AES

Advance Encryption Standard (AES) is a symmetric key algorithm used for encrypted data transmission. As any symmetric key algorithm, it relies on both the sending node and receiving node both have the same, secret key to encrypt and decrypt. It is a block cipher algorithm, meaning the data is encrypted and decrypted in a set size of data. Here’s a good explanation of the history and operation of the algorithm presented in an easy and interesting format:

[Stick Figure Guide to AES](http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html)

**Lab Exercise**

In this

While the solution is included, please work through the unfinished code before looking at the solution. As always, there is more than one way to implement this in code and you may find a more efficient implementation.

**NOTE**: In general, it is typically a poor security decision to implement cryptographic algorithms that are not widely reviewed and evaluated. The libraries used in this lab have little verification and are not endorsed by reputable cryptographic organizations. This is for demonstration and learning purposes only.