NTNU
Kunnskap for en bedre verden

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i TTM4100 Kommunikasjon – tjenester og nett

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

Eksamensdato: 14. aug 2019

Eksamenstid (fra-til): 0900-1300

Hjelpemiddelkode/Tillatte hjelpemidler: D (ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Målform/språk: Engelsk / Bokmål / Nynorsk

Antall sider (uten forside): 6

Antall sider vedlegg: 0

Informasjon om trykking av eksamensoppgave

Originalen er:

1-sidig ☐ **2-sidig** ☐

sort/hvit ☐ **farger** ☐

skal ha flervalgskjema ☐

Kontrollert av:

Dato Sign

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

Important: Should there be any print errors (or wrong translations?) in the following text, the *English version (***E:***)* is the original and valid one.

Viktig: Om det skulle være noen trykkfeil (eller feil i oversetting?) nedenfor er det *den engelske versjonen* **(E:***)* som er den originale og den som gjelder.

Viktig: Om det skulle vera nokon trykkfeil (eller feil i oversetting?) nedanfor er det *den engelske versjonen* (**E:**) som er den originale og den som gjeld.

1. Mix / Diverse (3+3+3+3+3+5 = 20 points)

1.1 E: Make a simple drawing of the five layer Internet protocol stack and explain the term "encapsulation" in this context.
B: Lag en enkel tegning av femlags Internett-protokollstakken og forklar begrepet "innkapsling" («encapsulation») i denne sammenhengen.
N: Lag ei enkel teikning av femlags Internett-protokollstakken og forklar omgrepet "innkapsling" («encapsulation») i denne samanhengen.

1.2 E: Given the data 101110 and the generator 1001, find the CRC code (bits) to be added to the data before transmission over a communication link.
B: Gitt data 101110 og generatoren 1001, finn CRC-koden (bits) som skal legges til data før overføring over en kommunikasjonslink.
N: Gitt data 101110 og generatoren 1001, finn CRC-koden (bits) som skal leggast til data før overføring over ei kommunikasjonslenke.

1.3 E: Assume that two-dimensional even parity is used to check for errors in transmission (parity bits are given in row *V* and column *e* in Figure 1). If the data and parity bits received are as shown in Figure 1, are you able to identify which bit(s) are in error? If so, give the position of this/these bit(s) by indicating either a combination of row and column (e.g. (*II*, *d*) or *(III*, *b*)), or the rows and columns where bits in error are detected (e.g. *II* or *c*). Can this/these bit(s) in error be corrected? Explain why or why not.
B: Anta at todimensjonal lik («even») paritet brukes til å kontrollere feil i overføringen (paritetsbiter er gitt i rad *V* og kolonne *e* i figur 1). Hvis dataene og paritetsbitene mottatt er som vist i figur 1, kan du identifisere hvilke(t) bit (biter) som er feil? Hvis ja, gi posisjonen til dette / disse bitene ved å indikere enten en kombinasjon av rad og kolonne (f.eks. (*II*, *d*) eller (*III*, *b*)) eller radene og kolonnene hvor det oppdages feilbiter f.eks. *II* eller *c*). Kan dette / disse bitene korrigeres? Forklar hvorfor eller hvorfor ikke.
N: Anta at todimensjonal lik («even») paritet blir brukt til å kontrollera feil i overføringa (paritetsbitar er gitt i rad *V* og kolonne *e* i figur 1). Viss data og paritetsbitene mottatt er som vist i figur 1, kan du identifisera kva for bit (eller bitar) som er feil? Viss ja, gi posisjonen til dette / desse bitane ved å indikera enten ein kombinasjon av rad og kolonne (t.d. (*II*, *d*) eller (*III*, *b*)) eller radene og kolonnane der det blir oppdaga feilbitar t.d. *II* eller *c*). Kan dette / desse bitane bli korrigerte? Forklar kvifor eller kvifor ikkje.

	a	*b*	*c*	*d*	*e*
I	1	0	0	1	0
II	0	1	0	0	0
III	0	1	0	1	0
IV	0	1	0	1	0
V	1	1	0	1	1

Figure 1: Data and parity bits as received / Data og paritetsbit som mottatt

1.4 E: Give at least two different ways that data packets can disappear on their way through a packet switched network.
B: Oppgi minst to forskjellige måter datapakker kan forsvinne på vei gjennom et pakkesvitsjet nett.
N: Oppgi minst to ulike måtar datapakkar kan forsvinna på veg gjennom eit pakkesvitsjet nett.

1.5 E: Make a sketch of a generic router architecture, including all necessary main parts in both the data plane and the control plane.
B: Lag en skisse av en generisk ruterarkitektur, inkludert alle nødvendige hoveddeler i både dataplanet og kontrollplanet.
N: Lag ein skisse av ein generisk ruterarkitektur, inkludert alle nødvendige hovuddelar i både dataplanet og kontrollplanet.

1.6 E: Given a broadcast channel with N nodes and transmission rate of R bit/s. The broadcast channel uses polling (with an additional polling node) for multiple access. Suppose the polling delay, which is the amount of time from when a node completes transmission until the subsequent node is permitted to transmit, is d. Within a polling round, a given node is allowed to transmit at most Q bits. What is the maximum throughput of the broadcast channel?
B: Gitt en kringkastingskanal med N noder og overføringshastighet på R bit/s. Kringkastingskanalen bruker polling (med en ekstra pollingnode) for multippel tilgang. Anta at pollingforsinkelsen, som er tiden fra når en node fullfører sin overføring til den påfølgende noden har lov til å starte sin overføring, er d. Innenfor en pollingrunde er det maksimale en gitt node kan overføre Q biter. Hva er maksimal gjennomstrømning («throughput») i kringkastingskanalen?
N: Gitt ein kringkastingskanal med N noder og overføringsfart på R bit/s. Kringkastingskanalen bruker polling (med ein ekstra pollingnode) for multippel tilgang. Anta at pollingforseinkinga, som er tida frå når ein node fullfører overføringa si til den følgjande noden har lov til å starta overføringa si, er d. Innanfor ein pollingrunde er det maksimale ein gitt node kan overføra Q bitar. Kva er maksimal gjennomstraumning («throughput») i kringkastingskanalen?

2. TCP and UDP / TCP og UDP (3+3+3+3+4+4 = 20 points)

2.1 E: Does a TCP segment contain IP addresses as part of its payload? Explain why or why not.
B: Inneholder et TCP-segment IP-adresser som en del av nyttelasten? Forklar hvorfor eller hvorfor ikke.
N: Inneheld eit TCP-segment IP-adresser som ein del av nyttelasta? Forklar kvifor eller kvifor ikkje.

2.2 E: Is there any difference in how checksums are implemented in TCP and UDP segments? If so, explain.
B: Er det noen forskjell på hvordan sjekksum er implementert i TCP og UDP segmenter? Hvis ja, forklar.
N: Er det nokon skilnad på korleis sjekksum er implementert i TCP og UDP segment? Viss ja, forklar.

2.3 E: UDP is an unreliable protocol compared to TCP, i.e. being connectionless and with no support for flow- or congestion control. However it also has some advantages for some uses compared to TCP. Give an example of at least one such use or case.
B: UDP er en upålitelig protokoll i forhold til TCP, siden den er forbindelsesløs og uten støtte for strømnings- eller overbelastningskontroll. Men den har også noen fordeler for noen bruksområder sammenlignet med TCP. Gi et eksempel på minst et slikt bruksområde eller tilfelle.
N: UDP er ein upåliteleg protokoll i forhold til TCP, sidan han er forbindelseslaus og utan støtte for strømnings- eller overbelastingskontroll. Men han har òg nokre fordelar for nokre bruksområde samanlikna med TCP. Gi eit døme på minst eit slikt bruksområde eller tilfelle.

2.4 E: Give a brief overview of how a TCP connection is established.
B: Gi en kort oversikt over hvordan en TCP forbindelse blir etablert (eller «satt opp»).
N: Gi ei kort oversikt over korleis eit TCP samband blir etablert (eller «sett opp»).

2.5 E: What do you (in general) want to achieve by using flow control? What type of flow control is implemented in TCP? (Short answers are sufficient on both questions; no detail of how flow control is implemented in TCP is necessary).
B: Hva vil du (generelt) oppnå ved å bruke flytkontroll? Hvilken type flytkontroll er implementert i TCP? (Korte svar er tilstrekkelige på begge spørsmålene, ingen detaljer om hvordan flytkontroll er implementert i TCP er nødvendig).
N: Kva vil du (generelt) oppnå ved å bruka flytkontroll? Kva for ein type flytkontroll er implementert i TCP? (Korte svar er tilstrekkelege på begge spørsmåla, ingen detaljar om korleis flytkontroll er implementert i TCP er nødvendig).

2.6 E: Give a brief high-level overview of congestion control as implemented in the TCP protocol. (Keywords: three major components, main objectives and functionalities of each component, details of implementation not necessary).
B: Gi en kort høy-nivå oversikt over overlastkontroll (“congestion control”) slik det er implementert i TCP protokollen. (Stikkord: tre hoveddeler, hovedhensikt og funksjonalitet for hver del; detaljer om implementering er ikke nødvendig å ta med).
N: Gje eit kort høg-nivå oversyn over overlastkontroll (“congestion control”) slik det er implementert i TCP protokollen. (Stikkord: tre hovuddelar, hovudføremål og funksjonalitet for kvar del; detaljar om implementering er ikkje naudsynt å ta med).

3. Multimedia (4+4+4+4+4 = 20 points)

3.1 E: To provide optimal streaming media delivery to customers, service providers (e.g. Netflix) needs to maximize its control over the three basic components in the delivery chain: video player, video server, and network in-between. Describe which network parameters affect the users' experience of streaming quality, and briefly what service providers (e.g. Netflix) does to ensure the best possible user experience.
B: For å levere optimal strømming («streaming») av media til kunder, må tjenesteleverandører (f.eks. Netflix) maksimere kontrollen over de tre grunnleggende komponentene i leveransekjeden: videospiller, videoserver, og nettverket imellom. Beskriv hvilke nettverksparametre som påvirker brukernes opplevelse av strømmekvalitet, og kort hva tjenesteleverandører (f.eks. Netflix) gjør for å sikre best mulig brukeropplevelse.
N: For å levera optimal strauming («streaming») av media til kundar, må tenesteleverandørar (t.d. Netflix) maksimera kontrollen over dei tre grunnleggande komponentane i leveransekjeden: videospelar, videoservar, og nettverket imellom. Beskriv kva for nettverksparametrar som påverkar opplevinga til brukarane med omsyn til straumekvalitet, og kort kva tenesteleverandørar (t.d. Netflix) gjer for å sikra best mogleg brukaroppleving.

3.2 E: Why and with what parameter does Netflix check your geolocation?
B: Hvorfor og med hvilken parameter sjekker Netflix din geolokasjon?
N: Kvifor og med kva for ein parameter sjekkar Netflix din geolokasjon?

3.3 E: Explain how an "unblock Netflix" service works; illustrate with a protocol stack drawing.
B: Forklar hvordan en «unblock Netflix» tjeneste fungerer; illustrer med en protokollstakktegning.
N: Forklar korleis ein «unblock Netflix» teneste fungerer; illustrer med ei protokollstakkteikning.

3.4 E: Some schemes exist to recover from packet loss when realizing real-time conversational voice over the internet (Voice-over-IP). Two variants of FEC are amongst these. Give brief explanations of both methods based on this principle.
B: Noen metoder eksisterer for å motvirke pakketap når man realiserer sanntids-talesamtaler over Internett (Voice-over-IP). To varianter av FEC er blant disse. Gi korte forklaringer av begge metodene basert på dette prinsippet.
N: Nokre metodar eksisterer for å motverka pakketap når ein realiserer sanntids-talesamtaler over Internett (Voice-over-IP). To variantar av FEC er blant desse. Gi korte forklaringar av begge metodane baserte på dette prinsippet.

3.5 E: When using the public Internet for interactive voice communication, what are the main challenges to achieve good quality?
B: Når en bruker det offentlige Internettet for interaktiv talekommunikasjon, hva er hovedutfordringene for å oppnå god kvalitet?
N: Når ein brukar det offentlege Internettet for interaktiv talekommunikasjon, kva er hovudutfordringane for å oppnå god kvalitet?

4. Information security / Informasjonssikkerhet (4+4+4+4+4 = 20 points)

4.1 E: What is a digital certificate and how is the validity of digital certificates validated?
B: Hva er et digitalt sertifikat og hvordan bekreftes gyldigheten av digitale sertifikater?
N: Kva er eit digitalt sertifikat og korleis blir gyldigheten av digitale sertifikat stadfesta?

4.2 E: How can a client check that a received public key is correct?
B: Hvordan kan en klient sjekke at en mottatt offentlig nøkkel er korrekt?
N: Korleis kan ein klient sjekka at ein mottatt offentleg nøkkel er korrekt?

4.3 E: Describe how a message M is encrypted and sent from A and to B, which then decrypts the message. Asymmetric encryption is used with A's key pair.
B: Beskriv hvordan en melding M krypteres og sendes fra A og til B, som så dekrypterer meldingen. Asymmetrisk kryptering med A sitt nøkkelpar skal benyttes.
N: Beskriv korleis ei melding M blir kryptert og blir send frå A og til B, som så dekrypterer meldinga. Asymmetrisk kryptering med A sitt nøkkelpar skal nyttast.

4.4 E: If a company with offices in multiple geographical locations around the world wants to create a Virtual Private Network (VPN) over the existing public Internet, what is the security protocol involved?
B: Hvis et selskap med kontorer på flere geografiske steder rundt om i verden ønsker å opprette et virtuelt privat nett (VPN) over det eksisterende offentlige Internett, hvilken sikkerhetsprotokoll er involvert i å realisere dette?
N: Viss eit selskap med kontor på fleire geografiske stader rundt om i verda ønsker å oppretta eit virtuelt privat nett (VPN) over det eksisterande offentlege Internettet, kva for ein sikkerhetsprotokoll er involvert i å realisera dette?

4.5 E: Three categories of firewalls are given in the curriculum: “Traditional packet filters”, “Stateful packet filters”, and “Application gateways”. Give short explanations of the functionality of each of these, with special attention to the differences between them.
B: Tre kategorier av brannmurer er gitt i pensum: “Traditional packet filters”, “Stateful packet filters”, og “Application gateways”. Gi korte forklaringer av funksjonaliteten til hver av disse, med spesiell fokus på forskjellene mellom dem.
N: Tre kategoriar av brannmurar er gitte i pensum: “Traditional packet filters”, “Stateful packet filters”, og “Application gateways”. Gi korte forklaringar av funksjonaliteten til kvar av desse, med spesiell fokus på skilnadene mellom dei.

5. Wireshark (4+4+4+4+4 = 20 points)

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	192.168.10.135	80.232.110.250		78	49279 > https(443) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=924892603
2	0.006918	80.232.110.250	192.168.10.135		74	https(443) > 49279 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK
3	0.006952	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=924892608 TSecr=171
4	0.007724	192.168.10.135	80.232.110.250		292	Client Hello
5	0.018918	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=1 Ack=227 Win=66560 Len=1448 TSval=171904247 TSec
6	0.018919	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=1449 Ack=227 Win=66560 Len=1448 TSval=171904247 T
7	0.018921	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=2897 Ack=227 Win=66560 Len=1448 TSval=171904247 T
8	0.018922	80.232.110.250	192.168.10.135		1288	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
9	0.018960	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=227 Ack=2897 Win=128864 Len=0 TSval=924892619 TSe
10	0.018962	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=227 Ack=5567 Win=126176 Len=0 TSval=924892619 TSe
11	0.019000	192.168.10.135	80.232.110.250		66	[TCP Window Update] 49279 > https(443) [ACK] Seq=227 Ack=5567 Win=131072 Len=0
12	0.547766	192.168.10.135	80.232.110.250		141	Client Key Exchange
13	0.547770	192.168.10.135	80.232.110.250		72	Change Cipher Spec
14	0.547771	192.168.10.135	80.232.110.250		167	Encrypted Handshake Message
15	0.557383	80.232.110.250	192.168.10.135		66	https(443) > 49279 [ACK] Seq=5567 Ack=409 Win=66304 Len=0 TSval=171904301 TSec
16	0.559636	80.232.110.250	192.168.10.135		173	Change Cipher Spec, Encrypted Handshake Message
17	0.559687	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=409 Ack=5674 Win=130944 Len=0 TSval=924893125 TSe
18	0.659774	192.168.10.135	80.232.110.250		615	Application Data
19	0.674109	80.232.110.250	192.168.10.135		967	Application Data
20	0.674138	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=958 Ack=6575 Win=130144 Len=0 TSval=924893230 TSe
21	13.888212	192.168.10.135	80.232.110.250		66	49279 > https(443) [FIN, ACK] Seq=958 Ack=6575 Win=131072 Len=0 TSval=924906288
22	13.894695	80.232.110.250	192.168.10.135		66	https(443) > 49279 [FIN, ACK] Seq=6575 Ack=959 Win=65792 Len=0 TSval=171905635
23	13.894745	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=959 Ack=6576 Win=131072 Len=0 TSval=924906293 TSe

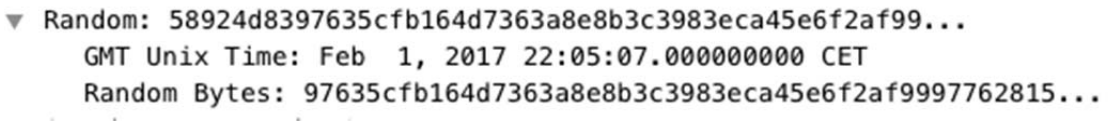
? (5.1)

Figure 2: Data from Wireshark

5.1 E: Enter the correct protocol in the protocol column for each package.
B: Angi riktig protokoll i protokollkolonnen for hver enkelt pakke.
N: Angi riktig protokoll i protokollkolonnen for kvar enkelt pakke.

5.2 E: What does the packet sequence represent?
B: Hva representerer pakkesekvensen?
N: Kva representerer pakkesekvensen?

5.3 E: Package No 4 / Client hello includes a random field, Random, with a random number (nonce = number used once). What two functions does this protocol field have?
B: Pakke No 4/Client hello, inkluderer et protokollfelt, Random, med en vilkårlig verdi («nonce = number used once»). Hvilke to funksjoner har dette protokollfeltet?
N: Pakke No 4/Client hello, inkluderer eit protokollfelt, Random, med ein vilkårleg verdi («nonce = number used once»). Kva for to funksjonar har dette protokollfeltet?



5.4 E: How is the algorithm to be used to encrypt user data decided?
B: Hvordan bestemmes hvilken algoritme som skal benyttes for å kryptere brukerdata?
N: Korleis vert det avgjort kva for ei algoritme som skal nyttast for å kryptera brukardata?

5.5 E: Which packages contain user data that is encrypted?
B: Hvilke pakker inneholder brukerdata som er kryptert?
N: Kva for pakkar inneheld brukardata som er kryptert?