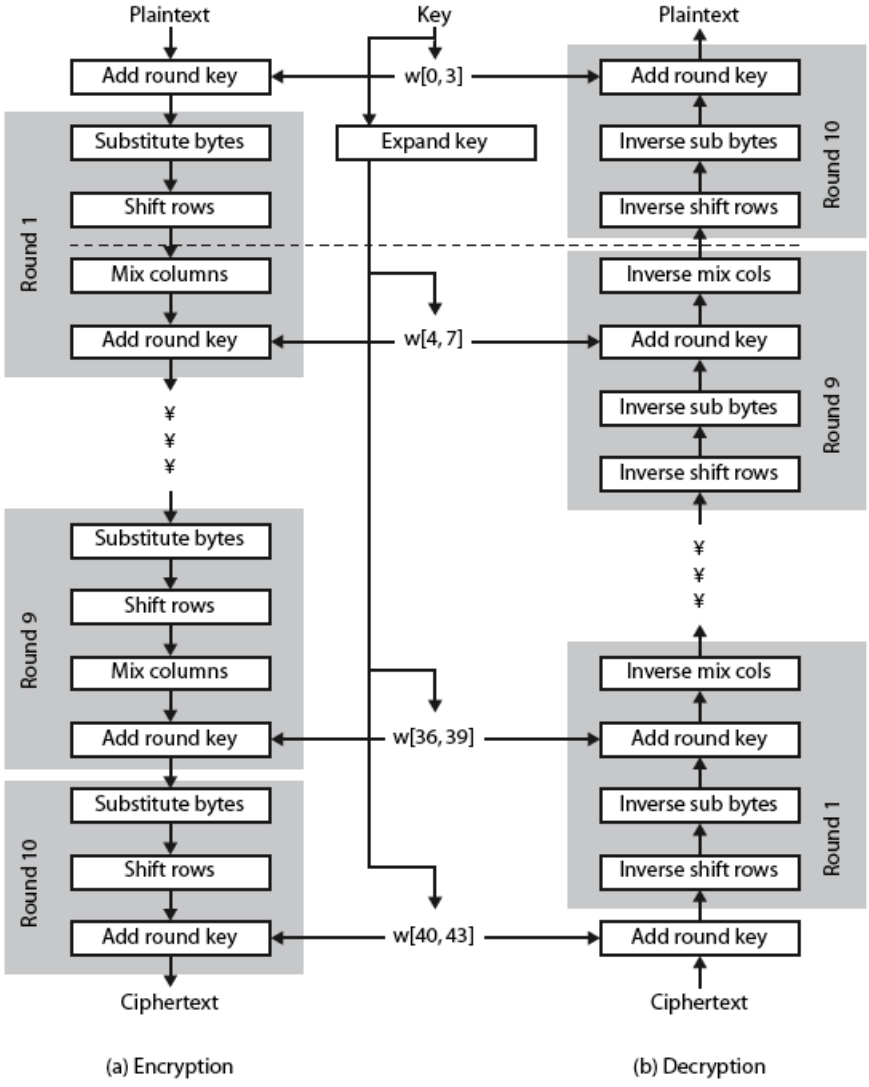
# AES-128 Encryption

Building blocks:

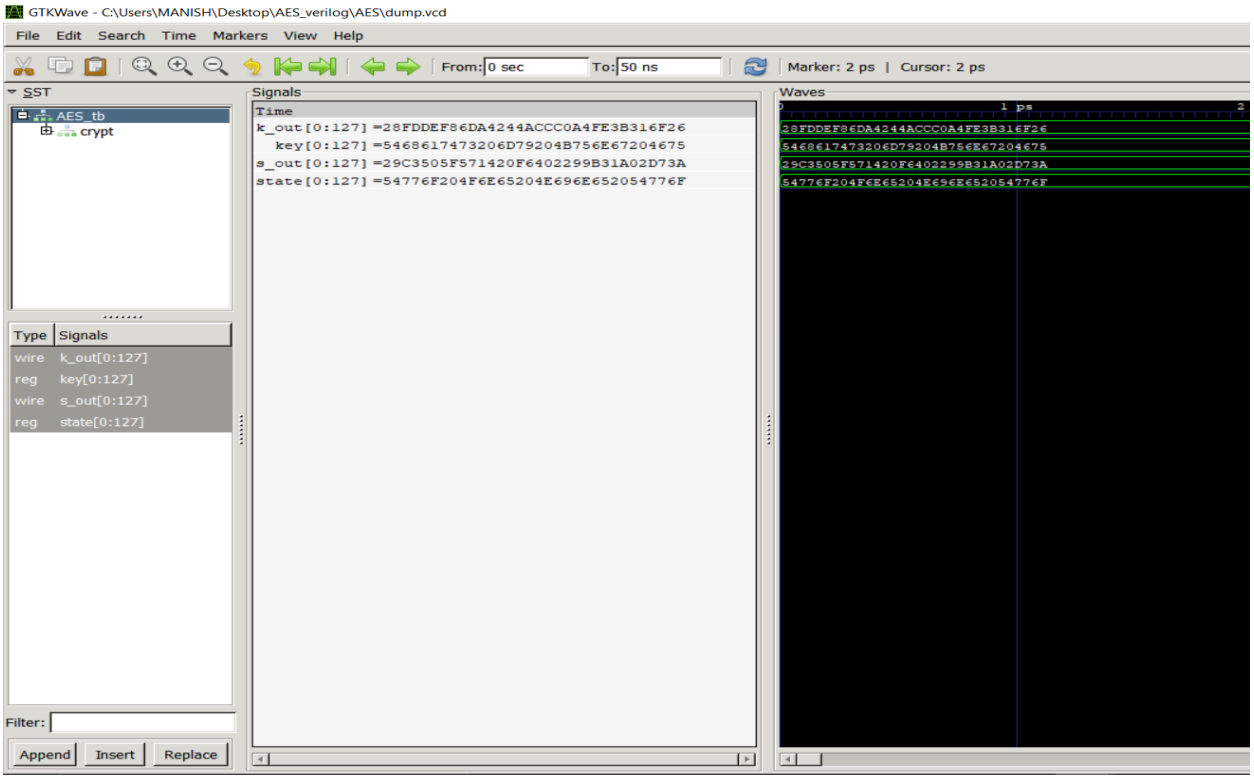
- Sub Bytes(Sbox)
- Shift Rows
- Mix Columns
- Add Round Key
- Round
- Round_last
- AES

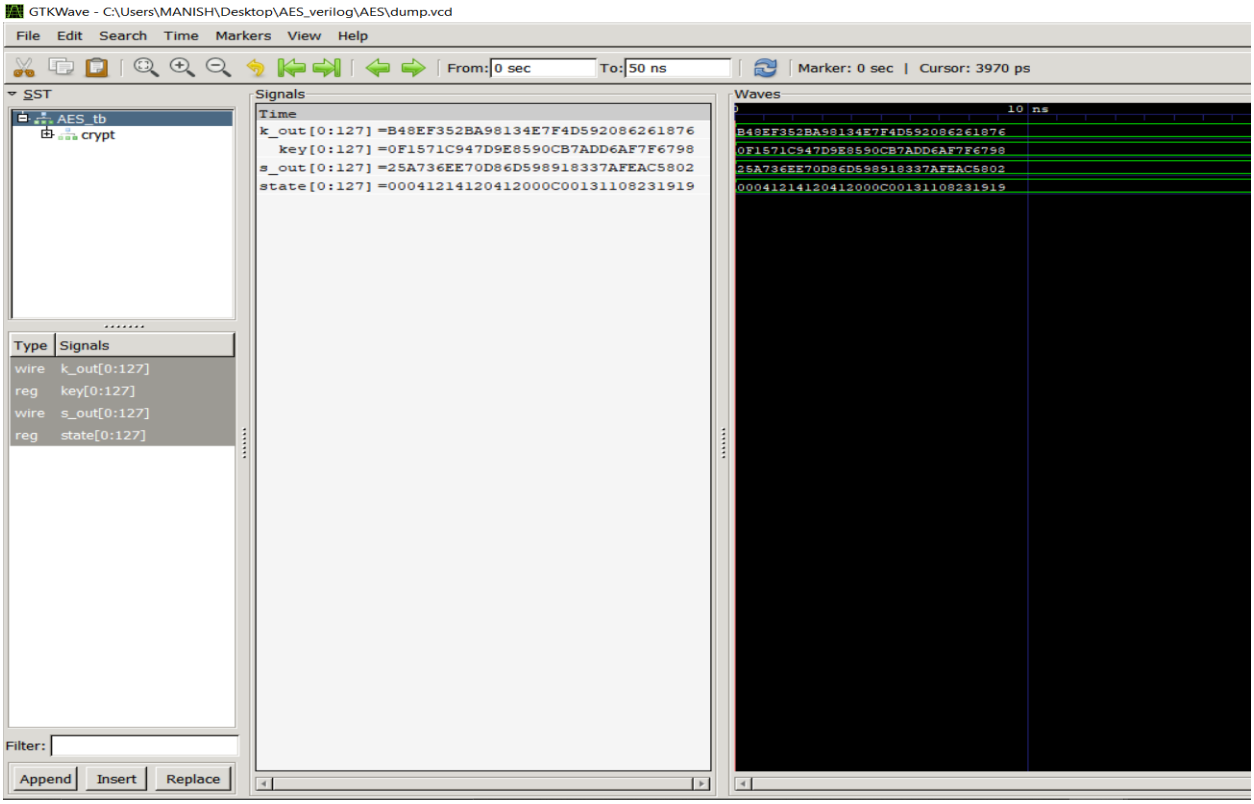
-




The algorithm was checked by using values from the 3rd reference.

Also for decryption part only few constant matrices need to be modified for which the details are mentioned in the 2nd reference.




2 values of plain text and key for which it was verified.

References:


1. https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf

2. https://www.researchgate.net/profile/Ako_Abdullah/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf

3. https://kavaliro.com/wp-content/uploads/2014/03/AES.pdf