**Rapport DM Sécurité – Guillaume ROTH**

Question 1 – On choisira d’utiliser une structure contenant les numéros des bits à extraire, ainsi qu’une liste chaînée contenant la valeur des bits. 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.

Question 2 – D’après Wikipédia, ainsi que le nombre incalculable de tutoriels trouvés via Google permettant de cracker les chiffrements à flots, je pense que sa sécurité actuelle est très relative, pour ne pas dire anecdotique.

Question 6 - On remarque que Von Neuman semble beaucoup plus régulier, même suivre un pattern, contrairement à Mersenne Twister. En effet, l’algo de Von Neuman ne fait pas vraiment entrer en compte de facteur aléatoire et a donc un pattern que l’on peut suivre.

Question 7 – Après application de la fonction Frequency() ainsi que la règle de précision à 1%, on peut s’apercevoir que la méthode de Von Neumann ne constitue pas un générateur réellement aléatoire (au sens du test), contrairement à la méthode de Mersenne-Twister qui semble particulièrement efficace. (Idem Question 8)

Question 10 -