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.

Solution 3.1. —

1. On a $n = 5 \times 53$ donc $\varphi(n) = 208$. Il s'agit de déterminer l'inverse de 139 modulo 208. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	2	69	
208	139	69	1	0
1	0	1	-2	
0	1	-1	3	

   On en déduit l'égalité $3 \times 139 - 2 \times 208 = 1$, donc 3 est l'inverse de 139 modulo 208. Par suite, la clé secrète est $(3,208)$.
2. Supposons $n = 3599$. On a les égalités
$$n = 3600 - 1 = 60^2 - 1 = 59 \times 61,$$
   d'où $\varphi(n) = 3480$. En utilisant l'algorithme d'Euclide, on obtient l'égalité
$$4 \times 3480 - 449 \times 31 = 1,$$
   donc l'inverse de 31 modulo 3480 est 3031. La clé secrète est ainsi $(3031,3480)$.
3. On a $n = 11 \times 17$, $\varphi(n) = 160$. L'inverse de 107 modulo 160 est 3 (algorithme d'Euclide). Par suite, le message m que Bob souhaite transmettre à Alice est
$$m = 9^3 \mod 187 = 168 \mod 187.$$
4. Soit (e,n) la clé publique d'Alice. On a $n = pq$ et $p < q$ premiers. On a les relations
$$\varphi(n) = (p-1)(q-1) = 88 \quad \text{et} \quad 3e \equiv 1 \mod 88.$$
   L'égalité $87 = 3 \times 29$ implique $e \equiv -29 \equiv 59 \mod 88$, d'où $e = 59$. Déterminons n. En considérant les factorisations de 88 comme produit de deux entiers, on en déduit que le couple (p,q) appartient à l'ensemble $\{(2,89),(5,23)\}$, ce qui correspond à $n = 178$ ou $n = 115$. Par ailleurs, d'après les hypothèses faites, on a la congruence
$$7^3 \equiv 113 \mod n.$$
   (Avec les notations du cours, on a $d = 3$ et dans $\mathbf{Z}/n\mathbf{Z}$ on a les égalités $x_0 = 113$, $7 = x_0^e$ puis $7^3 = 113$.) Ainsi n divise l'entier
$$7^3 - 113 = 343 - 113 = 230 = 2 \times 115,$$
   d'où $n = 115$, puis $(e,n) = (59,115)$.

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 $(A,B,C) = (1,1,5)$.

Solution 3.2. —

1. D'après le théorème chinois, il existe un entier x avec $0 \leq x < abc$ et un seul qui est congru à $A(\bmod a)$, à $B(\bmod b)$ et à $C(\bmod c)$, et on peut calculer x grâce aux identités de Bézout. Le protocole dit que M^3 vérifie ces congruences. Comme on a de plus $M^3 < abc$, on voit que $x = M^3$. Il suffit de calculer la racine cubique de x pour trouver M.
2. On veut $x \equiv 1(\bmod 35.38)$ et $x \equiv 5(\bmod 39)$. On peut passer par Bézout ou résoudre $5 \equiv x = 1 + 35.38 \equiv 1 + 4k$ ($\bmod 39$). On peut prendre $k = 1$, d'où $M^3 = 35.28 + 1 = 1331 = 11^3$

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 $a^{\frac{n-1}{2}} \equiv \pm 1 \,(\bmod n)$.
2. Il existe un entier b tel que l'on ait $b^{\frac{n-1}{2}} \equiv -1 \,(\bmod n)$.

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

Solution 3.3. — Pour tout entier a premier à n, on a $a^{n-1} \equiv 1 \bmod n$.

Montrons que n est sans facteur carré. Supposons que p^2 divise n, alors p divise $\varphi(n)$. Donc $(\mathbf{Z}/n\mathbf{Z})^*$ possède un élément $\overline{a}$ d'ordre p (théorème de Cauchy). Comme $\overline{a}^{n-1} = 1$, on déduit que p divise $n-1$. Comme p divise également n alors $p = 1$. Contradiction.

Supposons que $n = mm'$ avec $\text{pgcd}(m,m') = 1$. D'après le théorème chinois, il existe un entier c tel que l'on ait

$$c \equiv b \,(\bmod m) \quad \text{et} \quad c \equiv 1 \,(\bmod m').$$

On a donc

$$c^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1 \,(\bmod m) \quad \text{et} \quad c^{\frac{n-1}{2}} \equiv 1 \,(\bmod m').$$

Si $c^{\frac{n-1}{2}} \equiv \pm 1 \,(\bmod n)$ alors $1 \equiv -1 \,(\bmod m)$ ou $1 \equiv -1 \,(\bmod m')$ et 2 divise m ou m' ce qui est impossible car n est impair.

Exercice 3.4. — Soit p un nombre premier.

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

Solution 3.4. —

1. Le résultat est vrai si $p = 2$. On supposera donc $p \geq 3$.
   Supposons $2^{n-1} \equiv 1 \,(\bmod n)$. L'entier n est impair. Soit d l'ordre de 2 modulo n. On a $2^{2p} \equiv 1 \,(\bmod n)$, donc d divise $2p$. On en déduit que p divise d, sinon d divise 2 ce qui n'est pas. Par ailleurs, on a $2^{\varphi(n)} \equiv 1 \bmod n$. Par suite, p divise $\varphi(n)$ (car d divise $\varphi(n)$). On a $\varphi(n) \leq n-1$, d'où $\varphi(n) = p$ ou $2p$. Or $\varphi(n)$ est pair, donc $\varphi(n) = 2p = n-1$, ce qui prouve que n est premier. L'implication réciproque résulte du petit théorème de Fermat.
2. Supposons $2^{n-1} \equiv 1 \bmod n$. Soit d l'ordre multiplicatif de 2 modulo n. L'entier d divise $n-1 = hp$. La condition $2^h \not\equiv 1 \bmod n$ entraîne que d ne divise pas h. D'après le théorème de Gauss, on en déduit que p

divise d : si p ne divise pas d, d et p sont premiers entre eux. Puisque d divise $\varphi(n)$ (théorème d'Euler), p divise $\varphi(n)$. Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition de n en facteurs premiers. On a

$$\varphi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1-1)\cdots(p_r-1).$$

Par hypothèse, p divise $n-1$, donc il ne divise pas n, ainsi il existe i tel que $p_i \equiv 1 \mod p$. Posons $n = p_i m$. Vérifions que l'on a $m = 1$, ce qui prouvera que n est premier. On a $m \equiv 1 \mod p$ car tel est le cas de p_i et n. Posons $p_i = up+1$ et $m = vp+1$ où $u, v \in \mathbf{N}$. On a l'égalité $hp+1 = (up+1)(vp+1)$, d'où $h = uvp+u+v$. L'inégalité $h < p$ entraîne alors $v = 0$ et l'assertion.
Inversement, si $n \geq 3$ est premier, on a $2^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$, d'où le résultat.

Exercice 3.5. — Calcul de $[\sqrt{n}]$
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

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

   (a) Montrer que si $x \in \mathbf{N}$, alors $\lfloor \frac{1}{2}\big(x+\frac{n}{x}\big)\rfloor = \lfloor \frac{1}{2}\big(x+\lfloor\frac{n}{x}\rfloor\big)\rfloor$.
   (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 $y_r = \lfloor\sqrt{n}\rfloor$.

Solution 3.5. —

1. On a $x_0 - \sqrt{n} = 1/2(n+1-2\sqrt{n}) = 1/2(\sqrt{n}-1)^2 \geq 0$ donc $x_0 \geq \sqrt{n}$. Si $x_k \geq \sqrt{n}$, alors $x_{k+1} - x_k = 1/2(n/x_k - x_k) \leq 0$ et $x_{k+1} - \sqrt{n} = \frac{(x_k-\sqrt{n})^2}{2x_k} \geq 0$.

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

1. Montrer que $n = \big(\frac{p+q}{2}\big)^2 - \big(\frac{p-q}{2}\big)^2$.
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 $(N+c)^2 \,(\mathrm{mod}\, n)$ pour des petites valeurs de c en espérant trouver l'opposé d'un carré.

Solution 3.6. —

1. On a bien $(p+q)^2 - (p-q)^2 = 4pq$.
2. (a) On a $(p+q) - 2\sqrt{pq} = (\sqrt{p}-\sqrt{q})^2 > 0$.
   (b) Donc $\frac{p+q}{2} - \sqrt{n} = \frac{1}{2}(\sqrt{p}-\sqrt{q})^2$. Mais $\dfrac{\sqrt{p}-\sqrt{q}}{p-q} = \frac{1}{2}\dfrac{1}{\sqrt{q}+\varepsilon}$, d'aprs le théorme des accroissements finis et finalement $\dfrac{\sqrt{p}-\sqrt{q}}{p-q} \leq \dfrac{1}{2\sqrt{q}}$ et pour finir $\frac{p+q}{2} - \sqrt{n} \leq \frac{1}{8}\frac{(p-q)^2}{q}$.

(c) Si $N = [\sqrt{n}]+1$ alors $\frac{p+q}{2} - N < fracp+q2 - \sqrt{n} \leq \frac{1}{8}\frac{(p-q)^2}{q}$. Mais si $p-q \leq 2n^{1/4}$, alors $q > \sqrt{n} - n^{1/4}$ et $\frac{p+q}{2} - N \leq \frac{1}{2}\frac{\sqrt{n}}{\sqrt{n}-n^{1/4}} = \frac{1}{2}\frac{n^{1/4}}{n^{1/4}-1} < 1$ dès que $n > 16$.

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.

Solution 3.7. —

1. -1 est un carré a^2 si et seulement si a est d'ordre 4. $(\mathbf{Z}/p\mathbf{Z})^*$ possède un élément d'ordre 4 si et seulement si 4 divise $p-1$.
2. (a) G est un sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^*$ cyclique engendré par g d'ordre $2^s t$. $g^k \in G$ si et seulement si $2^s t$ divise $2kt$, c'est-à-dire, 2^{s-1} divise k. On trouve que $k = 2^{s-1}k'$ où $k' \in [\![0, 2t-1]\!]$.
   Si $y_0 = y^{2t} \neq 1$ alors $y^t \neq \pm 1$. Par ailleurs $y_s = (y_0)^{2^s} = 1$. Soit i le premier entier tel que $y_i = 1$. Alors $i \geq 2$ et $y_{i-2}^2 = -1$.
   (b) On calcule y_0 en $O(\log t)$ opérations dans $\mathbf{Z}/p\mathbf{Z}$ et la suite $(y_0, \ldots, y_s)$ en $O(s \log t) = O(\log p)$. Ainsi on calcule toute la suite en $O((\log p)^3$ opérations. On trouve une racine de -1 uniquement si $y_0 \notin G$ ce qui arrive avec probabilité $1 - 1/2^{s-1}$. Cette méthode nécessite donc en moyenne $2^{s-1}/(2^{s-1}-1) < 2$ tentatives soit $O((\log p)^3$ opérations binaires.

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 $\text{ppcm}\,(p-1, q-1)$ 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.

Solution 3.8. —

1. On a $\varphi(n) = (p-1)(q-1)$ et $n = pq$. A partir de p et q, on peut calculer n et $\varphi(n)$ en $O((\log p)(\log q))$ opérations binaires. Réciproquement, on a $p + q = n - \varphi(n) + 1$, donc p et q sont racines de

$$X^2 - (n - \varphi(n) + 1)X + 1 = (X - p)(X - q).$$

On calcule les racines de ce polynômes en calculant $\Delta = (n - \varphi(n) + 1)^2 - 4$ puis δ une racine de Δ, en utilisant l'exercice 3.5. On a alors

$$p = \tfrac{1}{2}(n - \varphi(n) + 1 \pm \delta), \quad q = \tfrac{1}{2}(n - \varphi(n) + 1 \mp \delta).$$

2. $x^2 \equiv 1 \pmod{n}$ si et seulement si $x^2 \equiv 1 \pmod{p}$ et $x^2 \equiv 1 \pmod{q}$. Si $x \neq \pm 1 \pmod{n}$ alors $x = \varepsilon \pmod{p}$ et $x \equiv -\varepsilon \pmod{q}$, où $\varepsilon = \pm 1$. Mais alors $(n, x^2 - 1) = n = (n, x-1) \cdot (n, x+1)$ et cette décomposition n'est pas triviale.

   On a utilisé le fait que $(a, bc) = (a, b)(a, c)$ si (a, b) et (a, c) sont premiers entre-eux. En effet (a, b) divise a et b donc a et bc donc (a, bc). De la même façon (a, c) divise (a, bc) donc leur produit divise (a, bc). Si p^r divise a et bc alors il divise bc donc p^r divise b ou c donc divise (a, b) ou (a, c). Ainsi, si $(a, bc) = p_1^{r_1} \cdots p_k^{r_k}$, on déduit que $p_k^{r_k}$ divise $(a, b)(a, c)$ et (a, bc) divise $(a, b)(a, c)$.

3.