1 **a)** IT security have a number of general goals that you almost always look at when you are evaluating and/or implementing some controls to increase security. These goals are summarized in the CIA model. Describe this model.

När man utvärderar och/eller implementerar IT-säkerhet brukar man alltid göra det mot bakgrund av ett antal generella målsättningar. Dessa brukar sammanfattas i den så kallade CIA-modellen. Beskriv den modellen.

b) IT Security threats are constantly changing. New specific threats appear now and then but also the long-term trends on types of attacks and the targets for these attacks are changing. Give a description of the current status in this field and also some of the changes that have occurred in recent years.

Hoten mot IT-säkerhet förändras kontinuerligt. Det handlar om olika former av nya specifika hot men också långsiktiga trender kring vilken form av attacker som sker och vad som är målet med dessa attacker. Ge en beskrivning av det aktuella läget och något om vilka förändringar som har skett på senare år.

(6+6 p)

2 **a)** What are the differences between Steganography, Encryption and Digital Watermarking? What is the purpose of each method?

Vilka skillnader finns mellan metoderna steganografi, kryptering samt digital vattenstämpling? Vad är syftet med respektive metod?

b) If you were to develop an application for an organisation that is to deal with sensitive information, what encryption algorithm would you use? Motivate your choice.

Om du ska utveckla en applikation som använder sig av kryptering för att skydda en organisations känsliga information, vilken algoritm skulle du då använda dig av? Motivera ditt val.

c) Asymmetric encryption algorithms have several different application areas (some algorithms only have one). Describe these possible applications.

Asymmetriska krypteringsalgoritmer har flera olika användningsområden (en del algoritmer kan bara användas för ett av dem). Beskriv kortfattat dessa olika områden.

(4+4+4 p)

3 To control the security in an organisation there is a need for several different strategic documents dealing with different areas of security. Give a short description of the purpose and content of the following documents.

För att styra säkerhetsarbetet i en organisation behövs det en rad olika strategidokument som behandlar olika områden. Ge en kortfattad beskrivning av vad syftet är med följande dokument och vad de innehåller.

- Information security policy / Informationssäkerhetspolicy
- Incident response plan / Incidentplan
- Security plan / Säkerhetsplan
- Business continuity plan / Kontinuitetsplan

(8 p)

4 **a)** Protecting Programs and Data can done in different ways. Briefly describe how the following options work and what they can protect; **Copyright**, **Patent** and **Trade Secret**.

Man kan skydda program och data på olika sätt. Tre olika metoder är: **Copyright**, **Patent** och **Trade Secret**. Beskriv kortfattat hur dessa metoder fungerar och vad de kan skydda.

b) As a buyer of software you also have some rights. This is partly covered in what is called *Redress for software failures*. Briefly describe this area of Computer security.

Som köpare av mjukvara har du också en del rättigheter. Detta hanteras delvis inom området ”*Redress for software failures*”. Beskriv kortfattat detta område inom datorsäkerhet.

(6+4 p)

5 a) Program Security defined by the text book have two main objectives. What are these two objectives?

Enligt lärobokens definition av programsäkerhet så finns det två olika överordnade målsättningar som man vill uppnå. Vilka är dessa båda mål?

b) Testing is one of many Developmental Controls for Program Security. There are different types of testing, briefly describe some of these types. There are also some problems with using testing as a control, briefly describe some of these problems.

Testning är en av de metoder man kan använda sig av för att hitta fel när man utvecklar program. Det finns olika typer av testning, beskriv kortfattat några av dessa. Det finns också problem med att använda testning, beskriv kortfattat några av dessa problem.

c) One of the types of errors you want to make sure a program does not have is buffer overflow. Describe how a buffer flow error can occur and what potential problems it may cause.

En av de feltyper som man undvika i program är buffertöverskridning. Beskriv hur ett sådant fel kan uppstå och vad det potentiellt kan innebära.

(4+4+4 p)

6 a) The Operating system is crucial for getting some level of security in a computer system. One basic technique used to get it is by separation. The most common form of separation used is logical separation. Describe how that type of separation works.

Ett operativsystem är väldigt viktigt för att kunna få ett datorsystem säkert. En metod som används för att få det är separation. Den vanligaste metoden här är logisk separation. Beskriv hur det fungerar.

b) Memory protection is one of the methods applied in operating systems. Shortly describe a few methods used to implement memory protection.

Skydd av minnet är en av de metoder som används i operativsystem. Beskriv kortfattat några olika alternativa metoder för att implementera minneskydd.

c) One of the tasks for the operating system is to handle access control. Name four different types of objects that need this type of protection.

En av uppgifterna för ett operativsystem är accesskontroll. Nämn fyra olika typer av objekt som behöver den här typen av skydd.

(4+4+4 p)

7 a) Privacy has become one of the major aspects of computer security in recent years. Not the least because the advances in surveillance. Principles for fair use of personal information have been developed to try to meet this. Name and describe three of these principles.

Personlig integritet (privacy) har blivit en av de viktigaste aspekterna på datorsäkerhet under senare år. För att skydda den personliga integriteten har det tagits fram ett antal principer för hur personlig information ska hanteras. Ange och beskriv tre av dessa principer.

b) One way to improve your privacy is to use different types of identities. What are the different options we have to use different identities and how does that help to improve our privacy?

Ett sätt att öka den personliga integriteten är att använda olika typer av identiteter. Vilka olika typer av identiteter kan vi välja mellan och på vilket sätt hjälper de oss att öka vår personliga integritet?

(6+4 p)