Cryptographie et arithmétique – Corrigé du DM

Partie I.

a. Mentionnons, même si cela est dispensable, que $1+n$ est bien inversible dans $(\mathbb{Z}/n^2\mathbb{Z})^*$, son inverse étant $1-n$ (un calcul direct le montre).
On a, pour $k \geqslant 0$, par la formule du binôme de Newton,

$$(1+n)^k = \sum_{i=0}^{k} \binom{k}{i} n^i = 1 + \underbrace{\binom{k}{1} n}_{=k} + \underbrace{\binom{k}{2} n^2 + \cdots + \binom{k}{k} n^k}_{\equiv 0 \bmod n^2}.$$

Donc $(1+n)^k \equiv 1 + kn \bmod n^2$. De cela, on voit que :

$$(1+n)^k \equiv 1 \bmod n^2 \Leftrightarrow 1 + kn \equiv 1 \bmod n^2 \Leftrightarrow kn \equiv 0 \bmod n^2,$$

ce qui équivaut au fait que n divise k ; autrement dit, la puissance vaut 1 si et seulement si l'exposant est un multiple de n. Ceci montre bien que n est le plus petit entier non nul k tel que $(1+n)^k = 1$ (dans $(\mathbb{Z}/n^2\mathbb{Z})^*$), et donc que $1+n$ est d'ordre n.

b. Rappelons d'abord la définition du logarithme discret d'un élément de $G = \langle 1+n \rangle$ en base $1+n$: tout élément de ce groupe s'écrit de façon unique (modulo n) comme une puissance de $1+n$. Autrement dit, l'application $\exp_{1+n} : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to & G \\ k \bmod n & \mapsto & (1+n)^k \end{cases}$ est une bijection, et même un isomorphisme de groupes, dont on note $\log_{1+n}$ l'application réciproque. Elle est caractérisée par les relations $\exp_{1+n}(\log_{1+n}(g)) = g$ et $\log_{1+n}(\exp_{1+n}(\bar{k})) = \bar{k}$. Autrement dit, pour tous $g \in G$ et $k \in \mathbb{Z}$,

$$(1+n)^{\log_{1+n}(g)} = g \text{ et } \log_{1+n}((1+n)^k) \equiv k \bmod n.$$

La question précédente a démontré, en passant, que $(1+n)^k \equiv 1+nk \bmod n^2$. Si $g \in G$ est un élément dont on veut calculer le logarithme discret, alors :

$$g = (1+n)^{\log_{1+n}(g)} \equiv 1 + n \log_{1+n}(g) \bmod n^2,$$

donc $\log_{1+n}(g) \equiv \frac{g-1}{n} \bmod n$ (la division est faite dans les entiers ; $g-1$ est forcément divisible par n, comme on peut le voir avec la formule du binôme de Newton). Ceci nous donne une méthode pour calculer le logarithme de g en base $1+n$ en temps polynomial : en calculant $\frac{g-1}{n} \bmod n$, tout simplement. La soustraction, la division et la réduction modulo n sont des opérations faites en temps polynomial.

c. L'identité $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, valable pour tout $n \geqslant 1$, est pertinente ici, parce que n et n^2 ont exactement les mêmes facteurs premiers, et donc $\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|n^2} \left(1 - \frac{1}{p}\right)$; ceci permet de lier très simplement $\varphi(n^2)$ et $\varphi(n)$. On a :

$$\varphi(n^2) = n^2 \prod_{p|n^2} \left(1 - \frac{1}{p}\right) = n \cdot n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n\varphi(n).$$

d. Vérifions d'abord que l'application $s : \begin{cases} (\mathbb{Z}/n\mathbb{Z})^* & \to & (\mathbb{Z}/n^2\mathbb{Z})^* \\ r \bmod n & \mapsto & r^n \bmod n^2 \end{cases}$ est bien définie, d'abord en vérifiant que si $r \equiv 1 \bmod n$, alors $r^n \equiv 1^n \bmod n^2$ (autrement dit, la classe

de congruence de 1 modulo n n'a bien qu'une seule image par s, donc $s(1 \bmod n)$ a bien un sens).
Si $r \equiv 1 \bmod n$, alors $r = 1 + kn$ avec $k \in \mathbb{Z}$, et donc $r \equiv 1 + kn \bmod n^2$. Alors,

$$r^n \equiv (1+kn)^n = 1 + \underbrace{\binom{n}{1}}_{=n} kn + \binom{n}{2}(kn)^2 + \cdots + \binom{n}{n} n^n \equiv 1 \bmod n^2,$$

Donc on a bien démontré que $s(1 \bmod n) \equiv 1^n \bmod n^2$ est uniquement défini. Maintenant, si $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et b est un entier tel que $b \equiv a \bmod n$, alors $ba^{-1} \equiv 1 \bmod n$, ce qui signifie (faire le raisonnement précédent avec $r = ba^{-1}$) que $(ba^{-1})^n \equiv 1 \bmod n^2$, et donc $b^n \equiv a^n \bmod n^2$. Là encore, $s(a \bmod n)$ est uniquement défini, peu importe l'entier b pris dans la classe de congruence de a, et ce raisonnement vaut pour tout entier a. Donc s est bien définie. C'est trivialement un morphisme : $s(ab) = s(a)s(b)$ revient à dire que $(ab)^n \equiv a^n b^n \bmod n^2$, ce qui est vrai par commutativité de la multiplication.

e. Si n et $\varphi(n)$ sont premiers entre eux, il existe u, v entiers tels que $un + v\varphi(n) = 1$. Alors :

$$r = r^1 = r^{un+v\varphi(n)} = (r^n)^u \cdot (r^{\varphi(n)})^v.$$

Par hypothèse, $r^n \equiv 1 \bmod n^2$ (et donc mod$n$ aussi), et par le théorème d'Euler, $r^{\varphi(n)} \equiv 1 \bmod n$, donc $r \equiv 1 \bmod n$.

Ces résultats liminaires serviront à construire les applications de chiffrement (l'application E) et de déchiffrement de Paillier dans la prochaine partie.

Partie II.

a. Vérifier que E est un morphisme revient à s'assurer que

$$E(m + m' \bmod n, rr' \bmod n) = E(m \bmod n, r \bmod n) \cdot E(m' \bmod n, r' \bmod n)$$

(ne pas oublier que $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour *l'addition* et $(\mathbb{Z}/n\mathbb{Z})^*$, $(\mathbb{Z}/n^2\mathbb{Z})^*$ pour la *multiplication* !). On déduit cette égalité des identités $(1+n)^{m+m'} = (1+n)^m(1+n)^{m'}$ et $(rr')^n = r^n r'^n$.
Pour montrer que E est un isomorphisme de groupes, c'est-à-dire un morphisme de groupes bijectif, il suffit de vérifier qu'il est injectif ; en effet, une application injective entre deux ensembles de même cardinal est nécessairement bijectif. On est dans ce cas de figure, étant donné que

$$\mathrm{card}((\mathbb{Z}/n^2\mathbb{Z})^*) = \varphi(n^2) = n\varphi(n) = \mathrm{card}(\mathbb{Z}/n\mathbb{Z})\mathrm{card}((\mathbb{Z}/n\mathbb{Z})^*),$$

d'après la question I.c. et la définition de φ. En principe, vérifier l'injectivité de E revient à montrer que $E(m \bmod n, r \bmod n) = E(m' \bmod n, r' \bmod n)$ implique $(m \bmod n, r \bmod n) = (m' \bmod n, r' \bmod n)$, mais un attrait des morphismes de groupes permet de limiter cette vérification au cas de l'élément neutre pour avoir l'injectivité [*]. Or, si $E(m \bmod n, r \bmod n) = E(0 \bmod n, 1 \bmod n)$, alors

$$(1+n)^m r^n = 1. \tag{1}$$

*. Expliquons brièvement pourquoi, dans le cas général d'un morphisme de groupes $f : (G, \cdot) \to (H, \times)$, faire la vérification pour 1_G implique immédiatement l'injectivité. Supposons que $f(g) = 1_H$ implique $g = 1_G$ (on a $f(1_G) = 1_H$). Alors, si $f(g) = f(g')$, on a $f(g) \times f(g')^{-1} = 1_H$, ce qu'on peut réécrire $f(g \cdot g'^{-1}) = 1_H$ par propriété d'un morphisme de groupes. Ceci implique, on l'a supposé, $g \cdot g'^{-1} = 1_G$, et donc $g = g'$: l'application f est bien injective.

Il serait commode, ici, de pouvoir d'abord se débarrasser de m ou r dans l'équation. Ce qui amène à l'idée d'élever à la puissance $\varphi(n)$ l'équation, puisque $r^{n\varphi(n)} = r^{\varphi(n^2)} \equiv 1 \bmod n^2$ par le théorème d'Euler (r est bien premier à n^2 : un diviseur premier commun à r et n^2 serait aussi un diviseur premier commun à r et n, mais il n'y en a pas). Faisons donc :

$$((1+n)^m r^n)^{\varphi(n)} = (1+n)^{m\varphi(n)}, \text{ et puis } (1+n)^{m\varphi(n)} = 1^{\varphi(n)} = 1,$$

dont nous déduisons que n divise $m\varphi(n)$ (voir I.a.). Par le théorème de Gauss, comme n est premier avec $\varphi(n)$ (hypothèse faite dans l'énoncé), on obtient finalement que n divise m, autrement dit : $m \equiv 0 \bmod n$. Il reste à montrer que $r \equiv 1 \bmod n$; partant de l'équation (1), comme nous avons montré que $m \equiv 0 \bmod n$, on a dorénavant $r^n = 1$. Donc, d'après la I.e., on a $r \equiv 1 \bmod n$.
Nous avons bien démontré que si $E(m \bmod n, r \bmod n) = E(0 \bmod n, 1 \bmod n)$, alors $(m \bmod n, r \bmod n) = (0 \bmod n, 1 \bmod n)$, d'où l'injectivité, puis la bijectivité par égalité des cardinaux.

b. Le calcul a été fait lors de la résolution de la question précédente, pour éliminer le r de l'équation : on a $c^{\varphi(n)} \equiv (1+n)^{m\varphi(n)} \bmod n$.
Déchiffrer le message revient à retrouver m partant de c (remarquons qu'on n'a pas besoin de r). Voici comment procéder :

- on calcule $c^{\varphi(n)}$ pour obtenir $(1+n)^{m\varphi(n)} \bmod n^2$ (cela nécessite la connaissance de $\varphi(n)$) ; cette exponentiation se fait en temps polynomial, par exponentiation binaire par exemple ;
- on calcule son logarithme discret en base $1+n$ pour obtenir $m\varphi(n) \bmod n$; on l'a vu en I.b., cela se fait également en temps polynomial ;
- comme $\varphi(n)$ et n sont premiers entre eux, multiplier $m\varphi(n)$ par l'inverse de $\varphi(n) \bmod n$ permet d'obtenir m ; le calcul d'inverse se fait grâce à l'algorithme d'Euclide étendu, lui aussi exécuté en temps polynomial.

En résumé, $m \equiv \log_{1+n}\left(c^{\varphi(n)}\right) \cdot \varphi(n)^{-1} \bmod n$. La clé privée de ce système est $\varphi(n)$ ou, c'est équivalent, l'ensemble des diviseurs premiers de n. Comme pour RSA, le système est d'autant plus robuste qu'il est difficile d'obtenir $\varphi(n)$ (ou l'ensemble des diviseurs premiers de n) malgré la connaissance de n. De plus, l'introduction d'un élément r qui peut être changé aléatoirement à chaque envoi de message chiffré permet d'éviter une attaque par analyse statistique. En principe, le chiffrement de Paillier est plus sûr que RSA.

c. On a $E(3 \bmod 35, 8 \bmod 35) \equiv 36^3 8^{35} \bmod 35^2 \equiv 2^{111} 3^6 \bmod 35^2$. C'est bien évidemment le calcul de 2^{111} qui nécessite le plus de précaution ; on procède par exponentiation binaire. En base binaire,

$$111 = 2^6 + 2^5 + 2^3 + 2^2 + 2^1 + 2^0 = 2(2(2\Big(2^2\Big(2+1\Big)+1\Big)+1)+1)+1,$$

et donc :

$$2^{111} = \left(\left(\left(\left(2^2 \cdot 2\right)^{2^2} \cdot 2\right)^2 \cdot 2\right)^2 \cdot 2\right)^2 \cdot 2.$$

Cette imbrication, malgré les apparences, rend les choses particulièrement simples à calculer (c'est le principe de l'exponentiation binaire), même à la main :

$$(2^2 \cdot 2)^{2^2} = 64^2 = 4096 \equiv 421 \bmod 1225, \quad \left((2^2 \cdot 2)^{2^2} \cdot 2\right)^2 \equiv (-383)^2 \equiv -311 \bmod 1225$$

$$\left(\left(\left(2^2\cdot 2\right)^{2^2}\cdot 2\right)^2\cdot 2\right)^2 \equiv -216 \bmod 1225, \quad \left(\left(\left(\left(2^2\cdot 2\right)^{2^2}\cdot 2\right)^2\cdot 2\right)^2\cdot 2\right)^2 \equiv 424 \bmod 1225,$$

$$2^{111} \equiv -377 \bmod 1225.$$

Plus rapidement, on obtient $3^6 = 27^2 = 729 \equiv -496 \bmod 1225$, donc

$$c = E(3 \bmod 35, 8 \bmod 35) \equiv (-377)\cdot(-496) \equiv -433 \bmod 1225.$$

J'ai choisi de procéder ainsi, mais on pouvait aussi calculer $36^3 \bmod 1225$ (très facile, même à la main) et 8^{35} par exponentiation binaire, sachant que $35 = 2^5 + 2^1 + 2^0$, et alors

$$8^{35} = \left(8^{2^4}\cdot 8\right)^2\cdot 8 \equiv \left(421^{2^2}\cdot 8\right)^2\cdot 8 \equiv \left((-384)^2\cdot 8\right)^2\cdot 8 \equiv (456\cdot 8)^2\cdot 8 \equiv -293 \bmod 1225.$$