README

Resources used:

https://anh.cs.luc.edu/331/code/aes.py

https://www.youtube.com/watch?v=K2Xfm0-owS4

https://www.youtube.com/watch?v=7uRK9iOk4uk

https://www.youtube.com/watch?v=dRYHSf5A4lw

https://www.youtube.com/watch?v=bERjYzLqAfw&t=359s

https://www.youtube.com/watch?v=4pmR49izUL0

https://github.com/boppreh/aes/blob/master/aes.py

How to run the code:

The code is written in python so the command "***python3 keySize keyFile inputFile outputFile mode***" will run it

The difference is that the keyFile should include a key of the form 1,2,3,…,16 for keySize 128 and 1,2,3,…,32 for keySize 256 (key represented as a comma separated list) instead of the one given in the task

Algorithm itself:

AES Encryption is a symmetric key encryption algorithm which means that the same key is used to scramble the data and unscramble it.

AES is a block cipher which encrypts 128 bits (16 bytes) of data at a time. It treats the 16 bytes as a grid of 4x4. Messages which are longer than 128 bits are broken into blocks of 128 bits. Each block is encrypted separately using exactly the same steps. If the message is not divisible by the block length, then padding is appended.

Stages of the algorithm:

1. Key Expansion
2. Initial Round:
   a) AddRoundKey
3. Rounds:
   a) SubBytes
   b) ShiftRows
   c) MixColumns
   d) AddRoundKey

   Repeat

4. Final Round:
   a) SubBytes
   b) ShiftRows
   c) AddRoundKey

Note: Step by step explanation in the code