Projet Cryptographie

L. Poinsot[a]

[a] *LIPN - UMR 7030*
CNRS - Université Paris 13
F-93430 Villetaneuse, France

Résumé

Il s'agit de programmer en langage C le procédé de chiffrement DES. L'objectif étant de pouvoir chiffrer et déchiffrer des fichiers texte à l'aide du cryptosystème DES.

Introduction

- Ce projet est à effectuer en groupe de **quatre à cinq élèves**.

- Code en **langage C uniquement**.

- Veiller à commenter très **soigneusement** votre code.

Évaluation du travail

Lors de la dernière séance de TP, chaque groupe présentera de façon informelle son travail sur machine. Suivront ensuite des questions (sur l'utilisation de votre programme et sur le code).

Programmation du cryptosystème DES

Dans le document "FIPS PUB 46-3", écrit en langue anglaise, vous trouverez les spécifications techniques du cryptosystème DES. Le but de projet est donc d'implanter ce procédé de chiffrement en **langage C**. L'algorithme de **chiffrement**, l'algorithme de **déchiffrement** devront ainsi être implantés; chacun d'eux utilise l'algorithme de **dérivation des sous-clefs** KeySchedule

Courrier électronique : `laurent.poinsot@lipn.univ-paris13.fr` (L. Poinsot)

(appelé **Key schedule** dans le document "FIPS PUB 46-3") qui sera également implanté. Le message clair M (qui est un bloc de 64 bits) et la clef principale, constituée de 64 bits, appelée KEY dans le document FIPS BUB 46-3, seront des arguments d'entrée de votre algorithme de chiffrement DESencrypt, alors que le message chiffré (qui est un bloc de 64 bits) et la clef principale seront les arguments d'entrée de l'algorithme de déchiffrement DESdecrypt.

En bref, il faut coder les fonctions en **langage C** :

- KeySchedule(KEY, i) qui prend en entrée un bloc de 64 bits KEY, ainsi qu'un entier entre 1 et 16 (représentant la ronde courante), et renvoie la sous-clef du $i$ème tour K_i. (Voir le document "FIPS PUB 46-3".)

- DESencrypt(M, KEY) qui prend en entrée un bloc de 64 bits M et un bloc de 64 bits KEY, et renvoie un bloc de 64 bits C représentant le message M chiffré avec la clef secrète KEY par DES. Cet algorithme fait appel à l'algorithme KeySchedule.

- DESdecrypt(C, KEY) qui prend en entrée un bloc de 64 bits C et un bloc de 64 bits KEY, et renvoie un bloc de 64 bits M représentant le message C déchiffré avec la clef KEY par DES. Cet algorithme fait également appel à l'algorithme KeySchedule.

  Avec votre implantation du DES il devra être possible de chiffrer et de déchiffrer des fichiers texte (il sera donc nécessaire de découper votre fichier en blocs de 64 bits chacun). La clef principale pourra être entrée en ligne de commande ou contenue dans un fichier texte (au choix de l'utilisateur).

  Remarque : Le document "FIPS PUB 46-3" précise l'emploi de bits de parité (les bits 8, 16, 24, 32, 40, 48, 56 et 64) de la clef principale KEY. En ce qui vous concerne vous les traiterez comme n'importe quel autre bit de la clef (en bref, vous n'êtes pas dans l'obligation de gérer la parité).

Vous disposez également de trois fichiers :

- FIPS PUB 46-3 contenant la description complète du DES.

- "tableaux.c" contenant les permutations PC1, PC2, P, les fonctions IP (Initial Permutation) et IP_INV (Inverse Initial Perm IP^{-1}), ainsi que les huit "S-boxes" $S_1, \cdots, S_8$.
- "deroulement.txt" donnant un exemple de déroulement de l'algorithme DES.