COMP444: Internet Infrastructure Security
Workshop 4: IPSec

Due at 11:55pm on 23 April 2015
Submission site: https://submit.comp.polyu.edu.hk/

1. (10 marks) IPSec AH
   a) (5 marks) Refresh the web page to check your IP again. What is your public IP before and after connecting to the VPN? How is the new IP related to your VPN setting?
   b) (5 marks) Apply display filter "ip.addr = *<vpn server ip>".* Inspect the packet trace. Are the data in the packets encrypted? Can this mode provide confidentiality? If no, what is the major usage of this mode?

2. (10 marks) IPSec ESP
   a) Start the Wireshark again, reconnect the VPN, and refresh the IP lookup webpage.
      - (3 marks) What is your IP reported by webpage?
      - (3 marks) Apply display filter "ip.addr = *<vpn server ip>".* Locate the packets with the protocol "ESP". These are the data packets. Are the content encrypted?
   b) (4 marks) Assume a malicious user can capture the traffic sourced from the VPN server, can s/he read the data you send to the Internet through the VPN server? Why?

3. (5 marks) IKE
   a) (3 marks) Locate the first ISAKMP packet. What kind of information this packet contains? List three of them.
   b) (2 marks) Locate the third and fourth ISAKMP packet. What is the usage of this pair of packets?