**Rapport DM Sécurité – Guillaume ROTH**

**2 – Implémentation de l’algorithme E0**

Question 1 – On choisira d’utiliser une structure contenant les numéros des bits à extraire, une liste chaînée contenant la valeur des bits, ainsi que la valeur à ajouter à la tête de celle-ci lors du prochain shift. Cela sera plus facile de manipuler et traiter les données, notamment pour le shift. En effet, la liste chaînée est plus « souple » qu’un tableau et permet par exemple la suppression du dernier élément, contrairement à un tableau, qui est beaucoup plus « rigide », et qui nous forcerait à décaler les cases une par une.