1. What are the three components that make a contract?

2. A PKI Certifying Authority wants to publish revoked certificates on the web. Assume that you use serial numbers in order to make lookups fast. (With serial numbers, you can revoke old certificate in a batch by posting the smallest serial number that belongs to a valid certificate.)
   - How do you prevent an attacker from posting an old copy of the site on a fake website?
   - How do you deal with the case of a dishonest employee from reusing a serial number of a good certificate in a bad certificate? If you then revoke the bad certificate, the good one is also revoked.

3. A shopping cart implementation stores all the state information in a cookie. This state information contains such things as the total due. Give an example how you can alter the cookie if the implementation uses XOR-based encryption.

4. Explain an SQL injection attack.

5. Explain an XSS attack.