CSCI-UA.0480-062
2021 Final (100 points)
December 13, 2021

Name: ....

Student (N) Number: ....

Instructions:

1. **Indicate your name, N number, and version on top of both the bubble sheet and the question booklet.**

2. **Enter your answers into the bubble sheet you were given. There are 5 possible answers per question. There is no negative marking. There is only a single answer per question.**

3. **Please use a pencil to fill in the bubbles.**

4. **All figures are at the end of the question booklet.**

5. Use the last page if you need scratch space. If you need even more space, ask us for additional sheets.

6. Some useful conversions: 1 Gbit $= 10^9$ bits, 1 Mbit $= 10^6$ bits, 1 kbit $= 10^3$ bits

7. You should have 50 questions. Each question is worth 2 points.

8. Write down any assumptions you make while answering questions on the cover sheet.

9. Once you are done, hand in the question and answer sheets please. Please do not hand in the cheat sheet.

1. Which of these is a form of network censorship?

   A Inspecting packets from a campus network.
   B Using Tor for criminal activity on the Internet.
   C Advertising a blackhole route for some IP address prefixes.
   D Using DNS to redirect requests to a geographically close server.
   E Asking WiFi users to authenticate themselves.

2. Through adding mechanisms like parity bits, repetition bits, and checksums we can...

   A sometimes detect errors, but we can never correct them.
   B sometimes detect errors, and sometimes correct them.
   C always detect errors, and sometimes correct them.
   D sometimes detect errors, and always correct those we find.
   E always detect errors, and always correct them.

3. Which one of the following is a true statement about ALOHA?

   A ALOHA prevents all collisions.
   B ALOHA is a deterministic protocol.
   C ALOHA is a decentralized protocol.
   D ALOHA allocates different frequencies to different competing users.
   E ALOHA is used primarily on top of a wired physical layer.

4. What is the purpose of packing many voltage levels within a finite range of voltages?

   A Transmitting information without being affected by noise.
   B Encoding information in the carrier wave.
   C Errors can be detected more efficiently.
   D Reducing power consumption of the transmitter.
   E Achieving a higher bit rate by sending more bits at once.

5. What is a shortcoming of OpenFlow that led to the emergence of programmable data planes?

   A OpenFlow is designed for existing packet formats and can not flexibly adapt to new packet formats.
   B Network engineers need to manually configure OpenFlow routers, which is a laborious process.
   C OpenFlow is unable to provide the performance needed by modern switching systems.
   D OpenFlow made it more challenging for data center operators to implement routing policies.
   E Because of its circuit-driven design, OpenFlow is not able to recover from Internet link failures as easily as a distributed system.

6. Why is WiFi more conservative about avoiding collisions than Ethernet?

   A WiFi is half-duplex, it cannot "hear" and "speak" at the same time, and cannot abort a packet partway through.
   B Ethernet was created before WiFi, and we didn't know that you got higher throughput from avoiding collisions then.
   C WiFi loses more packets because a signal becomes weaker as you move farther from the access point.
   D Because WiFi signals propagate through the air, there will be more bit flips. With this, it is hard to distinguish bit flips from collisions.
   E Collisions don't happen in Ethernet, only in WiFi.

7. Which of the following statements is true?

   A Shared memory is preferable to output queueing because it needs fewer operations per tick.
   B Queues in a switch are caused because packet lookups take much longer than expected.
   C Parallel Iterative Matching finds a maximum weight matching.
   D Input queueing without virtual output queues can cause head-of-line blocking.
   E Parallel Iterative Matching requires output queuing to work.

8. The link layer provides ___ delivery and the network layer provides ___ delivery.

   A local, global
   B global, local
   C out of order, in order
   D unreliable, guaranteed
   E out of order, out of order

9. Which of the following is **not** a way to protect against DoS attacks?

    A have firewalls drop suspicious packets.
    B enlist a third party to absorb the attack.
    C implement CAPTCHAs.
    D encrypt all end-to-end communications.
    E build models of the network traffic to flag suspicious behavior.

10. Refer to Figure 2. Which subfigure depicts amplitude modulation?

    A Amplitude Modulation 5
    B Amplitude Modulation 4
    C Amplitude Modulation 2
    D Amplitude Modulation 3
    E Amplitude Modulation 1

11. In a datacenter where there are multiple leaf-to-spine paths to pick from, how is a path picked?

    A A new path is picked at random for each packet.
    B A new path is picked from available paths in round-robin order.
    C A new path is picked at random for each application.
    D A new path is picked based on queue occupancy on all paths.
    E A new path is picked at random for each flow.

12. Which of the following is a property that TLS does **not** provide?

    A resistance to tampering
    B privacy
    C authentication
    D confidentiality
    E integrity

13. The hidden terminal problem consists of two transmitters, A and B, transmitting to a shared receiver C, and...

    A A and B cannot hear each other, but C can hear both A and B
    B C is unavailable because it is processing a different message.
    C A and B can both transmit at the same time without causing a collision because of different frequencies.
    D A and B can hear each other, but do not abort messages causing collisions midway.
    E A can transmit to B but not to C.

14. Let's assume a transmitter has 5 choices for its constellation with the following bits per symbol values: 2, 3, 4, 5, and 6 and the following bit error rates for each of these bits per symbol values respectively: 0.1, 0.3, 0.4, 0.6, 0.7. What bits per symbol value should the transmitter choose?

    A 5
    B 2
    C 3
    D 6
    E 4

15. When doing input queuing at a router, we find the maximal matching solution using something like PIM instead of the maximum matching solution because...

    A It is impossible to find the maximum solution in a reasonable amount of time.
    B Maximum solutions never provide any advantage over maximal solutions.
    C Maximum solutions perform worse than maximal solutions in the context of input queuing.
    D Finding the maximum solution is too complex to do fast, and the maximal is good enough.
    E It is a traditional to use PIM in networking.

16. Which of the following is a true statement about P2P applications?

    A P2P applications are forbidden, because they are used to host illegal content.
    B In P2P applications, each participant is considered an equal and can act as both a client and a server.
    C P2P applications are typically used in data centers as opposed to the global Internet.
    D P2P applications require TCP as transport protocol because UDP does not guarantee in-order, reliable data transport.
    E In P2P applications, a centralized arbiter assigns time slots to each participants.

17. Which of the following statements is true?

    A Symmetric encryption is more secure than asymmetric encryption.
    B Symmetric encryption is less secure than asymmetric encryption.
    C Asymmetric encryption makes the sender more secure than the receiver.
    D Symmetric encryption is identical during encryption and decryption.
    E Symmetric encryption is faster than asymmetric encryption.

18. How was the Mirai botnet created?

    A Through trying different login passwords.
    B Through a fork bomb.
    C Through a SYN FLOOD attack.
    D Through a buffer overrun.
    E Through the Heartbleed vulnerability.

19. Diffie-Hellman key exchange provides:

    A Anonymity
    B Confidentiality
    C Integrity
    D Authentication
    E Forward Secrecy

20. Assume that there are N nodes in ALOHA and each node has the same non-adaptive transmission probability p (meaning the node does not change p over the duration of the protocol). If N is kept constant, and p increases, then utilization …

    A Increases
    B Decreases
    C Does not change
    D Decreases, then increases
    E Increases, then decreases

21. Assume that there are N nodes in ALOHA and each node has the same non-adaptive transmission probability p (meaning the node does not change p over the duration of the protocol). If p is kept constant, and N increases, then utilization …

    A Decreases
    B Does not change
    C Increases
    D Decreases, then increases
    E Increases, then decreases

22. Refer to Figure 1. Assume that Eve is a malicious actor with access to the network. What is the anonymity property that Tor tries to guarantee about the communication of Alice and Bob, as defined by Nick Mathewson?

    A Eve is unable to detect that Alice and/or Bob communicate with another person.
    B Eve is unable to detect that Alice occasionally communicates with Bob.
    C Eve can not read Alice's and/or Bob's messages.
    D Eve can not pretend to be either Alice or Bob.
    E Eve can not alter or drop messages sent by Alice or Bob.

23. How can Alice and Bob defend against correlation attacks when using Tor?

    A Alice and Bob use IPSec to encrypt their IP addresses.
    B Alice uses a certificate, which only Bob can decrypt.
    C Alice and Bob listen to the network traffic and try to detect when Eve is eavesdropping.
    D Alice only communicates with Bob at a specific time that is negotiated out-of-band.
    E Alice and Bob send messages of the same size and always emit messages at fixed intervals.

24. What specific technique does Tor exploit to achieve anonymity?

    A VPNs
    B IPsec
    C Relays and onion routing
    D An overlay network using BGP
    E Intra-domain routing

25. In an input-queued switch, on a particular tick, assume that input ports 1 and 2 request output port A, and input port 3 and 4 request output port B. There are no other requests. The PIM algorithm is run at this tick for 4 iterations. Which of the following is **not** a valid pairing of input and output ports once PIM is complete?

    A Input port 2 to output port A
    B Input port 1 to output port B
    C Input port 1 to output port A
    D Input port 3 to output port B
    E Input port 4 to output port B

26. The ____ attack makes a process replicate itself until you exhaust all process IDs.

   A replication flood
   B amplification
   C malformed packet
   D fork bomb
   E LAND attack

27. What does a logically centralized control plane imply **in the context of SDN**?

   A Each router has both a central CPU and a switching ASIC. The CPU makes central control decisions, whereas the switching ASIC forwards packets.
   B Network operators from a logically centralized base configure each router individually instead of letting routers compute the routes.
   C Datacenter operators can reestablish circuit-switched networks because they do not require the same level of robustness as the global Internet.
   D The hardware chip of the routers can be programmed remotely using custom instruction sets.
   E Routers no longer compute forwarding decisions. Instead decisions are automatically loaded onto routers by central servers in the network.

28. Which of the following was **not** a good reason for choosing many cheap servers over fewer costly servers when data centers were still taking off?

   A Moore's law suggests that you will have to replace your servers within a few years.
   B Many servers meant that if there was one failure, a large part of the system wouldn't go down.
   C It simplifies data center topology.
   D Many engineers are already familiar with how cheap and widely used servers work.
   E There is more support and infrastructure for more widely used servers.

29. What is the effect of the signal-to-noise ratio on the bit error rate?

    A A higher signal-to-noise ratio means a lower bit error rate.
    B Bit error rate increases as a function of the signal-to-noise ratio and then asymptotically reaches a constant value.
    C A higher signal-to-noise ratio means a higher bit error rate.
    D There is no relationship between the two.
    E Bit error rate first increases then decreases as a function of the signal-to-noise ratio.

30. Which of the following would **not** break TLS' guarantees?

    A If private keys or session keys are stolen.
    B If the certificate authority is compromised.
    C If previously hard cryptographic problems become easier.
    D If a client loses a server's public key.
    E If the certificate authority does not validate someone sufficiently.

31. What is the purpose of a DNS amplification attack?

    A to exhaust a victim's ability to process incoming network packets.
    B to target routers in a local access network.
    C to degrade the performance of a DNS server.
    D to make a DNS server unavailable.
    E to create an infinite loop in the victim's TCP stack.

32. Which of the following is encrypted when looking at a TLS packet?

    A IP addresses
    B MAC addresses
    C application headers
    D link layer checksums
    E TCP ports

33. If one wishes to completely avoid stalls during video streaming, what should one do?

    A Stream the highest quality version of the video.
    B Stream the lowest quality version of the video.
    C Stream the lowest bitrate version of the video.
    D Keep switching video streams to avoid stalls.
    E Download the entire video before playing it.

34. Dropping packets with certain keywords in the payload happens at the ___ layer, dropping packets with certain port numbers happens at the ___ layer, and advertising blackhole routes happens at the ___ layer.

    A application, transport, link
    B transport, network, link
    C application, transport, network
    D transport, transport, network
    E application, physical, network

35. Which of these is **not** a property of the modern BitTorrent protocol?

    A When downloading a file, BitTorrent acquires the rarest chunk first, meaning the chunk that is hosted by the least number of users.
    B BitTorrent opens multiple connections at once to accelerate file downloads.
    C BitTorrent uses LEDBAT instead of TCP to avoid congesting the Internet.
    D BitTorrent is a P2P protocol.
    E BitTorrent exploits caching and content distribution networks to accelerate file downloads.

36. Which of the following proposals is **not** a viable design for the stored-video streaming problem?

    A Pick the highest video quality that the client can support.
    B Store the video on a file server and make the download available to the client.
    C Send the video to the client chunk by chunk. The client downloads each chunk individually.
    D Send only intra-coded frames periodically; then the client reconstructs the highest-quality video.
    E Pick the highest video quality that the client can support and lower the quality in the case of a rebuffering event.

37. Let k be the number of ports on a switch and n be the number of servers. To get a packet from one server to another in a 2-layer Clos topology, there are/is ___ possible path(s).

    A n
    B $\frac{n}{2}$
    C 2
    D 1
    E $\frac{k}{2}$

38. How many servers can be supported by a 2-layer and a 3-layer topology made up entirely of k-port switches?

    A $\frac{3k^2}{4}, \frac{5k^3}{6}$
    B $\frac{k^2}{2}, \frac{k^3}{4}$
    C k, k^2
    D $\frac{k^2}{4}, \frac{k^3}{6}$
    E k^2, k^3

39. Switched Ethernet deals with a/an ___ medium, whereas bus-based Ethernet deals with a/an ___ medium.

    A wired, wireless
    B unshared, shared
    C shared, unshared
    D wireless, wired
    E congested, uncongested

40. In the context of TLS certificates, signing is done with the ___ key, and verification is done with the ___ key.

    A public, public
    B symmetric, symmetric
    C private, private
    D public, private
    E private, public

41. What is a reason for using multiple intra-coded frames when compressing a video?

    A Transmitting intra-coded frames over the Internet causes fewer decompression errors than just using raw frames.
    B Intra-coded frames are more storage-efficient than inter-coded frames.
    C Intra-coded frames improve the overall quality of the video stream.
    D Intra-coded frames exploit temporal redundancy and only the difference from one frame to the next needs to be computed.
    E Intra-coded frames can be used as a start point for decompression because they do not depend on previous frames.

42. What is a general reason to favor P2P applications over a centralized, client-server architecture?

   A P2P guarantees higher throughput than a client-server architecture because every participant will contribute their bandwidth.
   B It is easier to make money with a P2P application because the more users join the more money each participant accumulates. For instance, consider Bitcoin.
   C P2P applications are decentralized and, with that, immune to DoS attacks.
   D P2P applications are future-proof because they do not depend on the number of participants.
   E The cost of operating the service can potentially be distributed across all participants and the application will not depend on a single point of failure.

43. What does a tracker server in BitTorrent do?

   A It stops peers from being shut down by law enforcement.
   B It tracks which files are requested but not available globally with BitTorrent.
   C It provides a lookup service to find a peer that stores a particular piece of the file.
   D Every peer in BitTorrent is a tracker server; it implements all parts of the BitTorrent protocol.
   E It provides a content distribution network, connecting BitTorrent peers to their closest neighbors.

44. Which of the following MAC protocols is well-suited to bursty traffic (e.g., Web browsing) and constant rate traffic (e.g., voice calls) respectively?

   A TDMA, FDMA
   B CSMA/CA, CSMA/CD
   C CSMA/CD, ALOHA
   D FDMA, TDMA
   E ALOHA, TDMA

45. Consider an error-correcting code, where each data bit is repeated 8 times in addition to the original bit itself (so a total of 9 bits). What is the maximum number of errors within each group of 9 bits that such a code is **guaranteed** to correct?

   A 3
   B 9
   C 5
   D 4
   E 1

46. Refer to the definition of SDN. Which of the following can realistically be implemented using logically centralized control, instead of being distributed across the routers of the network?

   A Reliable delivery
   B Shortest-path routing
   C Connectionless datagrams
   D Carrier sense multiple access
   E Prefix matching

47. Users of live video streaming have a tolerance for a metric that users of video conferencing systems do not. Which metric is this?

   A Latency between transmission and reception of a frame.
   B Video quality variation, i.e., not switching between streams too often.
   C The average size of chunks of video between intra-coded frames.
   D Highest possible video quality.
   E Low rebuffering rate, i.e., very few stalls in playback.

48. What is **not** a reason why BitTorrent lost popularity in favor of streaming service companies?

   A Streaming service companies acquired licenses to legally host and stream entertainment content.
   B The user interface offered by streaming companies is simpler and integrated with electronic appliances such as Smart-TVs.
   C Compared to classical BitTorrent, users did not have to wait for the file to be downloaded before they were able to start streaming.
   D The performance of streaming service companies is more predictable than BitTorrent, which depends on the amount of online users that are hosting content.
   E Using BitTorrent ended up being too expensive compared to simple pay-per-month solutions offered by companies such as Netflix.

49. Carrier sense is...

    A the ability to stop transmitting if others are transmitting.
    B the ability to correct bit flips.
    C the ability to hear others' transmissions on a shared medium.
    D the ability to send a jamming signal to others on a shared medium.
    E the ability to abort others' communications.

50. In the context of video streaming, which of these is something the user of a video streaming service does **not** care about?

    A Avoiding rebuffering events.
    B Maximizing chunk size.
    C Maximizing average video quality.
    D Reducing video quality variations.
    E Reducing startup delay.

Instructions:
- You finished the exam!
- Once you are done, hand in the question and answer sheets please. You do not need to hand in the cheat sheet.
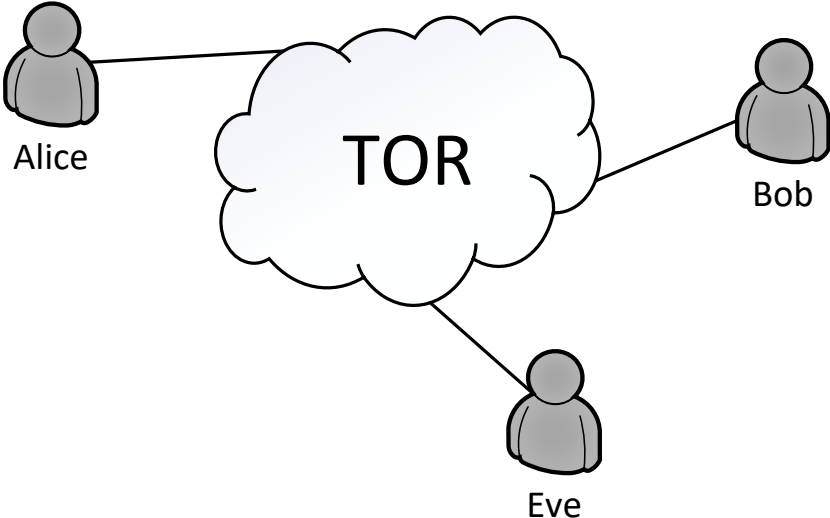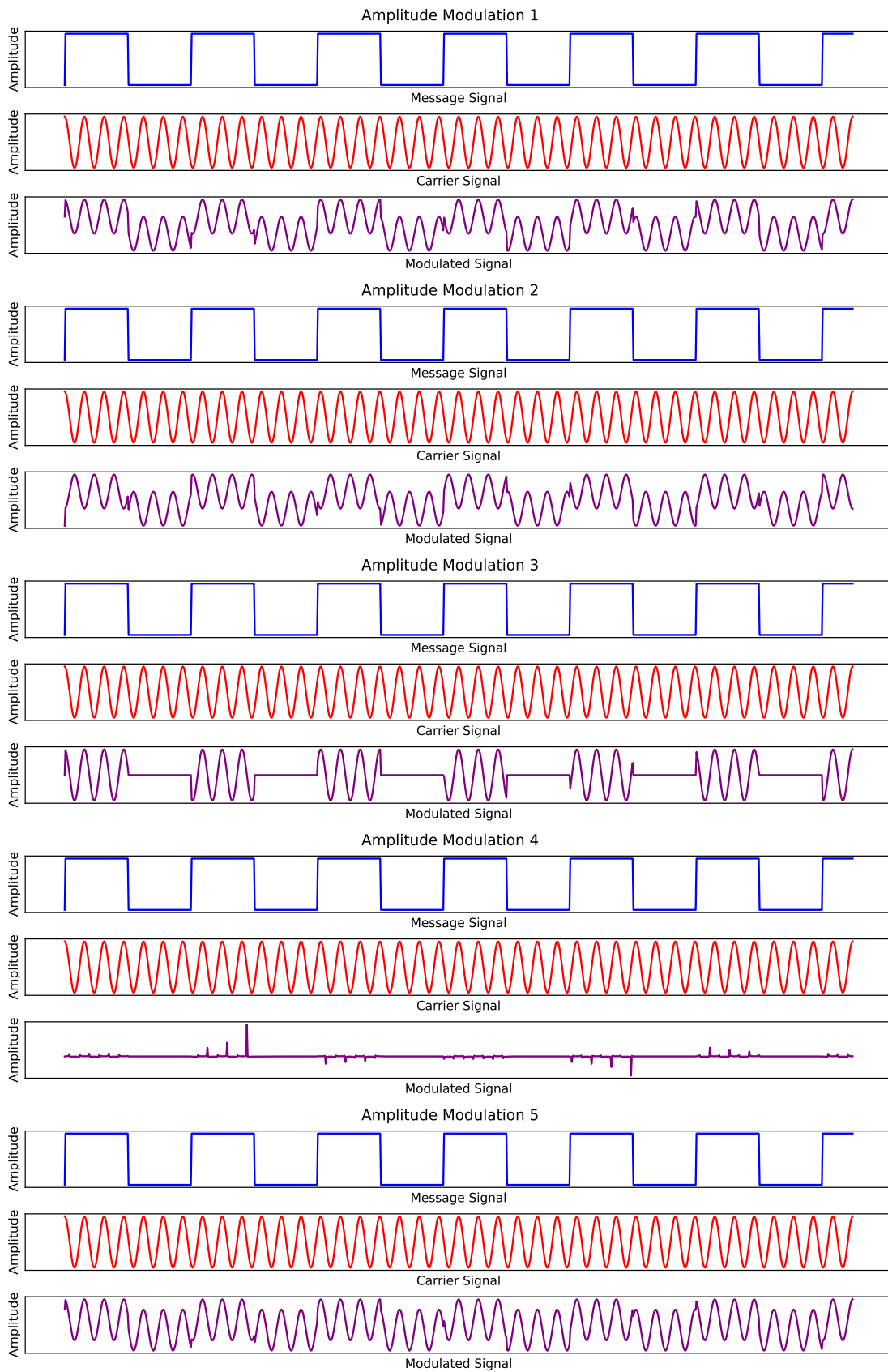
1 Figures

Figure 1: A simple Tor scenario. Alice and Bob are trying to communicate. Eve is a malicious actor.

Figure 2: Amplitude modulation.

This page intentionally left blank.