CMSC 417 Computer Networks, Fall 2014, Section 2
Homework 3
Due date: Dec 19, 2014, Friday, 10:00am

1. Describe *base64* encoding briefly. Give an example. Where is it used? Consult MIME RFC to find out how base64 encoding handles binary data of a length not evenly divisible by three bytes.

2. For a structured p2p network (like Pastry), briefly describe the *method* used to decide which object is placed in which node.

3. Briefly describe the possible mechanism(s) that can be used to *redirect* HTTP requests to proper servers in a CDN.

4. Why do we use a *challenge-response protocol*?

5. Describe the algorithm for computing the *digital signature* for a message (or document). Why do we need to encrypt the message? Is it not enough to compute the digest (using a cryptographic-hash like MD5) and append it without performing encryption?

6. Draw the timeline of messages (and their contents) of *Public-Key Authentication Protocol* (not requiring synchronization of parties) that is also used to establish a shared secret session key. Why timestamps are used? Why a messages is encrypted using the private key of the sender?