TD3 - Chiffrement asymétriques, logarithme discret et factorisation en nombres entiers

Nasko Karamanov Ludovic Perret Loïc Rouquette

Les problèmes de factorisation des entiers et logarithme discret

Le background mathématiques

Dans cette section on révise et complète les pré-requis pour le chapitre.

Question 1

Plusieurs cryptosystèmes utilises des calculs exponentiels. L'algorithme suivant permet d'accélérer ce type de calculs (**square and multiply**).

Soit:

$$e = \sum_{i=0}^{l} 2^i e_i \text{ où } e_i = \{0, 1\}$$

alors

$$m^e = \prod m^{2^i e_i}$$

Ceci montre qu'il suffit de calculer seulement les puissances de deux. Par exemple si $l = 4$ alors :

$$m^e = m^{2^4 e_4} \cdot m^{2^3 e_3} \cdot m^{2^2 e_2} \cdot m^{e_0}$$

On peut également obtenir le produit avec des multiplications successives. De nouveau si $l = 4$ alors,

$$\begin{aligned}
t_5 &= 1 \\
t_4 &= t_5^2 \cdot m^{e_4} = m^{e_4} \\
t_3 &= t_3^2 \cdot m^{e_3} = m^{2e_4+e_3} \\
t_2 &= t_2^2 \cdot m^{e_2} = m^{2^2 e_4+2e_3+e_2} \\
t_1 &= t_1^2 \cdot m^{e_1} = m^{2^3 e_4+2^2 e_3+2e_2+e_1} \\
t_0 &= t_0^2 \cdot m^{e_0} = m^{2^4 e_4+2^3 e_3+2^2 e_2+2e_1+e_0}
\end{aligned}$$

On remarque que dans chaque étape on calcule le carré et on multiplie par m^e, d'où le nom de l'algorithme. Si l'exponant est 0 alors il n'y a pas besoin de multiplier.

a. Déterminer $13^7 \mod 38$ avec cet algorithme.
b. Comparer la complexité (le nombre d'opérations effectuées) de la multiplication naïve et cet algorithme pour le calcul de m^e.

Question 2

Le petit théorème De Fermat dit que si p est premier et $0 < a < p$ alors

$$a^{p-1} \equiv 1 \mod p$$

Ce théorème peut être utilisé à la fois pour simplifier les calculs exponentiels mais aussi les calculs d'inverse multiplicatif modulo p. En effet $a \cdot a^{p-2} \equiv p$ donc $a^{-1} \equiv a^{p-2} \mod p$.

a. En utilisant la remarque précédente et l'algorithme d'exponentiation rapide, calculez $11^{187} \mod 31$
b. Calculer l'inverse de 5 dans $\mathbb{Z}/31\mathbb{Z}$.

Question 3

En utilisant l'algorithme d'Euclide étendu, déterminer si possible l'inverse multiplicatif de :

a. $7 \in \mathbb{Z}/38\mathbb{Z}$
b. $6 \in \mathbb{Z}/38\mathbb{Z}$

Question 4

Alice et Bob décident d'utiliser ElGamal avec $p = 23$ et $g = 5$.

a. Décrire l'ensemble des messages $\mathcal{M}$ et des chiffrés $\mathcal{C}$.
b. La clé publique de Bob est $pk = 17$. Alice souhaite envoyer le message $m = 13$ avec sa clé privée $a = 3$. Quelle message chiffré reçoit Bob ?
c. Bob a reçu un deuxième message d'Alice : $c = (21, 17)$ intercepté par Eve.

1. À quel problème est confronté Eve ?
2. Eve décide d'utiliser l'algorithme de Shank pour déterminer la clé de Bob. Quelle est cette clé ?
3. Quel est le message d'Alice ?

d. Alice et Bob décident de convertir les lettres en nombre en utilisant l'ordre alphabétique : $A \to 01, B \to 02, ...$ Alors ils chiffrent le message par blocs de deux lettres. Quel est le problème avec leur schéma actuel et comment le résoudre ?

Question 5

a. Alice et Bob communiquent en utilisant RSA. Bob reçoit un message chiffré avec sa clé publique (n, e). Peut-il être sûr que le message provient d'Alice ?
b. Alice a trouvé une solution à ce problème. Elle chiffre son message m avec lé clé publique de Bob, e_B mais envoie (c, c^{d_A}), où d_A est sa clé **privée**. Bob peut-il maintenant être sûr que le message provient d'Alice ?
c. Formaliser la notion de signature numérique contenant trois algorithmes : `KeyGen`, `Sign` et `Verify`.
d. Expliciter les algorithmes dans le cas d'Alice et Bob (signature RSA).
e. Est-ce que cette signature a un désavantage ? Si oui, quelle est la solution à ce problème ?
f. Que pouvez-vous dire sur la complexité de la signature ?
g. Cette signature est-elle post-quantique ?