Correction séance 8 (24 novembre)

Exercice 1. (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 :

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

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 2. (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 3.
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,

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