1 **a)** Säkerhetshot mot ett nätverk kan vara antingen aktiva eller passive. Beskriv skillnaden mellan dessa båda typer och ge exempel på hot från respektive kategori.

Security threats in a network can be either active or passive. Describe the difference between these two types and give examples from each category.

b) I säkerhetsstandarden X.800 anges ett antal säkertstjänster. Bland dessa finns konfidentialitet, oavvislighet och dataintegritet. Beskriv vad dessa begrepp betyder.

In the security standard X.800 a number of security services are defined. Among them are Confidentiality, Non-repudiation and Data integrity. Describe the meaning of these three services.

c) Ange för varje tjänst i uppgift b, minst en säkerhetsmekanism som används för att man ska kunna erbjuda den tjänsten.

Give for each service mentioned in task b, at least one security mechanism that is used to implement each service. (4+4+4 p)

2 **a)** När man angriper en krypterad text finns det lite olika alternativa metoder man kan använda. Beskriv följande fyra metoder: Frekvensanalys, algoritmisk svaghet, Brute force samt regnbågstabeller.

Someone attacking an encrypted text may have a number of different methods to use. Describe the following four methods: Frequency analysis, Algorithmic weakness, Brute force and Rainbow tables.

b) Dekryptera följande text som är krypterad med ett enkelt tranpositionschiffer. Beskriv också generellt hur tranpositionschiffer fungerar.

oh yuvj aese utrdeant o wridcesoct,gtanrlituan os

Decrypt the following text that is encrypted with a simple transposition cipher. Also give a general description of how transposition ciphers work.

oh yuvj aese utrdeant o wridcesoct,gtanrlituan os

(6+6 p)

3 **a)** TLS är ett protokoll som kan användas för att ge transportsäkerhet. Vad står TLS för? Vilka olika delprotokoll finns i TLS? Beskriv översiktligt hur TLS fungerar och de olika del-protokollen samverkar.

TLS is a protocol offering transport security. What does TLS stand for? What different sub protocols are parts of TLS? Describe briefly how TLS works and how the different sub protocols work together.

b) Ett annat protokoll som kan användas för transportsäkerhet är SSH. Vad står SSH för? Vad är det för grundläggande tjänst som SSH erbjuder? Transportsäkerhet ger SSH genom så kallad tunnling, förklara kortfattat hur det fungerar i SSH.

Another protocol offering transport security is SSH. What does SSH stand for? What is the basic service SSH offers? Transport security is offered through tunnelling; briefly explain how that works in SSH.

(5+5 p)

4 **a)** ISO och IEEE är två organisationer som tar fram standards inom bl.a. nätverk och datasäkerhet. Vad står förkortningarna för? Nämn en standard som respektive organisation står bakom.

ISO and IEEE are two standard organisations in the area of computer networks and data security. What is the full name of these organisations? Mention one standard that originates from each organisation.

b) En väldigt viktig typ av standardisering vad gäller IT-säkerhet styrs via RFCer. Beskriv vad RFC står för, vilken organisation som står bakom dessa samt något om processen för hur de tas fram.

One important type of standard documents in IT security is RFC documents. What does RFC stand for? What organisation is behind these documents? Shortly describe the process of how they are created.

(6+6 p)

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

PGP offers a number of different services. Give a short description of the following services: **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)

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? Vad är status för dessa protokoll idag?

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

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

There are also two modes available, Transport mode and Tunnel mode. Describe in general 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
- User control
- Direction control
- Behaviour control

c) Om man ansvarar för brandväggar är det viktigt att man testar dem ordentligt. Vad finns det 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)