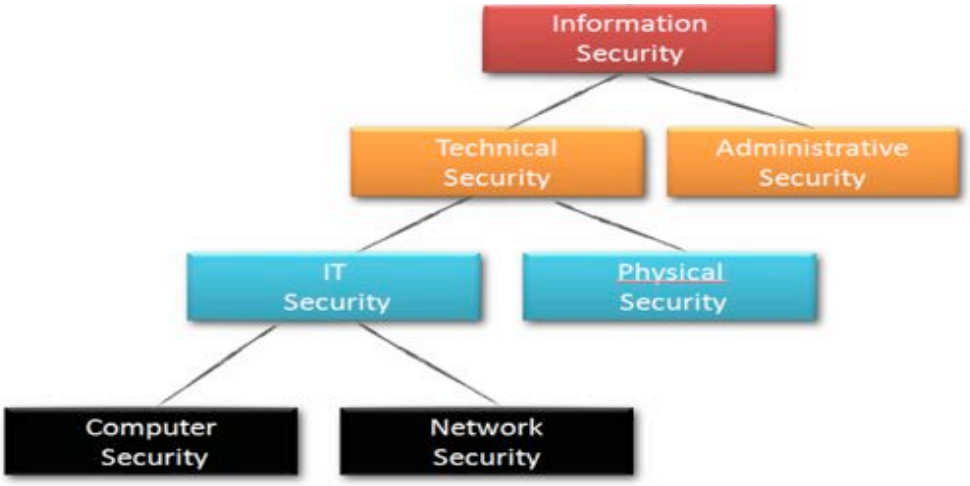
1 **a)** Information Security can be divided into different parts according to the figure below. Describe what each box in the figure covers and give a concrete example of what can be done.

Informationssäkerhet kan brytas ner i olika delområden enligt figuren nedan. Beskriv vad varje box innehåller och ge något konkret exempel på vad man gör inom varje område.



b) In Information Security you talk about different **Assets**. Give four examples of what these assets can be.

Inom informationssäker pratar man om olika **informationstillgångar**. Ge fyra exempel på vad en sådan tillgång kan vara.

(8+4 p)

2 **a)** Simple substitution ciphers can be broken by an attack where you calculate the relative frequency of different symbols in the ciphertext. Describe how this attack works and why it is successful.

Enkla substitutionskrypton kan knäckas genom att beräkna den relativa frekvensen av olika symboler i kryptotexten. Beskriv hur den attacken går till och varför den fungerar.

b) The following message have been encrypted using **Simple permutation** with the key 1432. Decrypt the message. What type of basic crypto method is used in Simple permutation?

Följande meddelande har krypterats med metoden **enkel permutation** och med nyckeln 1432. Dekryptera meddelandet. Vilken grundläggande krypteringsmetod använder sig enkel permutation av?

T ehwlrodsi w aoednrluf alpc e

c) To know that a message has not been changed you can use a **Message Authentication Code**. Describe how you calculate the code why it can be used to prove that a message is correct.

För att avgöra om ett meddelande har förändrats eller ej kan man använda en ”**Message Authentication Code**”. Beskriv hur en sådan beräknas och hur den kan användas för att bevisa att ett meddelande är korrekt.

(4+4+4 p)

3 **a)** Program flaws can be either **intentional** or **unintentional**. Give a short description of these types of flaws and give an example of a typical flaw from each category.

Fel i program kan vara **avsiktliga** eller **oavsiktliga**. Ge en kort beskrivning över dessa båda typer av fel och ge ett exempel på ett typiskt fel från varje kategori.

b) Malicious programs come in many different forms and shapes. Give a brief description of these two types: Rabbit and Dropper.

Det finns en mängd olika typer av skadliga program. Ge en kort beskrivning av följande två typer: ”Rabbit” och ”Dropper”.

(4+4 p)

4 **a)** Two important tasks for an Operating system is **Identification** and **Authentication**. Describe these two tasks and how they are related.

Två viktiga uppgifter för ett operativsystem är **identifiering** och **autentisering**. Beskriv dessa båda uppgifter och hur de är relaterade till varandra.

b) What is a **biometric** method and what different options do you have for this method?

Vad är en **biometrisk** metod och vilka olika alternativ finns det för den?

c) Two related concepts are "**Single-sign-on**" and "**Federated Identity Management**". Briefly describe these two concepts.

Två relaterade områden är "**Single-sign-on**" och "**Federerad identitetshantering**". Beskriv kortfattat båda dessa områden.

(4+4+4 p)

5 **a)** In Databases you implement something called **Two-phase Update**. What is that and why do you do it?

I databaser används något som kallas "**Two-phase Update**". Vad är det och varför används det?

b) What is considered to be **Sensitive data** can vary depending on many different factors. Describe some of the reasons data might be seen as Sensitive data.

Vad som anses vara **känsliga data** kan bero på en rad olika faktorer. Beskriv några anledningar till att data kan anses vara känsliga.

c) A typical security related attack on databases is the **Inference attack**. What is the goal with such an attack and how is performed?

En typisk attack mot en databas är den så kallade **inferensattacken**. Vad är målet med en sådan attack? Hur genomförs den?

(4+4+4 p)

6 **a)** A security plan consists of many different areas. Describe the content of the following areas: **Policy**, **Accountability** and **Maintenance**.

En säkerhetsplan innehåller en rad olika avsnitt. Beskriv kortfattat vad följande avsnitt behandlar: **Policy**, **Accountability** och **Maintenance**.

b) Study the table below. You will see the details of three different risks and for each risk two possible controls. Make the calculations that will fill in all the gaps in the table and then make an argument for what controls you would advice to implement.

Studera tabellen nedan. Du ser information om tre olika identifierade risker samt för varje risk två alternativa sätt att hantera dem. Fyll i siffror som saknas i tabellen och för sedan ett resonemang för vilka av åtgärderna som du rekommenderar att man implementerar.

Risk	Control	Impact	Probability	Exposure	Cost of control	Probability after control	Exposure after reduction	Leverage	Savings
1	I	20000	0,1		200	0,095			
	II	20000	0,1		1000	0,05			
2	III	100000	0,25		10000	0,1			
	IV	100000	0,25		5000	0,2			
3	V	1000	0,8		100	0,1			
	VI	1000	0,8		200	0,2			

(6+6 p)

7 **a)** The textbook give a number of examples of **Computer Crime**. Choose three of these types of crimes and briefly describe them.

Läroboken ger en rad olika exempel på vad som kan räknas som **datorbrott**. Ange tre av dessa och beskriv kortfattat vad brotten handlar om.

b) Ethics of people are important to understand how and why they will react in different situations. Two different types of ethics are **Egoism** and **Utilitarianism**. Briefly describe how these types of ethics affect how someone will react in different situations.

En persons etik är viktig för att förstå hur och varför man reagerar på olika situationer. Två olika typer at etik är ”**Egoism**” och ” **Utilitarianism**”. Beskriv kortfattat hur dessa båda typer av etik påverkar hur någon kommer att reagera på olika situationer.

(6+4 p)