CSE451 Computer & Network Security

Assignment 2: Advanced Encryption Standard (AES)

It is required to implement the AES algorithm in C.

AES supplementary material:

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Required build command:

```
gcc  -O3  studentID.c  -o  studentID
```

The submission is one C source file. No need to use any external libraries or headers.

Required program usage:

```
studentID.EXE  "e"  key  plaintext  ciphertext
studentID.EXE  "d"  key  ciphertext  plaintext
```

The command arguments (key, plaintext, and ciphertext) are all filenames. Use fopen(), fread(), fwrite(), and fclose() to access the data.

Use ECB block cipher mode: Divide the plaintext and ciphertext file into blocks and encode each block separately with the same key.

Declare the main function like this:

```c
int main(int argc, char **argv)
{
        return 0;
}
```

Then add your code.

Program speed is measured with the encryption and decryption of a message size 1 MB. Copied sources get zero grade.