SAE R3.09 Cryptographie

Martins Hugo

Implémentation du crypto-système de Kifli

Présentation LaTeX de la SAE de Cryptographie

IUT Informatique
Université de Bordeaux
France
30 novembre 2023
Equipe : Martins Hugo

Abstract

Ce court rapport réalisé en LaTeX va présenter l'implémentation du crypto-système de Kifli qui a été réalisé. En premier lieu, j'expliquerai de manière générale le cryptosystème avec quelques détails sur son fonctionnement et sur le fonctionnement d'un système de chiffrage asymétrique, et dans un second temps, une explication de l'implémentation réalisé (quelles fonctions sont présentes et en quoi elles sont essentielles) sera donné.

---

1 Présentation générale du cryptosystème

1. **Fonctionnement du cryptosystème de Kifli**

   Tout d'abord, pour avoir un crypto-système à clé publique, il faut s'appuyer sur un problème inversible mais fortement asymétrique d'un point de vue calculatoire.

   Désormais, on peut comprendre le problème asymétrique utilisé par Kifli : étant donné n entiers positifs $a_1, a_2, \ldots, a_n$ ainsi qu'un entier c, on cherche à trouver un choix judicieux parmi les a_i tel que leur somme vaille exactement c.

   Dans le cryptosystème de Kifli :

   (a) la clé privé est un pochon; résoudre un problème de pochon est très simple, il suffit de prendre le plus grand b_i tel que $b_i \leq c$, puis de recommencer avec $c - b_i$.

   (b) la clé publique est une poche réalisé à partir du pochon. Un problème de poche est considéré comme très difficile (en théorie de la complexité on parle de problème NP-complet).

   Comme on a désormais une clé privée simple et une clé publique supposé introuvable (car le problème de poche est jugé beaucoup trop difficile à résoudre, la partie théorique du cryptosystème est terminée).

2. **Réponses à la question du sujet**

   Il s'agit désormais de savoir si le cryptosystème est fiable et qu'il ne contient pas de brèche potentielle. Dans un premier temps, un point qui pourrait poser problème vis à vis de la sécurité du cryptosystème est que la taille du bloc du message à chiffrer correspond à la taille de la poche. Ce premier point pourrait constituer une brèche potentielle car en connaissant la clé publique, on connaît le nombre de caractères chiffrés. De plus, ce cryptosystème comporte des contraintes : si la taille du bloc du message n'est pas suffisamment grande, alors décoder le message ne poserait pas de problème même si c'est un problème NP-complet. En effet, en prenant par exemple un bloc de taille n=6 (on code un bloc de 6 caractères constituant, en partie ou totalement, le message), on remarque que trouver la

solution au problème de poche devient tout de suite une tâche très simple que n'importe quelle personne peut résoudre sans besoin d'aucune aide externe :

(a) Considérons la poche [491,540,682,378,575,801] et le message chiffré C=1974.

(b) On remarque alors que le problème parâit directement bien plus simple à résoudre : par exemple, pour trouver l'unité du message chiffré C, on peut voir que seuls 3 moyens sont possibles : 491+682+801, OU 491+378+575, OU 378+575+801. Il suffit donc de tester ces 3 possibilités, et on remarquera que ce genre de méthode peut assez facilement être appliqué tant que n est petit.

On a ainsi pu voir que le cryptosystème comporte des contraintes (comme avoir une taille de bloc n suffisamment grand), et qu'il n'est pas parfait dans sa sécurité (la taille du bloc du message est connue, autrement dit, on connaît la taille du message chiffré grâce à la clé publique) Ce sont ces raisons, et en particulier celle sur la taille du message qui est connue, qui me pousse à croire que c'est pourquoi l'algorithme de Kifli n'a pas été retenu par le NIST.