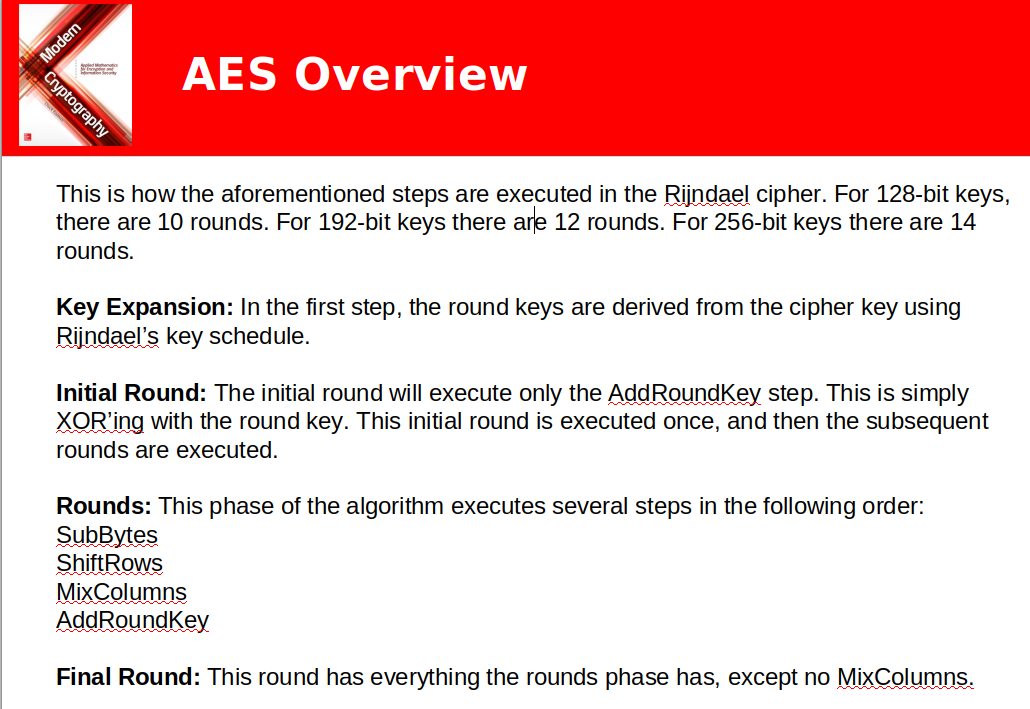
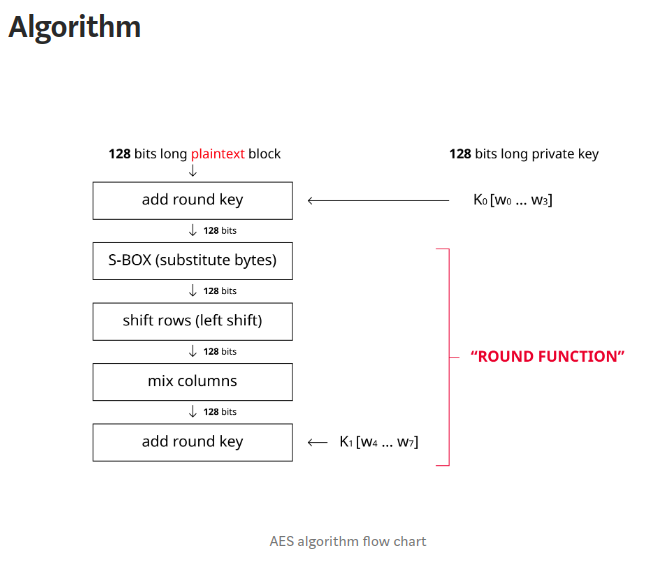
James Chad Ballay

**The Specification**

The Rijndael Block Cipher specification was selected in 2000 and became a US federal standard in 2002. (Rouse, Cobb) In their proposal, Joan Daemen and Vincent Rijmen laid out the steps for their block cipher. The key length will dictate the number of loops(rounds) we can cycle through. (128 bit key yields 10 rounds, while a 256 bit key yields 14 rounds.) For the sake of simplicity we’ll assume a 128 bit key for the example.



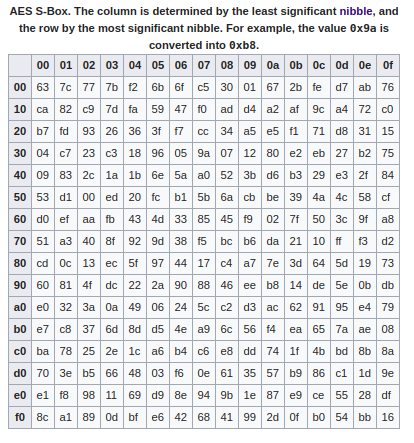
(Figure 1. Easttom)



(Figure 2 zeroFruit)

**S-Box**

A byte is comprised of two nibbles. The first half of the byte, or leading 4 bits, and the last half of the byte, or trailing 4 bits. So a byte that is 11001010 would be broken down into 1100 and 1010 nibbles. These are transformed in the S-box stage using a fairly complex formula. Thankfully it can be computed out for us and instead we can use this lookup table.



(Figure 3 – Rijndael S-box)

**Shift Rows**

For this step conceptualize that the 128 bytes are arranged in a 4 x 4 grid. Starting from the top left, proceeding sequentially to the right and downwards.

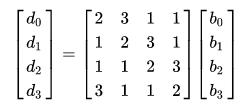
|  |  |  |  |
| --- | --- | --- | --- |
| a | b | c | d |
| e | f | g | h |
| i | j | k | l |
| m | n | o | p |

The row shifting step shifts each row to the left by the number from the top row down that it is. The cells wrap around.

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | c | d |
| f | g | h | e |
| k | l | i | j |
| p | m | n | o |

**Mix Columns**

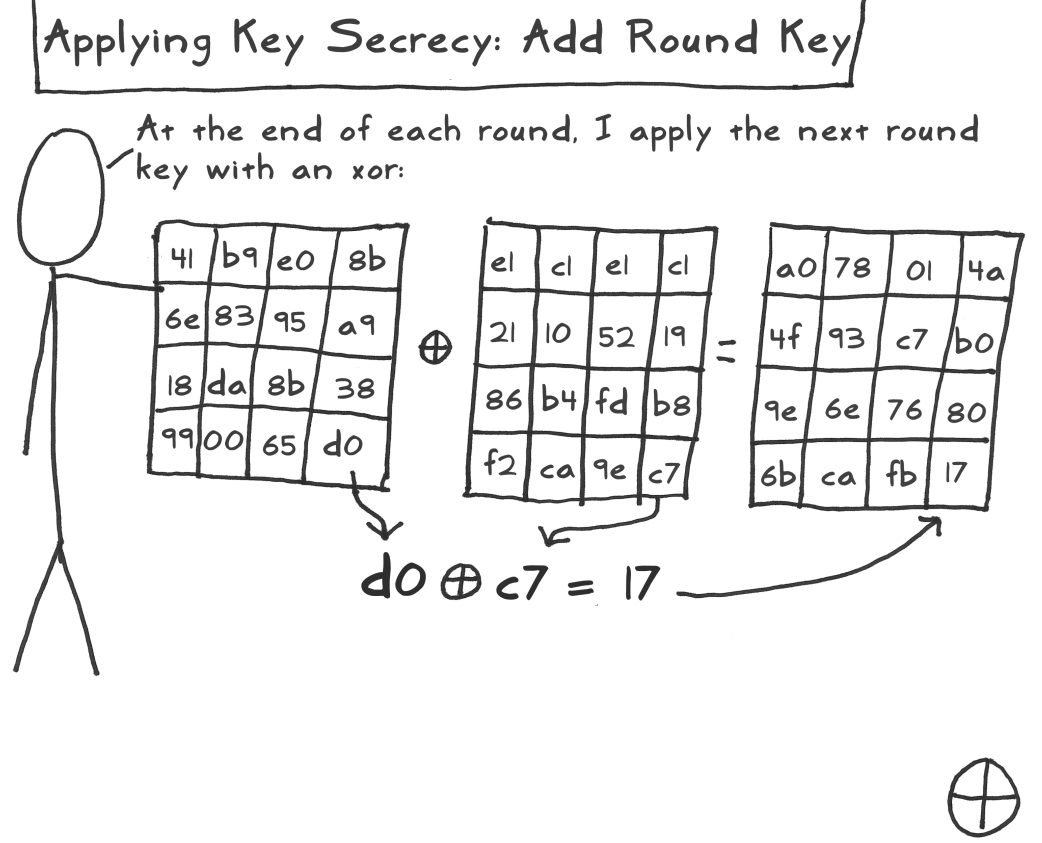
For this step take each column in turn and matrix multiply it against a fixed matrix. You’ll repeat this for each column.



(Figure 4 - Rijndael MixColumns)

**Add round Key**

For a 128 bit key we can do 10 rounds. Each of those rounds has a key generated during the initialization step of this cipher. At this point we take the next rounds key and XOR it against the data we have on hand.



(Figure 5 – Jeff Moser Stick Figure AES)

**Sources**

Rouse, M., & Cobb, M. (n.d.). What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com. Retrieved from <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>.

Easttom, C. (2016). *Modern cryptography applied mathematics for encryption and information security (pp 145)*. New York: McGraw-Hill Education.

zeroFruit. (2019, February 13). What is AES? - Step by Step. Retrieved from <https://medium.com/@14wnrkim/what-is-aes-step-by-step-fcb2ba41bb20>.

Rijndael S-box. (2019, November 15). Retrieved from https://en.wikipedia.org/wiki/Rijndael\_S-box#Forward\_S-box.

Rijndael MixColumns. (2019, April 17). Retrieved from <https://en.wikipedia.org/wiki/Rijndael_MixColumns#Matrix_representation>.

Moser, J. (n.d.). Retrieved from http://www.moserware.com/assets/stick-figure-guide-to-advanced/aes\_act\_3\_scene\_14\_add\_round\_key\_1100.png