Homework 3

Due: May 20, 2015 **Points:** 100

Questions

Remember to justify your answers.

1. (*40 points*) The following message was enciphered with a Vigenère cipher. Find the key and decipher it.

```
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
```

2. (*30 points*) Prove that two users who perform a Diffie-Hellman key exchange will have the same shared key.

3. (*30 points*) Reconsider the case of Alice and her stockbroker, Bob, in the example in section 10.1. Suppose they decide not to use a session key. Instead, Alice pads the message (BUY or SELL) with random data. Explain under what conditions this approach would be effective. Discuss how the length of the block affects your answer.

Extra Credit

4. (*20 points*) Alice and Bob are creating RSA public keys. They select different moduli n_{Alice} and n_{Bob}. Unknown to both, n_{Alice} and n_{Bob} have a common factor.
   (a) How could Eve determine that n_{Alice} and n_{Bob} have a common factor without factoring those moduli?
   (b) Having determined that factor, show how Eve can now obtain the private keys of both Alice and Bob.