Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Feuille de TD 3

11/02/2022

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

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/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 $\mathrm{QR}_n^\times$.

On considère p et q deux nombres premiers distincts. On note $n = pq$.

On définit $\mathrm{QR}_n^\times := \{x^2 \mid x \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ l'ensemble des résidus quadratiques inversibles modulo n.

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

On note également $\mathrm{QR}_n^\times$ le groupe des résidus quadratiques inversibles modulo n.

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

Soit

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

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 $p \equiv 3 \mod 4$.

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 (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 :** (n, x) où $n = pq$ avec p et q sont premier et 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, x) où $n = pq$ avec p et q sont premier et distincts.
> **Objectif :** calculer p et q .

On rappelle qu'on dispose d'algorithmes efficaces pour calculer des racines carrées modulo un nombre premier.

Question 1.– Démontrer que SQRT se réduit à FACT. Autrement dit, si 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. Pour cela, on appellera l'algorithme qui résout SQRT avec 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 $n = pq$.

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 note $\mathrm{QR}_n^\times := \{x^2 \mid x \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ l'ensemble des résidus quadratiques inversibles modulo n.

On appelle également « pseudo-carré inversible modulo n » un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\left(\frac{x}{n}\right) = 1$ mais $x \notin \mathrm{QR}_n^\times$. On note $\overline{\mathrm{QR}}_n^\times$ l'ensemble des pseudo-carrés inversibles modulo n.

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

Question 4.– $\overline{\mathrm{QR}}_n^\times$ 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 l'opération de chiffrement. 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 La **clé publique** est n, la **clé privée** est (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** $i = 1, \ldots, k$ **faire**
2 Choisir aléatoirement $y_i \in (\mathbb{Z}/n\mathbb{Z})^\times$
3 Définir $c_i = y_i^2(-1)^{m_i} \mod n$
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** $i = 1, \ldots, k$ **faire**
2 On calcule $a = c_i \mod p$.
3 Si a est un carré modulo p, on affecte $m_i = 0$
4 Sinon, on affecte $m_i = 1$.
5 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 de symbole de Jacobi, sans utiliser d'algorithme de factorisation. On pourra par exemple utiliser l'Algorithme 4.

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

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

```
Si a = 0
    Retourner 0
Si a = 1 ou n = 2
    Retourner 1
Si a = n − 1
    Si a ≡ 0 mod 4
        Retourner 1
    Sinon
        Retourner −1
Si a ≡ 0 mod 2
    Si p ≡ 1 mod 8 ou p ≡ 3 mod 8
        Retourner Jacobi(a/2, n)
    Sinon
        Retourner (−1)× Jacobi(a/2, n)
Si a ≥ n
    Retourner Jacobi(a mod n, n)
Si a ≡ 1 mod 4 ou n ≡ 1 mod 4
    Retourner Jacobi(n, a)
Sinon
    Retourner (−1)× Jacobi(n, a)
```