1 **a)** Det finns olika former av grundläggande säkerhetsattacker i nätverk som man måste kunna hantera. Beskriv kortfattat följande olika attacker: ”Interruption”, ”Interception”, ”Modification” och ”Fabrication”.

There are different forms of network security attacks you need to be able to deal with. Shortly describe the following attacks: Interruption, Interception, Modification and Fabrication.

b) Nedan tabell beskriver hur säkerhetsmekanismer och säkerhetstjänster hänger ihop. Kolumnerna för ”Encipherment” och ”Data Integrity” är dock inte ifyllda än. Ange ett par olika tjänster som utnyttjar de mekanismerna och beskriv på vilket sätt.

In the table below you can see how different security services and mechanisms are related. The columns for Encipherment and Data integrity are however blanked out. Describe a couple of services that use these mechanisms and how they do it.

	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication		Y			Y			
Data origin authentication		Y						
Access control			Y					
Confidentiality							Y	
Traffic flow confidentiality						Y	Y	
Data integrity		Y						
Non-repudiation		Y						Y
Availability					Y			

(4+4 p)

2 **a)** Beskriv vad som är speciellt med asymmetriska kryptometoder. Ange också någon algoritm som är asymmetrisk.

Describe what is special with asymmetric crypto methods. Also mention some algorithm that is asymmetric.

b) AES är troligen en av de mest använda krypteringsalgoritmerna idag. Beskriv historien bakom AES.

AES is probably one of the most used crypto algorithms today. Describe the history behind AES.

c) En hashfunktion är en så kallad envägsfunktion. Vad betyder det?

Hash functions are what is called one way functions. What does that mean?

(3+3+2 p)

3 **a)** Vad står förkortningen SSH för?

What does the abbreviation SSH stand for?

b) SSH innehåller flera olika funktioner och användningsområden. Vilka är dessa?

SSH contains a number of function and services, which ones?

c) Ange vilka delprotokoll som finns i SSH och förklara kortfattat vad respektive protokoll gör.

Name the sub protocols that are part of SSH and shortly describe what each sub protocol is doing.

(2+4+4 p)

4 **a)** Federationer är ett sätt att hantera distribuerade identiteter och tjänster. För att skapa en federation är det ett antal olika delar som måste på plats. Förklara kortfattat vad följande begrepp betyder i det här sammanhanget:

A federation is one way to deal with distributed identities and services. In this context, shortly describe the following concepts:

- Authentication
- Accounting
- Provisioning
- Delegated administration

b) Två olika standarder inom området är SAML och Shibboleth. Beskriv kortfattat vad dessa båda standarder innehåller.

Two different standards in this area are SAML and Shibboleth. Shortly describe what these two standards contain.

(4+4 p)

5 **a)** Det finns olika typer av inkräktare. Ett sätt att klassificera dem är att dela in dem i ”Hackers”, ”Criminals” och ”Internal threats”. Beskriv kortfattat dessa tre typer. Ge också ett exempel på en typisk attack som var och en av dessa skulle kunna utföra.

There are different types of intruders. One way to classify them is as Hackers, Criminals and Internal threats. Shortly describe these three types. Also give one example of a typical attack each of these types could do.

b) Ett IDS kan grundläggande fungera på olika sätt, innehålla olika typer av moduler och finnas på olika platser i ett nätverk. Ge en kort översikt över det här området.

An IDS can basically work in different ways, use different types of modules and be placed in different parts of a network. Shortly describe this area.

(4+4 p)

6 **a)** Malware är en term som används som samlingsbegrepp för många olika former av illasinnade program. Worms är en typ som påminner om virus men är en egen klass. Vad är likheterna mellan virus och worms och vad är det som skiljer dem åt?

Malware is a term used for many different types of malicious software. Worms and viruses are similar but two distinct types. What are the similarities between these two types and what is different between them?

b) För att kunna utföra en DDoS-attack behöver du ha tillgång till ett Botnet. Hur skapar man ett sådant och vad är det egentligen ett Botnet gör?

To launch a DDoD attack you need a Botnet. How do you create a Botnet and what does it do?

c) En form av DoS-attacker är en SYN-attack. Beskriv hur det fungerar.

One form of DoS attack is the SYN attack. Describe how this attack works.

(4+3+3 p)

7 **a)** Betalningar på Internet utvecklas starkt och kräver naturligtvis en hel del standardisering vad gäller IT-säkerhet. Två olika standarder inom det här området är **PCI DSS** samt **3-D Secure**. Vad är syftet med dessa två standarder?

Payments on Internet are growing rapidly and of course require standardization when it comes to IT Security. Two standards in this area are **PCI DSS** and **3-D Secure**. What is the purpose of each of these standards?

b) Begreppet elektroniska pengar kan definieras på ett smalt eller ett brett sätt. Vad är den smala definitionen av elektroniska pengar?

The concept Electronic money can be defined in a narrow or a broad view. What is the narrow definition?

c) Beskriv kortfattat vad Bitcoin är.

Shortly describe what Bitcoin is.

(4+2+2 p)