Projet informatique I / II (IFT592 / IFT692)

Titre :
CryptoDES

Sujet :

Élaboration d'un outil graphique didacticiel pour l'apprentissage du protocole de chiffrement symétrique DES (version simplifiée à des fins pédagogiques)

Spécification :

Les procédés de chiffrements cryptographiques basés sur les clefs de décryptages font partie des thèmes enseignés dans le cours IFT606 (sécurité et cryptographie). Le but de ce projet est de concevoir un outil didacticiel qui montre, à travers des exemples implémentés et/ou proposés (par téléversement), le fonctionnement détaillé de l'algorithme de chiffrement symétrique DES (*Data Encryption System*), étudié dans le cours IFT606. La phase 1 vise à implémenter une version simplifiée de l'algorithme DES.

Description sommaire :

L'outil doit être un programme exécutable portable (S*tandalone*) non-installable, codé dans un langage de programmation (à spécifier ultérieurement selon certaines praticabilités), qui permettrait à l'étudiant(e) de (1) tester le chiffrement DES, étape par étape (via l'interface graphique), (2) voir les détails de la trace de chiffrement (complète ou interactivement, pas-à-pas), et (3) comparer une solution élaborée (téléversée selon un format spécifique) avec la solution de l'algorithme implémenté.

Pré-requis académiques :

De préférence, l'étudiant(e) doit avoir compléter le cours IFT606.