CS 167 — Fall 2006 — Goodrich — Midterm 2

Name:

ID:

1:

2:

3:

4:

5:

total:

1. (20 points). Short Answers.

(a) What is the running time for computing $\gcd(a, b)$ using Euclid's algorithm?

(b) What is a composite number?

(c) What is a public-key cryptosystem?

(d) How can a public key encryption scheme, like the RSA algorithm, be used to compute a digital signature on a message M?

2. (20 points). Explain how to compute $a^{-1} \bmod n$ when $\gcd(a, n) = 1$.

3. (20 points). Briefly sketch the main steps of the repeated squaring algorithm for computing $a^b \bmod n$.

4. (20 points). Explain how encryption and decryption is done in the RSA cyptosystem.

5. (20 points). Alice wants to send Bob a message M that is the price she is willing to pay for his used car (M is just an integer in binary). She uses the RSA algorithm to encrypt M into the ciphertext C using Bob's public key, so only he can decrypt it. But Eve has intercepted C and she also knows Bob's public key. Explain how Eve can alter the ciphertext C to change it into C' so that if she sends C' to Bob (with Eve pretending to be Alice), then, after Bob has decrypted C', he will get a plaintext message that is twice the value of M.