Université Rennes **Année 2023-2024**
Département de Mathématiques
M1, module Crypto compléments

Projet implémentation de l'AES

Vous trouverez le standard fips-197 décrivant l'AES
— sur le site de la formation, dans la rubrique documents
— sur le Moodle du cours
— sur le site du NIST : `https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf`
Entre le cours, le TD et le TP du cours de Cryptographie, vous avez normalement tous les éléments pour comprendre ce document et implémenter l'AES **en C**.

Savoir lire un standard et en tirer une implémentation est très important et celui ci est particulièrement clair. Bien sûr il y en a 50 pages, mais l'essentiel est dans les pages 13 à 19.

N'essayez pas de tout faire a la fois. Commencez par une fonction de chiffrement d'un seul bloc avec une clé de 128 bits. Une fois que celle-ci marche, vous pourrez passez au déchiffrement et à d'autres tailles de textes et de clés. En annexe du document, il y a un exemple avec tous les états intermédiaires qui peut vous aider à trouver d'où vient une éventuelle (et bien sûr improbable) erreur.

Au minimum, votre programme doit être capable de chiffrer un document (de taille quelconque) en mode ECB avec une clé de 128 bits choisie par l'utilisateur (par défaut 0x000102030405060708090a0b0c0d0e0f).
Au plus, votre programme peut chiffrer et déchiffrer un document en mode ECB, CBC, CFB (ou OFB) et GCM (choisi par l'utilisateur) avec une clé de taille 128, 192 ou 256 bits.
Comme tout programme qui se respecte, il devra être **clair et bien documenté**. Vous y joindrez un **compte-rendu** contenant

(1) une notice d'utilisation
(2) un programme de test ou un script, en précisant la commande à utiliser (du type `gcc test test.c` puis `./test`) qui me permet de connaitre le temps de calcul pour effectuer 100 fois le chiffrement du fichier `alice.sage` en mode ECB avec la clé par défaut
(3) la description du fonctionnement de votre implémentation (mais pas de l'algorithme AES)
(4) les difficultés que vous avez rencontrées et les solutions trouvées pour les dépasser

Ce travail est indispensable pour les étudiants souhaitant continuer en M2 crypto. Il n'est noté que de façon minimale (l'équivalent d'environ 1 ECTS) car le but n'est pas scolaire mais de parfaire votre formation par quelque chose de concret qu'un employeur peut vous demander du jour au lendemain en plus de votre travail habituel. Il faudra d'ailleurs bien penser à le mettre (du style "projet AES en C") dans vos CV.

Il est à rendre pour le 25 mai sur Moodle **sans aucun retard toléré**. C'est un travail conséquent, mettez y vous rapidement.