.6	4.6	2.5	2.1	0.9	2.6	7.9	5	4.8	2.6	8.9	0.7	0.5	0.3
Freq x%3 + 1	3.9	4.4	6.7	1.2	1.4	1.6	7.9	0.6	5	0.9	4.9	2.1	8.5	3.4	2.3	4.3	6.4	2.3	0.6	6.1	6	7.2	6.1	2.1	0.7	3.2
Freq x%3 + 2	7.9	3.8	3.6	2.6	1.5	4.2	3.1	1.6	5.5	3.5	5.9	4.1	11.6	1.3	0.4	0.5	4	0.4	4.6	3.1	3.4	5.4	11.2	1.8	1.1	4

Cara	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
Freq x%4 + 0	7.5	5.6	3.8	2.2	1.3	2.4	2.3	1.7	6	2	4.7	4.3	12.9	0.8	0.4	0.5	5.8	0.6	3.1	4	3.5	6.6	10	2	1.1	4.9
Freq x%4 + 1	5.7	0.3	3.8	3.5	7.3	3.8	6.8	1.4	3.3	2.4	5.3	3.4	3.7	5.5	2.9	4.1	1.6	2.8	5.6	6.1	6.5	4.1	8.4	0.7	0.5	0.1
Freq x%4 + 2	6.7	5.4	4.5	2.6	1.6	2	2.1	1.2	7.2	2.6	5.6	4.9	13.7	1	0.6	0.8	5.7	0.3	2.4	3.6	3.4	5	8.4	2.7	1.2	4.8
Freq x%4 + 3	5.8	0.2	3.6	3.5	7	4.4	8.5	1.9	3.8	2.7	4.9	3.1	2.5	5.1	2.9	3.8	2	3.3	6.2	5.3	5.4	4.6	8.1	0.8	0.3	0.2

Cara	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
Freq x%5 + 0	5.7	2.7	3.5	3	4.8	4	4.2	1.8	4.6	2.8	4.6	3.4	8.6	2.7	2.5	2.3	3.8	1.8	4.2	4.4	5	5.8	8.7	2	0.8	2.3
Freq x%5 + 1	6.7	3.1	3.7	3.4	4.5	2.9	5.7	1.8	5.5	2.2	5.5	3.6	7.3	3	1.4	1.9	4.1	2	5.5	4.9	4.5	4.2	8.2	1.1	0.6	2.6
Freq x%5 + 2	7.6	3.3	3.7	2.6	3.9	2.9	4.6	1.4	4.4	2.4	5.2	4.6	9.2	2.9	1.2	2.4	3.8	2.1	3.6	4.9	4.6	5.1	8.6	1.6	1.3	2.2
Freq x%5 + 3	5.9	3.4	4.3	3.4	3.9	2.5	5.2	1.8	5.5	2.4	5.4	4.6	7.4	3	2	2.2	2.7	1.4	4	5.1	4.6	5	9.2	1.5	0.8	2.6
Freq x%5 + 4	6.2	1.8	4.6	2.3	4.5	3.5	5	0.8	5.4	2.3	4.9	3.5	8.6	3.9	1.6	2.7	4.4	1.5	4.5	4.5	4.9	5.2	9	1.4	0.3	2.7

Cara	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
Freq x%6 + 0	7.1	0.5	0	4.6	4.3	6.3	6.2	4.1	1.7	5.4	9	7.3	5.8	1.2	0	0.5	0.3	0	8.3	0.6	3.2	3.6	17.8	1.1	0.6	0.6
Freq x%6 + 1	0.5	0.1	8	0.8	2.8	3	15.6	1.1	0.9	0.8	6.9	0.4	0	6.1	3.7	8.1	3.8	3.9	1.2	7	8.1	8.1	7.8	1.2	0.1	0.1
Freq x%6 + 2	6.8	7.3	7.1	0.9	0	0.1	0.2	0.2	8.8	0.4	3.4	2.7	17.2	0.9	0.9	1	7.9	0.8	0	5.6	3.3	7.3	5.4	3.1	1.5	7.6
Freq x%6 + 3	7.8	0.4	3.3	5.4	15.6	1.1	1.4	0.8	7.7	0.4	0	3.8	3.4	8	5.1	3.7	1.4	5.3	7.4	9.5	6.3	1.5	0	0.4	0.4	0
Freq x%6 + 4	7.4	8.7	5.4	1.7	0.1	0.2	0.2	0.1	9.2	1.1	3	3.7	17	0.7	0.8	0.6	9	0.6	0	5.2	3.9	6.4	4.4	2.9	1.3	6.3
Freq x%6 + 5	8.9	0.3	0	4.4	3.1	8.3	6	3.1	2.1	6.5	8.5	5.6	6	1.8	0	0.1	0.1	0	9.1	0.7	3.5	3.5	17	0.6	0.7	0.4

Cara	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
Freq x%7 + 0	6.3	2.7	3.6	2.8	4.7	3.2	5.5	1.9	5.8	2.1	5.3	3.8	8	3.4	1.5	2.8	4	1.5	3.6	5.5	4.5	4.7	9.4	1.3	0.6	1.7
Freq x%7 + 1	6	2.9	4.5	3.1	3.8	3.2	5.3	1.7	6.9	2.5	4	4.6	8.6	2.6	1.7	2.1	3.6	1.2	4	4.5	4.7	6.8	7.5	1.1	0.7	2.2
Freq x%7 + 2	6.4	2.8	4.8	3.2	4.1	3	4.5	1.3	3.9	2.4	5.8	4.6	8.6	2.9	1.8	1.8	3.2	1.5	4.1	4.9	4.9	5.4	9.9	1.2	0.6	2.2
Freq x%7 + 3	6.2	2.6	3.1	1.9	4.6	2.8	4.8	1.2	5.6	1.7	6.3	3.7	7.7	3.1	1.6	1.7	4	2.7	4.8	4.9	5.2	4.4	9.7	2.1	1.1	2.5
Freq x%7 + 4	7.8	2.6	3.8	3.7	4	2.4	4.8	1.7	4.5	2.8	4.1	3.8	8.5	3.8	1	2.7	3.5	1.8	4.7	3.9	4.9	4.8	7.3	2.1	1.2	3.7
Freq x%7 + 5	6	3.7	4	2.2	4.7	3.9	5.4	1.7	3.2	2.5	5.4	3.8	8.3	2.9	1.9	2.1	4.5	1.8	4.5	4.3	4	4.5	9.6	1.6	0.6	2.9
Freq x%7 + 6	6.2	2.9	3.8	3.7	4.3	3.5	4.4	1.3	5.5	3	4.9	3.1	7.7	3	2.8	3	3.5	1.9	4.7	5.3	4.7	4.9	7.6	1.2	0.7	2.2

Correction

On observe que certain cryptogramme, ceux en rouge dans le texte, se répètent. Nous pouvons déterminer leur position (en comptant à partir de l'indicateur de position spécifié au début de la ligne). Par exemple nous avons :

- **TWGZSE** aux positions 259, 925, 997, 2485, 3973, 5377 et 6001. On en déduit donc que la clef est d'une longueur qui divise les écarts entre ces cryptogrammes. Ces écarts mesurent successivement : 666, 738, 2226, 3714, 5118, 5742, 72, 1560, 3048, 4452, 5076, 1488, 2976, 4380, 5004, 1488, 2892, 3516, 1404, 2028, 624, dont le PGCD vaut 6
- **USUJQ** aux positions 3520, 4036, 4966 et 5920. On en déduit donc que la clef est d'une longueur qui divise les écarts entre ces cryptogrammes. Ces écarts mesurent successivement : 516, 1446, 2400, 930, 1884, 954, dont le PGCD vaut 6
- **MFGWA** aux positions 1756, 2050, 2854 et 3316. On en déduit donc que la clef est d'une longueur qui divise les écarts entre ces cryptogrammes. Ces écarts mesurent successivement : 294, 1098, 1560, 804, 1266, 462, dont le PGCD vaut 6
- **GXGAS** aux positions 47, 1217, 2321 et 2369. On en déduit donc que la clef est d'une longueur qui divise les écarts entre ces cryptogrammes. Ces écarts mesurent successivement : 1170, 2274, 2322, 1104, 1152, 48, dont le PGCD vaut 6
- **AHDWA** aux positions 1540, 3730, 5134 et 5812. On en déduit donc que la clef est d'une longueur qui divise les écarts entre ces cryptogrammes. Ces écarts mesurent successivement : 2190, 3594, 4272, 1404, 2082, 678, dont le PGCD vaut 6

D'après le principe de Kasiski, il apparait que la clef est de longueur 6 (ou d'un de ses diviseurs mais cela pourrait difficilement en être autrement).

Observons à présent les statistiques.

- La lettre la plus fréquente par paquet de tous les 6, partant de 0 est, d'après le tableau W. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[0]` = S
- La lettre la plus fréquente par paquet de tous les 6, partant de 1 est, d'après le tableau G. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[1]` = C
- La lettre la plus fréquente par paquet de tous les 6, partant de 2 est, d'après le tableau M. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[2]` = I
- La lettre la plus fréquente par paquet de tous les 6, partant de 3 est, d'après le tableau E. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[3]` = A
- La lettre la plus fréquente par paquet de tous les 6, partant de 4 est, d'après le tableau M. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[4]` = I
- La lettre la plus fréquente par paquet de tous les 6, partant de 5 est, d'après le tableau W. Cela signifie que cette lettre code un E. En décalant donc de 4(=`codex('E')`), on en déduit que `clef[5]` = S

En conclusion la clef est SCIAIS.

HILL

Exercice 21

Calculer le déterminant de chacune des matrices suivantes. Identifier les matrices inversibles modulo 26 et donner leur inverse.

1. $A = \begin{pmatrix} 11 & 3 \\ 2 & 5 \end{pmatrix}$
2. $B = \begin{pmatrix} 3 & 1 \\ 4 & 6 \end{pmatrix}$
3. $C = \begin{pmatrix} 1 & -5 \\ -1 & 8 \end{pmatrix}$
4. $D = \begin{pmatrix} 1 & -5 \\ 1 & 8 \end{pmatrix}$
5. $E = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$
6. $F = \begin{pmatrix} 12 & 13 \\ 11 & 10 \end{pmatrix}$
7. $G = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
8. $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Correction

Si le déterminant est inversible modulo 26 alors la matrice est inversible et la formule est

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \det(A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

1. $A = \begin{pmatrix} 11 & 3 \\ 2 & 5 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(A) \equiv_{26} 49 \equiv_{26} 23$ et $\mathrm{PGCD}(23, 26) = 1$. On a de plus $23^{-1} \equiv_{26} -9 \equiv_{26} 17$. Dans ce cas
   $$A^{-1} \equiv_{26} 17 \begin{pmatrix} 5 & -3 \\ -2 & 11 \end{pmatrix} \equiv_{26} 17 \begin{pmatrix} 85 & -51 \\ -37 & 178 \end{pmatrix} \equiv_{26} \begin{pmatrix} 7 & 1 \\ 15 & 22 \end{pmatrix}$$
2. $B = \begin{pmatrix} 3 & 1 \\ 4 & 6 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(B) \equiv_{26} 14$ et $\mathrm{PGCD}(14, 26) = 2$. La matrice B n'est donc pas inversible modulo 26.
3. $C = \begin{pmatrix} 1 & -5 \\ -1 & 8 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(C) \equiv_{26} 3$ et $\mathrm{PGCD}(3, 26) = 1$. On a de plus $3^{-1} \equiv_{26} 9$. Dans ce cas
   $$C^{-1} \equiv_{26} 9 \begin{pmatrix} 8 & 5 \\ 1 & 1 \end{pmatrix} \equiv_{26} \begin{pmatrix} 72 & 45 \\ 9 & 9 \end{pmatrix} \equiv_{26} \begin{pmatrix} 20 & 19 \\ 9 & 9 \end{pmatrix}$$
4. $D = \begin{pmatrix} 1 & -5 \\ 1 & 8 \end{pmatrix}$. D'après la *règle du gamma* $\det(D) \equiv_{26} 13$ et $\mathrm{PGCD}(13, 26) = 13$. La matrice D n'est donc pas inversible modulo 26.
5. $E = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(E) \equiv_{26} -1$ et $\mathrm{PGCD}(1, 26) = 1$. On a de plus $(-1)^{-1} \equiv_{26} -1$. Dans ce cas
   $$E^{-1} \equiv_{26} (-1) \begin{pmatrix} 5 & -2 \\ -3 & 1 \end{pmatrix} \equiv_{26} \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} \equiv_{26} \begin{pmatrix} 21 & 2 \\ 3 & 25 \end{pmatrix}$$
6. $F = \begin{pmatrix} 12 & 13 \\ 11 & 10 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(F) \equiv_{26} -23 \equiv_{26} 3$ et $\mathrm{PGCD}(3, 26) = 1$. On a de plus $3^{-1} \equiv_{26} 9$. Dans ce cas

$$F^{-1} \equiv_{26} 9 \begin{pmatrix} 10 & -13 \\ -11 & 12 \end{pmatrix} \equiv_{26} \begin{pmatrix} 90 & -117 \\ -99 & 108 \end{pmatrix} \equiv_{26} \begin{pmatrix} 12 & 13 \\ 5 & 4 \end{pmatrix}$$

7. $G = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(G) \equiv_{26} 0$ et $\text{PGCD}(0, 26) = 26$. La matrice G n'est donc pas inversible modulo 26.
8. $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
   D'après la *règle du gamma* $\det(I) \equiv_{26} 1$ et $\text{PGCD}(1, 26) = 1$. On a de plus $1^{-1} \equiv_{26} 1$. Dans ce cas

$$I^{-1} \equiv_{26} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Exercice 22

Parmi les matrices suivantes, lesquelles sont des clefs du cryptosystème de Hill de dimension 2 par paquet de n ?

1. $n = 1$ et $A = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$
2. $n = 1$ et $B = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$
3. $n = 2$ et $C = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$
4. $n = 2$ et $D = \begin{pmatrix} 1 & 100 \\ 1001 & 1 \end{pmatrix}$
5. $n = 3$ et $E = \begin{pmatrix} 1 & 13 \\ 2 & 1 \end{pmatrix}$
6. $n = 2$ et $F = \begin{pmatrix} 2 & 0 \\ 2 & 13 \end{pmatrix}$

Correction

1. Par paquet de 1 on travail modulo 26. Il faut donc que $\text{PGCD}(\det(A), 26) = 1$. Or $\det(A) = 3$ et $\text{PGCD}(\det(A), 26) = 1$. La matrice A est donc une clef de chiffrement valide du cryptosytème de Hill.
2. Par paquet de 1 on travail modulo 26. Il faut donc que $\text{PGCD}(\det(B), 26) = 1$. Or $\det(B) = -8$ et $\text{PGCD}(\det(B), 26) = 2$. La matrice A n'est donc pas une clef de chiffrement valide du cryptosystème de Hill.
3. Par paquet de 2 on travail modulo 2526. Il faut donc que $\text{PGCD}(\det(C), 2526) = 1$. Or $\det(C) = 3$ et $\text{PGCD}(\det(C), 2526) = 3$. La matrice C n'est donc pas une clef de chiffrement valide du cryptosystème de Hill.
4. Par paquet de 2 on travail modulo 2526. Il faut donc que $\text{PGCD}(\det(D), 2526) = 1$. Or $\det(D) = -100099$ et $\text{PGCD}(\det(D), 2526) = 1$. La matrice D est donc une clef de chiffrement valide du cryptosystème de Hill.
5. Par paquet de 3 on travail modulo 252526. Il faut donc que $\text{PGCD}(\det(E), 252526) = 1$. Or $\det(E) = -25$ et $\text{PGCD}(\det(E), 252526) = 1$. La matrice E est donc une clef de chiffrement valide du cryptosystème de Hill.
6. Par paquet de 3 on travail modulo 252526. Il faut donc que $\text{PGCD}(\det(F), 252526) = 1$. Or $\det(F) = 26$ et $\text{PGCD}(\det(F), 252526) = 2$. La matrice E est donc une clef de chiffrement valide du cryptosystème de Hill.

Exercice 23

Par un chiffrement de Hill de dimension 2 par paquet de 1, chiffrer le mot *MATH* avec $\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ comme clef.

Correction
MYAH

Exercice 24

Par un chiffrement de Hill de dimension 2 par paquet de 1, chiffrer le mot *KAAMELOT* avec $\begin{pmatrix} 11 & 1 \\ 0 & 19 \end{pmatrix}$ comme

clef

Correction
GAMUDBRX

Exercice 25

On a utilisé un chiffrement de Hill de dimension 2 par paquet de 1 avec $\begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$ comme clef pour obtenir *QMPPEXZVIKUL*. Quel était le message clair ?

Correction
CESTPASFAUX

Exercice 26

On a utilisé un chiffrement de Hill de dimension 3 par paquet de 1 avec $\begin{pmatrix} 8 & 3 & 0 \\ 1 & 1 & 11 \\ 0 & 8 & 7 \end{pmatrix}$ comme clef pour obtenir *YNDKDUUHSLYZGEA*. Quel était le message clair ?

Correction
Ici la difficulté consiste à inverser la matrice donnée ; nommons la A.

Pour y arriver appliquons le processus de Gauss-Jordan pour déterminer la matrice inverse en étant précautionneux : les fractions n'existe pas mais il est possible que ça soit le cas pour les inverses modulaire (puisque nous sommes par paquet de 1, nous travaillons modulo 26). Voici le détail des itérations de cet algorithme.

1. Initialisation.
$$\begin{pmatrix} 8 & 3 & 0 & 1 & 0 & 0 \\ 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & 8 & 7 & 0 & 0 & 1 \end{pmatrix}$$
2. $L_1 \to L_2$, $L_2 \to L_1$, $L_3 \to L_3$
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 8 & 3 & 0 & 1 & 0 & 0 \\ 0 & 8 & 7 & 0 & 0 & 1 \end{pmatrix}$$
3. $L_1 \to L_1$, $L_2 \to L_2 - 8L_1$, $L_3 \to L_3$
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & -5 & -88 & 1 & -8 & 0 \\ 0 & 8 & 7 & 0 & 0 & 1 \end{pmatrix}$$
4. $L_1 \to L_1$, $L_2 \to L_2$, $L_3 \to 5L_3 + 8L_2$
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & -5 & -88 & 1 & -8 & 0 \\ 0 & 0 & -669 & 8 & -64 & 5 \end{pmatrix}$$
5. Modulo 26.
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & 21 & 16 & 1 & 18 & 0 \\ 0 & 0 & 7 & 8 & 14 & 5 \end{pmatrix}$$
6. $L_1 \to L_1$, $L_2 \to 5L_2$, $L_3 \to 3L_3$
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & 105 & 80 & 5 & 90 & 0 \\ 0 & 0 & 105 & 120 & 210 & 75 \end{pmatrix}$$
7. Modulo 26.
$$\begin{pmatrix} 1 & 1 & 11 & 0 & 1 & 0 \\ 0 & 1 & 2 & 5 & 12 & 0 \\ 0 & 0 & 1 & 16 & 2 & 23 \end{pmatrix}$$
8. $L_1 \to L_1 - 11L_3$, $L_2 \to L_2 - 2L_3$, $L_3 \to L_3$
$$\begin{pmatrix} 1 & 1 & 0 & -176 & -21 & -253 \\ 0 & 1 & 0 & -27 & 8 & -46 \\ 0 & 0 & 1 & 16 & 2 & 23 \end{pmatrix}$$
9. $L_1 \to L_1 - L_2$, $L_2 \to L_2$, $L_3 \to L_3$
$$\begin{pmatrix} 1 & 0 & 0 & -149 & -29 & -207 \\ 0 & 1 & 0 & -27 & 8 & -46 \\ 0 & 0 & 1 & 16 & 2 & 23 \end{pmatrix}$$
10. Modulo 26
$$\begin{pmatrix} 1 & 0 & 0 & 7 & 23 & 1 \\ 0 & 1 & 0 & 25 & 8 & 6 \\ 0 & 0 & 1 & 16 & 2 & 23 \end{pmatrix}$$

On en déduit que $A^{-1} = \begin{pmatrix} 7 & 23 & 1 \\ 25 & 8 & 6 \\ 16 & 2 & 23 \end{pmatrix}$

On a arrive alors

	YND	KDU	UHS	LYZ	GEA
X	$\begin{pmatrix}24\\13\\3\end{pmatrix}$	$\begin{pmatrix}10\\3\\20\end{pmatrix}$	$\begin{pmatrix}20\\7\\18\end{pmatrix}$	$\begin{pmatrix}11\\24\\25\end{pmatrix}$	$\begin{pmatrix}6\\4\\0\end{pmatrix}$
$A^{-1}X$	$\begin{pmatrix}470\\722\\479\end{pmatrix}$	$\begin{pmatrix}159\\394\\626\end{pmatrix}$	$\begin{pmatrix}319\\664\\748\end{pmatrix}$	$\begin{pmatrix}654\\617\\799\end{pmatrix}$	$\begin{pmatrix}134\\182\\104\end{pmatrix}$
$\equiv_{26}$	$\begin{pmatrix}2\\20\\11\end{pmatrix}$	$\begin{pmatrix}3\\4\\2\end{pmatrix}$	$\begin{pmatrix}7\\14\\20\end{pmatrix}$	$\begin{pmatrix}4\\19\\19\end{pmatrix}$	$\begin{pmatrix}4\\0\\0\end{pmatrix}$
	CUL	DEC	HOU	ETT	EAA

En conclusion, il n'est pas faux de dire que le cryptogramme se transforme en *CUL DE CHOUETTE*.

RSA

Exercice 27

On considère dans le système RSA, la clef publique $(319, 11)$.

1. Déterminer deux nombres premiers p et q tel que $p < q$ et $319 = pq$.
2. Justifier que $(319, 11)$ est une clef valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 11 en base 2.
   (b) Calculer 100^{11} modulo 319.
   (c) Quel est le message chiffré de $M = 100$?
4. Déterminer la clef privé associée à $(319, 11)$.
5. Déchiffrer le message $M' = 133$

Exercice 28

On considère dans le système RSA, la clef publique $(2581, 493)$.

1. Déterminer deux nombres premiers p et q tel que $p < q$ et $2581 = pq$.
2. Justifier que $(2581, 493)$ est une clef valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 493 en base 2.
   (b) Calculer 1421^{493} et 1308^{493} modulo 2581.
   (c) Quel est le message chiffré de *OVNI* ?
4. Déterminer la clef privé associée à $(2581, 493)$.
5. Déchiffrer le message *1972-2032*.

Exercice 29

Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est $(55, 3)$ et celle du secrétariat est $(33, 3)$.

1. Déterminer les clefs privés du professeur et du secrétariat.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef publique du secrétariat. Quel message chiffré correspond la note de 12 ?
3. Pour assurer l'authenticité des messages contenants les notes, le professeur signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

Exercice 30

Chiffrer le message suivant en RSA par la clef publique $(4559, 1705)$: CHIFFREMENTRSA.

Exercice 31

Déchiffrer le message suivant chiffrer en RSA de clef publique $(2047, 1931)$ et de clef privée inconnue :
$1141 - 2 - 1878 - 425 - 128 - 64 - 64 - 2 - 1434 - 1516 - 64 - 19 - 128 - 64$.

Exercice 32

Déchiffrer le message suivant chiffrer en RSA de clef publique $(444931, 97919)$ et de clef privée inconnue :
$32755 - 394934 - 234962 - 412077 - 169502 - 187788 - 83769$