Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Cryptographie à clé publique – Feuille de TD 3

05/02/2024

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`https://lvzl.fr/teaching/2023-24/cp.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 rappelle que l'on note

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

l'ensemble des résidus quadratiques inversibles modulo m.

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 le groupe $\mathrm{QR}_n^\times$ 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 $\mathrm{QR}_n^\times$.

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

Dans cet exercice, on considère 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 ($p \equiv 3 \mod 4$), 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 $\mathbb{F}_p$?

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 :** une paire (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 :** un entier 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.*

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

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

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).

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 $\boldsymbol{c} = (c_1, \ldots, c_k) \in (\mathbb{Z}/n\mathbb{Z})^k$
1 **Pour tout** $i = 1, \ldots, k$ **faire**
2 Choisir aléatoirement $y_i \in (\mathbb{Z}/n\mathbb{Z})^\times$.
3 Définir $c_i = y_i^2 \cdot (-1)^{m_i} \mod n$.
4 **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 $\boldsymbol{m} = (m_1, \ldots, m_k) \in \{0,1\}^k$
1 **Pour tout** $i = 1, \ldots, k$ **faire**
2 Calcule $a = c_i \mod p$.
3 **Si** *a est un carré modulo p*
4 Affecter $m_i = 0$.
5 **Sinon**
6 Affecter $m_i = 1$.
7 **Retourner** $\boldsymbol{m} = (m_1, \ldots, m_k)$.

Exercice 5. 💻 $(\star)$ 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).