Homework #12

(Due on 12:00am, Thursday, Jan 30th , 2014)

- Illustrate how Alice can send a confidential email to Bob using public/private keying.
- Why is a symmetric key used in most protocols to encrypt a data payload (the message etc.), even if a public/private key infrastructure exists?
- Please explain in your own words the structure of the following PGP signed message (especially: how does the signature work?):

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1
Bob: My husband is out of town tonight.Passionately yours,
    Alice
---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

- What are the three main phases of SSL?
- On what layer does SSL reside and why is that advantageous?
- Please sketch one typical scenario, where IPsec is used today.
- What are the two main protocols used in IPsec and what is their primary difference with respect to security properties?
- Who is handling the authentication information in an 802.11i scenario?
- What is the purpose of a firewall and what are filter rules?