**Résolution du logarithme discret a l’aide de tables de hachage.**

*Introduction :*

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 qui, bien que créé il y a plus de 20 ans, s’avère encore difficile à « casser », c'est-à-dire que, si l’on intercepte un message crypté, décrypter ce message sans clé est soit impossible, soit trop long pour être effectué en un temps raisonnable.

En effet, la sécurité de ce système repose sur le problème dit du « logarithme discret » dont la résolution informatique peut être particulièrement chargée. Afin de casser ce crypto-système à l’aide de l’algorithme de Shank (également appelé « Baby-step Giant-step »), j’ai été mené a utiliser mes ressources informatiques a bon escient en distribuant les données efficacement dans des « tables de hachage ».

*Problématique / Objectif :*

Comment peut-on distribuer ses ressources informatiques intelligemment afin de casser le système de cryptage d’El Gamal le plus efficacement possible ?

*Plan :*

I/ Présentation du problème et de l’algorithme de Shank.

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

II/ Un outil indispensable : les tables de hachage.

1. Définitions et concept.
2. Insertion.
3. Recherche.

III/ En pratique.

1. Détermination empirique d’une fonction de hachage uniforme.
2. Fonctionnement pratique de l’algorithme, efficacité.