

國立雲林科技大學資訊管理系
108 學年度第 1 學期博士班資格考
科目：資訊網路

時間：4 小時 (Closed book)

作答時，請注意各題之比例配分，並清楚標示題號

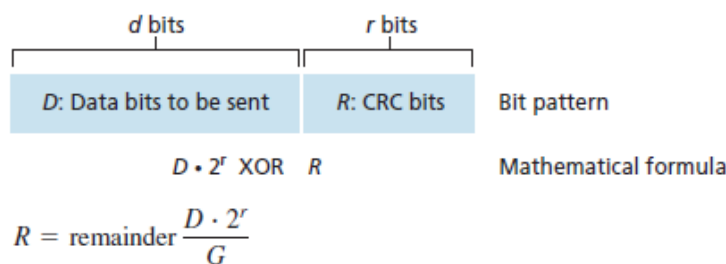
第一部分

- **必選題**：30 分(共 3 題，每題 10 分)

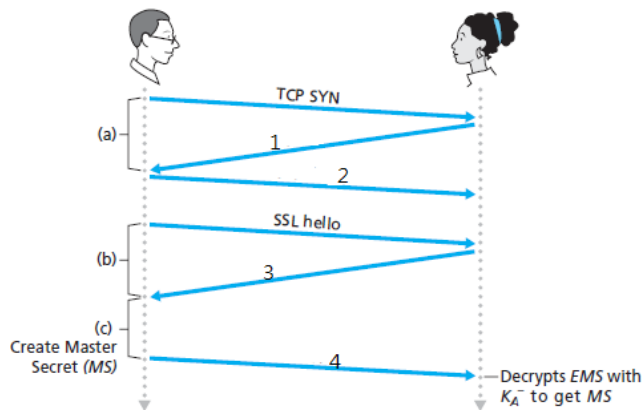
1. Complete the following figure: the service requirements for some selected applications.

Application	Data Loss	Throughput	Time-Sensitive
File transfer/download			
E-mail			
Web documents			
Internet telephony/ Video conferencing			
Streaming stored audio/video			
Interactive games			
Instant messaging			

2. What are the transmitted bits in the case of $D = 101110$, $d = 6$, $G = 1001$, and $r = 3$?
The key idea behind CRC codes is shown in the following:

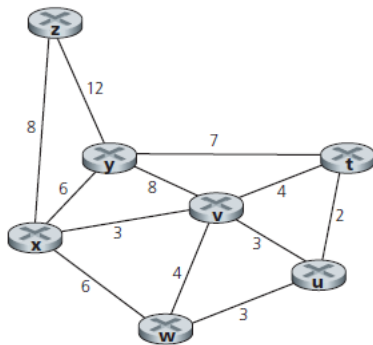


3. Complete the following figure: the almost-SSL handshake, beginning with a TCP connection.



● **可選題**：20 分(2 選 1，每題 20 分)

1. Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to do the following:
 - a. Compute the shortest path from z to all network nodes.
 - b. Compute the shortest path from w to all network nodes.



2. Answer the following questions:
 - a. Using RSA, choose $p = 5$ and $q = 7$, and encode the numbers 12, 19, and 27 separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message.
 - b. Choose p and q of your own and encrypt 1834 as one message m .

第二部分

● **必選題**：30 分(共 3 題，每題 10 分)

1. Please consider sending a packet from the source host to the destination host through a fixed route. Please list the delay factors in the endpoint-to-endpoint delay. Which of these delays are fixed? What are variable?
2. Please list five non-patent Internet applications and the application layer protocol they use.
3. Think about it on a certain planet, everyone belongs to a family of six people, each family living in their own house. Each house has a unique address, and everyone in each house has a unique name. Assuming the planet has a postal service, it can deliver the letter from the source house to the destination house. This postal service requires (1) the letter to be placed in the envelope, and (2) the address of the house at the destination should be clearly written on the envelope (other than this, there is nothing to write). Assume that each family member has a family member representative who collects and sends letters to other family members. The letter itself does not necessarily provide any indication of who the recipient is.
 - a. Please describing protocol that a family representative can use to deliver a letter from a family member of the mail to the family member of the recipient.
 - b. In your protocol, is it necessary for the postal service to open the envelope and view the letter to provide its services?

● **可選題**：20 分(11 選 10，每題 2 分)

1. Please consider Figure 3.58. Assuming TCP Reno is the protocol that caused the behavior, please answer the following questions. For each situation, you should provide a short discussion to explain your answer.
 - a. Please indicate the period in which TCP operates in slow start mode.
 - b. Please indicate the period in which TCP operates in the congestion avoidance mode.
 - c. After the 16th round of transmission, did we receive a three-repeated ACK, or did we detect a missing section because of a timeout event?
 - d. After the 22nd round of transmission, did we receive a three-repeated ACK, or did it detect a missing part because of a timeout event?
 - e. What is the initial value of ssthresh in the first round of transmission?

- f. What is the ssthresh value when transmitting in round 18?
- g. What is the ssthresh value when transmitting in the 24th round?
- h. Is the 70th segment sent during the first round of transmission?
- i. Suppose that after the 26th round of transmission, we receive three duplicate ACKs and detect the loss of the packet. What is the size and ssthresh value of the congestion pane?
- j. Suppose we use TCP Tahoe (instead of using TCP Reno) and assume that we receive three duplicate ACKs in round 16. What is the size and ssthresh value of the tamping pane in the 19th round?
- k. Again assume that we are using TCP Tahoe and that there is a timeout event in round 22. From the 17th round to the 22nd round, how many sections have you sent in the first and last rounds?

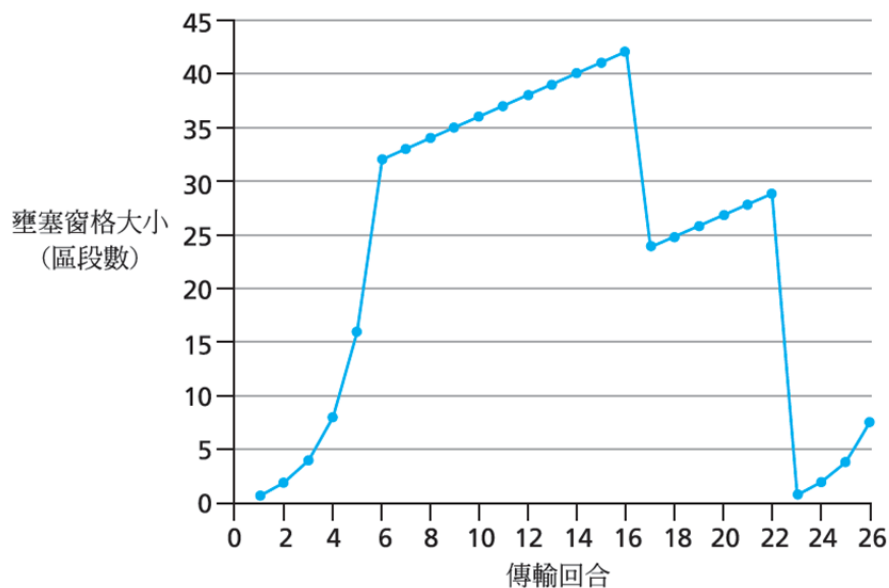


Figure 3.58