MATH EN INFO

MODULE PERMUTATION

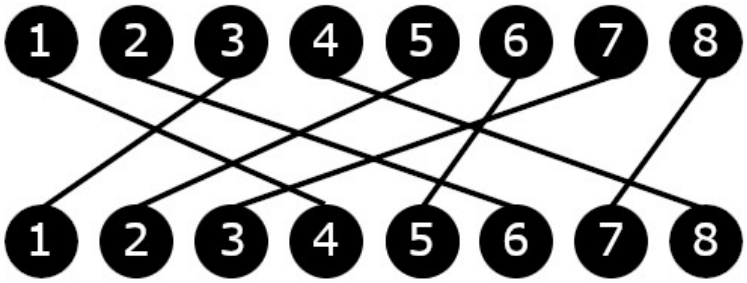
Phase 1

1 Présentation

Ce fichier contient quelques indications sur l'algorithme de permutation utilisé dans la fonction non-linéaire F du système de cryptage ainsi que des indications sur la phase 2 du module permutation.

2 Indications sur la permutation

La fonction non-linéaire utilise la permutation sur 8 bits suivante :



3 Indications pour la phase 2

3.1 Descriptif des phases

L'analyse du module de permutation du logiciel nous a permis de déterminer que celui-ci est composé de d'une seule communication (phase 2).

Lors de cette communication le logiciel génèrera un nombre aléatoire de mots binaires de 8 bits et attendra en retour leurs images par la permutation.

Bien évidemment, la communication devra commencer par l'envoi du mot de passe de celle-ci et se terminera par l'envoi par le logiciel de l'instruction "END".

3.2 Indications pour les mots de passes des communications

Le mot de passe de la communication a été encodé à l'aide d'un algorithme de masque jetable de clé "11011011110110". Le message obtenu est "1001000111000".