SORBONNE UNIVERSITÉ

Arithmétique et Cryptologie Moderne

Version du 11 janvier 2025

TD

Exercice 1 – Exponentiation modulaire et échange de clé

1. **(Complexité)** Pour a, n et e des entiers. Rappeler le principe de l'algorithme de calcul de a^e mod n de complexité $O(\log(e)\log(n)^2)$. Expliquer comment démontrer cette complexité.
2. **(Implémentation)** Donner une version séquentielle de cet algorithme. A-t-elle la même complexité que celle vue en cours ? Est-il avantageux en pratique d'utiliser cette version ? Si oui pourquoi ?
3. **(Application)** Quelle est la complexité du protocole de Diffie-Hellman-Merkle pour l'échange de clé ?

Exercice 2 – Complexités

Dans tout cet exercice, on s'intéresse aux complexités asymptotiques d'algorithme. On rappelle que la complexité d'un algorithme se calcule en fonction de la *taille* des entrées. Tous les logarithmes et exponentielles seront considérés en base 2.

1. Soit A et B deux algorithmes prenant en entrée un entier n. Le nombre de calculs (sur des mots machine) nécessaires pour obtenir le résultat sont $2n+3$ et n^2+7 en utilisant respectivement A et B. À quelle classe de complexité appartiennent ces algorithmes ? Comment se comparent-ils ?
2. Soit A un algorithme ayant une entrée de taille (en bits) ℓ. Supposons que A soit de complexité (exacte) $2^{4\ell}$. Si l'entrée de A augmente de 1 bit, de combien augmente le nombre d'opérations pour effectuer le calcul ?
3. Soit A un algorithme prenant en entrée un entier n et de complexité $2^{(\log(n))^\alpha)}$ avec $0 < \alpha < 1$. Montrer que A est de complexité sous-exponentielle en fonction de la taille de son entrée.

Exercice 3 – DLP et BSGS

Dans tout cet exercice, on s'intéresse à l'algorithme *Baby Step Giant Step* de Shanks pour la résolution du logarithme discret.

1. Rappeler la définition du problème DLP en général. Quel est l'algorithme de meilleur complexité connu pour le résoudre ?
2. Rappeler le principe de l'algorithme *Baby Step Giant Step* et sa complexité.
3. Démontrer l'algorithme et son estimation de complexité.

Exercice 4 – BSGS : Application

Le but de cet exercice est de résoudre des DLP dans le cas des corps finis premiers, c'est-à-dire trouver x tel que

$$g^x = n \bmod p$$

avec g un générateur de $\mathbb{F}_p^\times$ et $n \neq 0$ un élément de $\mathbb{F}_p$ donné.

1. Utiliser l'algorithme BSGS avec $p = 23$, $g = 11$ et $n = 3$.

Exercice 5 – Groupe multiplicatif $\mathbb{F}_p^\times$

Dans tout cet exercice, on s'intéresse au groupe multiplicatif issu de l'anneau $\mathbb{Z}/p\mathbb{Z}$ pour p un entier premier (noté $\mathbb{F}_p$).

1. Rappeler quels sont les éléments de $\mathbb{F}_p^\times$.
2. Quel est le cardinal (appelé aussi ordre) de $\mathbb{F}_p^\times$?
3. Rappeler la définition de l'ordre d'un élément a de $\mathbb{F}_p^\times$. Montrer que l'ordre de tout élément de $\mathbb{F}_p^\times$ divise $p-1$. Étant donné deux éléments a et b d'ordre respectif α et β, montrer que l'ordre de ab divise le ppcm(α, β).
4. (**Petit théorème de Fermat**) Montrer que $a^p = a \bmod p$ pour tout entier a.
5. Montrer que dans un anneau commutatif intègre, un polynôme non nul de degré n possède au plus n racines.
6. Sachant qu'un groupe d'ordre n est cyclique si et seulement s'il contient un unique sous-groupe d'ordre d pour tout diviseur d de n, montrer que le groupe multiplicatif $\mathbb{F}_p^\times$ est cyclique. (Indication : considérer un polynôme de la forme $X^d - 1$.)
7. Montrer qu'il y a $\varphi(p-1)$ générateurs différents pour $\mathbb{F}_p^\times$.

Exercice 6 – Diffie-Hellman-Merkle

Alice et Bob se sont mis d'accord pour utiliser le premier $p = 23$ pour un échange de clés en utilisant le protocole Diffie-Hellamn-Merkle.

1. Quel est l'ordre de 5 dans $\mathbb{F}_p^\times$
2. Pourquoi Alice peut choisir $g = 5$ dans le protocole Diffie-Hellman-Merkle d'échange de clés avec $p = 23$?
3. Bob n'a pas beaucoup de connaissances en arithmétique et vous demande de l'aider pour générer une clé. Alice lui a envoyé l'entier $A = 8$, expliquez lui comment générer et envoyer la clé K à Alice.

Exercice 7 – ElGamal

Alice et Bob se sont mis d'accord pour utiliser le nombre premier $p = 23$ et le générateur $\alpha = 5$ pour des échanges utilisant le cryptosystème ElGamal.

1. Si Alice a pour clé publique l'entier 10 quelle est sa clé privée ?
2. Bob a choisi $k_B = 6$ comme clé privée, la clé publique correspondante est $\beta_B = 8$. À l'aide de cette clé publique et de l'entier *éphémère* 17, Alice veut chiffrer le message $m = 21$. Quel est le message (c_1, c_2) chiffré correspondant ?
3. Alice a changé sa clé privé en 9, la clé publique correspondante est alors 11. Bob a envoyé le message chiffré $(17, 22)$ à Alice. Quel est le message d'origine de Bob ?

RSA et le CRT

Exercice 8 – CRT

1. Rappeler le principe de résolution d'un système d'équations linéaires modulaires.
2. En utilisant l'algorithme décrit en cours et en TD, résoudre le système suivant :

$$\begin{cases} x &= 1 \bmod 9 \\ x &= 2 \bmod 8 \\ x &= 3 \bmod 5 \\ x &= 1 \bmod 7 \end{cases}$$

Vous présenterez soigneusement l'ensemble de vos calculs intermédiaires (attention à ne faire figurer que des calculs modulaires).

Exercice 9 – Un exemple concret d'utilisation de RSA

On va dans cet exemple, faire les calculs nécessaires au déchiffrement d'un message envoyé à l'aide du cryptosystème RSA.

Sachant que vos clés publiques sont $n = pq$ avec $p = 3, q = 11$ et $e = 7$, répondez aux questions suivantes.

1. Donner les exposants de chiffrement et déchiffrement correspondant à une implantation du déchiffrement par CRT de RSA.
2. Déchiffrer le message $y = 14$ en utilisant le déchiffrement par CRT.

Exercice 10 – Bases mathématiques de RSA

On rappelle ici les éléments mathématiques qui permettent de mettre en place le crypto-système RSA.
Étant donné un entier n on note $\varphi(n)$ (indicatrice d'Euler) le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

1. (**théorème d'Euler**) (Re)Montrer que pour tout entier a premier avec n nous avons
$$a^{\varphi(n)} = 1 \mod n$$
2. (Re)Déduire de la question précédente le *petit théorème de Fermat*.
3. Rappeler la définition du cryptosystème RSA (i.e. les fonctions E_{RSA} et D_{RSA} qui respectivement permettent de chiffrer et déchiffrer), mettre bien en évidence la nature des différentes clés (privées, publiques).
4. Montrer que ce cryptosystème est toujours valide, i.e. que pour tout message $m \in \mathbb{Z}/n\mathbb{Z}$ nous avons $m = D_{\text{RSA}}(E_{\text{RSA}}(m))$. (Indication : on pourra utiliser le Théorème Chinois des Restes).
5. Doit-on limiter l'ensemble des messages possibles à un sous-ensemble strict de $\mathbb{Z}/n\mathbb{Z}$? Si oui, pourquoi et lequel exactement ?
6. Donner l'algorithme permettant de déchiffrer en utilisant le CRT.
7. En supposant que l'exposant de déchiffrement d est de l'ordre du module n montrer que le déchiffrement par CRT est plus rapide qu'en utilisant l'exponentiation directe et déterminer le facteur de gain pour la multiplication naïve et l'algorithme de multiplication de Karatsuba.
8. Décrire le problème $\mathcal{P}_{\text{RSA}}$ sur lequel se base le cryptosystème RSA. Montrer que la résolution du problème de la factorisation des entiers entraîne la résolution de $\mathcal{P}_{\text{RSA}}$. Le contraire est-il vrai ?

Exercice 11 – Arithmétique modulaire et fonction indicatrice d'Euler – partiel 2019

Dans tout l'exercice, on note φ la fonction indicatrice d'Euler. On rappelle que $\varphi(n)$ est le nombre d'entiers $a \in \{0, \ldots, n-1\}$ premiers avec n.

1. Calculer $17^{2019} \mod 36$.
2. Soient p un nombre premier. Montrer que $\varphi(p) = p - 1$.
3. Soient p un nombre premier et e un entier non nul. Montrer que $\varphi(p^e) = p^e - p^{e-1}$.
4. On suppose dans cette question que si s et t sont deux entiers premiers entre eux, alors $\varphi(s\,t) = \varphi(s)\,\varphi(t)$.
Montrer que si $n = p_1^{e_1} \cdots p_r^{e_r}$ avec les p_i des nombres premiers distincts deux à deux et les e_i des entiers strictement positifs, alors $\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.
5. À l'aide du résultat précédent, calculer $11^{43\,203} \mod 189\,000$.
Les questions suivantes sont en bonus.
Leur but est de prouver le résultat admis à la question 4, c'est-à-dire que si s et t sont premiers entre eux, alors $\varphi(s\,t) = \varphi(s)\,\varphi(t)$.
6. Soient s et t deux entiers premiers entre eux. Montrer que pour $a \in \{0, \ldots, t-1\}$ et $b \in \{0, \ldots, s-1\}$, les entiers $m_{a,b} = a\,s + b\,t \mod s\,t$ sont tous distincts deux à deux. En déduire que pour tout entier m, $0 \leqslant m < s\,t$, il existe a et b comme précédemment tel que $m = a\,s + b\,t \mod s\,t$.

7. Montrer que pour s et t premiers entre eux, pgcd$(a, t) > 1$ ou pgcd$(b, s) > 1$ si, et seulement si, pgcd$(a\,s+b\,t, s\,t) > 1$.
8. En déduire que si $a\,s + b\,t$ avec $a \in \{0, \ldots, t-1\}$ et $b \in \{0, \ldots, s-1\}$ est premier avec $s\,t$, alors a est premier avec t et b est premier avec s.
9. En déduire que le nombre de nombres $m \in \{0, \ldots, s\,t-1\}$ premiers avec $s\,t$ est $\varphi(s)\varphi(t)$.