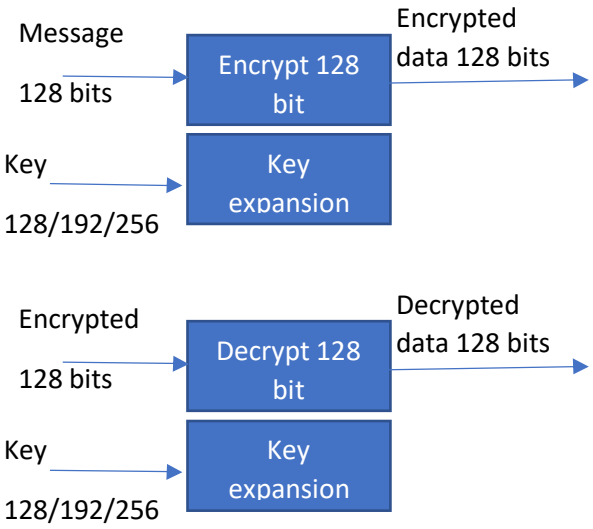
AES 128/192/256 Encryption Decryption



Galois Field arithmetic is done with primitive polynomial of degree 8
AES Encryptor/Decryptor has:

Encryptor:

The Encryptor is programmable to do different number of steps per clock, it can do 1,2,3,4,5 steps and can finish encryption in as little as 1 clock.

The Key expansion does twice as many steps per clock cycle as the encryptor and works in conjunction with it.

Decryptor:

The Decryptor is programmable to do different number of steps per clock, it can do 1,2,3,4,5 steps and can finish encryption in as little as 1 clock.

The Key expansion does same number of steps per clock cycle as the Decryptor and works in conjunction with it.

Contact: manish@secantecinc.com Phone: (409) 233-3312
http://www.secantecinc.com
AES page: http://secantecinc.com/aes_encrypt_decrypt/