1 **a)** För att hantera säkerhetshot mot ett nätverk behöver man ha mål för vilken säkerhet man ska ha. En vanlig modell för att hantera det är CIA-modellen. Utöver målen i den modellen kan man lägga till flera andra mål. Förklara kortfattat vad följande mål innebär: Authentication, Non-repudiation och Access control.

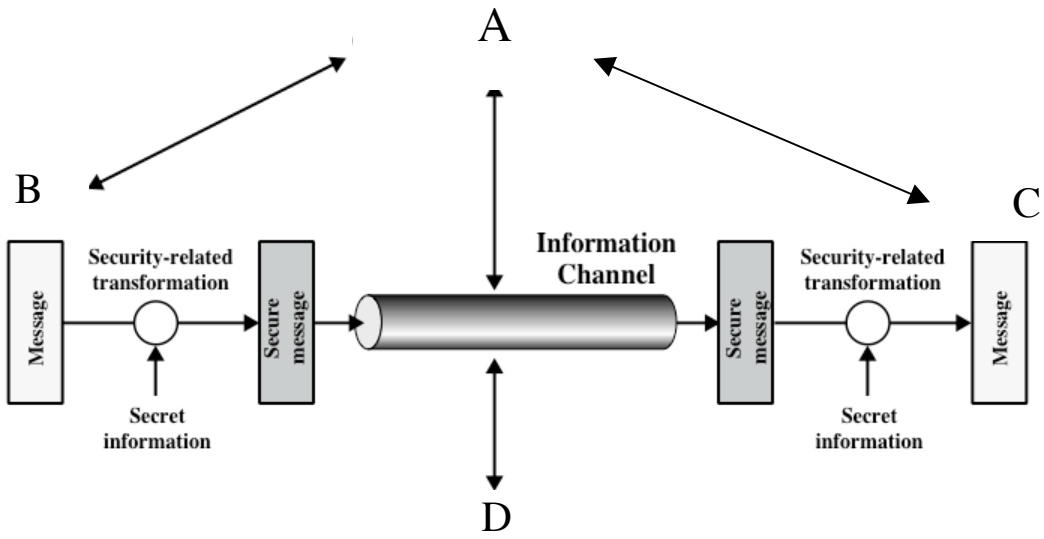
Security threats in a network can be handled by looking at the objectives that you have for the security. One model for this is the CIA model. Additional goals can be Authentication, Non-repudiation and Access control. Briefly describe these additional goals.

b) Beskriv begreppen attackyta och attackträd.

Describe the concepts Attack Surface and Attack tree.

c) Följande modell för nätverkssäkerhet innefattar fyra olika roller (markerade A-D). Beskriv dessa roller.

The following model for Network Security contains four roles (marked A-D). Describe these roles.



(4+4+4 p)

2 **a)** Förklara kortfattat varför nyckellängd är viktigt och ange vad som normalt sett anses vara tillräckligt långa nycklar för symmetrisk respektive asymmetrisk kryptering.

Describe briefly why the key length is important and what is generally seen as required key length for symmetrical and asymmetrical encryption.

b) Beskriv hur lösenord i Unix skyddas med hjälp av kryptering.

Describe how passwords in Unix are protected by use of encryption.

c) Hur kan hash-algoritmer användas inom IT-säkerhet?

How can hash algorithms be used in IT Security?

(4+4+4 p)

3 **a)** Hur är de två protokollen SSL och TLS relaterade?

How are the two protocols SSL and TLS related?

b) Vad är OpenSSL och vilka funktioner tillhandahåller det?

What is OpenSSL and what functions does it provide?

c) SSH (men även andra protokoll) erbjuder **Perfect forward secrecy**. Vad innebär det?

SSH (among other protocols) offers **Perfect forward secrecy**. What does that mean?

d) En tjänst som SSH erbjuder är **Port Forwarding**. Beskriv hur det fungerar och vad det används till.

A feature offered by SSH is **Port Forwarding**. Explain how it works and what it is used for.

(2+3+3+4 p)

4 **a)** PGP erbjuder en rad olika tjänster kring e-postsäkerhet. Ge en kortfattad beskrivning av följande tjänster och varför de finns med i PGP: **Authentication**, **Compression**, **E-mail compatibility** och **Segmentation**.

PGP offers a number of services. Give a short description of the following services and why they are part of PGP: **Authentication**, **Compression**, **E-mail compatibility** and **Segmentation**.

b) En tjänst som PGP dock inte erbjuder avsändaren är anonym e-post. Vad skulle en sådan tjänst innebär? Varför kan PGP inte erbjuda det? Hur kan man istället få tillgång till en sådan tjänst?

One service PGP does not offer is anonymous email. What would such a service mean if it could be offered? Why isn't it possible for PGP to offer it? How can you get that type of service instead?

(6+4 p)

5 **a)** I ett system för nätverksaccess kan man definiera tre olika komponenter. Det är **en Access requester**, and **Policy server** och en **Network access server**. Beskriv vad dessa tre olika komponenter har för uppgift.

In a system for Network access you can define three important components. These are an **Access requester**, a **Policy Server** and a **Network access server**. Describe what tasks each of these components have.

b) Ett viktigt protokoll för nätverksaccess är EAP. Vad står EAP för? Man kan se EAP som ett ramverk för en rad andra specifika protokoll. Vad är tanken med dessa andra protokoll och att ha ett sådant ramverk?

One important protocol for Network access is EAP. What does EAP stand for? You can see EAP as a framework for a number of other more specific protocols. What is the purpose of having these specific protocols and the framework itself?

(6+4 p)

6 **a)** IPSec innehåller tre olika delprotokoll; **AH**, **ESP** samt **ESP med autentisering**. Vad är skillnaden mellan dessa tre protokoll och varför finns det tre alternativ?

IPSec contains three sub protocols; **AH**, **ESP** and **ESP with authentication**. What is the difference between these protocols and why are there three alternatives?

b) Det finns också två olika moder, Transport mode och Tunnel mode. Beskriv hur dessa två olika moder fungerar.

There are also two modes available, Transport mode and Tunnel mode. Describe how these two modes work.

c) IPSec kan användas för att bygga ett VPN. Nämn två andra protokoll som också kan användas för att bygga VPN-lösningar.

IPSec can be used to build a VPN. Mention two other protocols that can be used to build VPN connections.

(4+4+2 p)

7 **a)** Brandväggar finns det olika typer av i form av mjukvara eller hårdvara. Beskriv översiktligt dessa olika typer, var i ett nätverk de placeras, vilken typ av hot de kan hantera mm.

Firewalls can be in the form of software or hardware. Give an overview of these types, where in a network they are placed, what types of threats they can handle etc.

b) Brandväggar använder sig av en eller flera av nedan specificerade tekniker. Beskriv kortfattat de olika teknikerna.

A firewall is using one or several of the following techniques. Shortly describe each control technique.

- Service control
- Direction control
- User control
- Behaviour control

c) Om man ansvarar för brandväggar är det viktigt att man testar dem ordentligt. Vad finns det för olika typer av verktyg som man kan använda sig av för brandväggstestning?

When you are responsible for Firewalls, testing them is an important activity. Describe some of the tools you may use doing this.

(4+4+2 p)