Université de Limoges

Développement Logiciel Cryptographique

Projet n° 14

Calculette cryptographique

Résumé

Développement à l'aide de GMP d'une calculette capable d'effectuer des calculs cryptographiques.

1 Calculette cryptographique

La bibliothèque GMP [1] fournit des types de données et des fonctions permettant notamment d'effectuer toutes sortes de calculs sur des entiers de taille arbitraire. Son utilisation permet ainsi de ne pas être limité par la capacité limitée des types de base du langage C.

En utilisant une librairie de fonction graphiques permettant de créer des IHM, vous développerez un outil de type calculette qui sera spécialisé dans les calculs de fonctions cryptographiques

Après avoir écrit un document de spécifications (quelques pages) décrivant les fonctionnalités retenues pour cette calculette vous en réaliserez l'implémentation et les tests.

À titre indicatif et non limitatif, votre calculette devra proposer les services suivants :

- génération de clés RSA en mode standard
- chiffrement/déchiffrement RSA
- signature/vérification RSA
- au moins une fonction de hachage
- au moins un algorithme de chiffrement symétrique
- chiffrement/déchiffrement de fichiers en mode ECB et CBC (crypto symétrique)
- calcul de MAC-CBC ou de H-MAC de fichiers
- ...

1. http://gmplib.org/