Homework 8
DUE DATE: Tuesday May 4th 2010 @ 11:59 pm

The objective of this assignment is to help you get comfortable with some very basic security operations. The assignment has been deliberately made very simple because we are at the end of the semester and there is the big term-paper deliverable that is also due. This assignment should be done in JAVA since it would make this really easy.

As part of this assignment, you are required to
(1) Generate a secret symmetric key that you will use for encryptions/decryptions. This key will be specified as an argument using a HEX String.
(2) Encrypt the specified plain-text. You will also output the encrypted text as a HEX string.
(3) Decrypt the cipher-text specified as a hex string. The retrieved plain-text should be output as regular String.
(4) Compute the message-digest of a specified text

You will use 128-bit AES as your symmetric algorithm.
For computing the message digest you will use SHA-1.

This what the commands would look like:
**We will be using [] to encapsulate our strings.** The string that will be the input to your commands will exclude the square brackets. You can use java.util.StringTokenizer to parse the input commands.

```
java SecurityAssignment
generateKey
   output key-in-hex

   encrypt [The plaintext string for encryption] [key-in-hex] 
   output ciphertext in hex

   decrypt [ciphertext-in-hex] [key-in-hex] 
   output plaintext

   digest [The test string for checksumming] 
   output-in-hex
```
Example Commands:
java SecurityAssignment

generateKey
6628d4816939295a900f9c6c07e0cda5

encrypt [The quick brown fox jumps upon the lazy dog. 123]
6628d4816939295a900f9c6c07e0cda5

Ciphertext:
6a8edcde97c04ccc73efba437d563d3601ed1e69b4b81ab0278912e2bd2050f4
3395375ff67525ece9553be44285d1b4

decrypt
[6a8edcde97c04ccc73efba437d563d3601ed1e69b4b81ab0278912e2bd2050f4
3395375ff67525ece9553be44285d1b4]
[6628d4816939295a900f9c6c07e0cda5]

Plaintext: The quick brown fox jumps upon the lazy dog. 123

digest [The quick brown fox jumps upon the lazy dog. 123]
SHA-1 digest: e48c249131c5e1df1b5e966e6ca7e822d45f92fa

Grading
The assignment will be worth 5 points towards your course grade. The assignment in itself
will be graded on 10 points. The points distribution is as follows.
2 points for each command for a total of 8 points
2 points for error checking

You are required to work alone in this assignment. Check the course website on late policy.

What to submit
All of your source files and a Makefile in a tarball or a zip. Follow usual naming conventions.