Correction TD4

Exercice 1. (Chiffre de César)

1. Les lignes correspondantes du carré de Vigenère donnent le tableau

	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
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

Ainsi, le `C` est codé en `M`, le `E` est codé en `O`... On trouve donc que `C'EST PAS FAUX` est codé par `M'OCD ZKC PKEH`.

2. Dans un espoir de garder la surprise du message à décoder, on va décoder un autre message que celui sur la feuille de TD (la méthode est bien-sûr la même). Regardons le message `LMTQKQWCA TIAB KWCZAM`. Sachant qu'il a été codé avec la clé `I`, on considère le tableau

	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
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

Qui nous apprend que la lettre `L` code la lettre `D`, donc la première lettre du message en clair est un `D`. De même la deuxième est un `E`, etc... On trouve que le message clair est `DELICIOUS LAST COURSE`.

Notons que la lettre `A` code la lettre `S` dans ce cas : en fait décoder un message qui a été codé via la clé `I` revient à encoder un message avec la clef `S`. Ça sera plus clair avec la question suivante.

3. La lettre `A` correspond à $0 \in \mathbb{Z}/26\mathbb{Z}$. Le codage par la lettre d'indice i envoie la lettre `A` sur la lettre en question. L'indice de `A` devient donc $0 + i = i \in \mathbb{Z}/26\mathbb{Z}$. De même, la lettre `B` est envoyé sur la suivante de la lettre d'indice i, donc la lettre d'indice $i+1 \in \mathbb{Z}/26\mathbb{Z}$. Et ainsi de suite on obtient que la transformation associée au codage est l'addition de i à l'indice des lettres (dans $\mathbb{Z}/26\mathbb{Z}$).

En particulier, on obtient que le décodage s'effectue en soustrayant i à l'indice, autrement dit en ajoutant $26 - i$: le décodage par la i-ème lettre est équivalent au codage par la $26 - i$-ème lettre, c'est ce qu'on a vu à la question précédente.

4. On pose $j := ai + b$. Pour que le chiffrement affine de clé a, b soit décodable, il faut et il suffit que la transformation affine associée soit inversible. On a

$$j = ai + b[26] \Leftrightarrow j - b = ai[26]$$

Si a n'est pas inversible, il existe i, i' tels que $ai + b = ai' + b[26]$, dans ce cas, le chiffrement affine est indécodable. Par exemple si $a = 2$ et $b = 1$, alors le message `ANANAS` et `NANANS` sont tous deux encodés en `AAAAAL`.
Si a est inversible dans $Z/26\mathbb{Z}$, alors il existe un $a' \in \mathbb{Z}$ tel que $aa' \equiv 1[26]$. On a alors $a'j - a'b = i[26]$. Le décodage existe et correspond alors à un chiffrement affine de clé $a', -a'b$.

5. Une fois encore dans un soucis de conserver la surprise, on décode un autre message : `UXFFL JSDAEBJS`, dont on suppose qu'il a été codé avec la même clef, à savoir $a = 9$, $b = 3$. On a $9 \cdot 3 = 27 \equiv 1[26]$, l'inverse de 9 modulo 26 est donc 3. D'après la question précédente, le décodage correspond à un chiffrement affine de clé $a' = 3, b' = -3 \cdot 3 = -9$.

Lettre codée	U	X	F	F	L	J	S	D	A	E	B	J	S
Indice j	20	23	5	5	11	9	18	3	0	4	1	9	18
Image $i = a'j + b'$	25	8	6	6	24	18	19	0	17	3	20	18	19
Lettre claire	Z	I	G	G	Y	S	T	A	R	D	U	S	T

6. Les lettres les plus fréquentes du message crypté sont respectivement le `Z` et le `D`, avec 19 et 18 occurrences respectivement. La lettre la plus fréquente suivante est le `V`, avec 13 occurrences.

On fait donc l'hypothèse raisonnable que l'une des lettres `Z`, `D` code le `E`, et l'autre code le `A` :

- Si Z code A et D code E, alors on a

$$\begin{cases} a \cdot 0 + b \equiv -1[26] \\ a \cdot 4 + b \equiv 5[26] \end{cases} \Leftrightarrow \begin{cases} b \equiv -1[26] \\ a \cdot 4 \equiv 6[26] \end{cases}$$

  Attention, comme 4 n'est pas inversible modulo 26, il y a plusieurs solutions à $4a \equiv 6[26]$:

$$4a \equiv 6[26] \Leftrightarrow 4a = 6 + 26k \Leftrightarrow 2a = 3 + 13k \Leftrightarrow 2a \equiv 3[13] \Leftrightarrow a \equiv 8[13]$$

  On a donc $a \equiv 8[26]$ ou $a \equiv 21[26]$. Le premier cas est impossible car alors a ne serait pas inversible modulo 26, on prend donc $a \equiv 21[26]$. On calcule $a' = a^{-1} = 5[26]$ et $b' = -a'b = 5[26]$. Le premier mot serait alors décodé par FAMUGH : raté.

- Si Z code E et D code A, alors on a

$$\begin{cases} a \cdot 4 + b \equiv -1[26] \\ a \cdot 0 + b \equiv 3[26] \end{cases} \Leftrightarrow \begin{cases} a \cdot 4 \equiv -4[26] \\ b \equiv 3[26] \end{cases}$$

  Attention : comme 4 n'est pas inversible modulo 26, on ne peut pas déduire que $a \equiv -1[26]$! Il y a une autre possibilité :

$$4a \equiv -4[26] \Leftrightarrow 4a = -4 + 26k \Leftrightarrow 2a = -2 + 13k \Leftrightarrow 2a \equiv -2[13] \Leftrightarrow a \equiv -1[13]$$

  On a donc $a \equiv -1[26]$ ou $a \equiv 12[26]$. Le second cas est impossible car alors a ne serait pas inversible modulo 26, on prend donc $a \equiv -1[26]$. On calcule $a' = a^{-1} = -1[26]$ et $b' = -a'b = 3[26]$, le premier mot serait alors décodé par DEMAIN, c'est un mot en français ! En décodant le reste du texte, on obtient :

DEMAIN DES L'AUBE, A L'HEURE OU BLANCHIT LA CAMPAGNE
JE PARTIRAI. VOIS-TU, JE SAIS QUE TU M'ATTENDS.
J'IRAI PAR LA FORET, J'IRAI PAR LA MONTAGNE.
JE NE PUIS DEMEURER LOIN DE TOI PLUS LONGTEMPS.

C'est la première strophe d'un célèbre poème de Victor Hugo.

Exercice 2. (Chiffre de Vigenère)
1. Comme indiqué, on répète la clé pour obtenir RATRATRATRA (de même longueur que le message). On obtient le codage suivant :

S	Y	N	A	P	T	O	S	O	M	E
↓R	↓A	↓T	↓R	↓A	↓T	↓R	↓A	↓T	↓R	↓A
J	Y	G	R	P	M	F	S	H	D	E

2. On retrouve le chiffre de César en prenant pour clé un mot d'une seule lettre.

3. a) Soit x la variable aléatoire donnant la valeur d'une lettre choisie au hasard dans le texte. Pour toute lettre l, on a $P(x = l) = \frac{n_l}{n}$: C'est une bonne vieille expérience de Bernoulli avec $p = \frac{n_l}{n}$.

On répète deux fois l'expérience de Bernoulli ci-dessus (avec remise→ répétitions indépendantes). On a donc deux variables x_1 et x_2. La probabilité d'avoir les deux lettres égales à l est alors $P(x_1 = l \text{ et } x_2 = l) = \frac{n_l^2}{n^2}$ (loi Binomiale).

La formule des probabilités totales nous donne alors

$$IC = \sum_{l=\text{A}}^{\text{Z}} P(x_1 = l \text{ et } x_2 = l) = \sum_{l=\text{A}}^{\text{Z}} \frac{n_l^2}{n^2}$$

b) Dans un texte totalement aléatoire, la fréquence de chaque lettre est $\frac{1}{26}$. On obtient alors dans ce cas

$$IC = \sum_{l=\mathtt{A}}^{\mathtt{Z}} \frac{1}{26^2} = \frac{26}{26^2} = \frac{1}{26} \approx 0,03846$$

c) Un chiffrement par permutation ne fait qu'intervertir les indices des lettres, sans changer leurs fréquences respectives. Le calcul de l'indice de coïncidence du texte crypté correspond alors a une simple permutation dans l'indice de la somme.

d) Dans un texte en français assez long, on choisi par hasard un sous-texte indépendant des différentes lettres lettres, de sorte que la fréquence de chaque lettre soit identique dans le sous-texte. Ainsi, l'indice de coïncidence n'est pas modifié dans le sous-texte. En pratique dans un texte plus court, on s'attend à ce que l'indice de coïncidence ne soit "pas trop modifié".

e) Chaque lettre de la forme x_{ik} pour $i \geqslant 0$ est codé par la première lettre de la clef : c'est un chiffre de César (il en va de même des sous-texte de la forme "x_{ik+j}"$_{i\geqslant 0}$ pour $j < k$).

Exercice 3. (Chiffre de Hill)
1. Un mot de p lettres v est encodé par $w := Mv$. Pour pouvoir décoder, il faut que l'application

$$\begin{array}{ccc} (\mathbb{Z}/26\mathbb{Z})^p & \longrightarrow & (\mathbb{Z}/26\mathbb{Z})^p \\ v & \longmapsto & Mv \end{array}$$

soit bijective, ce qui équivaut à $M \in \mathrm{Gl}_p(\mathbb{Z}/26\mathbb{Z})$ et $\det(M) \in\in (\mathbb{Z}/26\mathbb{Z})^\times$.

2. Le déterminant est donné par $3 \cdot 8 - 5 \cdot (-5) = 24 + 25 \equiv -3[26]$. Cet élément est inversible, d'inverse -9. Les formule d'inversion de matrice donnent alors

$$M^{-1} = \det(M)^{-1} \begin{pmatrix} 8 & 5 \\ -5 & 3 \end{pmatrix} = -9 \begin{pmatrix} 8 & 5 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 19 & -1 \end{pmatrix}$$

3. On décompose le mot à coder en sous-mots de longueur 2 : `HO`, `RT`, `IL`, `LO`, `NN`, `AG`, `ES`. Ces mots induisent respectivement les vecteurs suivants : $(7, 14)$, $(17, 19)$, $(8, 11)$, $(11, 14)$, $(13, 13)$, $(0, 6)$, $(4, 18)$. On fait le produit de ces vecteurs par la matrice M : on obtient $(3, 17)$, $(8, 3)$, $(21, 24)$, $(15, 11)$, $(0, 13)$, $(22, 22)$, $(0, 8)$. Qui donnent au final le mot `DRIDVYPLANWWAI`.

4. Le message a été encodé par la matrice M, donc on le décode par la matrice M^{-1} qu'on a calculé à la question 2.

Couple de lettres cryptées	`XO`	`EM`	`LO`	`PV`	`VJ`	`HD`	`YK`
Vecteur v	$(23, 14)$	$(4, 12)$	$(11, 14)$	$(15, 21)$	$(21, 9)$	$(7, 3)$	$(24, 10)$
Vecteur$M^{-1}v$	$(2, 7)$	$(4, 12)$	$(8, 13)$	$(3, 4)$	$(7, 0)$	$(11, 0)$	$(6, 4)$
Couple de lettres claires	`CH`	`EM`	`IN`	`DE`	`HA`	`LA`	`GE`

On retrouve le message décrypté `CHEMIN DE HALAGE`.

5. On pose

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

La matrice qui a servi à l'encodage du message. On a

Lettres claire	`CR`	`YP`	`TO`	Lettres cryptées	`MP`	`OD`	`XM`
Vecteur v	$(2, 17)$	$(24, 15)$	$(19, 14)$	Vecteur Mv	$(12, 15)$	$(14, 3)$	$(23, 12)$

On obtient donc les systèmes d'équations suivants :

$$\begin{cases} 2a + 17b \equiv 12[26] \\ 2c + 17d \equiv 15[26] \end{cases} \quad \begin{cases} 24a + 15b \equiv 14[26] \\ 24c + 15d \equiv 3[26] \end{cases} \quad \begin{cases} 19a + 14b \equiv 23[26] \\ 19c + 14d \equiv 12[26] \end{cases}$$

On isole les deux couples d'inconnues (a, b) et (c, d) :

$$\begin{cases} 2a + 17b \equiv 12[26] \\ 24a + 15b \equiv 14[26] \\ 19a + 14b \equiv 23[26] \end{cases} \qquad \begin{cases} 2c + 17d \equiv 15[26] \\ 24c + 15d \equiv 3[26] \\ 19c + 14d \equiv 12[26] \end{cases}$$

On résout ces systèmes comme des systèmes linéaires "classiques" :

$$\begin{cases} 2a + 17b \equiv 12[26] \\ 24a + 15b \equiv 14[26] \\ 19a + 14b \equiv 23[26] \end{cases}$$

$$(L_2 \leftarrow L_2 - L_1) \begin{cases} 2a + 17b \equiv 12[26] \\ 5a + b \equiv 17[26] \\ 19a + 14b \equiv 23[26] \end{cases}$$

$$\begin{cases} 2a + 17(17 - 5a) \equiv 12[26] \\ b \equiv 17 - 5a[26] \\ 19a + 14(17 - 5a) \equiv 23[26] \end{cases}$$

$$\begin{cases} 2a + 3 - 7a \equiv 12[26] \\ b \equiv 17 - 5a[26] \\ 19a + 4 - 18a \equiv 23[26] \end{cases}$$

$$\begin{cases} -5a \equiv 9[26] \\ b \equiv 17 - 5a[26] \\ a \equiv 19[26] \end{cases}$$

Ce système n'est pas contradictoire car on a bien $-5 \cdot 19 \equiv 9[26]$. On a donc $(a, b) = (19, 0)$. On effectue des manipulations similaires pour le deuxième système :

$$\begin{cases} 2c + 17d \equiv 15[26] \\ 24c + 15d \equiv 3[26] \\ 19c + 14d \equiv 12[26] \end{cases}$$

$$(L_2 \leftarrow L_2 - L_3) \begin{cases} 2c + 17d \equiv 15[26] \\ 5c + d \equiv -9[26] \\ 19c + 14d \equiv 12[26] \end{cases}$$

$$\begin{cases} 2c + 17d \equiv 15[26] \\ d \equiv -(9 + 5c)[26] \\ 19c + 14d \equiv 12[26] \end{cases}$$

$$\begin{cases} 2c \equiv 15 + 17(9 + 5c)[26] \\ d \equiv -(9 + 5c)[26] \\ 19c \equiv 12 + 14(9 + 5c)[26] \end{cases}$$

$$\begin{cases} 2c \equiv 15 + -3 + 7c[26] \\ d \equiv -(9 + 5c)[26] \\ 19c \equiv 12 + 22 + 18c[26] \end{cases}$$

$$\begin{cases} -5c \equiv 12[26] \\ d \equiv -(9+5c)[26] \\ c \equiv 8[26] \end{cases}$$

Ce système n'est pas contradictoire car on a bien $-5 \cdot 8 \equiv 12[26]$, on trouve $(c,d) = (8,3)$. Au final, on trouve que la matrice de codage N est donnée par

$$\begin{pmatrix} 19 & 0 \\ 8 & 3 \end{pmatrix}$$

Exercice 4. (RSA)

1. Si n est un nombre premier, on sait que $\mathbb{Z}/n\mathbb{Z}$ est un corps : tous les éléments non nuls sont inversibles, donc $|(\mathbb{Z}/n\mathbb{Z})^\times| = n-1$ comme annoncé. Autre méthode : soit $x \in [\![1, n-1]\!]$ et soit d un diviseur commun à x et à n. Comme n est premier, on a $d = 1$ ou $d = n-1$. Or on a $d \leqslant x < n$, donc $d = 1$ et x, n sont premiers entre eux.

2. Par le théorème des restes chinois, on a un isomorphisme d'anneaux

$$\mathbb{Z}/(pq)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

En particulier, les inversibles de $\mathbb{Z}/(pq)\mathbb{Z}$ sont formés par les couples d'inversibles de $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, il y a $\varphi(p)\varphi(q)$ tels couples, d'où le résultat. Ce résultat est en fait vrai dés que n est produit de deux entiers premiers entre eux.

3. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$, muni de la multiplication, est un groupe, fini, et d'ordre $\varphi(n)$ par définition. Donc l'ordre de tout élément divise $\varphi(n)$ (théorème de Lagrange), on a donc $k^{\varphi(n)} = 1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, autrement dit pour tout k premier avec n.

4. Par hypothèse, il existe un entier k tel que $cd = 1 + k\varphi(n)$. Si t est premier avec n, on a alors par la question précédente

$$t^{cd} = t^{1+k\varphi(n)} = t(t^{\varphi(n)})^k \equiv t \cdot 1^k[n] \equiv t[n]$$

Si n divise t, le résultat est immédiat.
Si t n'est pas premier avec n et $t < n$, alors p divise t ou q divise t. Par symétrie on suppose que p divise t. On a alors $t \equiv 0[p]$ et $t^{\varphi(n)} = 0 = t[p]$. Comme t est premier avec q, on a $t^{\varphi(n)} = 1^{\varphi(p)}[q] = 1[q]$. Donc l'entier $t^{cd} = tt^{\varphi(n)}$ respecte le système de congruence suivant

$$\begin{cases} t^{cd} \equiv 0[p] \\ t^{cd} \equiv t[q] \end{cases}$$

Or t est un entier respectant ce système. Comme p et q sont premiers entre eux, on a $t \equiv t^{cd}[n]$ par le théorème des restes chinois.

5. On décode le message crypté $t' = t^c[n]$ en le mettant à la puissance d, on retrouve $t \in \mathbb{Z}/n\mathbb{Z}$ d'après la question précédente.

6. Pour attaquer ce système, il faut pouvoir calculer un inverse de c modulo $\varphi(n)$. C'est relativement facile a faire avec l'algorithme d'Euclide, mais il faut à minima connaître $\varphi(n) = (p-1)(q-1)$, donc il faut connaître p et q, donc savoir factoriser n en produit de nombre premier. C'est ce dernier point qui est algorithmiquement très difficile.

En pratique, on prend des entiers p et q extrêmement grand (de l'ordre de 2^{2048} par exemple), factoriser de tels entiers est tout simplement hors de propos à l'heure actuelle.

7. Comme le codage est fait dans $\mathbb{Z}/n\mathbb{Z}$, on ne peut coder des entiers t que si ils sont inférieurs à n (autrement, deux messages différents seraient codés de la même manière).

Exercice 5.

1.a) Le principe est d'écrire un nombre n de manière unique sous la forme $\sum_{i=0}^{k} a_i 2^i$ avec $a_i \in \{0,1\}$. On calcule cette décomposition de la façon suivante :

- Pour n, trouver la plus grande puissance 2^k telle que $2^k \leqslant n$.
- Il y aura un 1 en position k.
- Calculer la décomposition de $n - 2^k$.

b) La plus grande puissance de 2 inférieure à 77 est $2^6 = 64$, donc $77 = 1 * * * * * *$. On a $77 - 64 = 13$. On a clairement $13 = 8 + 4 + 1$, donc $13 = 1101$ en binaire. On a alors $77 = 1001101$.

c). On a

$$\begin{aligned} n &= 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^4 + 2^3 + 2^1 + 2^0 \\ &= 2^7(2^3 + 2^2 + 2 + 1) + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 - 2^2 \\ &= 2^7(2^4 - 1) + 2^6 - 1 - 2^2 \\ &= 128 * 15 + 64 - 1 - 4 \\ &= 64 * 30 + 59 \\ &= 1920 + 59 \\ &= 1979 \end{aligned}$$

2. Soit $e = \sum_{i=0}^{k} a_i 2^i$ l'écriture de e en base 2. On a

$$b^e = b^{(\sum_{i=0}^{k} a_i 2^i)} = \prod_{i=0}^{k} b^{a_i 2^i} = \prod_{\substack{i \in [\![0,k]\!] \\ a_i \neq 0}} b^{2^i}$$

3. On a déjà vu que $77 = 1001101$ en binaire, on doit donc calculer 6^{2^i} modulo 50 pour $i \in [\![0,6]\!]$.

- On a $6^1 \equiv 6[50]$, $6^2 \equiv 36[50]$
- On a $6^3 = 6 \cdot 36 = 180 + 36 = 216 \equiv 16[50]$, donc $6^4 \equiv 6 \cdot 16 \equiv 96 \equiv -4[50]$.
- On a $6^8 \equiv (-4)^2 \equiv 16[50]$
- On a $6^{16} \equiv 16^2 \equiv 4 \cdot 64 \equiv 4 \cdot 14 \equiv 6[50]$
- On a donc $6^{32} \equiv 6^2 \equiv 36[50]$ et $6^{64} \equiv 36^2 \equiv -4[50]$.

Au total, on a

$$\begin{aligned} 6^{77} &= 6^{64} \cdot 6^8 \cdot 6^4 \cdot 6 \\ &\equiv (-4) \cdot 16 \cdot (-4) \cdot 6 \\ &\equiv 16^2 \cdot 6 \equiv 6 \cdot 6 \equiv 36[50] \end{aligned}$$

Ensuite, on a $22 = 16 + 4 + 2 = 10110$. On calcule donc 5^{2^i} modulo 23 pour $i \in [\![0,4]\!]$.

- On a $5^2 = 25 \equiv 2[23]$
- On a $5^4 \equiv 4[23]$
- On a $5^8 \equiv 16[23]$
- On a $5^{16} \equiv 16^2 \equiv 8 \cdot 2 \cdot 16 \equiv 8 \cdot 9 \equiv 2 \cdot 36 \equiv 3[23]$

Au total, on a

$$\begin{aligned} 5^{22} &= 5^{16} \cdot 5^4 \cdot 5^2 \\ &\equiv 3 \cdot 4 \cdot 2[23] \\ &\equiv 1[23] \end{aligned}$$

Exercice 6.
1.a) On a $n = 53 \cdot 11 = 530 + 53 = 583$.
b) On a $\varphi(n) = \varphi(53)\varphi(11) = 52 \cdot 10 = 520$.
c) On doit inverser $c = 3$ modulo 520, on trouve par l'algorithme d'Euclide que $3 \cdot 173 = 519$, l'inverse de 3 modulo 520 est alors donné par -173.

2. On a respectivement,

$$10^3 = 1000 \equiv 417[n], \quad 52^3 \equiv 105[n], \quad 215^3 \equiv 557[583], \quad 211^3 \equiv 52[583]$$

Exercice 7.
1. Comme p et q sont proches, on a $p - q$ proche de 0 et s est "petit". On a ensuite

$$\begin{aligned} t^2 - s^2 &= \frac{1}{4}\left((p+q)^2 - (p-q)^2\right) \\ &= \frac{1}{4}\left(p^2 + 2pq + q^2 - p^2 + 2pq - q^2\right) \\ &= \frac{4pq}{4} = pq = n \end{aligned}$$

2. L'algorithme proposé trouve le plus petit entier t tel que $z = t^2 - n = s^2$ soit un carré. On a alors $n = t^2 - s^2$, et p, q sont des entiers. On a ensuite

$$pq = (t+s)(t-s) = t^2 - s^2 = n$$

Et on a même $p + q = 2t$ et $p - q = 2\sqrt{z} = 2s$

3. On pose $n = 899$, on a $\lceil \sqrt{n} \rceil = 30$, et $z = 30^2 - n = 1$ est un carré. On pose donc $p = 30 + 1 = 31$ et $q = 30 - 1 = 29$, ces deux nombres sont premiers et on a $pq = 899$. L'indicatrice d'Euler vaut alors $\varphi(p)\varphi(q) = 28 \cdot 30 = 840$. Pour trouver la clé privée, il faut alors inverser $c = 17$ modulo 840. Par l'algorithme d'Euclide, on trouve $d = 593$ la valeur permettant de décoder les messages.