Le rendu du projet consiste en un rapport (d'une ou deux pages) au format PDF nommé `RAPPORT.PDF` *et accompagné par les fichiers sources de votre travail (programmes C ou Java). Un fichier* `Makefile` *permettant de compiler ces sources en lançant la commande* **`make`** *devra être joint au projet.*

Vous placerez dans un répertoire `AES` *l'ensemble des fichiers demandés puis créerez, via la commande Unix* **`tar -czvf AES.tgz AES`** *(ou une commande équivalente si vous travaillez sous Windows) une archive globale de vos programmes. Les archives ZIP seront également acceptées. Le fichier* `AES.tgz` *ou* `AES.zip` *obtenu devra ensuite être envoyé* ***avant le jeudi 14 décembre 2017 à midi****, attaché à un email destiné à* **`remi.morin@univ-amu.fr`** *avec pour sujet «* **`[AES-LUM] <vos noms>`***».*

Les projets en retard ne seront pas acceptés.

Le programme AES à programmer (5 points)

Le code à produire (en C ou en Java) repose sur celui que vous avez obtenu lors de l'implémentation de l'AES dans les exercices B.3, C.1, C.2, et F.2. En particulier *il ne devra pas s'appuyer sur la JCE (excepté pour le calcul d'un résumé MD5) si vous codez en Java*. Le programme `AES.java` ou `aes.c` produit acceptera 0, 1, 2 ou 3 paramètres lors de l'exécution.

— Si aucun paramètre n'est donné, le programme se contentera d'afficher le résultat du chiffrement du bloc nul (formé de 16 octets nuls) avec la clef nulle (formée de 16 octets nuls).

```
$ java AES
Résultat: 0x66E94BD4EF8A2C3B884CFA59CA342B2E
```

— Le premier paramètre, s'il est donné, devra obligatoirement être `-e` ou `-d`. Lorsqu'un seul paramètre est donné, le programme devra afficher le résultat du chiffrement du bloc nul avec la clef nulle si le paramètre `-e` est donné et le *déchiffrement* du bloc nul avec la clef nulle dans le cas contraire.

```
$ java AES -e
Résultat: 0x66E94BD4EF8A2C3B884CFA59CA342B2E
$ java AES -d
Résultat: 0x140F0F1011B5223D79587717FFD9EC3A
```

— Le second paramètre, s'il est donné, sera le nom d'un fichier existant. Le programme devra alors produire dans un nouveau fichier le résultat du chiffrement (cas `-e`) ou du déchiffrement (cas `-d`) du fichier donné. Pour cela, le mode opératoire CBC sera employé et le vecteur d'initialisation choisi sera placé au début du fichier produit. La clef utilisée sera encore dans ce cas celle formée de 16 octets nuls.

```
$ java AES -e butokuden.jpg
Chiffrement de butokuden.jpg en aes-butokuden.jpg
$ java AES -d aes-butokuden.jpg
Déchiffrement de aes-butokuden.jpg en aes-aes-butokuden.jpg
```

— Si un troisième paramètre est donné, il sera considéré comme un mot de passe : le programme fonctionnera comme indiqué précédemment, excepté le choix de la clef. Celle-ci sera dans ce cas le résumé MD5 du mot de passe.

```
$ echo -n "Alain" | md5
163f0dda0338e504f0a2ffc8abac45a2
$ java AES -e butokuden.jpg Alain
La clef utilisée est: 0x163F0DDA0338E504F0A2FFC8ABAC45A2
Chiffrement de butokuden.jpg en aes-butokuden.jpg
$ java AES -d aes-butokuden.jpg Alain
La clef utilisée est: 0x163F0DDA0338E504F0A2FFC8ABAC45A2
Déchiffrement de aes-butokuden.jpg en aes-aes-butokuden.jpg
```

Le code fourni devra être correctement indenté, utiliser des noms de variables explicites, et être organisé de manière modulaire (c'est-à-dire divisé en fonctions ou en fichiers séparés, en évitant les répétitions de code).

Le rapport au format PDF (3 points)

Votre rapport comportera une à deux pages et devra être compréhensible pour le correcteur indépendamment du code fourni par ailleurs. Il sera rédigé en français et décomposé en 3 points selon l'ordre ci-dessous :

Auto-évaluation Indiquez par une *note globale* entre 0 et 10 votre degré de réussite aux exercices B.3, C.1, C.2, et F.2 des travaux pratiques. Expliquez cette note.

Pédagogie Indiquez quel a été pour vous, parmi ces 4 exercices, celui qui a été le plus intéressant d'un point de vue pédagogique, c'est-à-dire pour votre compréhension du système AES ou simplement en matière de programmation. Justifiez ce choix.

Votre avis Le moyen employé ici pour produire une clef AES de 16 octets à partir du mot de passe vous semble-t-il adéquat ? Justifiez votre réponse.