THE HONG KONG POLYTECHNIC UNIVERSITY
HONG KONG COMMUNITY COLLEGE

Subject Title	: Computer Networking	**Subject Code**	: CCN2238
Session	: Semester Two, 2018/19	**Time**	: 09:30 – 12:30
Date	: 9 May 2019	**Time Allowed**	: 3 Hours
Subject Examiner(s)	: Dr Hon-sun CHIU Dr Candies LAM		

This question paper has a total of **FIFTEEN** pages (including this covering page).

Instructions to Candidates:

1. There are THREE sections in this paper.
   Section A (30%) – Multiple-choice Questions. Answer ALL questions in this section on the multiple-choice answer sheet provided. Select the most appropriate option for each question. Each question carries 1 mark.
   Section B (40%) – Short Questions. Answer any FIVE out of the SIX questions in this section in the answer book provided. Each question carries 8 marks. If you answer more than five questions, only the first five attempted questions will be marked. Indicate in your answer book clearly which five questions you are attempting.
   Section C (30%) – Long Questions. Answer any TWO out of the THREE questions in this section in the answer book provided. Each question carries 15 marks. If you answer more than two questions, only the first two attempted questions will be marked. Indicate in your answer book clearly which two questions you are attempting.
2. Unless specified in a question, you may assume $1K = 10^3$, $1M = 10^6$ and $1G = 10^9$.
3. Candidates are required to pay special attention to neatness and clarity of expression in their answers. Marks will be deducted for untidy work.
4. Electronic calculators, including programmable calculators, may be used provided that the calculators are battery powered, silent in operation, with neither printout nor graphic / word display facilities and do not use dot-matrix technology in the main display. All programmes stored in the calculator should have been cleared. Other electronic devices with graphic / word-display facilities (such as databank watches) are not permitted.

Authorised Materials:

	YES	NO
CALCULATOR (All programmes stored should be cleared.)	[✓]	[ ]
SPECIFICALLY PERMITTED ITEMS	[ ]	[✓]

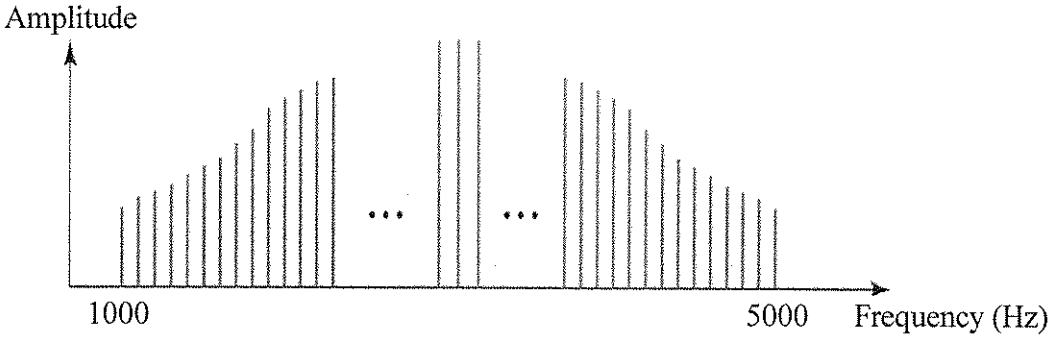
DO NOT TURN OVER THE PAGE UNTIL YOU ARE TOLD TO DO SO

Section B (40%) – Short Questions

Answer any FIVE out of the SIX questions in this section in the answer book provided. Each question carries 8 marks. If you answer more than five questions, only the first five attempted questions will be marked. Indicate in your answer book clearly which five questions you are attempting.

Question B1

Consider the following analog signal in frequency domain:



(a) Is it a periodic signal or an aperiodic signal? Why? (2 marks)

(b) If the above signal is converted to digital signal using PCM, what is the minimum sampling rate required? (2 marks)

(c) What will happen if the sampling rate is lower than that in (b)? (2 marks)

(d) If 256 quantization levels are used in PCM, what is the signal-to-noise ratio in terms of dB (SNR_{dB}) due to quantization error? (2 marks)

Question B2

(a) In stop-and-wait ARQ protocol, how is the acknowledgement (ACK) used for both flow control and error control? (3 marks)

(b) Suppose the data link layer receives a message of size 50000 bytes from upper layer. It is sent through a dedicated channel using stop-and-wait ARQ with the Ethernet frame format below:

Preamble	SFD	Destination Address	Source Address	Length or type	Data and padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	min. 46 bytes max. 1500 bytes	4 bytes

It is noted that the propagation time between the devices is 20ms, the channel bandwidth is 500kbps, and the processing time can be ignored. Assume that ACK frame contains no data and padding, and all frames are transmitted and received properly. Determine the time for the entire transmission to finish. (5 marks)

Question B3

An IP datagram has arrived with the following partial information in the header (in hexadecimal):

```
4800 0108 28AB 2900 1D06 ...
```

(a) What is the header size? (1 mark)

(b) Are there any options in the packet header? Why? (2 marks)

(c) What is the size of the data? (1 mark)

(d) How many more routers can the packet travel to? (1 mark)

(e) What is the protocol number of the payload being carried by the packet? (1 mark)

(f) Is it the first fragment, last fragment or a middle fragment? Why? (2 marks)

Question B4

(a) Given the classful IP address 171.168.12.3. Find

i. the class (1 mark)
ii. the network mask (1 mark)
iii. the network address (1 mark)
iv. the broadcast address. (1 mark)

(b) Given the classless IP address 23.41.13.66/21. Find

i. the network mask (1 mark)
ii. the network address (1 mark)
iii. the broadcast address (1 mark)
iv. the number of hosts supported by this network (1 mark)

Question B5

(a) Encrypt the message "COMPUTER NETWORKING" using a shift cipher with a key of 17. Ignore the space between words. (3 marks)

(b) Encrypt the message "CRYPTOGRAPHY" using a transposition cipher with the key: 2 5 4 3 1. (5 marks)

Question B6

In a network using the Go-Back-N protocol, assume m = 6 and the window size is 63, the values of variables are S_f = 10, S_n = 15 and R_n = 13. Assume that the network does not duplicate or reorder the packets.

(a) What are the sequence numbers of data packets in transit? (1 mark)

(b) At the sender, what is the sequence number of the next packet to send? (1 mark)

(c) If time-out happens. How many packets will be resent? What are their sequence numbers? (2 marks)

(d) If the sender receives an ACK with ackNo = 12. What are the next values of S_f and S_n? (2 marks)

(e) At the receiver, a packet with sequence number 13 arrives. What is the next value of R_n? What ackNo should be sent by the receiver? (2 marks)

- End of Section B -

Section C (30%) – Long Questions

Answer any TWO out of the THREE questions in this section in the answer book provided. Each question carries 15 marks. If you answer more than two questions, only the first two attempted questions will be marked. Indicate in your answer book clearly which two questions you are attempting.

Question C1

A 1-minute audio is encoded into digital file by PCM using 15 quantization levels (-7 to 7). The size of the generated digital file is 30000 bits. The file is then transmitted using CRC error protection. The CRC generator polynomial is x^4+x^3+x.

(a) What is the sampling rate of the PCM encoder? Hence, or otherwise, determine the highest possible frequency component of the audio signal. (4 marks)

(b) Consider the portion of the digital file below:

0011010000110000110011101101101000010010000 1

(i) How long is the above portion in terms of milliseconds (ms)? (3 marks)

(ii) With the sign bit 0 for positive and 1 for negative, sketch the audio signal of the above portion in time domain. (4 marks)

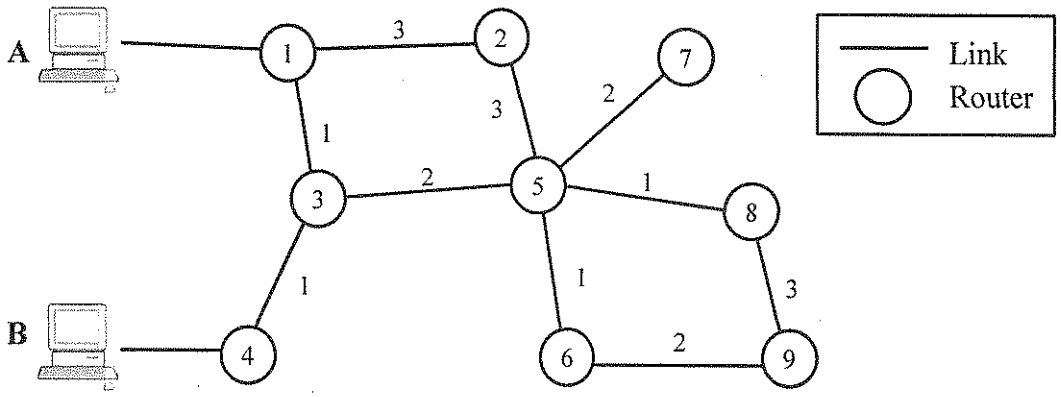
(c) The sender is sending a codeword of 1001011011001110 to a receiver.

(i) What is the divisor in binary format? Hence, calculate the CRC digits. (3 marks)

(ii) What is the message being sent out? (1 mark)

Question C2

Consider the network below that uses store-and-forward virtual-circuit packet switching. The number next to a link stands for the cost of using that link. Station A is going to send a 5000-bit message to station B. Assume there is no other transmission in the network. For each link, the bandwidth is 1000 bps and the propagation delay is 0.5 second. The processing delay of all routers and stations is 0.2 second. Data packet has a fixed size of 1024 bits, which includes the packet header of size 64 bits. All control packets have a fixed size of 64 bits.



Question C2 (continued)

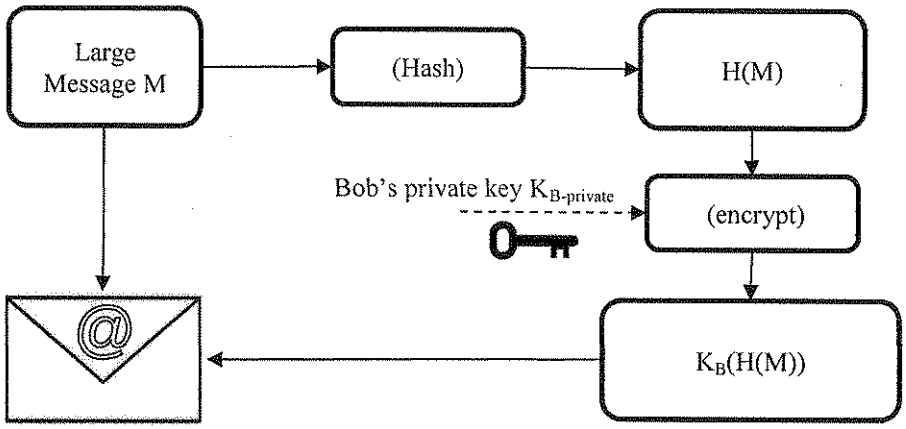
(a) Briefly compare the similarities and differences between circuit switching and virtual-circuit switching. (6 marks)

(b) Suppose the routing algorithm always chooses the *cheapest path* to the destination. Construct a routing table for **router 5** to all other routers using next-hop routing. You may use the column header "Destination" and "Next hop" in the routing table. (4 marks)

(c) Calculate the total delay for the transmission between stations A and B. (5 marks)

Question C3

Suppose Bob wants to send a message with a digital signature created in a public-key encryption system as illustrated below:



(a) In RSA, given two prime numbers $p = 11$ and $q = 13$. Find n and ϕ. (2 marks)

(b) Continue from (a). Suppose $e = 7$. Find d such that $(d \times e) \bmod \phi = 1$. (2 marks)

(c) By referring to the figure above, state the message digest and digital signature. (2 marks)

(d) What is the purpose of using a message digest? (2 marks)

(e) Explain how digital signature can ensure non-repudiation. (2 marks)

(f) Can digital signatures protect privacy of the message? Why? (2 marks)

(g) Draw a diagram in similar format to show the main steps of verifying the digital signature at the receiving side. (3 marks)

- End of Section C -

Appendix 1: List of selected well-known TCP and UDP port numbers

Port in Decimal	TCP or UDP	Service or Protocol Name	RFC
7	TCP/UDP	Echo	792
20	TCP	File Transport Protocol (FTP)	959
21	TCP	FTP control	959
22	TCP	Secure Shell (SSH)	4253
23	TCP	Telnet	854
25	TCP	Simple Mail Transfer Protocol (SMTP)	5321
53	TCP/UDP	Domain Name System (DNS)	1034
67	UDP	Bootstrap Protocol Server (BootP, bootps)	951
68	UDP	Bootstrap Protocol Client (bootpc)	951
69	UDP	Trivial File Transfer Protocol (TFTP)	1350
79	TCP	Finger	1288
80	TCP	Hypertext Transfer Protocol (HTTP)	2616
88	TCP	Kerberos	4120
106	TCP	Password Server(Unregistered Use)	-
110	TCP	Post Office Protocol (POP3) Authenticated Post Office Protocol (APOP)	1939
115	TCP	Simple File Transfer Protocol (SFTP)	913
119	TCP	Network News Transfer Protocol (NNTP)	3977
123	TCP/UDP	Network Time Protocol (NTP)	1305
137	UDP	Windows Internet Naming Service (WINS)	-
143	TCP	Internet Message Access Protocol (IMAP)	3501
161	UDP	Simple Network Management Protocol (SNMP)	1157
192	UDP	OSU Network Monitoring System	-
311	TCP	Secure server administration	-
427	TCP/UDP	Service Location Protocol (SLP)	2608
443	TCP	Secure Sockets Layer (SSL, or "HTTPS")	2818
445	TCP	Microsoft SMB Domain Server	-
464	TCP/UDP	kpasswd	3244
500	UDP	ISAKMP/IKE	2408
514	TCP	shell	-
514	UDP	Syslog	-
548	TCP	Apple Filing Protocol (AFP) over TCP	-
554	TCP/UDP	Real Time Streaming Protocol (RTSP)	2326
587	TCP	Message Submission for Mail (Authenticated SMTP)	4409
600-1023	TCP/UDP	Mac OS X RPC-based services	-
626	TCP	AppleShare Imap Admin (ASIA)	-
626	UDP	serialnumberd (Unregistered Use)	-
631	TCP	Internet Printing Protocol (IPP)	2910
636	TCP	Secure LDAP	-
660	TCP	Server administration	-
687	TCP	Server administration	-
749	TCP/UDP	Kerberos 5 admin/changepw	-
985	TCP	NetInfo Static Port	-
1085	TCP/UDP	WebObjects	-
1099 & 8043	TCP	Remote RMI and IIOP Acess to JBOSS	-

Appendix 2: 7-bit ASCII Table

Decimal	Octal	Hex	Binary	Value	
048	060	030	0110000	0	
049	061	031	0110001	1	
050	062	032	0110010	2	
051	063	033	0110011	3	
052	064	034	0110100	4	
053	065	035	0110101	5	
054	066	036	0110110	6	
055	067	037	0110111	7	
056	070	038	0111000	8	
057	071	039	0111001	9	
058	072	03A	0111010	:	(colon)
059	073	03B	0111011	;	(semi-colon)
060	074	03C	0111100	<	(less than)
061	075	03D	0111101	=	(equal sign)
062	076	03E	0111110	>	(greater than)
063	077	03F	0111111	?	(question mark)
064	100	040	1000000	@	(AT symbol)
065	101	041	1000001	A	
066	102	042	1000010	B	
067	103	043	1000011	C	
068	104	044	1000100	D	
069	105	045	1000101	E	
070	106	046	1000110	F	
071	107	047	1000111	G	
072	110	048	1001000	H	
073	111	049	1001001	I	
074	112	04A	1001010	J	
075	113	04B	1001011	K	
076	114	04C	1001100	L	
077	115	04D	1001101	M	
078	116	04E	1001110	N	
079	117	04F	1001111	O	
080	120	050	1010000	P	
081	121	051	1010001	Q	
082	122	052	1010010	R	
083	123	053	1010011	S	
084	124	054	1010100	T	
085	125	055	1010101	U	
086	126	056	1010110	V	
087	127	057	1010111	W	
088	130	058	1011000	X	
089	131	059	1011001	Y	
090	132	05A	1011010	Z	
091	133	05B	1011011	[	
092	134	05C	1011100	\	(back slash)
093	135	05D	1011101	]	
094	136	05E	1011110	^	
095	137	05F	1011111	_	(underscore)
096	140	060	1100000	`	

Decimal	Octal	Hex	Binary	Value
097	141	061	1100001	a
098	142	062	1100010	b
099	143	063	1100011	c
100	144	064	1100100	d
101	145	065	1100101	e
102	146	066	1100110	f
103	147	067	1100111	g
104	150	068	1101000	h
105	151	069	1101001	i
106	152	06A	1101010	j
107	153	06B	1101011	k
108	154	06C	1101100	l
109	155	06D	1101101	m
110	156	06E	1101110	n
111	157	06F	1101111	o
112	160	070	1110000	p
113	161	071	1110001	q
114	162	072	1110010	r
115	163	073	1110011	s
116	164	074	1110100	t
117	165	075	1110101	u
118	166	076	1110110	v
119	167	077	1110111	w
120	170	078	1111000	x
121	171	079	1111001	y
122	172	07A	1111010	z

Appendix 3

Nyquist Bit Rate

$$BitRate = 2 \times BW \times \log_2 L$$

Shannon Capacity

$$C = B \log_2 (1 + SNR)$$

Signal-to-noise ratio due to quantitation

$$SNR_{dB} = 6.02 n_b + 1.76 \text{ dB}$$

Conceptual Diagram of an IP Packet Format

VER	HLEN	SERVICETYPE	LEN	
IDENT			FLG	FRAGOFFSET
TTL		PROT	CHECKSUM	
SOURCEIP				
DESTIP				
... ...				

Conceptual Diagram of an UDP Segment Format

SOURCEPORT	DESTPORT
LEN	CHECKSUM
... ...	

Conceptual Diagram of an TCP Segment Format

SOURCEPORT			DESTPORT
SEQNO			
ACKNO			
HLEN	RESERVED	FLAGS	WINSIZE
CHECKSUM			URGPT
... ...			

- END OF PAPER -