Xi'an Jiaotong-Liverpool University

西交利物浦大學

Paper CODE	EXAMINER	DEPARTMENT	TEL
CAN201		CAN	

1st SEMESTER 2023/24 FINAL EXAMINATION

Undergraduate – Year 3

INTRODUCTION TO NETWORKING

TIME ALLOWED: 2 Hours

INSTRUCTIONS TO CANDIDATES

1. This is a closed-book examination, which is to be written without books or notes.
2. Total marks available are 100.
3. There are 5 questions. Answer all questions.
4. Answer should be written in the answer booklet(s) provided.
5. Only English solutions are accepted.
6. All materials must be returned to the exam supervisor upon completion of the exam. Failure to do so will be deemed academic misconduct and will be dealt with accordingly.

Question 1 (20 points)

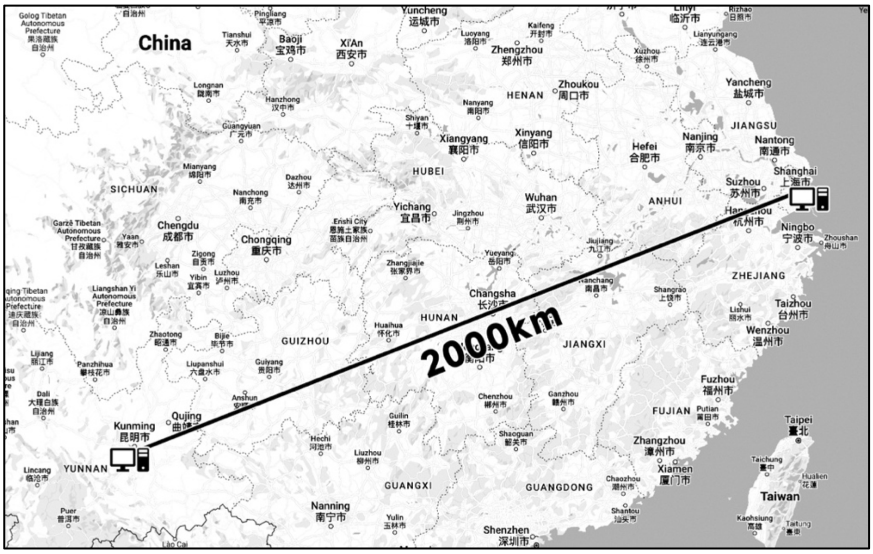


Fig 1. Locations of two hosts.

Suppose two hosts, located in Kunming and Shanghai, are separated by 2,000 kilometers, and are connected by a direct link of R = 2 Mbps. Suppose the propagation speed over the link is $2.5 \cdot 10^8$ meters/sec. (In this question, 1Mb=1,000Kb=1,000,000b)

1. Calculate the bandwidth-delay product: $R \cdot d_{prop.}$ (5 points) $\frac{2\times10^6}{2.5\times10^8} \times 2\times10^6 = 16000$ bits
2. Consider sending a file of 100,000 bits from the host in Kunming to the host in Shanghai. Suppose the file is sent continuously as one large image. What is the maximum number of bits that will be in the link at any given time? (5 points) 16000 bits
3. Provide a definition of the "*bandwidth-delay product*". (5 points) The maximum number of bits that will be in the link at any given time.
4. What is the width (in meters) of a bit in the link? (2 points) 2000000 ÷ 16000 = 125 m
5. Derive a general expression for the width of a bit in terms of the propagation speed s, the transmission rate R, and the length of the link m. (3 points)

$$\text{width} = \frac{m}{\frac{m}{s} \cdot R} = \frac{s}{R}$$

Question 2 (20 points)

The Hyper-Text Transfer Protocol (HTTP), one of the mostly used application-layer protocol, is at the heart of the Web.

1. Decide whether the following statements related to HTTP are correct (True / False):

False a) A user requests a Web page that consists of some text and 4 images. For this page, the client will send one request message and receive 5 response messages. (2 points)

False b) Two distinct Web pages (for example, https://www.suda.edu.cn/research.html and https://sat.xjtlu.edu.cn/staff.html) can be sent over the same persistent connection. (2 points)

False c) With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages. (2 points)

False d) HTTP response messages never have an empty message body. (2 points)

False e) The HTTP protocol can only be used for webpages. (2 points)

2. The text below shows the reply sent from the server in response to an HTTP GET message. Answer the following questions, indicating where in the message below you find the answer.

```
HTTP/1.1 200 OK<cr><lf>Date: Tue, 07 Mar 2023
12:39:45GMT+8<cr><lf>Server: Apache/4.0.52<cr><lf>Last-Modified: Sat,
10 Dec 2022 18:27:46 GMT+8<cr><lf>Accept-Ranges: bytes<cr><lf>Content-
Length: 3874<cr><lf>Keep-Alive: timeout=max=100<cr><lf>Connection:
Keep-Alive<cr><lf>Content-Type: text/html; charset=utf-
8<cr><lf><cr><lf><!doctype html public ”-//w3c//dtd html 4.0
transitional//en”><lf><html><lf><head><lf> <meta http-equiv=”Content-
Type”content=”text/html; charset=utf-8”><lf> <meta name=”GENERATOR”
content=”Mozilla/4.79 [en] (Windows NT 5.0; U) Netscape]”><lf>
<title>Unleash Yourselves and Dare to be Rationally
Unconventional</title><lf></head><lf><body><H1>Unleash Yourselves and
Dare to be Rationally Unconventional</H1><p>Last Modify Date: 1 Dec
2022</p> ...<much more document text following here (not shown)>
```

a) Was the server able to successfully find the document or not? What time was the document reply provided? (2 points) Yes, Tue, 07 Mar 2023 12:39:45 GMT+8

b) When was the document last modified? (2 points) Sat, 10 Dec 2022 18:27:46 GMT+8

c) How many bytes are there in the document being returned? (2 points) 3874

d) What are the first 9 bytes of the document being returned? (2 points) <!doctype

e) Did the server agree to a persistent connection? (2 points) Yes

Question 3 (20 points)

Complete the following table using Dijkstra’s algorithm. Compute the shortest path from node A to all network nodes shown in Fig. 2. Note: Possible ties are broken in favor of the leftmost column.

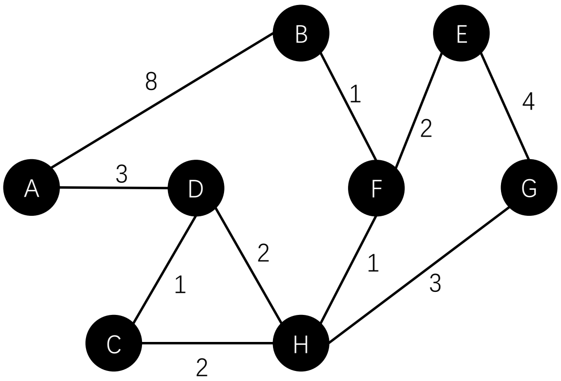


Fig. 2

Step	*N'*	*D(B), p(B)*	*D(C), p(C)*	*D(D), p(D)*	*D(E), p(E)*	*D(F), p(F)*	*D(G), p(G)*	*D(H), p(H)*
0	A	8, A	∞	3, A	∞	∞	∞	∞
1	AD	8, A	4, D	Done	∞	∞	∞	5, D
2	ADC	8, A	Done		∞	∞	∞	5, D
3								
4								
5								
6								
7								

Question 4 (20 points)

Consider the following Fig 3, where several subnets are interconnected.

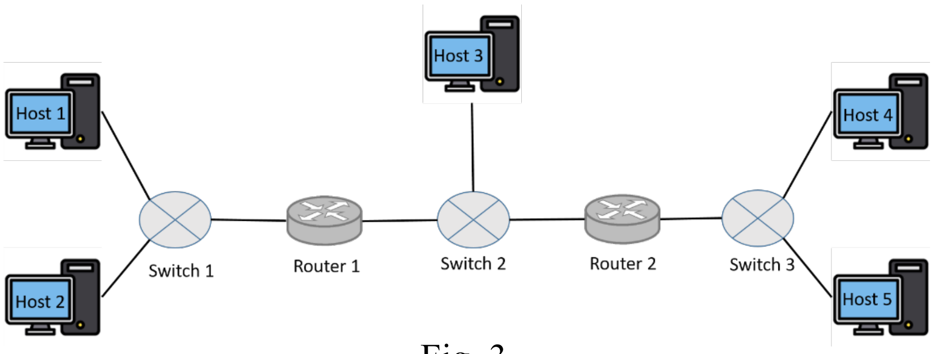


Fig. 3

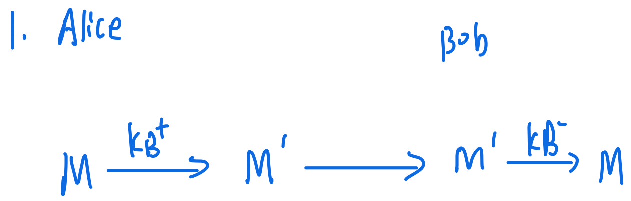
1. Please list all the subnets in this network? Hint: list them in terms of network interfaces. (9 points) 4 subnets. Router 1 left, Router 1 right , Router 2 left, Router 2 right
2. If Router 1 is removed, and Switch 1 and Switch 2 are linked directly, then there are how many subnets left? Explain what they are. (5 points) 2
3. Assuming the interface of Host 1 has an IP address 10.0.1.2, and the adapter for that interface has a MAC address aa-aa-aa-aa-aa-aa; the interface of Router 1 lined with Switch 1 has an IP address 10.0.1.1, and the adapter for that interface has a MAC address 11-11-11-11-11-11. Now, consider sending an IP datagram from Host 1 to Host 3. Suppose Host 1 has an empty ARP table, while Router 1 has the up-to-date ARP table and routing table respectively. Describe all the steps to succeed in sending the IP datagram. (6 points)

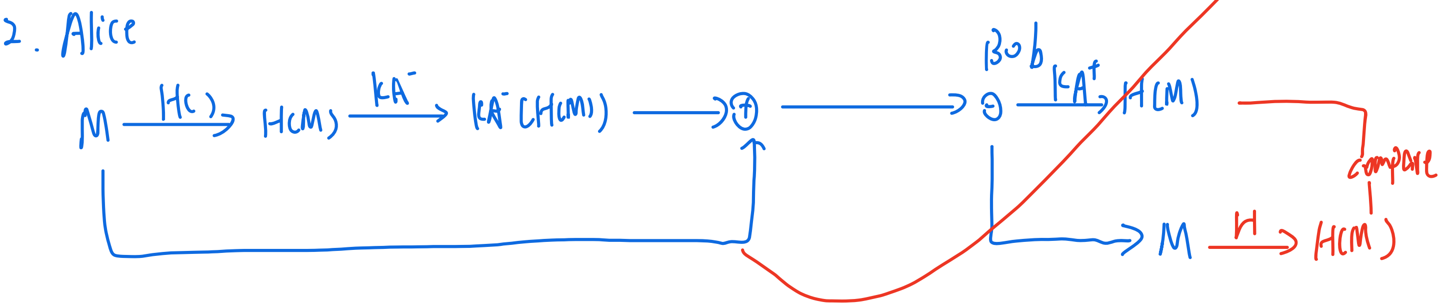
Question 5 (20 points)

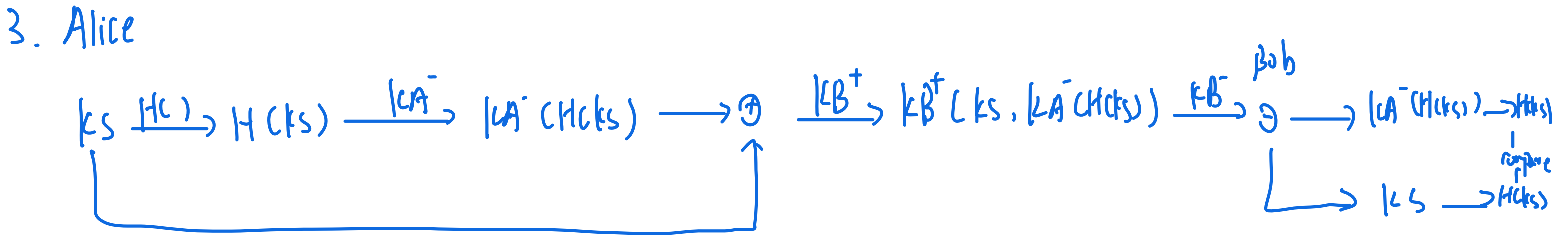
Alice wants to communicate with Bob. Assuming they are using public-key cryptography (e.g., RSA) directly, and so Alice has her public key K_A^+ and private key k_A^- while Bob has his public key K_B^+ and private key k_B^-. Also, we assume that Alice and Bob have got each other's public key through a certificate authority (CA). With the above, Alice now would like to send a message M to Bob.

1. If Alice would like to ensure the confidentiality of this message transmission. That means only Bob can decrypt the cipher-text of M. Please draw a diagram to show how Alice would encrypt the message M. (6 points)
2. If Alice would like to ensure the integrity of this message transmission. That means Bob can verify that M was sent by Alice and M was not altered during transmission. Please draw a diagram to show how Alice would transmit the message M. (Hint: you can use H(x) to express the hash function). (6 points)
3. Now if Alice and Bob want to share a secret key K_S and will use the secret key for encrypting the message. Please use a diagram to show how Alice would use the public-key cryptography to transmit K_S to Bob whereby both confidentiality and integrity should be guaranteed. (8 points)

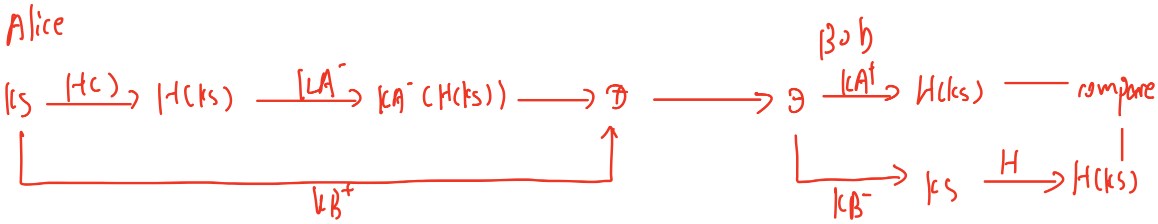
--------------------------END OF EXAM-------------------------







3.


Alice
Ks
H( )
H(Ks)
KA⁻
KA⁻(H(Ks))
⊕
KB⁺
Bob
⊕
KA⁺
H(Ks)
compare
KB⁻
Ks
H
H(Ks)