Votre AES [1]

Pour réaliser le TP vous avez besoin d'un AES en C, dont voici le fichier `aes.h` .

```
#ifndef AES_H
#define AES_H
#define DATA_SIZE 16
#define STATE_ROW_SIZE 4
#define STATE_COL_SIZE 4
#define ROUND_COUNT 10
#include <stdint.h>
// the round that will trigger
extern uint8_t targeted_round;
void AESEncrypt(uint8_t ciphertext[DATA_SIZE], uint8_t plaintext[DATA_SIZE] , uint8_t key[
    DATA_SIZE]);
void AddRoundKey( uint8_t state [STATE_ROW_SIZE][STATE_COL_SIZE], uint8_t roundkey [
    STATE_ROW_SIZE][STATE_COL_SIZE]);
void SubBytes(uint8_t state[STATE_ROW_SIZE][STATE_COL_SIZE]);
void ShiftRows(uint8_t state[STATE_ROW_SIZE][STATE_COL_SIZE]);
void MixColumns(uint8_t state [STATE_ROW_SIZE][STATE_COL_SIZE]);
void KeyGen(uint8_t roundkeys [][STATE_ROW_SIZE][STATE_COL_SIZE], uint8_t master_key [
    STATE_ROW_SIZE][STATE_COL_SIZE]);
//fill the first column of a given round key
void ColumnFill(uint8_t roundkeys[][STATE_ROW_SIZE][STATE_COL_SIZE] , int round);
//fill the other 3 columns of a given round key
void OtherColumnsFill(uint8_t roundkeys [][STATE_ROW_SIZE][STATE_COL_SIZE], int round);
void GetRoundKey(uint8_t roundkey [STATE_ROW_SIZE][STATE_COL_SIZE], uint8_t roundkeys [][
    STATE_ROW_SIZE][STATE_COL_SIZE], int round);
void MessageToState(uint8_t state [STATE_ROW_SIZE][STATE_COL_SIZE], uint8_t message [
    DATA_SIZE]);
void StateToMessage(uint8_t message [DATA_SIZE],uint8_t state [STATE_ROW_SIZE][
    STATE_COL_SIZE]);
void MCMatrixColumnProduct(uint8_t colonne [STATE_COL_SIZE]);
uint8_t gmul(uint8_t a, uint8_t b);
extern const uint8_t rcon [10];
extern const uint8_t sboxtab [256];
extern const uint8_t invsbox [256];
#endif
```

Références

[1] NIST. Specification for the Advanced Encryption Standard. *FIPS PUB 197*, 197, 2001.