TD 7

Algorithmique

On note $\mathbb{Z}_N$ l'anneau quotient $\mathbb{Z}/N \cdot \mathbb{Z}$, $\mathbb{Z}_N^\star$ le groupe multiplicatif de cardinal $\varphi(N)$ et $\text{len}(x)$ la longueur en bits d'un entier x.

Exercice 1: Exponentiation

1. On suppose que l'on a $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_N$, avec des entiers positifs $e_1, \ldots, e_k$, où $\text{len}(e_i) \leq \ell$ pour $i = 1, \ldots, k$. Montrer comment calculer
$$\beta = \alpha_1^{e_1} \cdots \alpha_k^{e_k}$$
en utilisant $\ell + O(1)$ élévations au carré dans $\mathbb{Z}_N$ et $\ell + 2^k + O(1)$ multiplications dans $\mathbb{Z}_N$.
2. Montrer comment calculer α^e, où $\alpha \in \mathbb{Z}_N$ pour un exposant e de ℓ bits. Montrer que pour tout paramètre entier positif k, on peut utiliser un précalcul qui utilise $\ell + O(1)$ élévations au carré dans $\mathbb{Z}_N$ et $2^{k-1}+O(1)$ multiplications dans $\mathbb{Z}_N$ et ensuite on peut calculer α^e pour tout exposant e de ℓ bits en utilisant seulement $\ell+O(1)$ élévations au carré et $2^{k-1}+\ell/k+O(1)$ multiplications.
3. Que peut-on faire si α est fixé ?

Exercice 2: Tests de Primalité

Un *nombre de Carmichael* est un nombre composé tel que pour tout $a \in \mathbb{Z}_n^\star$: $a^{n-1} = 1 \bmod n$.

Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$. Il y en a une infinité.

On rappelle que le groupe multiplicatif $\mathbb{Z}_N^\star$ est cyclique si et seulement si N vaut $1, 2, 4, p^k$ ou $2p^k$ pour un entier positif k et un nombre premier p impair.

On rappelle qu'un entier x est un résidu quadratique (carré mod N), s'il existe y tel que $x = y^2 \bmod N$.

1. Rappeler rapidement une démonstration du théorème d'Euler (pour tout $a \in \mathbb{Z}_N^\star$, $a^{\varphi(N)} = 1 \bmod N$) et du petit théorème de Fermat (N premier).
2. Montrer que si n est un nombre composé qui n'est pas de Carmichael, alors $Card(F_n) \leq Card(\mathbb{Z}_n^\star)/2$ où $F_n = \{a \in \mathbb{Z}_n^\star : a^{n-1} = 1 \bmod n\}$.
3. Soit p un nombre premier impair, et $g \in \mathbb{Z}_p^\star$ un générateur. Montrer alors que g^k est un résidu quadratique si et seulement si k est pair.
4. (Critère d'Euler): Montrer que pour un nombre premier p, un élément $a \in \mathbb{Z}_p^\star$ est un résidu quadratique si et seulement si $a^{\frac{p-1}{2}} = 1 \bmod p$.
On note $(a|p)$ le symbole de Legendre qui vaut 1 si a est un carré et -1 si a n'est pas un carré et 0 si p divise a. Montrer comment calculer ce symbole en utilisant et en déduire sa complexité :
   - $(ab|n) = (a|n)(b|n)$

- si $a = b \bmod n$, alors $(a|n) = (b|n)$
- $(1|n) = 1$
- la loi de réciprocité quadratique $(m|n) = (n|m)(-1)^{(m-1)(n-1)/4}$ si m et n sont impairs et premier entre eux
- $(2|n) = (-1)^{(n^2-1)/8}$

On définit de même le symbole de Jacobi $(a|n)$ quand n n'est pas premier et qui se calcule avec le même algorithme car il vérifie les mêmes égalités.

5. Donner le lien entre le symbole de Jacobi et le symbole de Legendre.
   Soit le test de Solovay-Strassen : choisir $a \in \mathbb{Z}_n^\star$ et si $(a|n) = a^{(n-1)/2} \bmod n$, retourner n premier, composé sinon.
6. Montrer que pour tout n impair composé, $Card(J_n) \leq Card(\mathbb{Z}_n^\star)/2$ si on note $J_n = \{a \in \mathbb{Z}_n^\star : (a|n) = a^{(n-1)/2} \bmod n\}$. (On écrira $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, $q = p_1^{k_1}$ et $m = p_2^{k_2} \dots p_t^{k_t}$. Soit g un générateur de $\mathbb{Z}_q^\star$, et considérer l'élément $a = g \bmod q$ et $a = 1 \bmod m$. Considérer deux cas suivant que $k_1 = 1$ et $k_1 \geq 2$.)
7. Montrer alors que la probabilité que l'algorithme de Solovay-Strassen retourne premier quand n est impair et composé est au plus $1/2$.

Exercice 3: Algorithme de Chiffrement RSA (Rivest-Shamir-Adleman)

Soit $N = p \times q$ le produit de deux nombres premiers très grand (512 bits par exemple). On dit que N est un module RSA. On note $\varphi(N)$ le cardinal de $\mathbb{Z}_N^\star$.

Soit un entier e et $d = e^{-1} \bmod \varphi(N)$.

1. Montrer comment trouver l'inverse d'un élément a dans $\mathbb{Z}_p^\star$ par deux méthodes différentes et évaluer leur complexité. (L'une des deux méthodes utilise le petit théorème de Fermat.) En déduire que l'on peut calculer d à partir de e et $\varphi(N)$.
2. Montrer que pour tout $x \in \mathbb{Z}_N$, $x^{ed} = x \bmod N$.
3. Déterminer la complexité du chiffrement $x \mapsto x^e \bmod N$ et du déchiffrement quand e est petit. Pourquoi prendre $e = 3$ ou $e = 2^{16} + 1$.
4. Montrer comment accélérer le calcul du déchiffrement $x \mapsto x^d \bmod N$ en utilisant le théorème des restes chinois.
5. Que vaut $\varphi(N)$ dans notre cas ici ? Montrer que la connaissance de $\varphi(N)$ est équivalente à la factorisation.
6. Montrer que la connaissance de la clé secrète est équivalent à la factorisation de N. (Le sens direct reposera ici sur un algorithme probabiliste. Variante de l'algorithme de primalité de Miller-Rabin.)
7. (a) Montrer que presque la moitié des bits de $\varphi(N)$ est connue. En déduire que presque la moitié des bits de d est connue quand e est petit $e = 3$ par exemple.
   (b) Donner une solution déterministe pour le sens direct quand $|ed| < N^{3/2}$.
8. Montrer que le problème RSA, étant donné $y \in \mathbb{Z}_N$, trouver $x \in \mathbb{Z}_N$ tel que $y = x^e \bmod N$ est plus facile que le problème de la factorisation.

9. Supposer qu'il existe un algorithme (randomisé) en temps polynomial A_1 inverse pour presque tous les éléments de $\mathbb{Z}_N^\star$ pour une fraction au moins ϵ, pour une constante $\varepsilon > 0$. Montrer alors qu'il existe un algorithme qui inverse presque tous les éléments en temps polynomial en $\log N$ et $1/\epsilon$.
10. Montrer comment factoriser N quand au moins un des facteurs ne contient que des petits facteurs ($\leq 2^{30}$ par exemple).

Exercice 4: Euclide étendu

Soit a et b des entiers avec $a \geq b \geq 0$. On définit les suites d'entiers $r_0, r_1, \ldots, r_{\ell+1}$ et $q_1, \ldots, q_\ell$, où $\ell \geq 0$ de la façon suivante:

$$\begin{aligned}
a &= r_0, \\
b &= r_1, \\
r_0 &= r_1 q_1 + r_2 (0 < r_2 < r_1), \\
&\vdots = \vdots \\
r_{i-1} &= r_i q_i + r_{i+1} (0 < r_{i+1} < r_i), \\
&\vdots = \vdots \\
r_{\ell-2} &= r_{\ell-1} q_{\ell-1} + r_\ell (0 < r_\ell < r_{\ell-1}), \\
r_{\ell-1} &= r_\ell q_\ell (r_{\ell+1} = 0)
\end{aligned}$$

Par définition, $\ell = 0$ si $b = 0$, et $\ell > 0$ sinon. Alors $r_\ell = \gcd(a, b)$. De plus, montrer que si $b > 0$, alors $\ell \leq \log b / \log \phi + 1$ où $\phi := (1 + \sqrt{5})/2 \approx 1.62$.

On définit en plus les suites $s_0, s_1, \ldots, s_{\ell+1}$ et $t_0, t_1, \ldots, t_{\ell+1}$ de la manière suivante:

$$\begin{aligned}
s_0 &:= 1, \quad t_0 := 0, \\
s_1 &:= 0, \quad t_1 := 1,
\end{aligned}$$

et pour $i = 1, \ldots, \ell$,

$$s_{i+1} := s_{i-1} - s_i q_i, \; t_{i+1} := t_{i-1} - t_i q_i,$$

alors montrer que:

1. pour $i = 0, \ldots, \ell + 1$, $s_i a + t_i b = r_i$; et en particulier $s_\ell a + t_\ell b = \gcd(a, b)$;
2. pour $i = 0, \ldots, \ell$, $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$;
3. pour $i = 0, \ldots, \ell + 1$, $\gcd(s_i, t_i) = 1$;
4. pour $i = 0, \ldots, \ell$, $t_i t_{i+1} \leq 0$ et $|t_i| \leq |t_{i+1}|$; pour $i = 1, \ldots, \ell$, $s_i s_{i+1} \leq 0$ et $|s_i| \leq |s_{i+1}|$;
5. $i = 1, \ldots, \ell + 1$, $r_{i-1}|t_i| \leq a$ et $r_{i-1}|s_i| \leq b$.

Devoir à la maison: Théorème des Restes Chinois avec erreur

On veut reconstruire un rationnel $\hat{y}$, mais on a seulement les informations suivantes:

- Supposons qu'on sache que $\hat{y}$ peut s'exprimer comme r/t où r et t sont des entiers bornés par r^* et par t^* en valeur absolue. On ne connaît pas r et t, mais les bornes sont connues.
- On suppose de plus qu'on connaît deux entiers y et n tels que n est relativment premier à t et $y = rt^{-1} \bmod n$.

Si n est suffisamment grand par rapport aux bornes r^* et t^*, alors on peut retrouver $\hat{y}$ en utilisant l'algorithme d'Euclide étendu appliqué à n et y. De plus la restriction n et t sont premiers entre eux n'est pas nécessaire si on cherche $r = ty \bmod n$ ou $r = sn + ty$ pour un entier s.

(a) Supposons que r^*, t^*, n, y sont des entiers tels que $n \geq 4r^*t^*$, $0 \leq y < n$, $r^* > 0$ et $t^* > 0$. Alors si on exécure l'algorithme d'Euclide étendu à $a := n$ et $b := y$, montrer que:

1. avec les notations de l'exercice 2, il existe un unique indice $i = 1, \ldots, \ell+1$ tel que $r_i \leq 2r^* < r_{i-1}$ et remarquer que $t_i \neq 0$ pour ce i. Soit $r' := r_i, s' := s_i$, et $t' := t_i$.
2. De plus, pour tout entier r, s, t tels que $r = sn + ty$, $|r| \leq r^*$ et $0 < |t| \leq t^*$, $r = r'\alpha, s = s'\alpha$, et $t = t'\alpha$ pour un entier α non nul.

Application:

Soit $n_1, \ldots, n_k$) k nombres premiers entre eux tels que $n = \prod_{i=1}^{k} n_i$. À partir de $(a_1, \ldots, a_k)$ où $z = a_i \bmod n_i$, on peut retrouver z efficacement en utilisant le théorème des restes chinois. Donner sa complexité.

Pour coder un message z on calcule $(a_1, \ldots, a_k)$ et en réception des valeurs (mais pas trop) des a_i seront modifiées. Pourra-t-on toujours retrouver z ? On suppose que le nombre d'indice modifié sera borné par ℓ. Soit P le plus grand produit d'au plus ℓ termes n_i. Supposons que $0 \leq z \leq Z$ et $n \geq 4P^2Z$.

(b) Montrer que l'algorithme suivant retrouve z à partir de $(\bar{a}_1, \ldots \bar{a}_k)$.

1. Appliquer le théorème des restes chinois pour obtenir y tel que $0 \leq y < n$ et $y = \bar{a}_i \bmod n_i$ pour $i = 1, \ldots, k$.
2. Exécuter euclide étendu à n et y et soient r', t' les valeurs obtenues avec $r^* = ZP$ et $t^* = P$.
3. Si $t' | r'$, retourner r'/t', sinon "erreur".