1 **a)** För att hantera säkerhetshot mot ett nätverk behöver man ha mål för vilken säkerhet man ska ha. En vanlig modell för att hantera det är CIA-modellen. Beskriv denna modell.

Security threats in a network can handled by looking at the objectives that you have for the security. In model for this is the CIA model. Describe this model.

b) Beskriv skillnaden mellan ett säkerhetshot och en säkerhetsattack riktad mot nätverkssäkerhet.

Describe the difference between a security attack and a security threat targeting Network security.

c) Säkerhetshot kan delas in i aktiva och passiva hot. Hur skiljer sig dessa åt vad gäller möjligheten att upptäcka dem och hur svårt det är att skydda sig mot dem?

Threats can be divided into active and passive threats. What is the difference between these in terms of the opportunity to detects them and how difficult it is to protect against them?

(4+4+4 p)

2 **a)** Förklara kortfattat varför nyckellängd är viktigt och ange vad som normalt sett anses vara tillräckligt långa nycklar för symmetrisk respektive asymmetrisk kryptering.

Describe briefly why the key length is important and what is generally seen as required key length for symmetrical and asymmetrical encryption.

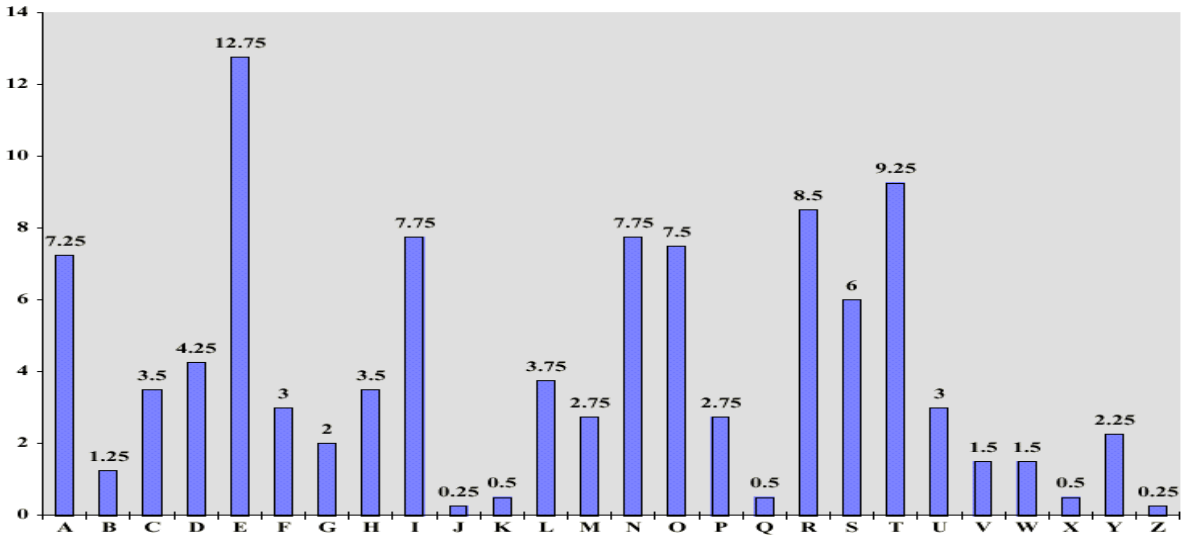
b) Vad är de två kriterierna som anses krävas för att en krypteringsalgoritm ska anses vara säker?

What are the two criteria required for an encryption scheme to be considered to be secure?

c) Nedan text är ett krypterat meddelande. Du misstänker att det är krypterad med en enkel substitutionsteknik. Beskriv den generella metoden för att dekryptera en sådan text. Kan du dekryptera den första meningen av meddelandet?

The following text is an encrypted message. You suspect it is encrypted with a simple substitution cipher. Describe the general idea for how you would decrypt the text. Can you decrypt the first sentence of the text?

af qkwxcdmkpxew, ifqkwxcadf ar cei xkdqirr du ifqdgafm p oirrpmi dk afudkopcadf af rvqe p tpw cepc dfnw pvcedkabig xpkcair qpf pqqirr ac. ifqkwxcadf gdir fdc acrinu xkisifc afcikuikifqi, hvc gifair cei afcinnamahni qdfcifc cd p tdvng-hi afcikqixcdk. af pf ifqkwxcadf rqeioi, cei afcifgig afudkopcadf dk oirrpmi, kiuikkig cd pr xnpafcizc, ar ifqkwxcig vrafm pf ifqkwxcadf pnmdkaceo – p qaxeik – mifikpcafm qaxeikcizc cepc qpf dfnw hi kipg au giqkwxcig. udk ciqefaqpn kiprdfr, pf ifqkwxcadf rqeioi vrvpnnw vrir p xrivgd-kpfgdo ifqkwxcadf liw mifikpcig hw pf pnmdkaceo. ac ar af xkafqaxni xdrrahni cd giqkwxc cei oirrpmi tacedvc xdrrirrafm cei liw, hvc, udk p tinn-giramfig ifqkwxcadf rqeioi, qdfragikphni qdoxvcpcadfpn kirdvkqir pfg rlannr pki kijvakig. pf pvcedkabig kiqaxaifc qpf ipranw giqkwxc cei oirrpmi tace cei liw xkdsagig hw cei dkamafpcdk cd kiqaxaifcr hvc fdc cd vfpvcedkabig vrikr.



(4+4+6 p)

3 **a)** SSL/TLS ligger på transportnivån i TCP/IP-stacken. Varför har man lagt de protokollen på den nivån?

SSL/TLS can be found on the transport level in the TCP/IP protocol stack. Why are they on that layer?

b) HTTP Strict Transport Security (HSTS) är ett protokoll som används tillsammans med HTTPS. Beskriv kortfattat syftet med HSTS och kortfattat hur det fungerar.

HTTP Strict Transport Security (HSTS) is a protocol used together with HTTPS. Describe briefly what the purpose with HSTS is and briefly how it works.

c) SSH har tre olika autentiseringsmetoder. Vilka är det?

SSH have three different authentication methods. What are they?

d) En tjänst som SSH erbjuder är **Port Forwarding**. Beskriv hur det fungerar.

A feature offered by SSH is **Port Forwarding**. Explain how that works.

(2+3+3+4 p)

4 **a)** För säker eposthantering finns det en rad olika saker att tänka på. En relativ ny standard inom detta område är DMARC som i sin tur huvudsakligen består av två andra standarder, DKIM och SPF. Vad är det huvudsakliga målet med DMARC (och tidigare DKIM)?

Security for e-mails requires many different considerations. One recent standard in this area is DMARC that in turn mainly consist of two earlier standards, DKIM and SPF. What is the main goal for DMARC (and previously also for DKIM)?

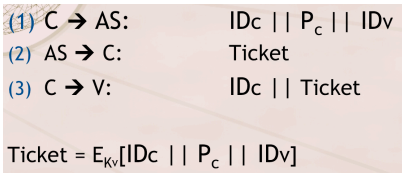
b) PGP och S/MIME är två andra standarder inom epostsäkerhet. Vad är syftet med de två standarderna? Vilka skillnader finns mellan dem?

PGP and S/MIME are two other standards in email security. What is the purpose with these two standards? What are the differences between them?

(4+6 p)

5 **a)** Nedan figur beskriver en första enkel modell för inloggning med hjälp av protokollet Kerberos. Det finns en rad problem med den här enkla modellen. Ange tre problem som finns i den och på vilket sätt det verkliga protokollet hanterat dessa problem.

In the figure below you can see a first simple model for login using the protocol Kerberos. This simple model has a number of obvious problems. Mention three of these problems and how they have been solved in the actual Kerberos protocol.



b) Kerberos bygger sin autentiseringsmodell på symmetrisk kryptering och lösenord. Ett alternativ till det är att använda publika nycklar och certifikat. Beskriv kortfattat hur det fungerar.

Kerberos is building its authentication model on symmetrical encryption and passwords. An alternative way is to use public keys and certificates. Briefly describe how that works.

c) Vad är skillnaden mellan identifiering och autentisering?

What is the difference between identification and authorization?

(6+4+2 p)

6 **a)** Betalningar på Internet utvecklas starkt och det krävs naturligtvis standardisering vad gäller IT-säkerhet. En standard inom det här området är **3-D Secure**. Beskriv översiktligt hur den standarden fungerar.

Payments on Internet are growing rapidly and of course require standardization when it comes to IT Security. One standard in this area is **3-D Secure**. Give an overview of how that standard works.

b) Ett område inom betalningar som ökar kraftigt är mobila betalningar (Apple Pay/ Samsung Pay). Hur fungerar det och hur säkert är det?

One area in electronic payments that is currently growing is mobile payments (Apple Pay/Samsung Pay). How does that work and how secure is it?

c) Bitcoin (och en rad andra nya tjänster) bygger på en teknik som kallas **Block chain**. Vad används den tekniken för i Bitcoin?

Bitcoin (and some other new services) is built around a technology called **Block chain**. What is the purpose of the block chain technology used for Bitcoin?

(4+4+2 p)

7 **a)** Nedan brandväggsregler finns i en brandvägg. Beskriv vilken typ av trafik som dessa regler kommer att tillåta passera brandväggen och vad som kommer att nekas. Vad händer med trafik som brandväggen bestämmer sig för att neka?

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

b) När man testar brandväggar behöver man en rad olika typer av verktyg. Beskriv kortfattat vad följande typer av verktyg används för i detta sammanhang: Network traffic generator, Network monitor, Port scanner och Vulnerability detection tools.

When you make firewall testing you need different types of tools. Shortly describe what the following types are used for in this context: Network traffic generator, Network monitor, Port scanner, and Vulnerability detection tools.

source address	**action**	**dest address**	**protocol**	**source port**	**dest port**	**flag bit**
222.22.1/24	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

(6+6 p)