Network Security Technology Spring, 2019
Tutorial 4, Week 5 (March 27) LIU Zhen
Due Date: April 3

Questions:

1. **Hash Function (50 Points)** Assume prime $p = 13$ and a generator $g = 7$.

   (a) Find two distinct positive integers x and y such that:

   $$g^x \mod p = g^y \mod p$$

   (b) Given the question 1a above, explain why $h(x) = g^x \mod p$ is not a good hash function.

   (c) Does the hash function $h(x) = g^x \mod p$ satisfy one-wayness, under the condition that p is a large prime?

2. **Digital Certificates (50 Points)**

   (a) Why can a public key not just be transmitted through email or be posted on a website?

   (b) A certificate does not necessarily have to be signed directly by a CA, there is something called a *certificate chain*. Can you imagine what a certificate chain is?

   (c) Who signs the certificate of a CA?