*Sujet :* Attaque du système de cryptage d’El Gamal.

*Description :*

Longtemps réservée au domaine militaire, la cryptographie est une science très jeune qui a véritablement éclos avec l’avènement de l’informatique et la généralisation des télécommunications. Dans le cadre de ce TIPE, je me suis plus spécifiquement intéressé au système cryptographique d’El Gamal dont la sécurité repose sur le problème dit du « logarithme discret ».

On dit qu’un crypto-système est difficile à « casser » si, lorsqu’on intercepte un message crypté, décrypter ce message sans la clé nécessaire est soit impossible, soit trop long pour être effectué en un temps raisonnable. Un message peut être une séquence de bits (0 et 1), un caractère (« A »), une chaine de caractères ou encore un nombre. Dans un souci de simplification j’ai uniquement considéré des messages sous forme d’entiers puisque le système de sécurité El Gamal réalise des opérations sur des entiers.

Pour cerner la complexité du problème du logarithme discret, j’ai commencé par tester les limites d’un algorithme naïf. Lorsque les données sont trop volumineuses, l’algorithme naïf n’est plus capable de donner une solution en un temps raisonnable ; j’ai alors eu recours à un autre algorithme plus performant : l’algorithme de Shank (également appelé « Baby-step Giant-step »). Cependant, une implémentation efficace de cet algorithme requiert que l’on distribue intelligemment ses ressources informatiques. Pour exécuter une telle distribution, j’ai fait appel à la structure de donnée des « tables de hachage ».

*Plan :*

I/ Présentation du problème et des algorithmes.

1. Crypto-système d’El Gamal et problème du logarithme discret.
2. Algorithme naïf.
3. Une méthode plus efficace : Algorithme de Shank.

II/ Un outil indispensable : les tables de hachage.

1. Définitions.
2. Gestion des collisions par chainage.
3. Etude d’une fonction de hachage.

III/ Efficacité et limites de l’algorithme de Shank.

*Sources :*

-Wikipédia (encyclopédie libre) :

Algorithme Baby-step Giant-step : <http://fr.wikipedia.org/wiki/Baby-step_giant-step>

Système El Gamal : <http://fr.wikipedia.org/wiki/Cryptosyst%C3%A8me_de_ElGamal>

Anneau Z/nZ : <http://fr.wikipedia.org/wiki/Anneau_%E2%84%A4/n%E2%84%A4>

Logarithme discret : <http://fr.wikipedia.org/wiki/Logarithme_discret>

Inverse modulaire : <http://fr.wikipedia.org/wiki/Inverse_modulaire>

- Shishir Agrawal, “Shank’s baby-step giant-step algorithm” :<https://math.berkeley.edu/~sagrawal/su14_math55/notes_shank.pdf>

- Conférence de presse du CNRS, « les enjeux de la cryptologie » : <http://www2.cnrs.fr/sites/communique/fichier/6_enjeux_charte.pdf>

- CPAS , “Liste des nombres premiers en ligne” : <http://compoasso.free.fr/primelistweb/page/prime/liste_online.php>

- François Brunault, « TD/TP sur les corps finis » : http://perso.ens-lyon.fr/francois.brunault/enseignement/1415/TD\_Corps\_finis.pdf

- Thomas Cormen, Charles Leiserson et Ronald Rivest , « Introduction à l’algorithmique » , DUNOD, 1994.

- Christine Froideveaux, Marie-Claude Gaudel et Michèle Soria, « Types de données et algorithmes », EDISCIENCE international, 1993.

*Contact :*

Jacques Patarin, cryptologue et professeur à l'université de Versailles-Saint-Quentin-en-Yvelines.