Supplemental Problem for Problem Set #5

Due Friday, October 21, 2016

This point of these exercises is to give you some experience using RSA to exchange the key that is used in AES.

- ⊙ You will want to download the *Mathematica* notebook Supplemental_PS5.nb that you can find on the Problem Sets page of the course website. This is an updated version of the notebook from the last problem set.

- ⊙ You should use the site `http://people.eku.edu/styere/Encrypt/JS-AES.html` for performing the AES 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 to follow.

S-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 $k_{pub} = (n, e)$.

```
16bdfeabd1e02c54b88bf510ed7458f7092b1988ba09eb61de4c6765f7
a97fc97b352e033cfc802011c7fc0230f12e71c378c10836d2ab6156ab
dc082bdfe0a0844ec97b88504c863d6a4db0f3cdbd7f212521d12cda78
e3b49e7cd58c604792a893ca70220d10b9fa4cb139aab7307bb5c7b015
739c35aafb7da28154c4e4deebdfdca9d5fb1156d7fb7cb3cc80d529ab
380012204a1f9bd3d1a3a9c01e654376ae3cb95aa2cf40c4220c44b464
a490afb72fbd553d9d706073bbb72e5312b59943a0042422c9507e265b
6470426358a9def7826cbf3e2d91cda158d24dcfbca67aa5f85edade91
476c40ab308d7795ef0fa0b8ce7bc5ca8ec9844ee66a3052
```
$_{16}$

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) Decrypt the following message, and tell me something interesting about the quote. The message was generated by converting each character in the plaintext to its ASCII value in hexadecimal and then encrypting with AES:

```
a1 c9 d2 45 f3 ff 00 49 c3 3d c4 44 8a 46 ac 44 9f ba 5f 53
9e ed f8 3b 8e e6 73 95 4b 47 00 90 b9 e4 67 41 68 0e 8a 6f
7c 6b 72 a9 6d 38 bc 3b 58 bc 37 80 45 85 20 f0 18 d7 29 ff
c3 97 27 e9 79 0c 13 45 69 39 cb 07 c4 60 c3 a2 6c 27 3a a2
```

S-2. For RSA parts of this problem, use the values of n and e given in the *Mathematica* notebook as $k_{pub}(n, e)$.

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

(b) Share with me another interesting quote, different from the one you used last week. Use the *Mathematica* notebook and the AES emulator with the key you shared in part (a) to encrypt the quotation and enter it in onCourse.