Décodages itéractifs de registres à décalage à rétroaction linéaire

Type de contenu : Texte

Titre(s) : Décodages itéractifs de registres à décalage à rétroaction linéaire : Mémoire de fin d'étude - Réalité virtuelle

Auteur(s) : Avignon (EN 1999)

Autre(s) responsabilité(s) : Alquié M., ingénieur principal de l'armement, responsable de la section Etudes cryptographiques du centre d'électronique de l'armement (Gestionnaire de projet)
Bonnard (EN 1999) Bonnard (EN 1999) (Gestionnaire de projet)

Editeur, producteur : Ecole navale : Ecole navale, 2001

Description matérielle : 43 p.
: Ill.

Note(s) : Annexes
Bibliogr.

Note de thèses et écrits académiques : CELAR/CASSI, Bruz, France

Résumé ou extrait : Ce projet se situe dans le domaine de la cryptologie. Il consiste à concevoir et réaliser un programme de décodage itératif de registres à décalage à rétroaction linéaire, mettant en oeuvre un nouvel algorithme. Le cahier des charges prévoyait le découverte des registres et des algorithmes classiques de décodage, puis la programmation d'une nouvelle méthode présentée par Anne Canteault et Michaël Trabbia lors du congrès EUROCRYPT 2000. Nous avons rédigé une synthèse des principales techniques de décodage itératif connues à ce jour, rétablissant, en particulier, le détail des démonstrations et unifiant les notations. Puis nous avons élaboré un algorithme précis à partir de l'article qui nous était proposé. Nous l'avons programmé en langage C++. Enfin, nous avons réalisé diverses simulations à l'aide de ce programme. Elles nous ont permis de dégager des liens entre les différents paramètres intervenant dans le décodage, facilitant ainsi le travail des futurs utilisateurs.

Sujet(s) : Décodage
Itération
Registre décalage
Syndrome
cryptologie