Checkup 1

Your Name: _____ **UVa Computing ID:** _____

For this quiz, you should **work alone**. You may not use any resources other than your own brain, body, and a simple writing instrument.

For each question, write a correct, clear, insightful, and delightful answer in the space provided. The space provided is more than sufficient for a full-credit answer, but if you need to use additional space, make sure your answers are clearly marked.

1. What are the most essential properties something must have to be used as a currency?

2. What are the drawbacks of using a centralized bank to record transactions?

3. Where is asymmetric cryptography used in a bitcoin wallet?

4. Find x such that $2^x \mod 7 = 1$.

5. The problem in the previous question is an instance of the *discrete logarithm problem*. Why do cryptographers consider discrete logarithm to be a *hard* problem?

6. Alice owns coin X and has public/private key pair (KU_A, KR_A); Bob has public/private key pair (KU_B, KR_B) for the strong asymmetric cryptosystem E (the notation $E_K(m)$ denotes the encryption of input m with key K). What message should Alice send to the public ledger to transfer X to Bob?