Projet AES cryptographie

1. Auto-évaluation

Nous pensons que pour la réalisation des différents exercices des TPs nous aurions eu la note de 8/10 car toutes les réalisations fonctionner sans aucun bug et elles étaient réaliser de tel manière à ce qu'elles puissent être facilement réutilisé et adapté au projet effectué par la suite. Mais il y a certainement des améliorations à apporter pour optimiser le programme ou encore nous aurions pu réaliser certains de ces exercices plus rapidement.

2. Pédagogie

Tous les exercices ont permis de comprendre chaque partie de l'AES mais nous avons trouvé que la question C.1 fut la plus intéressante et nous a permis de bien comprendre le fonctionnement de l'AES. Il était bien expliqué avec ses schémas et bien diviser en petite fonction à implémenter nous permettant de pouvoir avancer petit à petit, apprendre à diviser en plusieurs fonctions notre programme et à les faire marcher ensemble.

3. Notre avis

Le moyen utilisé qui est de faire le résumé md5 d'un mot de passe est dans notre cas une bonne méthode du point de vue pédagogique car elle permet de comprendre le fonctionnement du hachage et comment se servir du md5. Mais bien sur c'est n'ai pas la meilleure méthode pour créer des clefs de 16 octets. En effet en 2004 il a été prouvé que le résumé md5 n'est pas fiable car il y avait des collisions. Si on veut optimiser la sécurité on devrait utiliser les méthodes de hachage plus récentes et sécurisées qu'ils sont, à l'heure actuelle, encore fiable tel que SHA1 par exemple.