CRYPTOGRAPHIE ALGÉBRIQUE **4M035** **Feuille 3**
P. V. Koseleff

RSA - Attaques

Exercice 3.1. — Cryptosystème RSA
Soit $n \geq 1$ un entier. Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés par des éléments de $\mathbf{Z}/n\mathbf{Z}$. Soit (e,n) sa clé publique.

1. Déterminer sa clé secrète si $(e,n) \in \{(139,265),(31,3599)\}$.
2. Alice choisit le couple $(e,n) = (107,187)$. Bob lui envoie le cryptogramme 9. Quel est le message secret que Bob souhaite transmettre à Alice ?
3. Alice a perdu sa clé publique et ne possède que sa clé privée égale à $(3,88)$. Parmi ses papiers, elle retrouve le cryptogramme 7 envoyé par Bob, ainsi que le message décrypté égal à 113. Déterminer sa clé publique.

Exercice 3.2. —
Lors d'un protocole RSA, un même message M (considéré comme un entier) est chiffré en utilisant trois clés publiques distinctes : $(3,a),(3,b)$ et $(3,c)$, avec a,b,c premiers entre-eux deux à deux (en particulier, on a $M < \min(a,b,c)$. Notons A,B et C les cryptogrammes correspondants ($0 < A < a$, $0 < B < b$ et $0 < C < c$).

1. Montrer qu'il est possible de déterminer M en ne connaissant que A,B et C.
2. Trouver M, sachant que $(a,b,c) = (35,38,39)$ et $(A,B,C) = (1,1,5)$.

Exercice 3.3. — Soit $n \geq 3$ un entier impair vérifiant les deux conditions suivantes :

1. Pour tout entier a premier avec n, on a $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$.
2. Il existe un entier b tel que l'on ait $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.

Montrer que n est sans facteur carré, puis que n est premier.

Exercice 3.4. — Soit p un nombre premier.

1. Posons $n = 2p+1$. Montrer que n est premier si et seulement si on a $2^{n-1} \equiv 1 \pmod{n}$.
2. Plus généralement, soit $h < p$ un entier naturel non nul. Posons $n = hp+1$ et supposons $2^h \not\equiv 1 \pmod{n}$. Montrer n est premier si et seulement si on a $2^{n-1} \equiv 1 \pmod{n}$.

Exercice 3.5. — Calcul de $\lfloor\sqrt{n}\rfloor$
Soit à calculer une approximation de $\sqrt{n}$, où $n \in \mathbf{N}$.

1. On utilise la méthode de Héron. $x_0 = \frac{1}{2}(n+1)$, $x_{k+1} = \frac{1}{2}\left(x_k + \frac{n}{x_k}\right)$.
   (a) Montrer que $(x_k)_k$ est décroissante et converge vers $\sqrt{n}$.
   (b) Montrer que $\frac{x_{k+1}-\sqrt{n}}{\sqrt{n}} \leq \frac{1}{2}\left(\frac{x_k-\sqrt{n}}{\sqrt{n}}\right)^2$ et finalement, $x_k \leq \sqrt{n} + \frac{1}{2}\left(\frac{\sqrt{n}-1}{2\sqrt{n}}\right)^{2^k}$.
2. On considère une variante qui calcule $\lfloor\sqrt{n}\rfloor$. Pour cela, on calcule t tel que $4^t \leq n < 4^{t+1}$ et on calcule

$$y_0 = 2^{t+1}, \quad y_{k+1} = \lfloor\tfrac{1}{2}\left(y_k + \tfrac{n}{y_k}\right)\rfloor, k \geq 0.$$

   (a) Montrer que si $x \in \mathbf{N}$, alors $\lfloor\frac{1}{2}\left(x+\frac{n}{x}\right)\rfloor = \lfloor\frac{1}{2}\left(x+\lfloor\frac{n}{x}\rfloor\right)\rfloor$.
   (b) Montrer que la suite y_k est strictement décroissante puis, si $y_r \leq \sqrt{n}$, on a $y_{r+1} \geq y_r$. Montrer alors que $y_r = \lfloor\sqrt{n}\rfloor$.

Exercice 3.6. — Attaques contre RSA
Soit $n = pq$, le produit de deux nombres premiers.

1. Montrer que $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.
2. Si $p > q$ et $p-q$ est petit, on montre que $(p+q)/2$ est proche de $N = [\sqrt{n}]+1$.
   (a) Montrer que $\frac{p+q}{2} - \sqrt{n} \geq 0$.
   (b) Montrer que $\frac{p+q}{2} - \sqrt{n} \leq \frac{1}{8}\frac{(p-q)^2}{q}$
   (c) En déduire que si $p-q < 2n^{1/4}$ alors $p+q = 2[\sqrt{n}]+2$
   (d) Montrer que dans ce cas on peut factoriser n.

Si $p-q$ est petit, alors $\frac{p+q}{2} = N+c$ où $c \in \mathbf{N}$ n'est pas trop grand. On calculera $(N+c)^2 \pmod n$ pour des petites valeurs de c en espérant trouver l'opposé d'un carré.

Exercice 3.7. — Racines carrées de -1

1. Montrer que -1 est un carré si et seulement si 4 divise $p-1$.
2. On pose $p-1 = 2^s t$. Si $y \in \mathbf{F}_p^*$ on définit la suite $y_i = y^{2^i t}, 0 \leq i \leq s$.
   (a) Soit $G \subset \mathbf{F}_p^*$ l'ensemble des éléments y tels que $y^{2t} = 1$. Montrer que $|G| = 2t$, et que toute suite $(y_i)_{i=0,\ldots,s}$ de donnée initiale $y_0 \in \mathbf{F}_q^* - G$ contient une racine carrée de $-1 \pmod p$.
   (b) En déduire un algorithme probabiliste qui détecte, en $O(\log p)$ opérations modulo p, une racine carrée de $-1 \pmod p$. Le comparer avec l'algorithme déterministe qui donne $x_0 = \left(\frac{p-1}{2}\right)!$ comme racine carrée de -1 modulo p.

Exercice 3.8. — Partage d'une partie de la clé de déchiffrement
Soit $n = pq$, où p et q sont deux nombres premiers distincts. On suppose connus deux entiers e et d tels que pour tout $x \in \mathbf{Z}/n\mathbf{Z}$, on ait $x^{ed} = x$.

1. Montrer que la connaissance de n et de $\varphi(n)$ est équivalente à la connaissance de p et de q. Expliquer comment calculer p et q à partir de n et $\varphi(n)$.
2. Soit $x \neq \pm 1$, tel que $x^2 \equiv 1 \pmod n$. Montrer que $n = (n, x-1)\cdot(n, x+1)$ est une factorisation non triviale de n.
3. Montrer que $\mathrm{ppcm}\,(p-1, q-1)$ divise $ed-1$.
4. On pose $ed-1 = 2^s \cdot t$, où t est impair. Soit u un élément pris au hasard dans $(\mathbf{Z}/n\mathbf{Z})^*$.
   (a) Quelle est la probabilité que $u^t = \pm 1$?
   (b) En déduire une méthode de factorisation de n.