1. (10 points) Suppose you are given two integers $n_1$ and $n_2$ such that $n_1 \geq n_2 > 0$. How long does it take to find the greatest common divisor (GCD) of these two numbers using the Euclid algorithm? Express your result in the $\theta$ notation. Carry out the mathematical steps the best you can. Be as precise as you can.

2. (10 points) Write a very simple or naïve algorithm to find all primes equal to or smaller than a certain positive integer $n$. Write the algorithm using a pseudocode format. Now, clearly analyze the time requirement of the algorithm. Specify the final result in $\theta$ notation. Show each step.

3. (5 + 5 = 10 points) Consider the repeated squaring algorithm for computing $a^m \ mod \ n$. What is the time complexity of this algorithm in terms of the number of bits $\beta$ in the numbers $a$ and $n$. Compute the value of $3^{651} \ mod \ 13$ with this algorithm.

4. (10 points) Briefly explain how you can write your own packet sniffer. Be as specific as you can. Consider a Unix (Linux, Solaris or Mac OS X) or PC environment.

5. (5 + 5 = 10 points) Consider any two participants in SET. Let us call them Alice and Bob. How many keys are involved when the two parties want to communicate securely following the SET protocol and what are the keys called? Describe the encryption and decryption processes in detail using diagrams.

6. (10 points) What is a suffix tree? Draw the complete suffix tree for the string $acbabacabc$. What is the size of the alphabet $\Sigma$ used in this string? Assume the size of the alphabet used is given as $|\Sigma|$. What is the maximum size, in terms of number of nodes, the suffix tree can attain in the worst case? What is the worst case time required to find if a string of length $m$ is a suffix of the original string?

7. (10 points) Discuss clearly a mechanism whereby an FTP server and an FTP client can authenticate each other beyond any reasonable doubt. Draw diagrams to explain. Why is it so difficult to break the authentication mechanism you describe?

8. (6 + 3 + 6 + 6 + 9 = 30 points)

(a) What is the approximate number of prime numbers in the range from 1 to $n$? What is the approximate number of prime numbers between 1 and $10^{100}$?
(b) What is a *Carmichael number*? What does it signify in the context of finding prime numbers?

(c) What are the five or six main security services that an information security facility should provide?

(d) What is a certificate? What is a certificate authority? What do you mean by the phrase a *hierarchy of trust*?

(e) If we have *n* entities in a network and the entities want to communicate with each other securely using symmetric keys, how many symmetric keys do we need? If we use RSA-based public-key cryptography to exchange session keys, how many permanent keys do we need for the *n* parties to communicate securely? If we use Diffie-Hellman key exchange, how many pieces of information do we need for *n* parties to be able to communicate?