**Lab 3: Hash Function and Digital Signature**

I decide to lower the difficulty in the final lab of this course. There are two reasons to do so:

1. When the lab problem is difficult, many of you would use Xue Ba’s codes or results. Although “sharing”, a.k.a. cheating, in class is typical in China, it is my responsibility to tell you that in most countries of the civilized world, cheating is not as fashionable. I do hope everyone to work out this lab independently and grow up with courage to refuse cheating even at the cost of hard efforts or failure.
2. You are facing numerous final exams. An easy lab could help ease your stress.
3. We have investigated and identified cheaters from previous lab reports. The evidence of cheating and every student’s accumulated score will be published before final exam.

In this lab, your task is to create a self-signed digital certificate which at least contains your student number, your public key, a hash value, and a digital signature. You can use the X.509 format but any format from your creativity is welcomed too. You are responsible to explain the format of your certificate and the difference of self-signed certificate and CA signed certificate.