



DAT204 Exam h2018

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

☒

DAT204-G, general information

Emnekode: DAT204

Emnenavn: Datakommunikasjon

Dato: 19.12.2018

Varighet: 3 timer

Tillatte hjelpemidler: Kalkulator

Merknader: Eksamen er både på engelsk og norsk (med noen overskrifter og uttrykk på engelsk). Hver korrekt besvart oppgave gir fra 2 til 16 poeng, totalt 100 poeng. For hver del av en oppgave:

- Korrekt svar gir 0,25 - 2 poeng for hvert spørsmål, avhengig av vanskelighetsgrad.
- Feil svar gir 0 poeng for alle spørsmål, unntatt flersvarsoppgavene.
- Feil svar i flersvarsoppgavene gir en negativ poengsum, slik at klikker du på alle valgmulighetene i oppgaven vil summen bli 0 poeng. En negativ poengsum er ikke mulig.

Eksamen inneholder oppgaver av typen flervalg, flersvar, nedtrekksmeny, fast tekst og beregning. Det finnes et åpent tekstfelt på den siste siden som kan brukes til å skrive ytterligere kommentarer og antagelser til oppgavene til eksamenen. Dette tekstfeltet gir ingen poeng i seg selv, men det kan påvirke vurderingen av kommenterte oppgaver. Det er ikke nødvendig å bruke tekstfeltet, siden riktig svar på alle spørsmålene vil gi full score. Hvis spørsmålet ikke er riktig, kan du få flere poeng hvis du forklarer en delvis korrekt løsning eller gir en god antagelse i tekstfeltet.

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

Tillater du at din eksamensbesvarelse blir brukt til slikt formål?

- ☐ Ja
- ☐ Nei

1 Wireshark HTTP

PDF-dokumentet viser to utdrag fra en Wireshark-fangst. Begge utdragene er fra den samme TCP forbindelsen og viser starten og slutten av en økt. Svar på følgende spørsmål: (16 poeng)

Hvilken linklagsprotokoll brukes her? (DHCP, SSL, UDP, IEEE 802.11, ARP, Ethernet, HTTP, IP, TCP)

Hvilken protokoll er innkapslet i linklagsrammen? (SMTP, ARP, IPv4, HTTP, UDP, TCP, SSL, Ethernet, IPv6, DHCP, IEEE 802.11)

Hvor stor er den annonserte vindustørrelsen i antall byte i pakken 129? (67179, 257, 5155, 256, 438, 65792)

Hva slags vindu er dette? (Metningsvindu ("congestion window"), Vindustørrelsen på brukergrensesnittet, Mottakervindu, Glidende vindu i antall pakker)

Hvilken fase av en TCP forbindelse tilhører pakker 126 - 131? (Forbindelse, Frakobling, Dataoverføring, Treveis håndtrykk, Lytt til nye forbindelser (LISTEN))

Hvilken applikasjonslagsprotokoll brukes her? (DHCP, ARP, IPv4, HTTP, Ethernet, UDP, IPv6, TCP)

Hvem sender pakke 129? (Serveren, Ingen, Klienten)

Hva er det velkjente portnummeret til servere som kjører applikasjonslagsprotokollen som benyttes her?

Hvilken type forbindelse bruker applikasjonslagsprotokollen? (Tidsstyrt forbindelse, Vedvarende forbindelse, Ikke-vedvarende forbindelse, Engangs forbindelse)

Applikasjonslagsprotokollen i bruk her benytter informasjonskapsler ("cookies"). Men hva er en "cookie"? (Det er en liste over tidligere åpnete nettsteder., Det er en liten tekstfil som er sendt fra et nettsted og lagret på klientens slutt-system., Det er en cache for tidligere nedlastede nettsideobjekter., Det er en fil som lagrer server autentiseringsdata.)

Er "cookie" informasjon utvekslet i pakke 129? (Nei, Ja)

Hvor mange bytes med applikasjonsdata er sendt med pakke 129?

Hvor mange rutere kan pakken 129 passere før den blir forkastet?

Hvem initierer avslutning av denne TCP forbindelsen? (Ingen, Klienten, Serveren)

Hvor mange bytes med applikasjonsdata har blitt overført i løpet av denne TCP sesjonen?

Klienten har sendt: Serveren har sendt:

Maks poeng: 16

2 E-mail

Svar på spørsmålene nedenfor angående elektronisk post: (4 poeng)

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr ... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Hvilken protokoll er vist i eksemplet ovenfor og ansett som hjertet av Internett elektronisk post?

Velg ett alternativ:

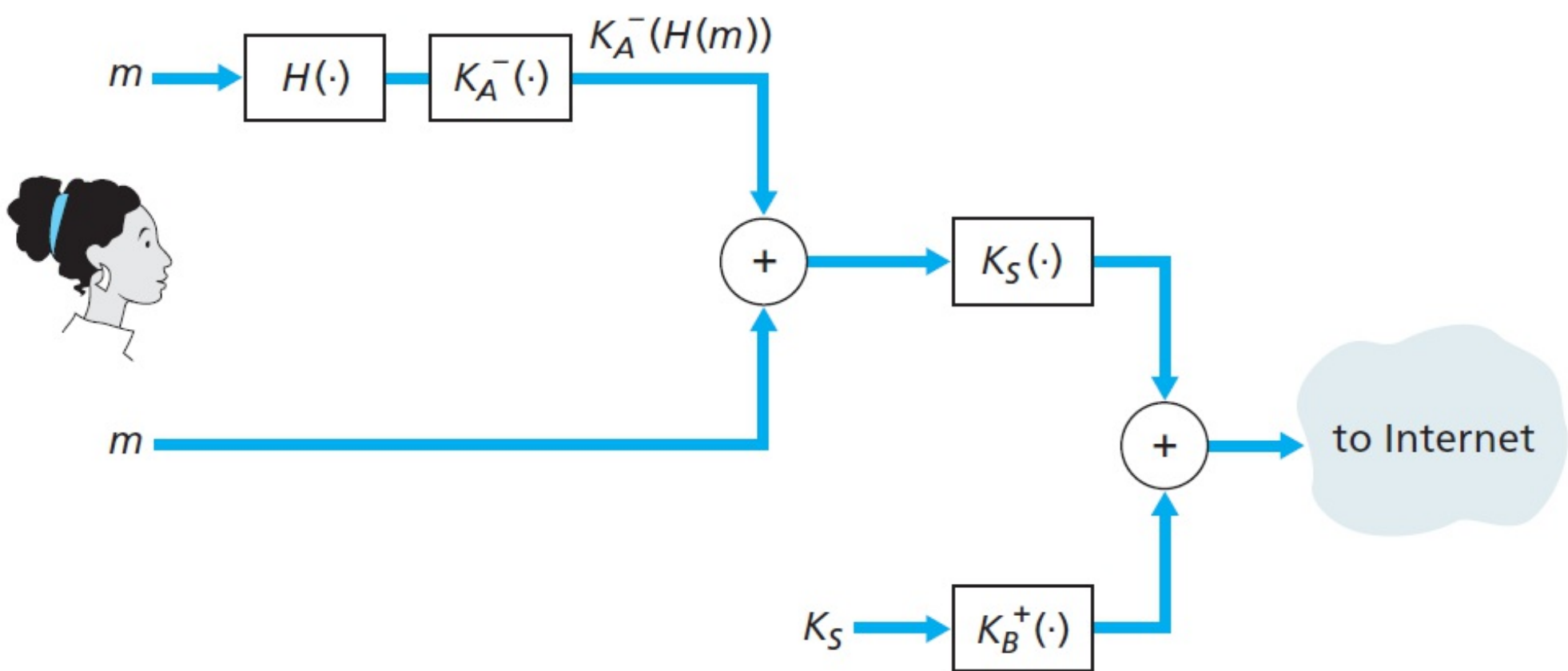
- ☐ SMTP
- ☐ HTML
- ☐ POP3
- ☐ IMAP
- ☐ HTTP

Hvilke av de følgende protokollene er definert som e-post tilgangsprotokoller?

Velg ett eller flere alternativer:

- ☐ HTTP
- ☐ POP3
- ☐ SNMP
- ☐ IMAP
- ☐ SMTP

Hvilken protokoll er illustrert i figuren under og betraktet som de-facto standard e-post krypteringsmetode?



Velg ett alternativ:

- ☐ MIME (Multipurpose Internet Mail Extension)
- ☐ DSA (Digital Signature Algorithm)
- ☐ RSA (Rivest, Shamir, Adelman)
- ☐ PGP (Pretty Good Privacy)
- ☐ TLS (Transport Layer Security)

Maks poeng: 4

3 DHCP

Nedenfor er noen uttalelser om DHCP og hvordan den fungerer. (3 poeng)

Velg riktige alternativer:

- ☐ DHCP gir IP-adresser til TLD DNS-servere.
- ☐ DHCP gir LAN nettverksmaske.
- ☐ DHCP gir IP-adresser til root DNS servere.
- ☐ DHCP gir IP-adresse til nærmeste svitsj.
- ☐ DHCP gir IP-adresser til lokale DNS servere.
- ☐ DHCP gir ISP nettverksmaske.
- ☐ DHCP er en applikasjonslagsprotokoll.
- ☐ DHCP gir IP-adresse til gateway (nærmeste ruter).
- ☐ DHCP er en nettverkslagprotokoll.
- ☐ DHCP tillater en vert å skaffe en IP-adresse automatisk.
- ☐ DHCP tillater en vert å skaffe en MAC-adresse automatisk.
- ☐ DHCP er en klient-server protokoll

Maks poeng: 3

4 **TCP/UDP sockets**

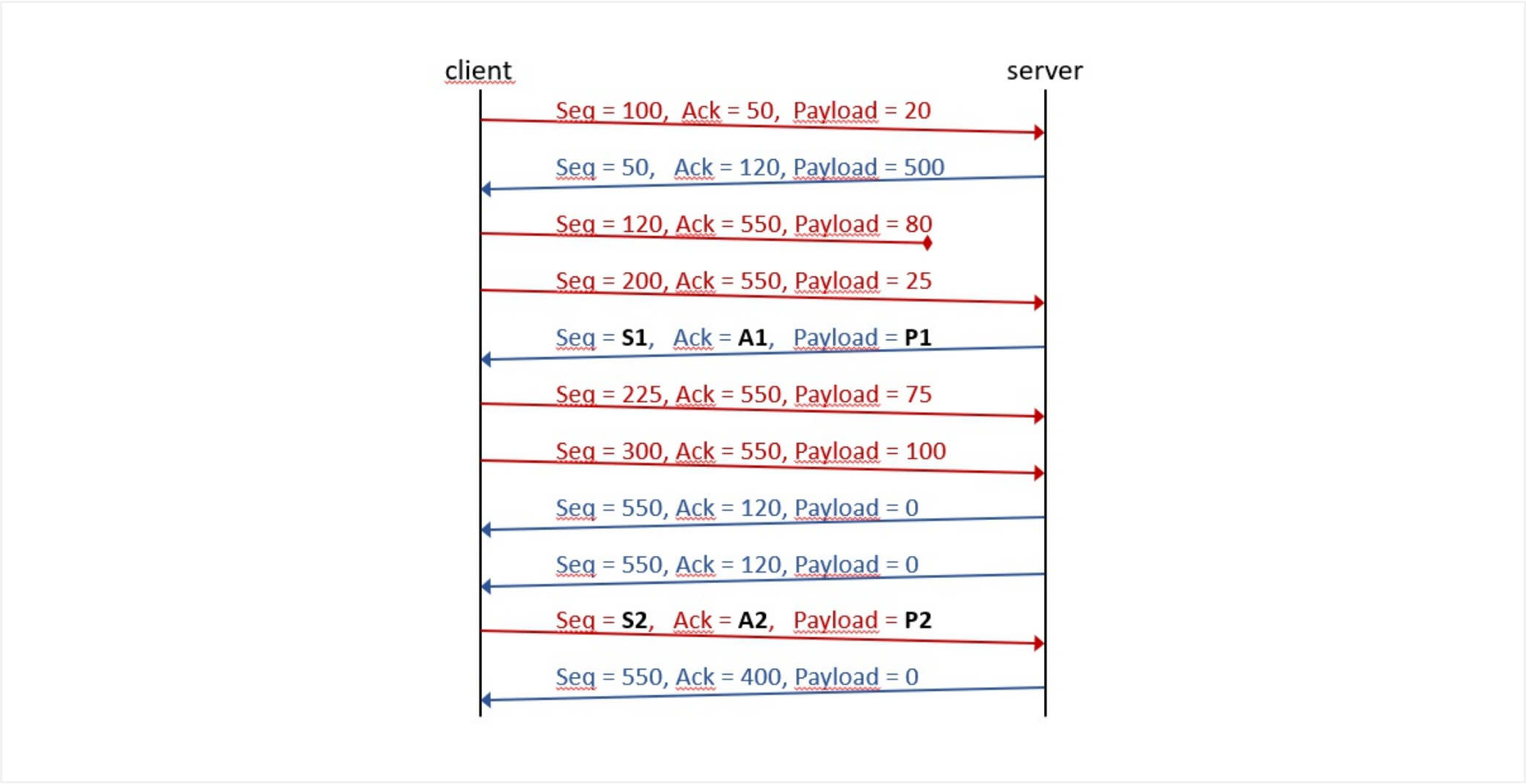
Hvilken påstand om TCP versus UDP sockets er riktig? (3 poeng)

Velg ett alternativ:

- ☐ En UDP socket er identifisert ved hjelp av sender og mottakers IP-adresser samt sender og mottakers port nummer.
- ☐ TCP trafikk fra forskjellige klienter til den samme applikasjonen bruker en felles socket fra forbindelsen blir satt opp til den tas ned og skiller mellom sender og mottaker IP-adresse samt sender og mottaker port nummer.
- ☐ TCP bruker to sockets for å opprette en forbindelse, en som mottar oppkoblingsforespørsler og en for datautveksling.
- ☐ En UDP socket er identifisert ved hjelp av senderens port og IP-adresse.

Maks poeng: 3

5 TCP sequence



Ovenfor er et utdrag av en TCP (Reno versjon) overføring. Hva vil sekvensnummeret, bekræftelsesnummeret og nyttelastlengden benevnt **S1**, **A1**, **P1**, **S2**, **A2** og **P2** være i segmentene vist på figuren? (6 poeng)

S1= A1= P1=

S2= A2= P2=

Den tredje meldingen går tapt et sted i nettverket på sin vei til serveren. Hvordan sikrer TCP at denne meldingen blir levert som vist i utdraget over?

(Det er opp til applikasjonslaget å sende den tapte meldingen på nytt., Meldingen sendes på nytt ved tidsavbrudd., Meldingen sendes på nytt etter å ha mottatt trippel duplikat ACK., Linklaget vil sikre pålitelig dataoverføring i dette tilfellet.)

TCP har også en re-transmisjonstimer. Hva skjer når denne timeren utløper?

(Ved tidsavbrudd tas forbindelsen ned., Ved tidsavbrudd sendes kun det segmentet som forårsaket tidsavbruddet på nytt., Ved tidsavbrudd sendes alle ubekreftede segmenter på nytt.)

Maks poeng: 6

6 **TCP and UDP statements**

Hvilke av påstandene angående TCP og UDP er riktige? (4 poeng)

Velg ett eller flere alternativer:

- ☐ UDP flytkontroll sikrer at mottakeren ikke oversvømmes.
- ☐ UDP tilbyr kun en upålitelig dataoverføringstjeneste over et upålitelig internett.
- ☐ For en TCP forbindelse kan antallet ubekreftede bytes ikke være større enn mottakerens annonserte vindusstørrelse.
- ☐ TCP header parameter "Window size" er del av TCP metningskontroll algoritme.
- ☐ UDP segmenter med feil sjekk sum blir forkastet og sendt på nytt når rundturtiden (RTT) er utløpt.
- ☐ TCP har ingen flytkontroll mekanisme.
- ☐ TCP tilbyr en pålitelig dataoverføringstjeneste over et upålitelig internett.
- ☐ Når UDP brukes, må eventuell feilkorleksjon gjøres i applikasjonen.

Maks poeng: 4

7 **TCP congestion handling**

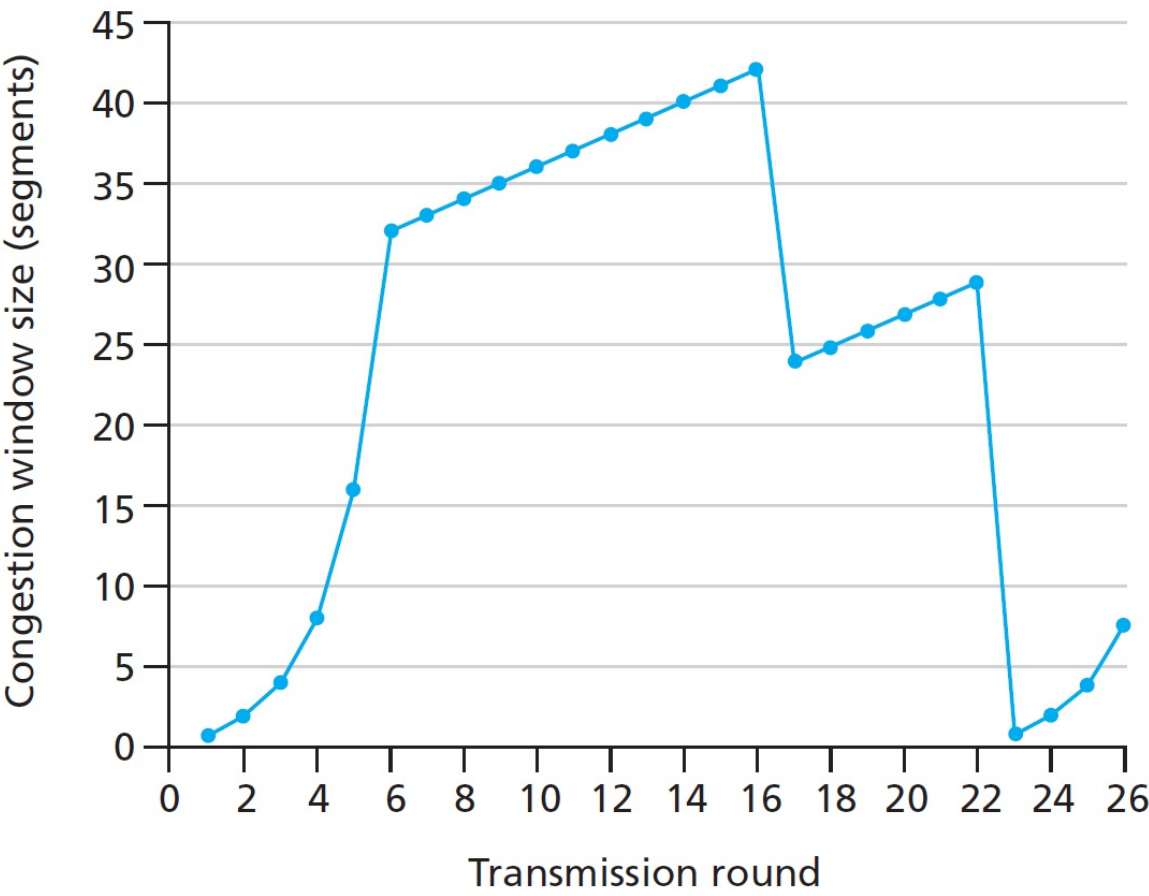
Nedenfor er noen påstander om hvordan TCP protokollen fungerer. Velg riktig påstand. (2 poeng)

Velg ett alternativ:

- ☐ "Congestion avoidance" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker lineært.
- ☐ "Fast recovery" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker eksponensielt raskt.
- ☐ "Congestion avoidance" er relatert til "Receive window" i TCP headeren.
- ☐ TCP tidsavbrudd trigger "fast recovery".

Maks poeng: 2

8 TCP congestion window



Figuren viser størrelsen på TCP Reno sitt metningsvindu (congestion window) i antall segmenter som en funksjon av overføringsrunden. Svar på følgende spørsmål: (5 poeng)

Identifiser et intervall der TCP slow start fungerer. ([17,22], [1,6], [16,17], [22,23], [6,16])

Hvordan er segmenttap identifisert etter den 16. overføringsrunden?

(Trippel duplikat ACK, Explicit Congestion Notification (ECN), RM celle med Congestion Indication (CI), Tidsavbrudd på ACK)

Hvordan er segmenttap identifisert etter den 22. overføringsrunden?

(Trippel duplikat ACK, RM celle med Congestion Indication (CI), Explicit Congestion Notification (ECN), Tidsavbrudd på ACK)

Hva er slow-start terskelen ved den 24. overføringsrunden?

Anta at Maximum Segment Size (MSS) er 1460 bytes og rundturtiden RTT=200 millisekunder, hva er gjennomsnittelig båndbredde i Mbits/s benyttet av TCP forbindelsen i overføringsintervallet [6,16]?

Maks poeng: 5

9 Binary to IP

IP-adressen 01101001.00010000.01010000.10101011 kan skrives på punktum desimalform som: (2 poeng)

.

.

.

Maks poeng: 2

10

IP and subnet

Anta at en ISP eier adresseblokken på formatet 105.16.80.0/23. Anta at den vil skape åtte subnett fra denne blokken, hvor hver blokk har samme antall IP-adresser. (6,5 poeng)

Hva er prefiksene (på formatet a.b.c.d/x) for de åtte subnettene i stigende rekkefølge?

Subnett 1: 105.16../

Subnett 2: 105.16../

Subnett 3: 105.16../

Subnett 4: 105.16../

Subnett 5: 105.16../

Subnett 6: 105.16../

Subnett 7: 105.16../

Subnett 8: 105.16../

Hvor mange bits utgjør vertsdelen av prefiksene som er opprettet for de åtte subnettene?

Hvor mange verter kan tildeles en IP-adresse innenfor hvert av de åtte subnettene?

Maks poeng: 6.5

11

Routers and SDN

I de senere årene, har Software-Defined Networking (SDN) fått økende interesse. Nedenfor er noen uttalelser angående tradisjonelle rutere og SDN. (3 poeng)

Velg riktige alternativer:

- ☐ SDN pakkesvitsjer er kun i stand til å utføre destinasjonsbasert videresending.
- ☐ Med tradisjonelle rutere håndteres både videresending og ruting funksjonen (kontroll, kommunikasjon, beregning av videresendingstabeller) per-ruter.
- ☐ Tradisjonelle rutere utfører videresending ved å matche flere felter i linklagets, nettverkslagets og transportlagets headere mot deres respektive videresendingstabell.
- ☐ Med SDN håndteres både videresending og ruting funksjonen (kontroll, kommunikasjon, beregning av flyt tabeller) av et sentralisert miljø.
- ☐ SDN pakkesvitsjer kan utføre videresending ved å matche flere felter i linklagets, nettverkslagets og transportlagets headere mot deres respektive flyt tabell.
- ☐ Tradisjonelle rutere utfører destinasjonsbasert videresending ved å matche destinasjonens IP-adresse mot deres respektive videresendingstabell.

Maks poeng: 3

12 **Routing tables**

I denne oppgaven er målet å bestemme den riktige videresendingslinken gitt ruting tabellen nedenfor. (5 poeng)

En ruter har følgende oppføringer i sin videresendingstabell:

- Link1: 00001010.10101000.00000100.00000000/22
- Link2: 00001010.10101000.00000110.00000000/23
- Link3: 00001010.10101000.00000111.00000000/24
- Link4: 00001010.10101000.00000000.00000000/16
- Link5: Alle andre adresser

Anat at ruteren mottar datagramer med følgende destinasjonsadresser og bestem hvilken link de skal videresendes til:

- A: 00001010.10101000.00000111.11111110
- B: 00001010.10101000.00000011.00000000
- C: 00001010.10101000.00000111.00000001
- D: 00001010.10101000.00000110.10000000
- E: 00001010.10111000.00000101.00000000

På hvilken link vil de bli videresendt?

A: link

B: link

C: link

D: link

E: link

Maks poeng: 5

13 **Routing protocols**

Nedenfor er noen spørsmål om klasser av ruting protokoller og hvordan de opererer. Fyll inn riktig uttrykk i setningene under og svar på spørsmålene: (4,5 poeng)

Dijkstra's korteste vei algoritme er mye brukt med (distance-vector (DV), traffic-control (TC), link-utilization (LU), link-state (LS)) ruting protokoller. Hvilke utsagn passer til en ruter som kjører denne klassen av ruting protokoller?

Velg ett eller flere alternativer:

- ☐ Ruterer kjemmer bare fysisk tilkoblete naboer.
- ☐ Ruterer kan kjøre OSPF.
- ☐ Ruterer kan kjøre RIP.
- ☐ Ruterer er avhengig av at direkte tilknyttede naboer annonserer sine vektortabeller for å kunne oppdatere sin egen rutingtabell.
- ☐ Ruterer kjemmer kun avstand til fysisk tilkoblete naboer.
- ☐ Ruterer har fullstendig informasjon om alle link kostnader innenfor sitt autonome system.
- ☐ Ruterer har fullstendig informasjon om alle link kostnader i hele Internettet.
- ☐ Ruterer har fullstendig topologi over alle andre rutere i hele Internettet.
- ☐ Ruterer har fullstendig topologi over alle andre rutere innenfor sitt autonome system.

Bellman-Ford ligningen er mye brukt med (distance-vector (DV), link-state (LS), link-utilization (LU), traffic-control (TC)) ruting protokoller. Hvilke utsagn passer til en ruter som kjører denne klassen av ruting protokoller?

Velg ett eller flere alternativer:

- ☐ Ruterer har fullstendig topologi over alle andre rutere i hele Internettet
- ☐ Ruterer har fullstendig topologi over alle andre rutere innenfor sitt autonome system.
- ☐ Ruterer kjemmer bare fysisk tilkoblete naboer.
- ☐ Ruterer kan kjøre RIP.
- ☐ Ruterer kan kjøre OSPF.
- ☐ Ruterer er avhengig av at direkte tilknyttede naboer annonserer sine vektortabeller for å kunne oppdatere sin egen rutingtabell.
- ☐ Ruterer kjemmer kun avstand til fysisk tilkoblete naboer.
- ☐ Ruterer har fullstendig informasjon om alle link kostnader innenfor sitt autonome system.
- ☐ Ruterer har fullstendig informasjon om alle link kostnader i hele Internettet.

Maks poeng: 4.5

14 **Link layer**

Nedenfor er noen generelle uttalelser om hvordan linklaget fungerer. Velg riktig alternativer. (3 poeng)

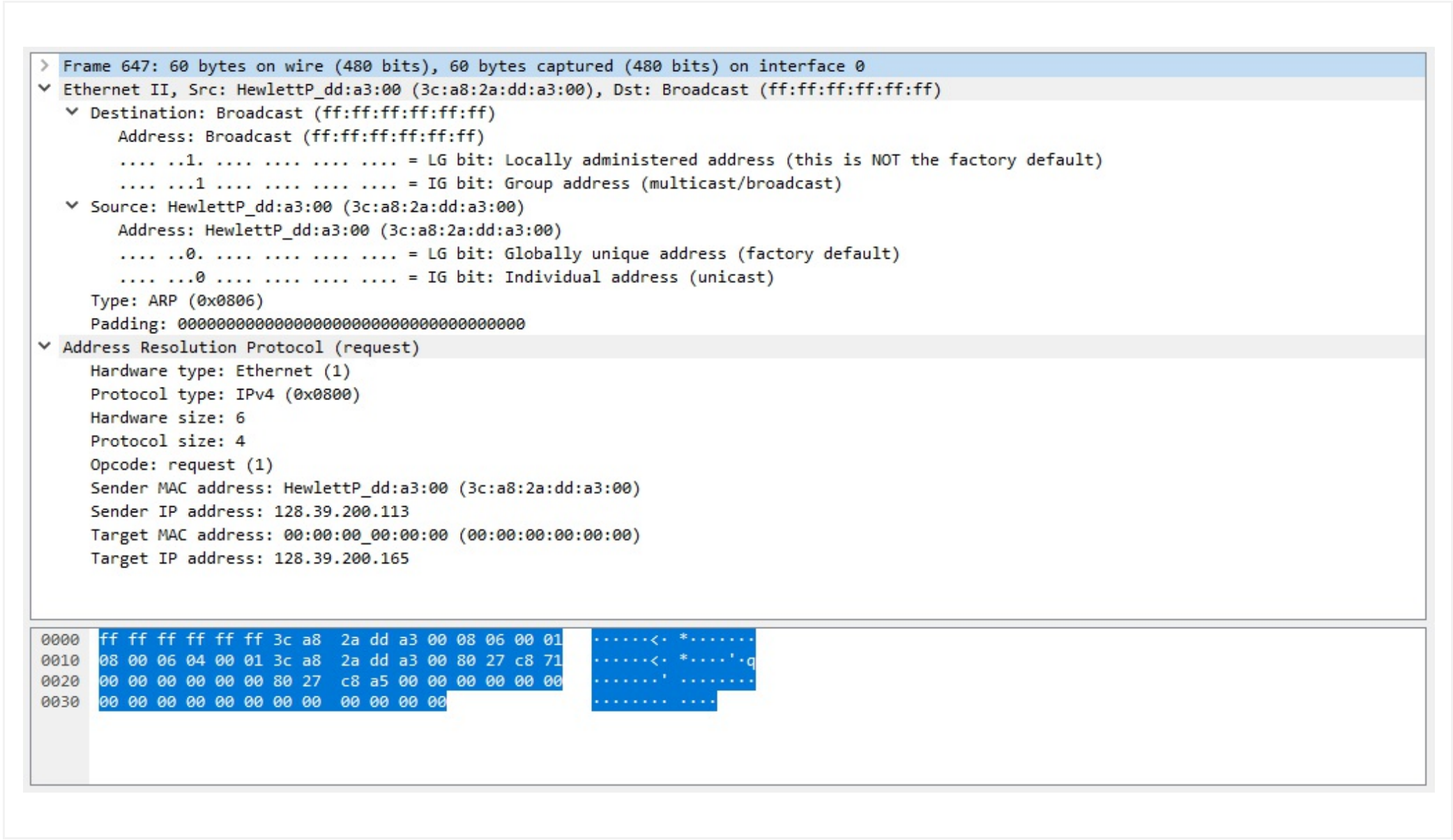
Velg ett eller flere alternativer:

- ☐ Linklaget utfører innramming av datagramer.
- ☐ Linklaget er det stedet i protokollstakken hvor software møter hardware.
- ☐ Linklaget kan ikke tilby noen form for pålitelig dataoverføring.
- ☐ Linklaget er kun implementert i hardware.
- ☐ Linklaget utfører feildeteksjon.
- ☐ Linklaget er implementert kun i software.

Maks poeng: 3

15

ARP



Se gjennom Wireshark-fangsten ovenfor og vurder påstandene nedenfor angående Address Resolution Protocol (ARP). (3 poeng)

Velg ett eller flere alternativer:

- ☐ ARP er en protokoll som ligger et sted mellom nettverkslaget og linklaget i Internett protokollstakken.
- ☐ Verter og rutere bruker ARP til å knytte en IP-adresse til en MAC-adresse og vedlikeholde en ARP-tabell i sitt minne.
- ☐ ARP svar bruker alltid kringkastingsadressen som destinasjons adresse.
- ☐ Vert med IP-adresse 128.39.200.113 har MAC-adresse 3c:a8:2a:dd:a3:00.
- ☐ ARP forespørsler ender opp hos en DHCP server som tilordner en MAC-adresse til den spørrende verten.
- ☐ ARP kringkastingsadresse er 00:00:00:00:00:00.

Maks poeng: 3

16 Ethernet LAN

Ethernet er den mest brukte teknologien for kablede Local Area Network (LAN). Svar på følgende spørsmål: (3 poeng)

Hvilke IEEE standarder spesifiserer kablet Ethernet? (802.5, 802.11, 802.13, 802.3)

Hvilken kablet LAN topologi er den aller mest vanligste i dag?

(Buss med alle noder i samme kollisjons-domene.,
Stjerne med punkt-til-punkt linker og svitsj i midten., Ring med token passering.)

Hvilken kabel type er mest vanlig i LAN i dag? (To-parkabel, Fiberoptisk kabel, Tvunnet parkabel, Koaksialkabel).

Maks poeng: 3

17 Ethernet switch

Hvilke av de følgende utsagn om Ethernet svitsjer er riktige? (3 poeng)

Velg ett eller flere alternativer:

- ☐ Svitsjer videresender rammer basert på destinasjonens MAC-adresse.
- ☐ Svitsjer er enkle, raske og relativt billige.
- ☐ Svitsjer videresender rammer basert på destinasjonens IP-adresse.
- ☐ Svitsjer må få sine svitsjetabeller konfigurert av nettverksadministrator.
- ☐ Svitsjer må vedlikeholde sine svitsjetabeller på egenhånd.
- ☐ Svitsjer er komplekse, raske og ganske kostbare.

Maks poeng: 3

18

Wireless concepts

Nedenfor er noen generelle utsagn om trådløs overføring, samt noen mer konkrete utsagn om hvordan IEEE 802.11 trådløse LAN fungerer. (6 poeng)

Fyll inn det korrekte uttrykket i hver setning:

I (ad-hoc modus, rate tilpasning, signal svekking (path loss), interferens, flerveisinterferens (multipath propagation), infrastrukturmodus, beacon rammer) er hver trådløs vert tilkoblet Internettet via et tilgangspunkt (aksesspunkt).

I (flerveisinterferens (multipath propagation), interferens, signal svekking (path loss), beacon rammer, infrastrukturmodus, rate tilpasning, ad-hoc modus) må de trådløse vertene selv sørge for ruting, tildeling av adresser og DNS.

Trådløse stasjoner oppdager og identifiserer tilgangspunktet (aksesspunktet) ved hjelp av (signal svekking (path loss), flerveisinterferens (multipath propagation), ad-hoc modus, beacon rammer, rate tilpasning, interferens, infrastrukturmodus).

Demping av det trådløse signalet når det forplanter seg gjennom materie kalles (signal svekking (path loss), infrastrukturmodus, interferens, ad-hoc modus, rate tilpasning, beacon rammer, flerveisinterferens (multipath propagation)).

Når to eller flere kilder innenfor et "basic service set" (BSS) sender samtidig på den samme frekvensen så kan (infrastrukturmodus, signal svekking (path loss), ad-hoc modus, flerveisinterferens (multipath propagation), beacon rammer, rate tilpasning, interferens) oppstå.

Utflyting i mottatt signal på grunn av flere refleksjoner av den elektromagnetiske bølgen fra objekter og bakken kalles (interferens, signal svekking (path loss), rate tilpasning, beacon rammer, flerveisinterferens (multipath propagation), infrastrukturmodus, ad-hoc modus).

Maks poeng: 6

19

SSL nonces

Hva er hensikten med med nonces i SSL/TLS? (2 poeng)

Velg ett alternativ:

- ☐ Beskytte mot Denial-of-Service angrep
- ☐ Beskytte mot "replay" angrep
- ☐ Beskytte mot "man-in-the-middle" angrep
- ☐ Data autentisering
- ☐ Beskytte mot "known plaintext" angrep
- ☐ Beskytte mot "chosen plaintext" angrep

Maks poeng: 2

20

SSL certificate and cryptographic algorithms

Nedenfor er noen uttalelser angående digitale sertifikater og kryptografiske algoritmer som brukes av SSL sockets i typiske klient/server sesjoner. (7 poeng)

Fyll inn det riktige uttrykket i hver setning:

I typiske klient/server sesjoner, SSL bruker et digitalt sertifikat for å

- (tillate lovlig sending av meldinger, autentisere serveren, autorisere klienten for kommunikasjon med serveren, skape signaturer for meldingene) og til å
- (kryptere master secret med CA offentlig nøkkel, kryptere master secret med serverens offentlige nøkkel, utveksle et signert avtrykk (hash value) av master secret, kryptere master secret med serverens private nøkkel).

SSL sockets vil typisk utveksle applikasjonsmeldinger kryptert med en

(symmetrisk-nøkkel blokk chiffer, offentlig-nøkkel chiffer, asymmetrisk-nøkkel blokk chiffer, kryptografisk avtrykk (hash) algoritme). (MD5, RSA, AES, SHA) er et eksempel på en slik algoritme.

For å sikre at en melding ikke blir endret, vil SSL vanligvis bruke en (symmetrisk-nøkkel blokk chiffer, asymmetrisk-nøkkel blokk chiffer, offentlig-nøkkel chiffer, kryptografisk hash algoritme) til å lage et avtrykk av meldingen. (RSA, SHA, 3DES, AES) er et eksempel på en slik algoritme.

Ved å inkludere en autentiseringsnøkkel til avtrykket, blir en (digital signature, Message Authentication Code (MAC), godkjenningsskode, Certified Message Code (CMC)) laget og utvekslet sammen med den krypterte meldingen.

Maks poeng: 7

21

SSL statements

Nedenfor er noen påstander om SSL protokollen. Hva er riktig utsagn om SSL? (2 poeng)

Velg ett alternativ:

- ☐ SSL bruker alltid AES etter håndtrykksfasen.
- ☐ SSL forbindelser kobles ned ved å avslutte transportlagets tilkobling.
- ☐ SSL implementerer sekvensnummer i klartekst i SSL records.
- ☐ SSL forhandler chiffer suite i løpet av håndtrykksfasen.

Maks poeng: 2

22 **SSL quality of service**

Nedenfor er noen spørsmål om SSL sockets og tjenestekvaliteter: (7 poeng)

Hvilken socket type forbedrer Secure Socket Layer (SSL) med sikkerhetstjenester?

Velg ett alternativ:

- ☐ HTTP
- ☐ IPv6
- ☐ IPv4
- ☐ TCP
- ☐ UDP

Hva heter den oppdaterte, sikrere og i dag mest brukte versjonen av SSL protokollen?

Velg ett alternativ:

- ☐ Network Layer Security (NLS)
- ☐ Application Layer Security (ALS)
- ☐ Link Layer Security (LLS)
- ☐ Transport Layer Security (TLS)

Hvilke servicegarantier gir SSL sockets?

Velg ett eller flere alternativer:

- ☐ I rekkefølge data levering
- ☐ Avgrenset forsinkelse
- ☐ Server autentisering
- ☐ Garantert båndbredde
- ☐ Applikasjonsprogram troverdighet
- ☐ Data konfidensialitet
- ☐ Pålitelig data overføring
- ☐ Data integritet

Maks poeng: 7

23

Comments and assumptions

Her kan du skrive antagelser, avklaringer og kommentarer til svarene dine. Disse kommentarene gir ikke flere poeng i seg selv, men kan påvirke vurderingen av kommenterte oppgaver. (maks 500 ord)

Skriv antagelser og kommentarer til oppgavene her:

Format

B


I


U


x_2


x^2


I_x
































Words: 0

Maks poeng: 0

18/18

Lastet ned av Dragondagger superpoison (gogdds778@gmail.com)

Question 1

Attached



Start of session:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	128.39.200.255	85.165.93.169	TCP	66	60466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.013867	85.165.93.169	128.39.200.255	TCP	66	80 → 60466 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
3	0.013990	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
4	0.014379	128.39.200.255	85.165.93.169	HTTP	454	GET / HTTP/1.1
5	0.027949	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [ACK] Seq=1 Ack=401 Win=30336 Len=0
6	0.029970	85.165.93.169	128.39.200.255	TCP	329	80 → 60466 [PSH, ACK] Seq=1 Ack=401 Win=30336 Len=275 [TCP segment of a reassembled PDU]
7	0.030895	85.165.93.169	128.39.200.255	TCP	659	80 → 60466 [PSH, ACK] Seq=276 Ack=401 Win=30336 Len=605 [TCP segment of a reassembled PDU]
8	0.030896	85.165.93.169	128.39.200.255	HTTP	467	HTTP/1.1 200 OK (text/html)
9	0.030957	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=401 Ack=1294 Win=64256 Len=0
10	0.074978	128.39.200.255	85.165.93.169	HTTP	428	GET /assets/delta-vod-webapp.css.gz HTTP/1.1
11	0.091886	85.165.93.169	128.39.200.255	TCP	1454	80 → 60466 [ACK] Seq=1294 Ack=775 Win=31360 Len=1400 [TCP segment of a reassembled PDU]

<

>

> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)

> Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5a8b (23179)
> Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 128.39.200.255
Destination: 85.165.93.169

> Transmission Control Protocol, Src Port: 60466, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 60466
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window size value: 257
[Calculated window size: 65792]
[Window size scaling factor: 256]
Checksum: 0xfc8f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]

End of session:

No.	Time	Source	Destination	Protocol	Length	Info
125	5.639047	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=4279 Ack=66750 Win=64512 Len=0
126	6.609348	128.39.200.255	85.165.93.169	HTTP	492	GET /api/delta/fan/status HTTP/1.1
127	6.625013	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
128	6.671326	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=4717 Ack=67179 Win=65792 Len=0
129	7.644949	128.39.200.255	85.165.93.169	HTTP	492	GET /api/delta/fan/status HTTP/1.1
130	7.660899	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
131	7.701551	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=5155 Ack=67608 Win=65280 Len=0
132	12.583914	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [FIN, ACK] Seq=67608 Ack=5155 Win=42112 Len=0
133	12.583989	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=5155 Ack=67609 Win=65280 Len=0
134	12.757137	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [FIN, ACK] Seq=5155 Ack=67609 Win=65280 Len=0
135	12.770847	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [ACK] Seq=67609 Ack=5156 Win=42112 Len=0

>

> Frame 129: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0

> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)

> Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 478

Identification: 0x5af5 (23285)

> Flags: 0x4000, Don't fragment

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 128.39.200.255

Destination: 85.165.93.169

> Transmission Control Protocol, Src Port: 60466, Dst Port: 80, Seq: 4717, Ack: 67179, Len: 438

Source Port: 60466

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 438]

Sequence number: 4717 (relative sequence number)

[Next sequence number: 5155 (relative sequence number)]

Acknowledgment number: 67179 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 257

[Calculated window size: 65792]

[Window size scaling factor: 256]

Checksum: 0xfe45 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

> [Timestamps]

TCP payload (438 bytes)

> Hypertext Transfer Protocol

> GET /api/delta/fan/status HTTP/1.1\r\n

Host: fanctrl.andersenitc.no\r\n

Connection: keep-alive\r\n

Accept: application/json, text/plain, */*\r\n

DateX: Mon, 26 Nov 2018 08:22:35 GMT\r\n

Authorization: None\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n

Referer: http://fanctrl.andersenitc.no/\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n

\r\n