1 **a)** Beskriv kortfattat den historiska utvecklingen vad gäller krypteringsalgoritmer de senaste 2000 åren men med tonvikt på de senaste 100 åren. Vilka är de viktiga upptäckterna som har gjorts vilket lett fram till nya typer av algoritmer?

Describe the general historical development for encryption algorithms the last 2000 years but with en emphasis on the last 100 years. What are the important new ideas discovered that led to new types of algorithms?

b) Digital signering av dokument kräver att man använder sig av flera grundläggande säkerhetsfunktioner; hashfunktioner, krypteringsalgoritmer och certifikat. Beskriv hur de olika delarna fungerar och hur de tillsammans kan användas för att ge en digital signering.

To digitally sign a document we need to use several basic security functions like hash functions, encryptions algorithms and certificates. Describe these basic parts and how they together can be used to give a digital signature.

(6+6 p)

2 Nyckeldistribution är ett allmänt problem som måste lösas i många olika typer av system.

Key distribution is a general problem that needs to be solved in many different types of systems.

a) Förklara kortfattat vad nyckeldistributionsproblemet är.

Describe briefly what the key distribution problem is.

b) Att använda sig av publika nycklar är ett sätt att angripa detta problem. Hur fungerar den lösningen?

Using public keys is one way to deal with this problem. Describe this solution.

c) Om man använder symmetriska krypteringsalgoritmer måste man använda någon annan lösning. Man kan t.ex. utnyttja nyckeldistributionscentraler. Hur fungerar det och vad krävs för att det ska fungera?

If you are using symmetrical encryption algorithms you have to find some other solution. You can for instance use a Key Distribution Center (KDC). How does that work and what is required for it to work?

(2+4+4 p)

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

SSL is a protocol offering transport security. What does SSL stand for? What different sub protocols are parts of SSL? Describe briefly how SSL 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? Ange vilka delprotokoll som finns i SSH och kortfattat vad respektive protokoll gör.

Another protocol offering transport security is SSH. What does SSH stand for? What is the basic service SSH offers? Name the sub protocols that are part of SSH and shortly what each sub protocol is doing.

(5+5 p)

4 **a)** ISO och NIST 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 NIST 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 standard för säkerhet är PCI DSS. Beskriv vad syftet med denna standard är, kortfattat vad den innehåller samt vad man måste göra för att uppfylla standarden.

One standard for data security is the PCI DSS standard. Describe the purpose with this standard, shortly what it contains and what you need to do to comply with the standard.

(6+6 p)

5 **a)** Ett IDS kan fungera på lite olika sätt. Vad står IDS för? Det finns två huvudtyper beskrivna i boken, vardera nedbruten i två undertyper (sammanlagt fyra olika typer). Beskriv kortfattat skillnaderna mellan dessa olika typer.

An IDS can work in different ways. What does IDS stand for? There are two main types described in the textbook, each one further divided into two subtypes (in total four different types). Shortly describe the differences between these different types of IDS.

b) Vad är skillnaden mellan ett IDS och ett IPS?

What is the difference between an IDS and an IPS?

c) En Honeypot kan vara en del av ett större IDS. Vad är det för något? Vilka syften har det?

One part of a bigger IDS can be a Honeypot. What is that? What are the purposes with such a system?

(4+2+4 p)

6 **a)** Malware är en term som används som samlingsbegrepp för många olika former av illasinnade program. Vad har de gemensamt? Hur kan vi klassificera olika typer av Malware?

Malware is a term used for many different types of malicious software. What do they have in common? How can we classify different types of Malware?

b) Det finns en del lite nyare former av Malware. Beskriv kortfattat nedan typer:

There are some more recent types of Malware. Shortly describe the types below:

- Root kit
- Bacteria
- Mobile code
- Metamorphic virus

(4+4 p)

7 **a)** Vad är skillnaden mellan en ”stateless” och en ”stateful” paket-filtrerande brandvägg?

What is the difference between a stateless and a stateful packet filtering firewall?

b) Nedan brandväggsregler finns i en brandvägg. Beskriv vilken typ av trafik som dessa regler kommer att tillåta passera brandväggen och vad som kommer att stoppas. Vad händer med trafik som brandväggen bestämmer sig för att stopps?

Below rules are taken from a firewall. Describe what traffic the firewall will allow to pass and what will be stopped. What happens with traffic that the firewall decides should be stopped?

source address	**action**	**dest address**	**protocol**	**source port**	**dest port**	**flag bit**
222.22.1/8	deny	outside of 222.22/16	TCP	> 1023	80	any
222.22/16	allow	outside of 222.22/16	TCP	> 1023	80	any
outside of 222.22/16	allow	222.22/16	TCP	80	> 1023	ACK
222.22/16	allow	outside of 222.22/16	UDP	> 1023	53	---
outside of 222.22/16	allow	222.22/16	UDP	53	> 1023	----
all	deny	all	all	all	all	all

(4+6 p)