Projet informatique
Cryptographie

Sébastien Pedreau
Christian Ingouff

Année 2012/2013
Semestre 4

Cryptographie

Introduction

La cryptographie une science qui implique le codage ou le décodage de messages à l'aide d'algorithmes précis. Ce projet est une introduction pour nous dans le domaine de la cryptographie. Nous nous intéresserons plus précisement à la cryptographie qui utilise des algorithmes de cryptographie asymétrique, c'est-à-dire l'utilisation d'un clé publique pour chiffrer le message, et d'une clé privée pour le déchiffrer.

Nous utiliserons ici deux algorithmes de cryptage asymétrique : le cryptage Merkle-Hellman (abrégé MH), et le cryptage Rivest, Shamir et Adleman (RSA) qui est très connu et très utilisé dans le commerce électronique.

Utilisation

Notre réalisation sera capable de crypter ou de décrypter des messages depuis des fichiers textes ou par insertion à l'écran, grâce aux deux méthodes demandées : MH et RSA. Elle retournera ses résultats dans des fichiers qu'elle affichera à l'écran si l'utilisateur le veut.

Notre projet est de plus capable de générer les clés privée et publique, une fois de plus pour les deux méthodes énoncées ci-dessus.

Lors de l'exécution, notre réalisation gère toutes les exceptions classiques, telles que l'absence d'un fichier, erreur de lecture ou d'écriture, etc.

Compilation

Pour compiler notre projet, l'exécution de ces commandes est nécessaire :

- ocamlc nums.cma -c Toolbox.ml Gmh.ml Cmh.ml Dmh.ml Grsa.ml Crsa.ml Drsa.ml (compilation des librairies)
- ocamlc nums.cma Toolbox.cmo Gmh.cmo Cmh.cmo Dmh.cmo Grsa.cmo Crsa.cmo Drsa.cmo crypto.ml -o crypto (compilation du programme)

Afin de vous familiariser au fonctionnement de notre programme, nous vous invitons à taper ensuite la commande :

./crypto -h