Supplemental Problem for Problem Set #4

Due Friday, October 14, 2016

This point of these exercises is to give you some experience using AES.

- ⊙ You'll definitely want to download the *Mathematica* notebook Supplemental_PS4.nb that you can find on the Problem Sets page of the course website.

  This notebook contains one function for converting a 16 character string to a 32-digit hex number corresponding to the ASCII values of the characters in the string and another function for performing the opposite conversion.

- ⊙ You should use the site `http://people.eku.edu/styere/Encrypt/JS-AES.html` for performing the AES encryption and decryption. Use the key

  f6 cc 34 cd c5 55 c5 41 82 54 26 02 03 ad 3e cd

  for all 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. Decrypt the following message. It was generated by converting each character in the plaintext to its ASCII value in hexadecimal and then encrypting with AES:

```
1f 4a 0a 5f 40 3f 79 12 77 9e 60 b6 ee 9f d2 37 8e 19 64 ec
d7 a7 b5 cc ee eb 7c 73 26 ed d2 b8 08 ee 58 e9 71 5b 5c 5f
12 aa 18 5e 1c 4d f8 97 55 80 85 83 e1 2d 5f da 72 f1 5b de
a3 26 13 43 ec b6 3e eb 18 66 51 62 c8 c0 af b3 ef 2b 91 af
53 24 ae 5a f1 34 09 3b fe 6c 7b 0b 65 61 55 1c
```

Notice that you'll need to break this up into appropriate sized chunks in order to decrypt using the AES emulator. You will then need to use the *Mathematica* notebook to convert your result from the ASCII values in hexadecimal into a string.

Tell me something interesting about the person who said this.

S-2. Share with me one of your favorite quotes.

Use the *Mathematica* notebook and AES emulator to encrypt the quotation and enter it in onCourse.