Université Paris 8 — Année 2022–23 — J. Lavauzelle

Master 1 Mathématiques et applications

Cryptographie à clé publique – Solutions feuille de TD 3

10/02/2023

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/clef-publique.html`

($\star$) exercice fondamental ($\star\star$) pour s'entraîner ($\star\star\star$) pour aller plus loin 💻 sur machine

---

Exercice 1. ($\star$) Structure de $\mathrm{QR}_n^\times$.

Pour $m \geq 2$ un entier, on note

$$\mathrm{QR}_m^\times := \{x^2 \mid x \in (\mathbb{Z}/m\mathbb{Z})^\times\}$$

l'ensemble des résidus quadratiques inversibles modulo n. Dans cet exercice, on considère p et q deux nombres premiers impairs distincts et on note $n = pq$.

Question 1.– Démontrer que si $x \in \mathrm{QR}_n^\times$, alors x est un carré modulo p.

Question 2.– Démontrer que $\mathrm{QR}_n^\times$ est isomorphe au groupe produit $\mathrm{QR}_p^\times \times \mathrm{QR}_q^\times$. En déduire que le cardinal de $\mathrm{QR}_n^\times$ est $\phi(n)/4$, où $\phi(n)$ est l'indicatrice d'Euler de n.

Considérons maintenant l'application d'élévation au carré

$$\begin{array}{rccc} f: & \mathrm{QR}_n^\times & \to & \mathrm{QR}_n^\times \\ & m & \mapsto & m^2 \mod n \end{array}$$

Question 3.– On suppose ici que $p \equiv q \equiv 3 \mod 4$. Démontrer que f est un automorphisme du groupe $\mathrm{QR}_n^\times$.

Solutions de l'Exercice 1.

Solution Q1. Si $x \in \mathrm{QR}_n^\times$, alors il existe $y \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $x = y^2 \mod n$, autrement dit $x = y^2 + kn$ avec $k \in \mathbb{Z}$. Comme p divise n, il s'ensuit que $x \equiv y^2 \mod p$, donc x est un carré modulo p.

Solution Q2. L'application

$$\begin{array}{rccc} g: & \mathrm{QR}_n^\times & \to & \mathrm{QR}_p^\times \times \mathrm{QR}_q^\times \\ & x & \mapsto & (x \mod p, x \mod q) \end{array}$$

est un morphisme de groupe. En effet, on a vu dans la question précédente sue si x est un carré modulo n, alors c'en est également un modulo p et q. Par ailleurs, l'application préserve clairement la multiplication et l'inverse, et 1 est bien un carré.

L'application est également bijective d'après le théorme des restes chinois.

Par conséquent, on a :

$$|\mathrm{QR}_n^\times| = |\mathrm{QR}_p^\times| \cdot |\mathrm{QR}_q^\times| = \frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4} = \frac{\phi(n)}{4}.$$

Solution Q3. Soit $y \in \mathrm{QR}_n^\times$. On rappelle que les quatre racines carrées de y dans$(\mathbb{Z}/n\mathbb{Z})^\times$ sont

$$\begin{cases} x_1 = a_p \cdot p \cdot r_q + a_q \cdot q \cdot r_p \\ x_2 = n - x_1 \\ x_3 = -a_p \cdot p \cdot r_q + a_q \cdot q \cdot r_p \\ x_4 = n - x_3 \end{cases}$$

où r_q est une racine carrée de y dans $\mathbb{F}_q$, r_p une racine carrée de y de $\mathbb{F}_p$, et $a_p p + a_q q = 1$.

Il faut démontrer qu'une seule d'entre elles est un carré modulo n. On calcule $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$. On a alors

$$\left(\frac{x_1}{p}\right) = \left(\frac{-x_2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x_2}{p}\right) = -\left(\frac{x_2}{p}\right).$$

De même, $\left(\frac{x_3}{p}\right) = -\left(\frac{x_4}{p}\right)$. Donc, exactement deux racines sont des carrés modulo p ; supposons par exemple que ce sont x_1 et x_3.

Alors

$$\left(\frac{x_1}{q}\right) \equiv (a_p \cdot p \cdot r_q + a_q \cdot q \cdot r_p)^{(q-1)/2} \equiv r_q^{(q-1)/2} \mod q.$$

De même, $\left(\frac{x_3}{q}\right) \equiv (-r_q)^{(q-1)/2} \equiv (-1) r_q^{(q-1)/2} \equiv -\left(\frac{x_1}{q}\right) \mod q$ car $q \equiv 3 \bmod 4$.

Donc, parmi x_1 et x_3, une seule est un carré modulo q.

Exercice 2. ($\star$) Racine carrée modulo p pour $p \equiv 3 \mod 4$.

Soit p un nombre premier tel que $p \equiv 3 \mod 4$.

Question 1.– Soit y un carré dans $\mathbb{F}_p$. Démontrer que $y^{(p+1)/2} = y$.

Question 2.– En déduire que dans le contexte de l'exercice, on peut obtenir une racine carrée de y dans $\mathbb{F}_p$ en calculant $y^{(p+1)/4}$.

Question 3.– Quelle est la complexité du calcul précédent, en nombre d'opérations élémentaires dans $\mathbb{F}_p$?

Solutions de l'Exercice 2.

Solution Q1. On sait que pour p impair, le groupe $\mathrm{QR}_p^\times$ des résidus quadratiques non-nuls est d'ordre $(p-1)/2$. En effet, ce groupe est l'image de l'application $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $x \mapsto x^2$. Le noyau de cette application est $\{-1, 1\}$, donc le cardinal de $\mathrm{QR}_p^\times$ est

$$|\mathrm{QR}_p^\times| = |\operatorname{im}\phi| = \frac{|(\mathbb{Z}/p\mathbb{Z})^\times|}{|\ker\phi|} = \frac{p-1}{2}.$$

Par conséquent, d'après le théorème de Lagrange (ou d'Euler) on a $y^{(p-1)/2} = 1$, puis $y^{(p+1)/2} = y^{(p-1)/2+1} = y$.

Solution Q2. Lorsque $p \equiv 3 \mod 4$, on peut bien diviser par $p+1$ par 4 (cela donne un entier), et on obtient :

$$(y^{(p+1)/4})^2 \equiv y^{(p+1)/2} \equiv y \mod p$$

Par conséquent, $x = y^{(p+1)/4}$ est bien une racine carrée de y modulo p.

Solution Q3. Le calcul se fait en $O(\log(p))$ multiplications et élévations au carré (par l'algorithme d'exponentiation modulaire rapide).

Exercice 3. ($\star\star$) Réduction de la factorisation à l'extraction de racine carrée.

Soit SQRT le problème du calcul de racine carrée modulo n :

> **Instance :** (n, x) où $n = pq$ avec p et q des nombres premiers distincts, et $x = y^2 \mod n$ pour un certain $y \in (\mathbb{Z}/n\mathbb{Z})^\times$.
> **Objectif :** calculer un y tel que $y^2 \equiv x \mod n$.

Soit également FACT le problème de la factorisation d'un entier produit de deux nombres premiers distncts n :

> **Instance :** n où $n = pq$ avec p et q des nombres premiers distincts.
> **Objectif :** calculer p et q .

On admet qu'on dispose d'algorithmes efficaces pour calculer, si elles existent, des racines carrées modulo un nombre premier.

Question 1.– Démontrer que SQRT se réduit à FACT. Autrement dit, démontrer que si l'on dispose d'un algorithme qui factorise n, alors on peut extraire n'importe quelle racine carrée modulo n.

Question 2.– Démontrer que FACT se réduit à SQRT.

Indication : pour cela, on pourra appeller l'algorithme qui résout SQRT*, en fournissant des entrées dont on connaît* a priori *une racine carrée.*

Solutions de l'Exercice 3.

Solution Q1. On a vu que grâce à au théorème des chinois, on peut réduire le calcul des racines carrées de x modulo $n = pq$ au calcul des coefficients de Bezout de p et q et aux calculs des racines carrées de x modulo p et q. Factoriser n sous la forme $p \times q$ permet donc d'extraire des racines carrées modulo n.

Solution Q2. Soit A un algorithme qui résout SQRT.

On construit un algorithme B pour factoriser n :

1. Choisir x aléatoirement dans $\mathbb{Z}/n\mathbb{Z}$
2. Appeler l'algorithme A avec comme entrée $c = x^2 \mod n$ et n. On note y la sortie de l'algorithme.
3. Si $x \not\equiv \pm y \mod n$, retourner $\text{pgcd}(x - y, n)$ et $\text{pgcd}(x + y, n)$.
4. Sinon, retourner à l'étape 1.

Analyse de l'algorithme. L'algorithme A retourne y, l'une des quatre racines carrées de $c = x^2 \mod n$. On a donc

$$n \mid x^2 - y^2 = (x - y)(x + y)\,.$$

Si $x \not\equiv \pm y \mod n$, alors n ne divise ni $x - y$, ni $x - y$. Donc, les entiers $\text{pgcd}(x - y, n)$ et $\text{pgcd}(x + y, n)$ sont deux diviseurs non-triviaux de n.

Le test de l'étape 3 réussit avec probabilité $1/2$: il y a deux racines $x \not\equiv \pm y \mod n$ et deux racines $x \equiv \pm y \mod n$.

Exercice 4. ($\star\star$) Autour du chiffrement de Goldwasser–Micali.

On considère p et q deux nombres premiers distincts tels que $p \equiv q \equiv 3 \mod 4$. On note $n = pq$ et on rappelle que

$$\mathrm{QR}_n^\times := \{x^2 \mid x \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

représente l'ensemble des résidus quadratiques inversibles modulo n.

Question 1.– Démontrer que pour $x = n - 1$, on a

$$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1\,.$$

Question 2.– Le résultat de la question précédente reste-t-il vrai si $p \not\equiv 3 \mod 4$?

On appelle « pseudo-carré inversible modulo n » un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que

$$\left(\frac{x}{n}\right) = 1 \quad \text{et} \quad x \notin \mathrm{QR}_n^\times\,.$$

On note $\overline{\mathrm{QR}}_n^\times$ l'ensemble des pseudo-carrés inversibles modulo n.

Question 3.– Démontrer que $n - 1 \in \overline{\mathrm{QR}}_n^\times$.

Question 4.– L'ensemble $\overline{\mathrm{QR}}_n^\times$ est-il un groupe ?

Question 5.– Fixons $y \in \overline{\mathrm{QR}}_n^\times$. Démontrer que $\mathrm{QR}_n^\times$ et $\overline{\mathrm{QR}}_n^\times$ ont même cardinal. Pour cela, on pourra construire une bijection entre ces deux ensembles.

On rappelle dans les Algorithmes 1, 2 et 3 comment fonctionne le cryptosystème de Goldwasser–Micali dans le cas où $p \equiv q \equiv 3 \mod 4$ et où l'on choisit l'élément public $x = n - 1$.

Question 6.– Rappeler de quelle taille doit être n pour qu'il soit supposé calculatoirement infaisable de le factoriser.

Question 7.– Pour des raisons d'efficacité, Bob choisit d'utiliser un générateur de nombres aléatoires tels que les y_i sont tous $\leq 2^{128}$. Il pense que comme il y a 2^{128} possibilités pour chaque y_i, le système reste sûr. Est-ce vraiment le cas ? Justifier.

Question 8.– On note E la fonction de chiffrement de Goldwasser–Micali, pour une paire de clé fixée. Démontrer que si

$$\boldsymbol{m} = \boldsymbol{a} \oplus \boldsymbol{b} := (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)\,,$$

alors $E(\boldsymbol{a}) \star E(\boldsymbol{b})$ est un chiffré valide de $E(\boldsymbol{m})$, où $\star$ représente le produit coordonnée par coordonnée. On parle alors de *chiffrement homomorphe*.

Algorithme 1 : Génération de clés dans le cryptosystème de Goldwasser–Micali

Entrée : un paramètre de sécurité
Sortie : une paire de clés publique/privée

1 Choisir aléatoirement deux grands nombres premiers distincts p et q tels que $p \equiv q \equiv 3 \mod 4$.
2 Calculer $n = pq$.
3 **Retourner** la clé publique n, et la clé privée (p, q).

Solutions de l'Exercice 4.

Solution Q1. On a $x \equiv n - 1 \equiv -1 \mod p$, donc $\left(\frac{x}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$. Comme $(p-1)/2$ est impair vu que que $p \equiv 3 \mod 4$, on obtient $\left(\frac{x}{p}\right) = -1$. Même raisonnement pour $\left(\frac{x}{q}\right)$.

Algorithme 2 : Chiffrement dans le cryptosystème de Goldwasser–Micali

Entrée : la clé publique n, un message $\boldsymbol{m} = (m_1, \ldots, m_k) \in \{0,1\}^k$
Sortie : un chiffré $\boldsymbol{c} = (c_1, \ldots, c_k) \in (\mathbb{Z}/n\mathbb{Z})^k$

Pour tout $i = 1, \ldots, k$ **faire**
  Choisir aléatoirement $y_i \in (\mathbb{Z}/n\mathbb{Z})^\times$.
  Définir $c_i = y_i^2 \cdot (-1)^{m_i} \mod n$.
Retourner $\boldsymbol{c} = (c_1, \ldots, c_k)$.

Algorithme 3 : Déchiffrement dans le cryptosystème de Goldwasser–Micali

Entrée : la clé privée p,q, un chiffré $\boldsymbol{c} = (c_1, \ldots, c_k) \in (\mathbb{Z}/n\mathbb{Z})^k$
Sortie : un message $\boldsymbol{m} = (m_1, \ldots, m_k) \in \{0,1\}^k$

Pour tout $i = 1, \ldots, k$ **faire**
  Calcule $a = c_i \mod p$.
  Si *a est un carré modulo p*
    Affecter $m_i = 0$.
  Sinon
    Affecter $m_i = 1$.
Retourner $\boldsymbol{m} = (m_1, \ldots, m_k)$.

Solution Q2. Non, par exemple avec $p = 5$, on a $4 = 2^2 \mod 5$ donc $\left(\frac{4}{5}\right) = 1$. De même avec $q = 17$, on a $16 = 4^2 \mod 17$.

D'ailleurs, le raisonnement de la question précédent montre que $n - 1$ est toujours un carré mod n lorsque $p \equiv q \equiv 1 \mod 4$.

Solution Q3. L'élément $n - 1$ n'est pas un carré modulo n car sinon, il serait également un carré modulo p et q (voir question 1). Il suffit maintenant de démontrer que $\frac{n-1}{n} = 1$. Par multiplicativité du symbole de Jacobi, on obtient

$$\left(\frac{n-1}{n}\right) = \left(\frac{n-1}{p}\right)\left(\frac{n-1}{q}\right) = (-1) \times (-1) = 1\,.$$

Solution Q4. Non car le neutre 1 n'est pas dans $\overline{\mathrm{QR}}_n^\times$ (c'est bien un carré modulo n).

Solution Q5. On va trouver une bijection entre ces deux ensembles. Comme $n - 1 \in \overline{\mathrm{QR}}_n^\times$, on peut prendre l'application $x \mapsto (n-1)x \mod n$, autremeent dit $x \mapsto -x$.

On a que si x est un carré modulo n, alors $(n-1)x$ ne l'est pas (mais son symbole de Jacobi reste 1). Et cette application est clairement bijective $(-1)^{-1} = (-1)$.

Solution Q6. L'entier n doit être de taille au moins 2048 bits.

Solution Q7. Non, car y_i^2 est alors $\leq 2^{256}$, donc (par exemple dans le cas où $m_i = 0$, on $c_i = y_i^2 \leq 2^{256}$. La réduction $\mod n$ nest donc pas utile, et l'attaquant peut retrouver y_i à partir de c_i en calculant une racine carrée **entière** (il y a un algorithme efficace pour cela).

Pour le as $m_i = 1$, le raisonnement est similaire en utilisant $n - c_i$ à la place de c_i.

Solution Q8. Le bit i de $E(\boldsymbol{a}) \star E(\boldsymbol{b})$ est

$$E(a_i)E(b_i) = y_i(a)^2 x^{a_i} y_i(b)^2 x^{b_i} = (y_i(a)y_i(b))^2 x^{a_i+b_i} \mod n\,.$$

Par ailleurs, si $y_i(\boldsymbol{a})$ et $y_i(\boldsymbol{b})$ sont tirés uniformément dans $(\mathbb{Z}/n\mathbb{Z})^\times$, alors leur produit l'est aussi. Donc $E(a_i)E(b_i)$ s'écrit comme $z_i^2 x^{a_i+b_i} \mod n$, avec z_i uniforme dans $\mathrm{QR}_n^\times$.

Exercice 5. 💻 (⋆) Implantation du calcul du symbole de Jacobi.

Question 1.– Implanter un algorithme de calcul du symbole de Jacobi $\left(\frac{a}{n}\right)$, où a et n sont deux entiers tels que n est impair. On n'utilisera pas d'algorithme de factorisation, mais on pourra se référer par exemple à l'Algorithme 4.

Algorithme 4 : Algorithme Jacobi pour le calcul du symbole $\left(\frac{a}{n}\right)$

Entrée : $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ impair
Sortie : le symbole de Jacobi $\left(\frac{a}{n}\right)$

Si $a = 0$
  Retourner 0
Si $a = 1$
  Retourner 1
Si $a = n - 1$
  Si $a \equiv 0 \bmod 4$
    Retourner 1
  Sinon
    Retourner -1
Si $a \equiv 0 \bmod 2$
  Si $n \equiv 1 \bmod 8$ *ou* $n \equiv 7 \bmod 8$
    Retourner Jacobi$(a/2, n)$
  Sinon
    Retourner $(-1) \times$ Jacobi$(a/2, n)$
Si $a \geq n$
  Retourner Jacobi$(a \bmod n, n)$
Si $a \equiv 1 \bmod 4$ *ou* $n \equiv 1 \bmod 4$
  Retourner Jacobi(n, a)
Sinon
  Retourner $(-1) \times$ Jacobi(n, a).

Solutions de l'Exercice 5.

Voir script à l'adresse suivante :

`https://www.math.univ-paris13.fr/ lavauzelle/teaching/2022-23/docs/CP/td/scripts/jacobi.py`