

CMSC 417 Final (Fall 1999)

- 1.) (15 points) Define **and** explain the following terms:
 - a) IMP
 - b) One Time Pad
 - c) Link-state Routing
 - d) Forbidden Region
 - e) Hamming distance
- 2.) (15 Points) Explain why there is an inherent tension between error detection/correction and encryption.
- 3.) (20 points) In the garbler, a packet is first considered for dropping, then if not dropped is considered for corrupting. If you are trying to establish a connection to a host 2 hops away (i.e., one intermediate node), what is the chance of a TCP connection establishment being successful (without any re-transmission required) if the probability of dropping is 10% and the probability of corrupting is 10%.
- 4.) (15 points) Explain what the difference is between one-way and mutual authentication and explain why mutual authentication is better.
- 5.) (20 points) Explain the difference between how IPv4 and IPv6 handle passing packets through sub-networks with MTU (Maximum Transmission Units) smaller than the originating sub-network could handle. Make sure to explain the advantages of each approach.
- 6.) (15 Points) What is the maximum possible data rate over a 4Khz pass-band channel with 20 dB signal to noise ratio and using quad-ary encoding?