Checklist

Baseline

- One round of AES-128 algorithm working in testbench, for both encryption and decryption.
- Receive messages from a laptop over USB UART
- Transmit messages to a laptop over Ethernet

Expected

- Encrypt and decrypt 32x32 color images in AES-128 ECB mode
- Send ciphertexts from one FPGA to another over an Ethernet cable
- Display decrypted images on a VGA monitor

Stretch

- Encrypt and decrypt plaintexts in AES-128 CBC mode
- Securely negotiate encryption keys using a Diffie-Hellman algorithm or similar
- Transmit 800x600 color images and display them from a buffer in DDR2 RAM
- Make the system resilient to dropped or out-of-order packets, which would be important in AES CBC-mode encryption