Supplement for Problem Set #5

This point of these exercises is to give you some experience using RSA to exchange the key that is used in AES. Problem 1 is intended to simulate receiving a message encrypted with your public RSA credentials, and Problem 2 is intended to simulate sending a message using my public RSA credentials.

- ⊙ You will want to download the *Mathematica* notebook Supplement_PS5.nb that you can find on the Problem Sets page of the course website.

- ⊙ You should use the site

  `http://www.cryptogrium.com/aes-encryption-online-ecb.html`

  to perform the AES-ECB 128-bit encryption and decryption.

- ⊙ You do not need to turn in any work on paper for these exercises. There is a form at onCourse where you can fill out your answers, and *you must upload the Mathematica notebook that you used to work on your solutions!* You should spend a little time cleaning up your notebook so that it's easy for me to follow.

  Only one person from each group needs to submit to onCourse.

---

1. For the RSA parts of this problem, use the values of p and q given in the *Mathematica* notebook to form $n = pq$. Use a value of $e = 2^{16} + 1$.

   (a) The following ciphertext, in hexadecimal, contains the 128-bit AES key that you will need for part (b) of this problem. This ciphertext was encrypted using RSA with $k_{pub} = (n, e)$.

   ```
   4cdbda541e31c9d4ce57074cc7f50e79770fde21be7e7255f66aed2a7771
   a818b1f23f392fb988bec1be3fe8ee6d87235bc0a7158c7ee8b89b0cd5bf
   0f5d84a9eab4e73f566483743e7c14991c4e85265df55cf4e380c32dc78a
   9c0ce8222991367d4f68c6c2d768fbae6cd8e783080d15a055f88683ba2f
   16bf4c8806a8e43633bb50a31035a6f797e6dbc43ba2e6d3d38d0c784243
   e6efbcfcb43a586f030d5d78a6fd7580934c2387885857e06916987f5423
   57a3c573714b6d1565ecd20a883c70782b392aacf92f9ec7dd4afa40f6fc
   aea8ada1847718bdfa0f550d26406f879801413efb32d8e52328e0d9da23
   c4c316159ffccffc51a28fcdc707c010
   ```

   What is the key? Notice that you will need to determine $k_{pr} = d$ in order to decrypt, but you can calculate this since you know the values of p and q.

   (b) The following message was encrypted using the AES-ECB 128-bit key you found in part (a). The message was generated by converting each character in the plaintext to its ASCII value in hexadecimal and then encrypting with AES. Decrypt the message, and tell me something interesting about the person referenced in the message.

   Note that you will need to break this into 128-bit blocks to decode.

   ```
   f1ac6e1354d93f8c5166a7ca674f26f9a1b32ab03ae58ccc743adcf7e0402b06
   ```

2. For the RSA parts of this problem, use the values of n and e given in the *Mathematica* notebook as $k_{pub}(n, e)$. Note that these are the same values used in Problem 1 so that you can double-check your encryption. In practice, you would not actually know my private key k_{pr}.

   (a) Pick a different 128-bit AES key from was used in the first problem, and encrypt it using RSA with $k_{pub} = (n, e)$.

   (b) Pick an interesting quote or message. Use the *Mathematica* notebook and the AES emulator with the key you shared in part (a) to encrypt the message and enter it in onCourse.