1 Tutorial 1

1. Give real life examples of information where you'd primarily protect it for a subset of "confidentiality," "integrity," and "availability". For example, data whose integrity you care about but not its confidentiality or availability etc. etc. Some bit of contrivance is ok!
2. Give examples of how your favorite operating system realizes (or fails to realize) one or more of Saltzer & Schroeder's design principles for secure systems.
3. What are "canaries" and how do they help in a specific kind of buffer overflow.
4. Compute GCD(1875, 405) showing every step in the computation. Explain why

$$a \times b \bmod n = (a \bmod n \times b \bmod n) \bmod n$$

5. Encrypt the following text using Vigenère's encryption with the keyword "NUS".

   The moon began to rise, and I thought of the placid look at the white ceiling, which had passed away. The moon began to rise, and I thought of the pressure on my hand when I had spoken the last words he had heard on earth.

6. Find the index of coincidence of the encrypted text in the previous question. From the IC, can you make a determination of the size of the keyword used for Vigenère encryption.
7. Consider the Linear Congruential Generator

$$r_{i+1} = (a \times r_i + b) \bmod n$$

   where $n = 2^{31} - 1$, $a = 16807, b = 0$. Starting with a seed of 32 generate the next hundred (pseudo) random numbers and comment on whether the numbers are uniformly distibuted over $0 \ldots (n-1)$.