Homework 3

Due: May 9, 2018 at 11:59pm **Extended; due date is now May 11** **Points:** 100

Questions

Remember to justify your answers.

1. (*20 points*) A physician who is addicted to a pain-killing medicine can prescribe the medication for herself. Please show how RBAC in general, and Definition 8-14 specifically, can be used to govern the dispensing of prescription drugs to prevent a physician from prescribing medicine for herself.

2. (*20 points*) The following message was enciphered with a Vigenére 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
```

3. (*20 points*) Consider the RSA cipher with $p = 5$ and $q = 7$. Show that $d = e$ for all choices of public key $(e, 35)$ and private key d.

4. (*20 points*) Consider the public keys (e_1, n_1) and (e_2, n_2) of two RSA cryptosystems.

   (a) You have discovered that n_1 and n_2 have a common factor but do not know what it is. How would you find it?

   (b) You have intercepted a message c enciphered using the first public key. You also know the common factor of n_1 and n_2. Show how to decrypt c.

5. (*20 points*) Consider the Otway-Rees protocol. Assume that each enciphered message is simply the bits corresponding to the components of the message concatenated together. So, for example, in the first message, one must know the names "Alice" and "Bob", and the length of the random numbers r_1 and n, to be able to parse the portion of the first message that is enciphered with k_{Alice}. The separate parts of the enciphered message have no indicators; the recipient is expected to determine them.

   (a) Consider Alice when all 4 steps of the protocol have been completed. How does Alice know that steps 2 and 3 have taken place?

   (b) Massicotte asks us to assume that an adversary Edgar is impersonating Bob, and has sufficient control over the exchange so that he receives the messages intended for Bob. Bob never sees them. What components of the protocol does Edgar know — that is, does he know r_1, r_2, n, or $k_{session}$, or the names of "Alice" and "Bob"? How?

   (c) Given this, in step 4 of the protocol, how might Edgar provide Alice with a session key that he knows?

   (d) How might someone fix this?