Homework 3

Due Date: Friday, November 1, 2013 at 5:00pm **Points:** 100

1. (*30 points*) A bank has thousands of ATMs that it must control. It does so by building into each ATM a small server that accepts commands from the bank's master computer. The ATM software consists of a general purpose operating system (such as Windows or Linux) with some specific software designed to allow the bank to check the amount of money in the ATM, download a record of transactions conducted on the ATM, and perform specific supervisor functions such as shut down or disable the ATM.

   (a) The Principle of Least Privilege says that a system should not run unnecessary software. Do you believe the bank's ATM system obeys this principle? Why or why not?

   (b) Why do you think the bank did not write its own operating system?

2. (*20 points*) Please decipher the following Cæsar cipher: `TEBKFKQEBZLROPBLCERJXKBSBKQP`.

3. (*20 points*) Let k be the number corresponding to the encipherment key for a Caesar cipher. For example, in English, "A" is 0, "B" is 1, and so forth. The decipherment key is not the same as the encipherment key, though; it is $(26-k) \bmod 26$. Continuing the example, the decipherment key corresponding to the encipherment key "B", or 1, is $(26-1) \bmod 26 = 25$, or "Z". One of the characteristics of a public key system is that the encipherment and decipherment keys are different. Why then is the Cæsar cipher a classical cryptosystem, not a public key cryptosystem? Be specific.

4. (*30 points*) This question asks about federated identity management.

   (a) What is "federated identity management"?

   (b) Does UC Davis use federated identity management?

   (c) Educause is an organization of academic institutions to which UC Davis belongs. Suppose another member of Educause wanted to allow students, staff, and staff of other Educause institutions to use their wireless networks when visiting. For example, when a UC Davis user connects to the wireless network, the wireless network provider gets the user's name and UC Davis password, contacts UC Davis' central server, and requests the name and password be validated. The UC Davis central server does so, and if it confirms the credential is correct, the wireless network provider allows the user to connect. Please suggest simple ways for the user to indicate he or she is from UC Davis, bearing in mind that the members of Educause can change quickly (so a menu of members would confuse users, and make logging in quite difficult — so don't suggest that). Remember, whatever you suggest must be something very easy for the user to do!

Extra Credit

1. (*40 points*) The following ciphertext was created using a Vigenère cipher. Find the key and the plaintext.

```
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
```

   Be sure to show your work. ***Warning***: This problem is hard, but can become quite addicting!