考試時間	月 日上午 下午第 節 (星期) 晚間	份數		任課教師	

國立臺灣科技大學 108學年度第 2 學期 考試命題用紙 第 1 頁共 1 頁

考試科目：Computer Networks ☑研究所 ☐大學部 ☐工程在職進修 系班別：博士班資格考

1. (10%) Describe the key differences between traditional telephone networks and IP networks on which the Internet is based upon.

2. (1) (10%) What is the hidden terminal problem and the exposed terminal problem in random access wireless environments?
   (2) (10%) Please explain the scheme provided by IEEE 802.11 to avoid the hidden terminal problem.

3. Suppose that four senders use the following codes in a CDMA system.
   A: (-1 -1 -1 +1 +1 -1 +1 +1)
   B: (-1 -1 +1 -1 +1 +1 +1 -1)
   C: (-1 +1 -1 +1 +1 +1 -1 -1)
   D: (-1 +1 -1 -1 -1 -1 +1 -1)
   Assume that all the senders sent one data bit simultaneously, and a receiver received the following chips: (-1 +1 -3 +1 -1 -3 +1 +1).
   (1) (5%) What data bit did A send? Justify.
   (2) (5%) What data bit did B send? Justify.

4. (10%) Suppose that the Cyclic Redundancy Code (CRC) is used for error checking in a data transmission system. Consider the generator polynomial $G(x) = x^3 + x^2 + 1$. A receiver receives 11110100001. Were there any errors in the transmission? Justify.

5. Answer the following questions about TLS/SSL.
   (1) (10%) during the handshake, both hosts send nonces to each other to create session keys. What is nonce? and what is the main purpose to adopt nonces in the creation of session keys?
   (2) (6%) the generated session keys include data encryption keys and MAC keys. What does MAC stand for and what is the main purpose of MAC in TLS/SSL?
   (3) (4%) Explain the vulnerability caused by the famous heartbleed bug of OpenSSL project.

6. Answer the following questions regarding to DNS.
   (1) (5%) Why DNS queries and replies are by default sent via UDP instead of TCP?
   (2) (15%) Explain interactive DNS and recursive DNS. Give one reason why interactive DNS is considered more secured than recursive DNS?

7. (10%) Pick up 6 states from the following TCP states, and arrange them in order for a typical sequence of successful TCP connection visited by a client TCP. Do the same thing for server-side TCP. Note that both sequences must end with the CLOSED state.
   LISTEN, SYN_SENT, SYN_RCVD, ESTABLISHED, CLOSE_WAIT, TIME_WAIT, LAST_ACK, FIN_WAIT_1, FIN_WAIT2, CLOSED