Utilisation d'algorithmes génétiques en cryptographie

Type de contenu : Texte

Titre(s) : Utilisation d'algorithmes génétiques en cryptographie : Mémoire de fin d'étude - Systèmes informatiques et modélisation

Auteur(s) : Delfour Frédéric (EN 2004)

Autre(s) responsabilité(s) : Dr. J. Van Hamme (Gestionnaire de projet)
Stolz Frédéric (EN 2004)

Editeur, producteur : Lanvéoc-Poulmic : Ecole navale, 2006

Description matérielle : 44 p.
: Figures
: Tableaux

Note(s) : Bibliogr.

Note de thèses et écrits académiques : Chaire de mathématiques
Ecole Royale Militaire

Résumé ou extrait : Certains problèmes de cryptographie peuvent se ramener à des problèmes d'optimisations, on peut donc envisager de les résoudre en utilisant des algorithmes génétiques. Le cahier des charges prévoyait l'utilisation d'algorithmes génétiques pour résoudre un cas simple et leur application sur l'algorithme de chiffrement DES (Data Encryption Standard) complet. Nous avons choisi pour cas simple, un DES réduit à 8 tours (principalement pour les temps de calculs). Les résultats ainsi obtenus nous ont orientés vers l'application des algorithmes génétiques à un autre algorithme plutôt que de poursuivre sur le DES à 16 tours. Après une étude théorique des principes du DES, et des algorithmes génétiques nous nous sommes rapidement orientés vers la programmation. L'élaboration du programme pour un DES à N tour a constitué la plus grande part du travail, ce programme ayant connu diverses versions. Grâce à la manière dont nous avons conçu ce programme, nous avons pu le réutiliser pour le deuxième algorithme au prix de peu d'adaptations. Nous procéderons enfin à une étude des résultats obtenus.

Sujet(s) : algorithme génétique