Programming Assignment AES

In this assignment, you must decrypt a challenge ciphertext generated using AES in CBC-mode with PKCS #5 padding. (Note: technically this is PKCS #7 padding, since the block size of AES is 16 bytes. But the padding is done in exactly the same way as PKCS #5 padding.) To do so, you will be given access to a server that will decrypt any ciphertexts you send it (using the same key that was used to generate the challenge ciphertext)...but that will only tell you whether or not decryption results in an error!

All the files needed for this assignment are available here, including a README file that should explain everything.

Note that this assignment requires the ability to perform basic networking. Because we do not assume students necessarily know this, we have provided stub code for doing basic networking in C, Java, Ruby, and Python, but you are welcome to use any language of your choice as long as you are able to write code for basic networking functionality in that language. (Students may feel free to post stub code in other languages for the networking component on the discussion boards.)

The first step in this project is to send the challenge ciphertext to the server, and verify that you receive back a "no error" message. Once you can do that, the rest is "just" crypto...

The plaintext, when converted to ASCII, is readable English text, and so you should be able to tell once you have been successful. Once you have successfully recovered the plaintext (in ASCII).