Xi'an Jiaotong-Liverpool University

西交利物浦大学

Paper CODE	EXAMINER	DEPARTMENT	TEL
CAN201	Fei Cheng	CAN	9089

1st SEMESTER 2021/22 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)

Accessing web pages through a browser is one of the most commonly used network operations.

1. Suppose the IP address for the associated URL is not cached in your local host and n DNS servers are visited before your host receives the IP address from DNS; the successive visits incur an RTT of RTT1,...,RTTn. Let RTT_0 denote the RTT between the local host and the server containing the object. Assuming zero transmission time of the object. Web page associated with the link contains exactly one object, consisting of a small amount of HTML text. How much time elapses from when the client clicks on the link until the client receives the object? (5 points)

Answer:

The time required to resolve the IP address is: RTT1+RTT2+...+RTTn.

To establish a TCP connection and request HTML text, you need to go back and forth, that is, double the local host and the server containing the object 2RTT0.

In the question stem, it is assumed that the transmission time of the object is zero, and there is no need to add it.

The total time required is: 2RTT0+RTT1+RTT2+...+RTTn.

Suppose your computer is connected to the Internet through a router, and you enter https://www.xjtlu.edu.cn/ in the address bar of your browser and open the homepage of the university, which contains texts and images. Please briefly introduce all the related protocols in different layers of IP stack used in the mentioned webpage visiting. Tips: You should consider the provided network condition and the type of web address. (15 points)

2.Answer: When you enter https://www.xjtlu.edu.cn/ in the address bar of your browser and open the homepage of the university, the following protocols in different layers of the IP stack will be used:

Application layer:
HTTP (Hypertext Transfer Protocol) is used to request and transfer web resources, such as HTML documents, images, and other media, from the server to the client.
HTTPS (HTTP Secure) is used to encrypt the communication between the client and the server to ensure the confidentiality and integrity of the data being transmitted. HTTPS uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt the data.
Transport layer:
TCP (Transmission Control Protocol) is used to establish a connection between the client and the server, transmit data between them, and ensure that the data is received correctly.
Network layer:
IP (Internet Protocol) is used to route the data packets from the client to the server and back.
Data link layer:
The data link layer protocols used will depend on the type of network the client is connected to. If the client is connected to the Internet through a router, the protocols used may include Ethernet, Wi-Fi, or a similar protocol for transmitting data over a local area network (LAN).
Physical layer:
The physical layer protocols used will depend on the type of network the client is connected to. For example, if the client is connected to the Internet through a router, the protocols used may include physical cables, such as Ethernet cables, or wireless signaling, such as radio waves for Wi-Fi.
In summary, when visiting the mentioned webpage, the client will use HTTP or HTTPS at the application layer, TCP at the transport layer, IP at the network layer, and various data link and physical layer protocols depending on the client's network connection.

Question 2 (20 points)

Due to the issues such as interferences and device errors, bit errors often occur in networking communication. In order to receive the correct information through the internet, error detection and correction methods are applied in some layers.

1. Please list error detection methods for all IP stack five layers. If no error detection method is used for some layers, please indicate them. (5 points)

A: A practical communication system must have the ability to detect errors and take some measures to correct them, so that errors can be controlled within the smallest possible range. This is the error control process.

So, error detection has become one of the main functions of the data link layer.

In the physical layer, the physical layer only transmits bit streams and cannot control whether there are errors.

At the data link layer, error detection methods can include parity check bits, checksums, and cyclic redundancy check (CRC).

In the network layer, error detection methods can include parity, checksum, and cyclic redundancy check (CRC)

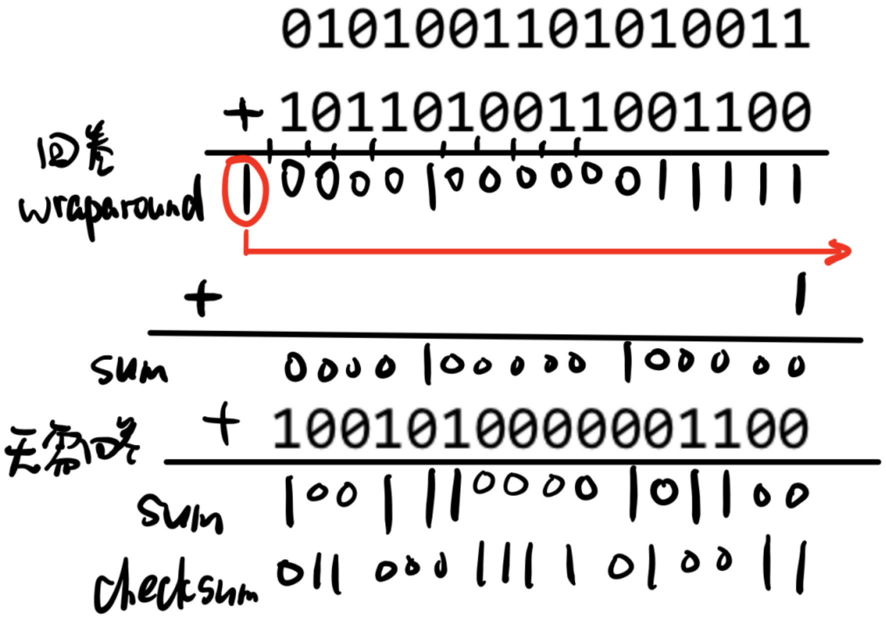
In the transmission layer, error detection methods can include checksum and cyclic redundancy check (CRC).

In the application layer, error detection is usually not used because it involves more advanced functions, such as user interface and data representation, rather than reliable data transmission.

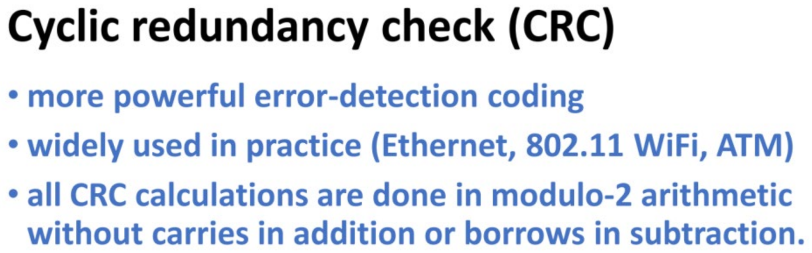
2. Suppose you have the following three 16-bit bytes: `0101001101010011`, `1011010011001100`, `1001010000001100`. What is the 1s complement of the sum of these 16-bit bytes? (10 points)

答：反码的和结果为：011000111101001，具体过程如下。

Answer: The sum of the reverse codes is 0110001111101001. The specific process is as follows.



3. Cyclic redundancy check (CRC) is also widely used in network communication. Please briefly introduce features of CRC. (5 points)



Cyclic redundancy check (CRC)

- more powerful error-detection coding
- widely used in practice (Ethernet, 802.11 WiFi, ATM)
- all CRC calculations are done in modulo-2 arithmetic without carries in addition or borrows in subtraction.

Note ↑

Answer: Cyclic redundancy check (CRC) is an error detection method widely used in network communication. It is a checksum calculated from the transmitted data and a set of predetermined values (called polynomials).

The following are some of the key features of CRC:

All odd dislocations can be detected; All double bit errors can be detected; Burst errors less than or equal to the check bit length can be detected.

This is a simple but effective method to detect transmission data errors.

It can detect a wide range of errors, including single bit errors, burst errors and errors that cause changes in the total length of data.

This is relatively effective because it requires only a few extra bits to be transmitted with the data.

It is widely used in network protocols, such as Ethernet, as well as in storage systems, such as disk drives and memory cards.

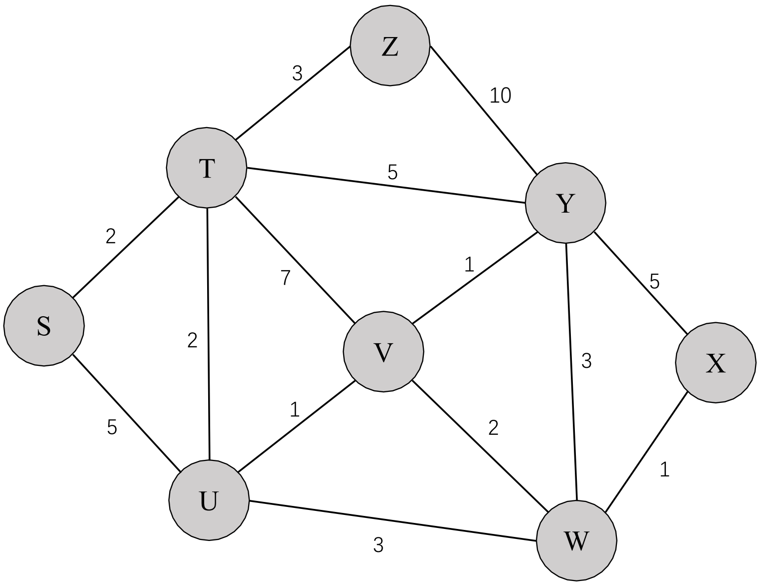
It is relatively easy to implement because it requires only simple mathematical operations.

In general, the main advantage of CRC is that it can detect a large number of errors with relatively small overhead, which is in terms of the amount of additional data to be transmitted. This makes it a popular choice for error detection in applications where network and other data integrity is important.

Question 3 (20 points)

Complete the following table using Dijkstra's algorithm. Compute the shortest path from node Z to all network nodes shown in Fig. 3. Note: Possible ties are broken in favor of the leftmost column.

Fig. 3



Step	*N'*	*D(S), p(S)*	*D(T), p(T)*	*D(U), p(U)*	*D(V), p(V)*	*D(W), p(W)*	*D(X), p(X)*	*D(Y), p(Y)*
0	Z	∞	3, Z	∞	∞	∞	∞	10, Z
1	ZT	5, T	Done	5, T	10, T	∞	∞	8, T
2	ZTS	Done		5, T	10, T	∞	∞	8, T
3	ZTSU			Done	6,U	8,U	∞	8,T
4	ZTSUV				Done	8,U	∞	7,V
5	ZTSUY					8,U	12,Y	Done
6	ZTSUYW					Done	9,W	
7	ZTSUYWX						Done	

Question 4 (20 points)

Consider the following Fig.4, where several subnets are interconnected by two routers, i.e., R1 and R2.

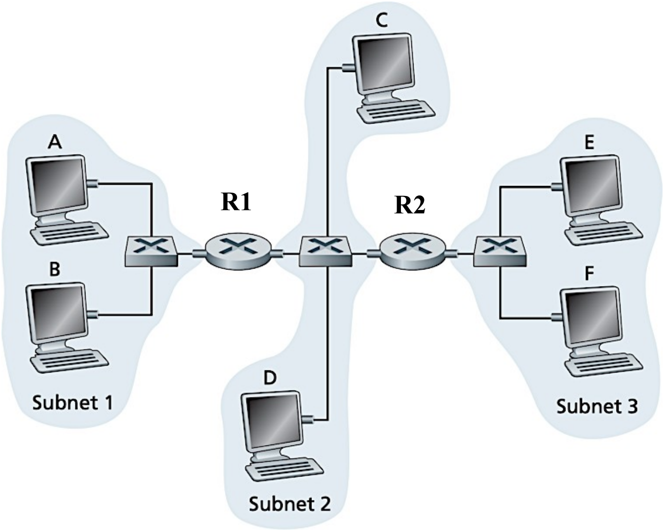


Fig. 4

1. If the interface of R1 in subnet 2 has an IP address 192.168.2.1, assign IP addresses to all the other interfaces in subnet 2, and also, show the network mask you used for those IP addresses. (6 points)

可分配的地址：192.168.2.2-192.168.2.254

子网掩码：255.255.255.0

2. Assuming the interface of A has IP address 192.168.1.2, and the adapter for that interface has MAC address aa-aa-aa-aa-aa-aa; the interface of R1 in subnet 1 has IP address 192.168.1.1, and the adapter for that interface has MAC address 11-11-11- 11-11-11. Now, consider sending an IP datagram from Host A to Host E. Suppose A has an empty ARP table, while R1 and R2 both have up-to-date ARP tables and routing tables respectively. Enumerate all the steps for sending the IP datagram. (8 points)

Here are the steps for sending the IP datagram from Host A to Host E:

Host A checks its ARP table to see if it has an entry for the IP address of R1 in subnet 1.

1. ARP table is empty; it sends an ARP request message to the broadcast address of subnet 1.

2. R1 receives the ARP request message and checks its ARP table to see if it has an entry for the IP address of Host A. Since it does not have an entry, it sends an ARP reply message to Host A, providing

its MAC address (11-11-11-11-11-11).

3. Host A receives the ARP reply message and updates its ARP table with the MAC address of R1 in subnet 1 (11-11-11-11-11-11).

4. Host A constructs an IP datagram with the destination IP address of Host E and the MAC address of R1 in subnet 1 (11-11-11-11-11-11) as the destination MAC address.

Host A sends the IP datagram to R1 in subnet 1.

5. R1 receives the IP datagram and checks its routing table to see if it has an entry for the destination IP address of Host E. Since it does, it sends the IP datagram to R2 using its MAC address.

6. R2 receives the IP datagram and checks its routing table to see if it has an entry for the destination IP address of Host E.

7. R2 sends the IP datagram to Host E using its MAC address.

8. Host E receives the IP datagram and processes it.

3. If we replace the center switch (the device between R1 and R2) with a router R3, then how many subnets are in this figure? List them. (6 points)

After replacement, there are four subnets as follows:

1.AB；

2.C；

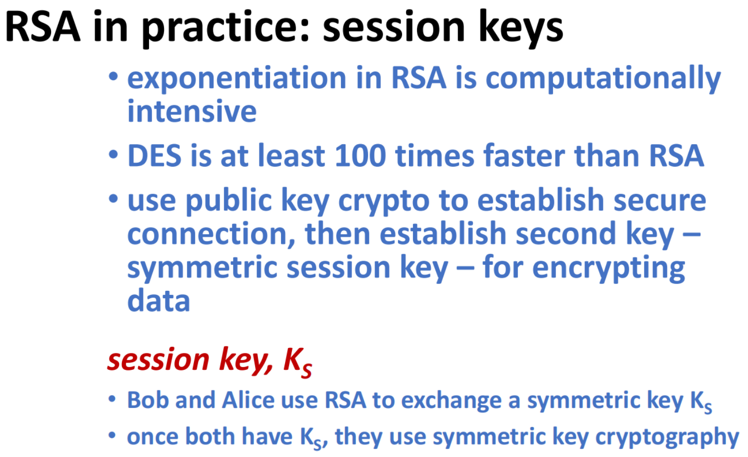
3.D；

4.EF

Question 5 (20 points)

Alice wants to communicate with Bob using symmetric-key cryptography (e.g. DES) with a session-key K_S. In the lectures we learned how public-key cryptography (e.g. RSA) can be used to distribute a session key K_S from Alice to Bob. Suppose the private keys of Alice and Bob are k_A and k_B, while the public keys are K_A and K_B. Also, we assume that Alice and Bob have got each other’s public key through a trusty method.

1. What is the main advantage of first distributing a session key and then using symmetric-key cryptography rather than using public-key cryptography techniques for the whole communication? (5 points)



RSA in practice: session keys

- exponentiation in RSA is computationally intensive
- DES is at least 100 times faster than RSA
- use public key crypto to establish secure connection, then establish second key – symmetric session key – for encrypting data

session key, K_S

- Bob and Alice use RSA to exchange a symmetric key K_S
- once both have K_S, they use symmetric key cryptography

The session key refers to the key used by two communication end users during a call or data exchange. When used to protect the transmitted data, it is called the data encryption key, and when used to protect files, it is called the file key. The role of the session key is to make people do not have to change the basic key too frequently, which is conducive to the security and management of the key. This kind of key can be agreed by both parties in advance, or can be dynamically generated by the system through the key establishment protocol and given to both communication parties. It is dedicated to both communication parties, so it is also called private key.

The conference key can increase the complexity and make the message less vulnerable to cracking. There are two main reasons for using symmetric conference key encryption:

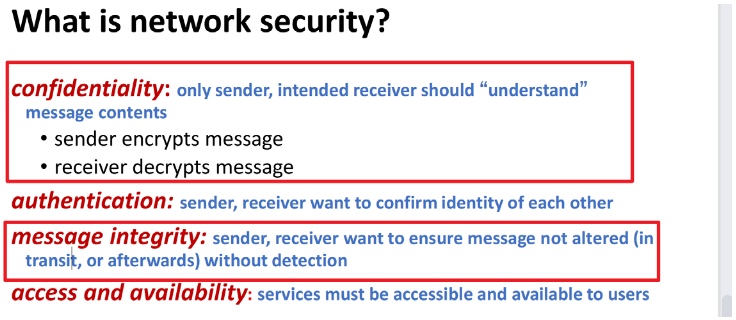
Several cryptanalysis attacks are easier because more messages are encrypted using a specific key. By limiting the amount of data processed with a specific key, these attacks can be more difficult.

Although asymmetric encryption is relatively secure and does not need to consider how to exchange keys, it requires more resources to perform operations, which is too slow for many requirements; All secret key algorithms require the key to be distributed securely. By using an asymmetric encryption algorithm to encrypt the secret key of another faster symmetric encryption algorithm, the overall performance can be significantly improved. This is the application process of PGP and GPG.

2. Draw a diagram that shows the message exchange between Alice and Bob which achieves this, i.e., using the public-key cryptography to distribute a symmetric session-key. (7 points)

Alice -> Bob: Send public key KA+ Bob -> Alice: Send public key KB+
Alice -> Bob: Encrypt KS using KB+ and send Bob -> Alice: Decrypt KS using kB-

3. Describe the difference between confidentiality and integrity (using digital signature) using public-key cryptography. (8 points)



What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

RSA and other public key cryptographic algorithms can only ensure the confidentiality of data, and can be used together with hash algorithm to ensure data integrity.
RSA is block encryption. If the ciphertext loses a block directly, it will not be found during decryption.
In the case of short messages, m-bit plaintext and k-bit random number form a block of m+k-bit. When each block is unwrapped, m-bit plaintext and k-bit random number can always be solved. There is no correctness verification mechanism.
Confidentiality: ensure that data is always kept private in three different states: static, transmission and use
The reason why public key cryptography is more secure than traditional cryptography is that public key cryptography uses the principle of trapdoor one-way function to make the encryption key public and decrypt the secret key. It is also called asymmetric key password or double key password.
The encryption key is made public by using the principle of trapdoor one-way function, and the secret key is decrypted. It is also called asymmetric key password or double key password. The encryption key is public, and the decryption key is secret. It is not feasible to calculate the secret key from the public key. The security theory of public key cryptography is based on computational complexity theory.
Digital signature can guarantee integrity.
Integrity: ensure that the data has not been changed without authorization

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