1. (5 points) Consider the QoS approach for routers pictured at right, in which four queues are used to handle different levels of transmission priority: high, medium, normal, and low. A queue at a higher priority receives absolute preferential service over the lower-priority queues. Not until the high queues are empty do low queues receive service from the packet dequeueing mechanism. As a result, lower-priority queues may starve as the router services high-priority queues. Explain what aspects of this approach could be modified to decrease the probability of queue starvation.

2. (5 points) Consider a second QoS scheduling algorithm that gives low-bandwidth, interactive messages priority over high-demand messages. The fairness of the algorithm comes from the ability to avoid starvation of high-demand messages while fulfilling the network demands of applications with lower bandwidth, smaller packets, and intermittent access requirements. Traffic is automatically categorized into flows with low- and high-demand bandwidth requirements. It is assumed that low-demand, interactive traffic uses small packet sizes and that high-demand traffic uses large packets. The flows are sorted in terms of their demand and serviced equally by the packet removal mechanism. The low-bandwidth flows are given priority, while the remaining available bandwidth is shared among the high-demand flows.

A dynamic set of queues is created for traffic flows. Each flow is assigned to a queue and serviced with a bit-wise round-robin algorithm, taking into consideration the size of the packets to decide the order of transmission of the flows. This prevents flows with larger packets from starving flows with smaller packets. Flows are identified by hashing TCP/IP information, such as source/destination IP addresses, TCP/UDP ports, protocol, and IP Precedence. The hashed value provides an index into the individual queue housing the respective flow. Flows with higher precedence are given a lower weight and therefore a greater allocation of overall bandwidth. In the example pictured at right, the router uses the IP Precedence field to calculate the ratio of the overall link bandwidth by setting its link proportion to the IP precedence divided by the sum of all IP precedences. In the example, the three flows that concurrently traverse a 1.544 Mbps T1 serial link have IP precedences 3, 4, and 5, respectively, so the sum of the IP precedences equals 12. Therefore, the proportions of bandwidth for the three flows are 3/12ths (25%), 4/12ths (33%), and 5/12ths (42%), respectively. Explain the primary drawbacks of this QoS approach compared to the one presented in #1 above.

3. (5 points) Compared to the approach in #2 above, the #1 approach provides much better service to high-priority traffic and is preferable for real-time applications using the Real-Time Transport Protocol (RTP). As a result, a third approach, combining those two approaches and pictured at right, might be considered. Here, the router assigns a single high-priority queue for RTP traffic, which preempts traffic in other queues. The router services the high-priority queue until it is empty, and services the remaining traffic using the approach in #2. Explain the principal drawbacks of this QoS approach.

4. (5 points) Voice synchronization is a serious problem in a packet switching network. The proper time for passing the arrived packets to the decompression step and on to the speaker must be determined. If the receiver plays back the packets too soon, then the slowest packets will be lost, but if it waits too long, then the total end-to-end delay introduces annoying artificial pauses within a conversation. Suggest a way in which the actual pauses in a conversation could be effectively used by a network to help maintain voice synchronization (i.e., taking advantage of those time intervals when nothing needs to be transmitted).
5. (5 points) Credit cards and bank cards that use magnetic stripes and PIN codes have an inherent security problem; the merchant’s point-of-sale equipment is the input point for both the information on the card and the user’s PIN code, so the merchant could retain that information and abuse it by applying it to unauthorized transactions in the future. Newer "smart" cards have been developed to help eliminate this problem by replacing the magnetic stripe on the card with integrated circuitry, including a CPU and RAM. Explain how this type of card can avoid the security problem mentioned above.

6. (5 points) The ISO recommends that encryption services should be provided at a protocol layer above the Transport Layer. Explain the rationale for this recommendation (i.e., why not provide encryption services at the Transport Layer or below?).

7. (5 points) One common approach to public-key encryption uses the following steps:
   - Choose two prime numbers \( p \) and \( q \). Define \( n \) to be the product of \( p \) and \( q \).
   - Find a number \( e \) that is relatively prime to \( (p-1)(q-1) \) and a whole number \( d \) such that \( e \cdot d \mod (p-1)(q-1) = 1 \).
   - To encrypt your message as one big integer \( t \), encrypt the message by calculating \( c = (t^e) \mod n \).
   - To decrypt \( c \), calculate \( (c^d) \mod n \).

Using \( p = 29 \) and \( q = 43 \), the smallest prime number possible for \( e \), and the integer represented by the last three digits of your SID number as \( t \) (omitting leading zeros, if any), confirm that this will technique will actually work. That is, calculate \( c \) and then confirm that \( (c^d) \mod n \) will actually produce the original \( t \) value. Note: take advantage of the fact that \( (A^0) \mod M = (A^0 \mod M) \mod M \).

Show your work.

8. (5 points) The figure above illustrates the Google Android operating system’s structure for communication between applications on a mobile device. At the Linux system level, each application has a unique ID, while Android itself supplies a reference monitor that ensures that an applications can access another application’s components only if the appropriate permission labels match (as illustrated at right). Explain how this combination limits the extent to which a user’s mobile device is vulnerable to outside attack.

9. (5 points) Moe, Larry, and Curly are negotiating a three-way contract, but don’t completely trust each other. Moe is supposed to send his part of the contract to Larry, who is supposed to add his part of the contract and forward it to Curly. Explain specifically how public-key encryption (with each stooge having a single public key and a single private key) could be used to eliminate Curly’s fears that the message he’ll receive will either be from Moe, with a fake Larry portion attached, or be from Larry, with a fake Moe portion attached. Remember that Larry must also be sure that the message he receives really came from Moe, and that only Curly will be able to read his (Larry’s) portion of the message. Finally, Moe needs to be sure that both Larry and Curly can read his portion of the message, but also that Larry can’t change that portion before forwarding it to Curly.

10. (5 points) Two competing approaches to providing Video-On-Demand (VOD) services to residential users have been proposed by telephone and cable television companies. The telephone company proposal, called Fiber-To-The-Curb (FTTC) involves having fully switched optical fiber running from the telephone company end office into every residential neighborhood, terminating in a special device that is connected by fast copper wiring to every home in that neighborhood. The cable television alternative, called Hybrid Fiber Coax (HFC), uses a shared fiber optical system running from the cable company to every residential neighborhood, terminating in a fiber node that transfers signals onto a fast coaxial cable into which each house in the neighborhood is tapped. Specify which of these systems require the video servers to encrypt their video streams, and which one does not. Explain the rationale for these encryption decisions.