

AES Cipher/Inverse Cipher Block Diagram

Alex Pearson ECE 571 Final Project
Daniel Collins SP2016
Scott Lawson

Derived from the AES Standard, Nov 26 2001, issued by NIST
Available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Key:

- Nb Number of 32-bit words comprising the State, input, and output widths
 This value always 4 according to the current version of the standard, so these vectors are
 always 128 bits wide
- Nk Number of 32-bit words comprising the Cipher Key
 Allowed values are 4, 6, or 8 (128-, 196-, and 256-bit wide keys, respectively)
- Nr Number of rounds
 Is 10 when $N_k=4$, 12 when $N_k=6$, and 14 when $N_k=8$



