Homework #3 (due on 12/07)

Dr. Jun Li's contact info:

Office: 3-412, FIT Building
Phone: 62796400
email: junl@tsinghua.edu.cn

Mohammad Hashem Haghighat (阿里) (TA)'s contact info:

Office: 3-421, FIT Building,
Phone: 18510655774
email: l-a16@mails.tsinghua.edu.cn

1. According to the description of RSA in the textbook, prove completely that

   $(m^e \bmod n)^d \bmod n = m$

   including the proof of

   $x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$

   and

   $(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$

2. In PGP, why is a message signed first and then encrypted together with the signature, instead of the other way around (encrypt the message and then sign)? Other than PGP, are there cases where message (including network packet) can be encrypted and then signed?

3. In PGP, it compresses the message before encrypting it. In SSL, it does compression before encryption as well. Do we have to do compression first and then encryption, if we want to do both? Why or why not?

4. (Bonus) In IPSec, SPI is used to index SA. Can we remove SPI from IPSec header and still get it work? What's the impact to communication and computation load (overhead) respectively?

- Don't forget to write done your comments and ideas from textbook chapter(s) reading.
- This is the last homework for this course but there are more textbook chapter reading assignments. If you have comments and/or ideas, you can still submit via email.