**RSA, primalité, factorisation**

## Variantes et attaques de RSA

**Exercice 1.** Bob a choisi la clef RSA publique $(n,3)$. Alice envoie à Bob le chiffré $c$ du message $m$ et le chiffré $c'$ du message $m+r$.

1. Exprimer $c' - c + 2r^3$ et $c' + 2c - r^3$ en fonction de $m$ et $r$.
2. Oscar intercepte $c$ et $c'$. On suppose qu'il connaît $r$ et que $c' - c + 2r^3 \not\equiv 0 \bmod n$. Comment peut-il obtenir $m$ en temps polynomial ?
3. Supposons $n = 2173$, $r = 1$, $c = 793$ et $c' = 2083$. Retrouver le message $m$.

**Exercice 2. (attaque de Wiener)** Soit $n = pq$ avec $p, q$ des nombres premiers, et $p \in ]q, 2q[$.

1. Montrer que si, pour une clé RSA publique $(n, e)$, on a $d < \frac{1}{3}\sqrt[4]{n}$, alors un attaquant peut calculer $d$ en temps polynomial à partir de $n$ et $e$. On utilisera, pour cela, le théorème suivant :

   **Théorème 1** *Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux fractions sous forme irréductible, telles que $\left|\frac{a}{b} - \frac{c}{d}\right| \leqslant \frac{1}{2d^2}$. Alors $\frac{c}{d}$ est une des réduites du développement de $\frac{a}{b}$ en fraction continuée.*

2. Pour éviter cette attaque, on donne $(n, e')$ comme clé RSA publique où $e' = e + t \cdot \varphi(n)$ avec $t$ grand. Montrer que si $e' > n\sqrt{n}$, alors même si $d < \frac{1}{3}\sqrt[4]{n}$, l'attaque ci-dessus ne peut pas être effectuée en temps rapide.

**Exercice 3. (chiffrement de Paillier)** Soit $n \geqslant 1$ un entier.

1. (a) Montrer que $1 + n$ est d'ordre $n$ dans le groupe $(\mathbb{Z}/n^2\mathbb{Z})^*$.
   (b) Notons $G = \langle 1 + n \rangle \subseteq (\mathbb{Z}/n^2\mathbb{Z})^*$. Comment calculer en temps polynomial le logarithme discret d'un élément de $G$ en base $1 + n$ ?
   (c) Exprimer $\varphi(n^2)$ en fonction de $n$ et $\varphi(n)$.
   (d) Construire un morphisme de groupes $s : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n^2\mathbb{Z})^*$ tel que $s(r \bmod n) = r^n$ pour tout $r \in (\mathbb{Z}/n^2\mathbb{Z})^*$.
   (e) Supposons $n$ et $\varphi(n)$ premiers entre eux. Montrer que $s$ est injectif.
2. Soit $n \geqslant 1$ un entier tel que $n$ et $\varphi(n)$ soient premiers entre eux. Soit

$$E : \begin{cases} \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^* & \to & (\mathbb{Z}/n^2\mathbb{Z})^* \\ (m \bmod n, r \bmod n) & \mapsto & (1+n)^m r^n \end{cases}.$$

   (a) Montrer que $E$ est un isomorphisme de groupes.
   Le cryptosystème de Paillier utilise $n$ comme clef publique. Pour chiffrer $m \in \mathbb{Z}/n\mathbb{Z}$, on choisit $r \in (\mathbb{Z}/n\mathbb{Z})^*$ et on calcule $c = E(m, r)$.
   (b) Calculer $c^{\varphi(n)}$. En déduire l'algorithme de déchiffrement et la clef privée de ce cryptosystème. Sur quoi repose sa sécurité ?

## Primalité

**Exercice 4. (critère de Korselt)** Soient $m, n \geqslant 2$ deux entiers. Montrer que les propriétés suivantes sont équivalentes :

- pour tout entier $a$, $n$ divise $a^m - a$ ;
- pour tout premier $p$ divisant $n$, $p^2$ ne divise pas $n$ et $p - 1$ divise $m - 1$.

En déduire qu'un nombre de Carmichael a nécessairement au moins trois facteurs premiers impairs, et que 561 en est un.

**Exercice 5. (nombre pseudo-premier en base $a$)** Soit $a \geqslant 2$ un entier. On dit qu'un entier $n$ est pseudo-premier en base $a$ s'il est composé et vérifie $a^{n-1} \equiv 1 \bmod n$ (les nombres de Carmichael sont donc des nombres pseudo-premiers en base $a$ pour tout entier $a$ premier avec eux).

1. Montrer que 341 est pseudo-premier en base 2.
   Soit $p$ un nombre premier impair qui ne divise pas $a^2-1$. On pose $n = \frac{a^{2p}-1}{a^2-1}$.
2. Montrer que $n$ n'est pas un nombre premier.
3. Montrer que $a^{2p} \equiv 1 \mod n$.
4. Calculer $(a^2-1)(n-1)$, puis montrer que $p$ divise $n-1$.
5. Montrer que 2 divise $n-1$, et en déduire que $n$ est pseudo-premier en base $a$, puis qu'il existe une infinité de nombres pseudo-premiers en base $a$.

**Exercice 6. (test de Lucas-Lehmer)** On pose $s_0 = 4$, et on définit par récurrence la suite $(s_i)_{i\geqslant 0}$ en posant $s_{i+1} = s_i^2 - 2$ pour tout $i \geqslant 1$. Soit $n \geqslant 2$ un entier, et supposons que $s_{n-2} \equiv 0 \bmod 2^n - 1$. Soit $p$ un diviseur premier de $2^n-1$, notons $A = \mathbb{Z}/p\mathbb{Z}[X]/(X^2-4X+1)$ et désignons par $\alpha$ la classe de $X$ dans $A$. Posons $\beta = 4-\alpha$.

1. Montrer par récurrence que $s_i = \alpha^{2^i} + \beta^{2^i}$ pour tout $i \geqslant 0$.
2. Déterminer l'ordre de $\alpha$ dans le groupe $A^*$.
3. En déduire que $2^n - 1$ est premier.

La réciproque est vraie, donc permet de détecter les nombres de Mersenne composés.

**Exercice 7. (théorème de Pocklington)** Soient $n \geqslant 2$ et $d \geqslant 2$ deux entiers. On suppose que pour tout facteur premier $p$ de $d$, il existe un entier $a_p$ tel que : $n$ divise $a_p^d - 1$ et $\operatorname{pgcd}(n, a_p^{d/p} - 1) = 1$. Considérons $q$ un facteur premier de $n$.

1. Soit $p$ un facteur premier de $d$. On note $v_p(d)$ le plus grand entier $k$ tel que $p^k$ divise $d$. Montrer que $p^{v_p(d)}$ divise l'ordre de $a_p$ dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$.
2. En déduire que $d$ divise $q-1$.
3. Prouver que si $d+1 > \sqrt{n}$, alors $n$ est premier.

**Exercice 8. (test de Rabin-Miller)** Soit $n \geqslant 3$ un entier impair. Écrivons $n-1 = 2^s m$, avec $m$ impair. Soit $a$ un entier premier à $n$.

1. Montrer que si $n$ est premier, alors soit $a^m \equiv 1 \mod n$, soit il existe $r \in [\![0, s-1]\!]$ tel que $a^{2^r m} \equiv -1 \mod n$.
   Si $n$ est composé, il existe tout de même certains entiers $a$ vérifiant ces congruences. On cherche à les compter ; il s'avère qu'au plus $\frac{1}{4}$ des éléments de $(\mathbb{Z}/N\mathbb{Z})^*$ sont concernés. Dorénavant, on suppose que $n$ n'est pas premier.
2. Soit $t \geqslant 0$. Écrivons $n = 1 + 2^s m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, avec $m$ impair. Posons $p_i - 1 = 2^{s_i} m_i$ (avec $m_i$ impair), $s_i' = \min(t, s_i)$ et $t_i = \operatorname{pgcd}(m, m_i)$. Montrer que le nombre d'éléments $a$ de $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $a^{2^t m} \equiv 1 \mod n$ égale $2^{s_1'+\cdots+s_k'} \cdot t_1 \cdots t_k$. En déduire qu'il y a soit zéro, soit autant d'éléments $a$ de $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $a^{2^t m} \equiv -1 \mod n$, ce dernier cas étant vérifié uniquement pour $t < \min_j s_j$.
3. Si $S$ est l'ensemble des éléments $a$ de $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $a^m \equiv 1 \mod n$ ou $a^{2^r m} \equiv -1 \mod n$ pour un certain $r \in [\![0, s-1]\!]$, montrer que

$$\frac{\operatorname{card}(S)}{\operatorname{card}((\mathbb{Z}/n\mathbb{Z})^*)} = \frac{t_1 \cdots t_k}{m_1 \cdots m_k} \frac{2^{-(s_1+\cdots+s_k)}}{p_1^{\alpha_1-1} \cdots p_k^{\alpha_k-1}} \left( \frac{2^{k s_1} + 2^k - 2}{2^k - 1} \right).$$

4. En déduire que $\mathrm{card}(S) \leqslant \frac{1}{4}\mathrm{card}((\mathbb{Z}/n\mathbb{Z})^*)$. Pour plus d'aisance, on traitera d'abord les cas $k = 1$, puis $k \geqslant 2$ et $\alpha_i > 1$ pour au moins un $i$. Ensuite, si $k \geqslant 2$ et $\alpha_i = 1$ pour tout $i$, on montrera d'abord que l'inégalité voulue est vérifiée pour $k \geqslant 3$ dès que l'un des $m_i$ est distinct de $t_i$. Les cas restants à traiter sont alors $m_i = t_i$ pour tout $i$ et $k \geqslant 3$, puis $k = 2$.
5. Décrire un algorithme polynomial qui prend en entrée un couple d'entiers naturels $(n, k)$ avec $n$ impair, et renvoie en sortie « Premier » si $n$ est premier, et renvoie « Composé avec probabilité au moins $1 - \frac{1}{4^k}$ » si $n$ est composé. Ainsi, avec un grand choix de $k$, il y a peu de nombres composés qui trompent ce test de primalité, appelé test de Miller-Rabin.

## Factorisation

**Exercice 9. (algorithme $p+1$ de Williams)** Soit $p$ un nombre premier. Soit $F = X^2 - bX + c \in \mathbb{Z}[X]$ tel que la réduction de $F$ modulo $p$ soit irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$. On pose $G_1 = 1$ et $G_2 = b$ ; on définit par récurrence la suite d'entiers $(G_n)_{n\geqslant 1}$ en posant $G_{n+2} = b \cdot G_{n+1} - c \cdot G_n$ pour tout $n \geqslant 1$.

1. Soit $n$ un multiple de $p + 1$. Démontrer que $p$ divise $G_n$.
2. Soit $N \geqslant 2$ un multiple de $p$. Soit $m \geqslant 3$ un entier tel que pour tout facteur premier $q$ de $p + 1$, on ait $q^{v_q(p+1)} \leqslant m$. Notons $M$ le ppcm de $1, 2, \ldots, m$. Montrer que $\mathrm{pgcd}(N, G_M) > 1$. Cet algorithme trouve donc un facteur non trivial de $N$ si $G_M \not\equiv 0 \bmod N$.

**Exercice 10.**

1. Soit $n \geqslant 2$ un entier impair. Compter le nombre de solutions à l'équation $x^2 = 1 \bmod n$.
2. Montrer comment factoriser $n$ à l'aide d'un entier $x \not\equiv \pm 1 \bmod n$ tel que $x^2 \equiv 1 \bmod n$.

**Exercice 11.** Supposons que $n$ soit un entier produit de deux nombres premiers impairs distincts $p$ et $q$. On note $e$, premier avec $\varphi(n)$, l'exposant public d'un système RSA de module $n$. Le but de l'exercice est de montrer que si un attaquant connaît $d$, alors il peut factoriser $n$ en temps polynomial.

1. Montrer comment, à partir de $e$, $d$ et $n$, on peut construire un multiple $B$ de $\varphi(n)$.
2. On note $m = \mathrm{ppcm}(p - 1, q - 1)$. Montrer que pour tout $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $\bar{a}^m = \bar{1}$. Montrer que $\bar{a}^{\frac{m}{2}}$ peut prendre quatre valeurs et que deux de ces valeurs permettent de factoriser $n$.
3. On pose $H = \{\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*; a^{\frac{m}{2}} \equiv \pm 1 \mod n\}$. Montrer que $H$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.
4. Montrer qu'il existe $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $\bar{b}$ soit d'ordre $p - 1$ modulo $p$ et d'ordre $\frac{q-1}{2}$ modulo $q$.
5. On pose $p - 1 = 2^{v_p} p'$ et $q - 1 = 2^{v_q} q'$ avec $p', q'$ impairs et on suppose, sans perte de généralité, que $v_p \geqslant v_q$. Exprimer $\frac{m}{2}$ en fonction de $v_p$ et du ppcm de $p'$ et $q'$. En déduire que $\bar{b}$ n'appartient pas à $H$. Si on prend $\bar{x}$ au hasard dans $(\mathbb{Z}/n\mathbb{Z})^*$, montrer que la probabilité que $\bar{x}$ n'appartienne pas à $H$ est supérieure ou égale à $\frac{1}{2}$.
6. Montrer que $m$ divise $B$ et en déduire qu'il existe un entier naturel $k$ tel que pour tout $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $x^{\frac{m}{2}} \equiv x^{B/2^{k+1}} \bmod n$.
7. En déduire un algorithme probabiliste polynomial qui factorise $n$ étant donnés $n$, $e$ et $d$, et donner sa probabilité de succès.

**Exercice 12. (algorithme $\rho$ de Pollard)** Soit $n$ un nombre entier à factoriser, et soit $p$ le plus petit facteur premier (inconnu) de $n$. L'idée est de construire une suite « aléatoire » $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_i, \ldots$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$, de sorte qu'une collision $x_i \equiv x_j \bmod p$ pour $i < j$ permette de trouver un facteur de $n$, donné par $\mathrm{pgcd}(x_i - x_j, n)$.

1. Montrer le paradoxe des anniversaires : la probabilité que $r$ nombres modulo $p$ soient tous distincts est $P_r = \left(1-\frac{1}{p}\right)\left(1-\frac{2}{p}\right)\cdots\left(1-\frac{r-1}{p}\right) \leqslant \exp\left(-\frac{r(r-1)}{2p}\right)$. Ainsi, si $r \geqslant 1+\sqrt{p}$, la probabilité d'avoir une collision est minorée par la constante $1-\exp\left(-\frac{1}{2}\right) \simeq 0{,}393$.
   On définit $(\bar{x}_i)_{i\geqslant 1}$ par la donnée de $\bar{x}_1$ et de la formule de récurrence $\bar{x}_{i+1} = \overline{P(x_i)}$, où $P \in \mathbb{Z}[X]$.
2. Montrer que si $x_i \equiv x_j \bmod p$, alors $x_{i+1} \equiv x_{j+1} \bmod p$.
3. En déduire que, si $x_i \equiv x_j \bmod p$ avec $i < j$ alors $x_u \equiv x_{2u} \bmod p$ pour un indice $u$ tel que $u < j$.
4. Comment calculer $(\bar{x}_{i+1}, \bar{x}_{2(i+1)})$ à partir de $(\bar{x}_i, \bar{x}_{2i})$ ?
5. On suppose que la suite $(\bar{x}_i)_{i\geqslant 1}$ obtenue a le même comportement qu'une suite de tirages indépendants dans $\mathbb{Z}/n\mathbb{Z}$, et donc qu'on peut appliquer le paradoxe des anniversaires. En déduire un algorithme qui nécessite environ $\sqrt{p}$ calculs de pgcd de nombres entiers naturels inférieurs à $n$ pour factoriser $n$.

**Exercice 13.** Soient $p$ et $q$ des nombres premiers impairs distincts et $n = pq$.

1. Soit $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. On note $(\alpha_p, \alpha_q)$ son image dans $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. Montrer que l'ordre de $\alpha$ égale le ppcm des ordres de $\alpha_p$ et de $\alpha_q$.
2. Soit $d = \text{pgcd}(p-1, q-1)$. Montrer qu'il existe un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $\frac{\varphi(n)}{d}$.
   Dans la suite on suppose de plus que $p > 3$, $q > 3$ et $\text{pgcd}(p-1, q-1) = 2$.
3. Montrer que $2n < 3\varphi(n)$.
4. Soit $\alpha$ un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $\frac{\varphi(n)}{2}$ et $0 \leqslant a < \frac{\varphi(n)}{2}$ le logarithme de $\alpha^n$ en base $\alpha$. Montrer que $n - a = \varphi(n)$.
5. Écrire un algorithme polynomial en la taille de $n$ qui prend pour entrées $n$ et $a$ et qui renvoie les facteurs $p$ et $q$ de $n$.