Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Cryptographie à clé publique – Feuille de TD de révision

08/04/2024

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. Questions de cours (interro 2022-23).

Question 1.– Que signifie le sigle IND-CPA ?

Question 2.– On considère un système de chiffrement à clé publique, que l'on suppose valide et sûr. On note $\mathcal{M}$ l'ensemble de tous les messages que l'on peut chiffrer, et $\mathcal{C}$ l'ensemble de tous les chiffrés que l'on peut obtenir.

1. Est-il possible que $|\mathcal{C}| > |\mathcal{M}|$? Justifier rapidement (avec un argument, un exemple, etc.).
2. Est-il possible que $|\mathcal{C}| < |\mathcal{M}|$? Justifier rapidement (avec un argument, un exemple, etc.).

Question 3.– Soit $\mathbb{G}$ un groupe cyclique d'ordre r, de générateur g.

1. Rappeler les définitions du problème de Diffie–Hellman calculatoire (CDH), et du problème du logarithme discret (DL) dans $\mathbb{G}$.
2. L'un de ces deux problèmes est-il plus facile que l'autre ? Sont-ils équivalents ? Ne pas justifier.
3. Supposons que $|\mathbb{G}| = r = 2^{1000}$. Donner une borne supérieure, sur la sécurité en nombre de bits d'un cryptosystème reposant sur logarithme discret dans $\mathbb{G}$. Justifier.

Question 4.– Supposons que l'on dispose d'un système de signature `sign/verif` et d'un système de chiffrement `enc/dec`, tous deux à clef publique. Donner un protocole d'identification, où Alice s'identifie auprès de Bob. On pourra utiliser les deux systèmes, ou seulement l'un des deux.

Question 5.– En quelques lignes, donnez des intérêts et inconvénients à utiliser des courbes elliptiques en cryptographie à clef publique.

Exercice 2. Chiffrement de Paillier (interro 2021-22).

Dans cet exercice, si $n \geq 2$ est un entier, on note $\phi(n)$ l'indicatrice d'Euler de cet entier, c'est-à-dire le nombre d'entiers $x \in \{1, \ldots, n-1\}$ qui sont premiers avec n.

En 1999, Paillier a proposé le système de chiffrement à clef publique décrit ci-dessous.

Algorithme 1 : Génération de clefs dans le cryptosystème de Paillier

Entrée : une taille minimale $t \geq 1$ (paramètre de sécurité)
Sortie : une paire de clefs publique/privée

1 Choisir aléatoirement p et q deux nombres premiers d'au moins t bits chacun.
2 Calculer $n = pq$ et $\phi(n) = (p-1)(q-1)$.
3 **Si** $\text{pgcd}(n, \phi(n)) \neq 1$
4 revenir à l'étape 1.
5 **Sinon**
6 retourner la clef publique $\texttt{pk} = n$ et la clef privée $\texttt{sk} = \phi(n)$.

L'espace des clairs du cryptosystème est $\mathcal{M} := \{0, 1, \ldots, n-1\}$ et l'espace des chiffrés est $\mathcal{C} := (\mathbb{Z}/n^2\mathbb{Z})^\times$, c'est-à-dire l'ensemble des inversibles modulo n^2. Les algorithmes de chiffrement et de déchiffrement sont alors les suivants.

Algorithme 2 : Chiffrement dans le cryptosystème de Paillier

Entrée : un message $m \in \mathcal{M}$, une clé publique n
Sortie : un chiffré $c \in \mathcal{C}$

1 Tirer uniformément $r \in (\mathbb{Z}/n\mathbb{Z})^\times$.
2 Calculer $c = (1+n)^m r^n \mod n^2$.
3 Retourner c.

Algorithme 3 : Déchiffrement dans le cryptosystème de Paillier

Entrée : un chiffré $c \in \mathcal{C}$, une clé privée $\phi(n)$
Sortie : un message $m' \in \mathcal{M}$

1 Calculer $u = c^{\phi(n)} \mod n^2$.
2 Calculer (dans $\mathbb{Z}$) l'entier $v = \frac{u-1}{n}$.
3 Calculer $m' = v \cdot \phi(n)^{-1} \mod n$.
4 Retourner m'.

Dans tout l'exercice, on considère $n = pq$ où p et q sont deux nombres premiers impairs distincts créés dans la génération de clefs. **On suppose également que n et $\phi(n)$ sont premiers entre eux.**

Question 1.– Comment fait-on, en pratique, pour tirer uniformément $r \in (\mathbb{Z}/n\mathbb{Z})^\times$?

Question 2.– Donner la complexité de la deuxième étape de l'algorithme de chiffrement (calcul de c). On exprimera cette complexité comme une approximation, en fonction de n, du nombre d'opérations arithmétiques (additions et multiplications modulaires) modulo n^2.

On souhaite ensuite démontrer que le chiffrement est valide, dans le sens où le déchiffrement d'un chiffré correctement constitué, retourne bien le message d'origine.

Question 3.– Exprimer le cardinal de $(\mathbb{Z}/n^2\mathbb{Z})^\times$ en fonction de n et $\phi(n)$.

Question 4.–

1. Démontrer que $1+n$ est inversible modulo n^2.
2. Soit x un entier naturel. On note a le reste de la division euclidienne de $(1+n)^x$ par n^2, et b le reste de division euclidienne de x par n. Démontrer que $a = 1+nb$ dans $\mathbb{Z}$.
3. En déduire l'ordre de $1+n$ dans le groupe $(\mathbb{Z}/n^2\mathbb{Z})^\times$.

Question 5.– Soit $u \in \{1, \ldots, n^2-1\}$ l'entier calculé à l'étape 1 du déchiffrement. Démontrer que $u = 1 + n \cdot (m\,\phi(n) \mod n)$. En déduire que le déchiffrement est valide.

Maintenant, on s'intéresse sommairement à la sécurité du chiffrement de Paillier.

Question 6.– Démontrer que si l'on sait factoriser n, alors on casse le cryptosystème de Paillier. Préciser le type et les moyens de l'attaque.

Question 7.– En déduire une valeur minimale pour t, la taille minimale de p et q en nombre de bits, afin que le cryptosystème de Paillier puisse être considéré comme sûr à long terme (sécurité ≥ 128 bits).

Question 8.– (plus difficile). Supposons que l'on détienne un algorithme `INV`, qui prend en entrée un entier n, et qui retourne $n^{-1} \mod \phi(n)$. Démontrer que, grâce à l'algorithme `INV`, on peut alors casser le cryptosystème de Paillier.

Exercice 3. $(\star\star)$ Vérification simultanée de signatures RSA.

Dans cete exercice, on s'intéresse au schéma de signature RSA « brut ». Soit $(n = pq, e)$ une clé publique RSA, et d la clé privée associée. On suppose que n est de taille t bits.

Question 1.– En fonction de t, quel est le coût algorithmique (en nombre de multiplications et carrés dans $\mathbb{Z}/n\mathbb{Z}$) d'une signature RSA ?

Bob reçoit une série de $\ell \geq 2$ messages signés par Alice : $(m_1, s_1), \ldots, (m_\ell, s_\ell)$. Pour vérifier ces signatures RSA plus rapidement, Bob décide de multiplier tous les messages entre eux : il calcule ainsi

$$m = m_1 m_2 \cdots m_\ell \mod n \quad \text{et} \quad s = s_1 s_2 \ldots s_\ell \mod n\,.$$

Puis, il décide d'accepter la série de messages signés par Alice si et seulement si $s^e = m \mod n$.

Question 2.– Démontrer que si tous les messages ont bien été signés par Alice, alors Bob a raison d'accepter la série de signatures d'Alice.

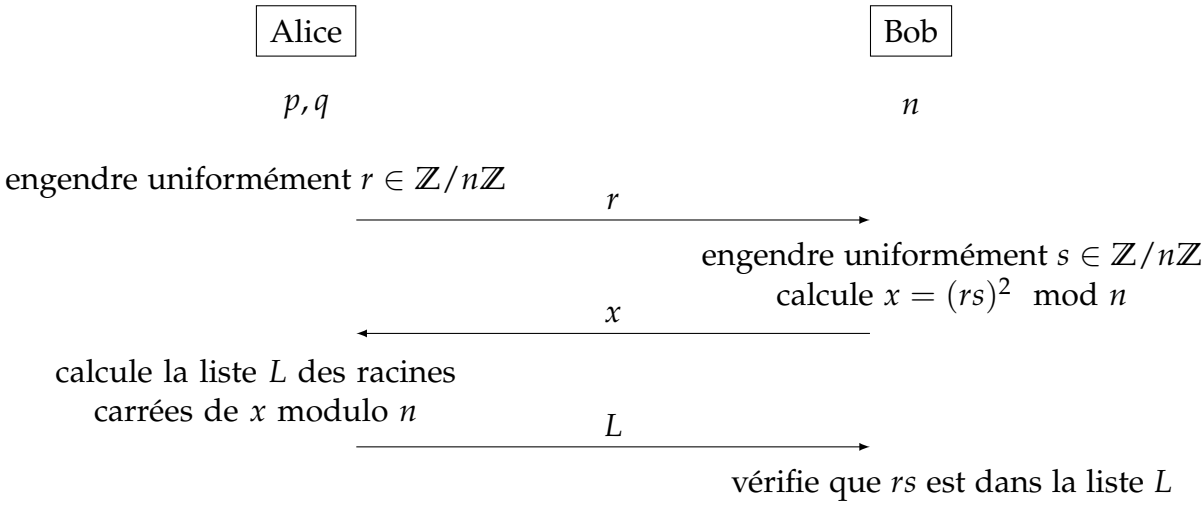
Question 3.– Quantifier le gain de calcul de Bob en utilisant cette méthode.

Question 4.– Charlie sait que Bob utilise cette méthode pour vérifier les signatures d'Alice. Charlie intercepte une série $(m_1, s_1), \ldots, (m_\ell, s_\ell)$ de messages signés par Alice (Charlie n'a donc pas choisi les messages). Comment peut-il intégrer un autre message m' à la série pour faire croire à Bob qu'Alice a également signé m' ?

Exercice 4. Un protocole d'identification (interro 2021-22).

Dans cet exercice, on s'intéresse à un protocole d'identification dans lequel Alice souhaite s'identifier auprès de Bob.

Dans une phase de génération de paramètres, Alice engendre deux nombres premiers p et q distincts et de grande taille, et calcule $n = pq$. Puis, elle publie la valeur de n et garde secrètement le couple (p, q).



Question 1.– Nommer les trois passes du protocole d'identification.

Pour simplifier, on suppose que p et q sont congrus à 3 modulo 4. Dans ce cas, on sait alors que si t est un carré modulo p, alors $t^{(p+1)/4} \mod p$ est l'une de ses racines carrées.

Question 2.– Expliquer comment Alice peut calculer la liste des racines carrées de x modulo n. Pourquoi est-elle la seule à pouvoir le faire ?

Question 3.– Supposons qu'un attaquant observe les échanges entre Alice et Bob. Est-il possible, pour Alice, de réutiliser les mêmes valeurs de p, q, n pour une seconde identification ? Justifier.