

Homework #12

(Due on 12:00am, Thursday, Jan 28th, 2010)

1. Illustrate how Alice can send a confidential email to Bob using public/private keying.
2. 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?
3. 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
yhHJRHhGJGhg/12EpJ+l08gE4vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

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