Homework 3

Due Date: May 13, 2011 **Points:** 100

Corrections

- In Problem 3, I changed d to be the private key and e to be the public key to conform with the textbook's notation. (It won't affect your answer, of course.)
- In the Extra Credit problem, "problem 5" should be "problem 4".

These are corrected below.

Questions

1. (*15 points*) In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution?
   (*text*, §6.8, exercise 8).

2. (*30 points*) The following message was enciphered with a Vigenère cipher. Find the key and decipher it. Show your work.

   ```
   TSMVM MPPCW CZUGX HPECP RFAUE IOBQW PPIMS FXIPC TSQPK SZNUL
   OPACR DDPKT SLVFW ELTKR GHIZS FNIDF ARMUE NOSKR GDIPH WSGVL
   EDMCM SMWKP IYOJS TLVFA HPBJI RAQIW HLDGA IYOUX
   ```

   (*text*, §9.8, exercise 8).

3. (*25 points*) Consider the RSA cipher with $p = 5$ and $q = 7$. Show that $d = e$ for all choices of public key e and private key d.

4. (*30 points*) The section on public key cryptosystems discussed nonrepudiation of origin in the context of public key cryptosystems. Consider a secret key system (in which a shared key is used). Bob has a message that he claims came from Alice, and to prove it he shows both the cleartext message and the ciphertext message. The ciphertext corresponds to the plaintext enciphered under the secret key that Alice and Bob share. Explain why this does *not* satisfy the requirements of nonrepudiation of origin. How might you modify a classical cryptosystem to provide nonrepudiation?
   (*text*, §9.8, exercise 17).

Extra Credit

1. (*20 points*) Assume that a cryptographic checksum function computes hashes of 128 bits. Prove that the probability of finding two messages with the same hash (that is, with the value of neither message being constrained) is 2^{-64}.
   (*text*, §9.8, exercise 21).