Devoir à rendre le vendredi 1 avril.

La concision et la précision de la rédaction seront des qualités appréciées.

Exercice 1 1. Soit $n > 1$ un entier sans facteur carré (c'est-à-dire tel qu'il n'existe pas d'entier $k > 1$ vérifiant $k^2 \mid n$). Montrer que pour tout entier m,

$$m^{\phi(n)+1} \equiv m \pmod{n}.$$

2. Calculer $2^5 \pmod{12}$. Le résultat de la question précédente est-il vrai pour tout entier $n > 1$?
3. Soit p et q deux nombres premiers distincts et e un nombre premier avec $(p-1)(q-1)$. Rappeler pourquoi il existe un entier $0 < d < (p-1)(q-1)$ tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$. Calculer d pour $p = 23$, $q = 29$ et $e = 13$.
4. On pose $n = pq$. Montrer que pour tout entier m,

$$m^{ed} \equiv m \pmod{n}.$$

5. Principe du codage RSA :
   - L'interlocuteur X veut envoyer un message crypté à l'interlocuteur Y.
   - Pour ce faire Y choisit deux "grands" nombres premiers distincts p et q (qu'il ne communique pas) et il fournit sa clé publique (n, e) où $n = pq$ et e est un nombre premier avec $(p-1)(q-1)$.
   - Par ailleurs Y calcule d tel que $0 < d < (p-1)(q-1)$ et $ed \equiv 1 \pmod{(p-1)(q-1)}$. L'entier d constitue la clé privée de Y et n'est pas communiquée par celui-ci.
   - L'interlocuteur X décompose son message en une suite $M_1, \ldots, M_k$ d'entiers strictement inférieurs à n et calcule pour $0 < i \leq k$, $M_i' < n$ tel que $M_i^e \equiv M_i' \pmod{n}$ (en utilisant uniquement la clé publique (n, e) de Y). Il envoie alors le message (cryptée) $M_1', \ldots, M_k'$.

   D'après ce qui précède, expliquer comment Y peut décoder le message envoyé à l'aide de sa clé privé d. (A priori un autre interlocuteur ne pourra pas facilement décoder le message par ce procédé car le calcul de d repose sur la connaissance de la décomposition de n en facteurs premiers.)
6. Supposons que la clé publique de Y est le couple $(143, 7)$ et que le message de X est constitué de l'unique entier 101. Quel message crypté X envoie à Y ?
7. Supposons que la clé publique de X est le couple $(667, 13)$ et que Y envoie le message crypté 486. Décrypter ce message sachant que $667 = 23 \times 29$. On pourra pour cela calculer $486^d \pmod{23}$, puis $486^d \pmod{29}$ où d est la clé privée de X.