Binary fields in an Elliptic Curves Cryptosystem Implementation

Type de contenu : Texte

Titre(s) : Binary fields in an Elliptic Curves Cryptosystem Implementation ; JADDA, Zoubida ; KURES, Miroslav ; SLT DEGENNE, Colas

Autre(s) responsabilité(s) : JADDA, Zoubida (Directeur de thèse)
KURES, Miroslav (Directeur de thèse)
SLT DEGENNE, Colas Promotion Chef de bataillon Bulle (2010-2013) (Secrétaire)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef de bataillon Bulle Date de soutenance : 01/01/2013

Résumé ou extrait : PRESENTATION : On dit que la connaissance peut mener à la victoire, C'est la raison pour laquelle, en temps de guerre, les services de renseignements de chaque camp tentent de découvrir quels sont les plans et les pensées de l'autre camp. C'est pourquoi, dans les conflits actuels, il faut être sûr que toute information envoyée dans un but militaire ne sera pas lue par l'ennemi. Mais face aux avancés en termes d'attaques informatiques, la sécurité des systèmes de cryptages ne peut pas cesser d'être améliorée sous peine d'être rendus obsolètes. Afin que leurs programmes restent utiles, les scientifiques recherchent de nouvelles façons d'augmenter la sureté de leurs procédés en tentant de rendre le problème mathématique sous-jacent à ces procédés plus difficile à résoudre. Notre but est de présenter, puis d'utiliser, un problème mathématique qui permet l'amélioration de l'une des façons actuelles de crypter des données. Nous tenterons alors d'implémenter un programme qui utilisera un procédé amélioré par le susmentionné problème mathématique. Ce programme devra être capable de crypter un message donné puis de le décrypter. RESTRICTIONS : Afin d'être productif au cours du court intervalle de temps qui nous est donné, nous devons restreindre les outils mathématiques que nous allons utiliser et ne sélectionner que ceux qui seront les plus importants dans la conduite de l'implémentation de notre programme. Cela implique que des améliorations pourront être apportées à notre programme final en utilisant les outils mathématiques qui auront initialement été mis de côté. RESULTAT FINAL : Nous avons géré le précédent problème en sélectionnant les polynômes irréductibles directement dans une base de données. Ensuite, en utilisant le problème mathématique que nous avions étudié, nous avons réussis à finaliser l'implémentation de notre programme. Comme nous le souhaitions initialement, notre programme final est capable de sélectionner un message dans un fichier, de crypter ce message, puis de l'injecter dans un autre fichier. Après avoir envoyé le message crypté à son destinataire, le décryptage est possible de la même façon. Dans le même temps, le programme peut être utilisé comme un outil mathématique. En effet, son implémentation nécessitant d'utiliser plusieurs notions mathématiques difficiles, des programmes de calculs y ont été incorporés et peuvent être utilisés de façon indépendantes.

LIMITES : Il y a malgré tout quelques limites à notre résultat : La première d'entre elles est que la sécurité de notre programme n'a pas été testée pour le moment. Ainsi, malgré la théorie qui implique que notre procédé consiste en une amélioration en termes de sécurité, il n'y a aucune expérience qui prouve qu'il serait sûr face à des attaques. La seconde limite provident du fait que la méthode que nous utilisons pour attribuer un nombre à un caractère utilise le code ASCII basique, qui ne code pas tous les caractères. Il ne serait sans doute pas difficile d'y remédier, mais cela nécessiterait un peu plus de temps. Pour l'instant, le message que nous voulons crypter ne doit pas contenir d'accents, par exemple.
CONCLUSION : Notre programme final nous permet de prouver deux choses : qu'il existe des façons simples d'améliorer les procédés de cryptage utilisés actuellement et que les mathématiques peuvent encore procurer de nouveaux sujets qu'il faudra étudier afin de trouver un programme acceptable en termes de sécurité. Une autre chose qui mérite d'être soulignée est qu'il est relativement aisé d'implémenter un programme utilisé un système de cryptage amélioré comme le notre. Il n'y a donc aucun obstacle à l'application de tels procédés de manière industrielle, si ce n'est le test de sécurité qui doit être fait. En effet, notre programme final n'est pas optimal, de la même façon que plusieurs autres programmes qui ont été implémenté avant lui et dont certaines recherches en cryptanalyse ont prouvé qu'ils n'étaient pas sécurisés. Le futur de ces programm

Sujet(s) : cryptage
mathématiques : science
piratage informatique
programme informatique
securité des données
services de renseignement
sécurité informatique