Easy

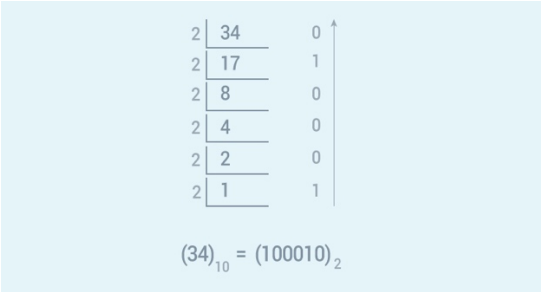
COMP9121 Week 1 Review of Basic Concepts

1. Binary/decimal/hexadecimal numbers, bit and byte

A binary number is a number expressed in the base-2 numeral system or binary numeral system, which uses only two symbols: "0" (zero) and "1" (one). In the binary system, each digit represents an increasing power of 2, with the rightmost digit representing 2^0, the next representing 2^1, then 2^2, and so on.

$100101_2 = [\,(\mathbf{1}) \times 2^5\,] + [\,(\mathbf{0}) \times 2^4\,] + [\,(\mathbf{0}) \times 2^3\,] + [\,(\mathbf{1}) \times 2^2\,] + [\,(\mathbf{0}) \times 2^1\,] + [\,(\mathbf{1}) \times 2^0\,] = 37_{10}$

To convert from a base-10 integer to its base-2 (binary) equivalent, the number is divided by two. The remainder is the least-significant bit. The quotient is again divided by two; its remainder becomes the next least significant bit. This process repeats until a quotient of one is reached.



A hexadecimal number is expressed in the base-16 numeral system. The mapping to binary or decimal number is as follows.

$\mathbf{0}_{hex}$	$= 0_{dec}$	=	0	0	0	0
$\mathbf{1}_{hex}$	$= 1_{dec}$	=	0	0	0	1
$\mathbf{2}_{hex}$	$= 2_{dec}$	=	0	0	1	0
$\mathbf{3}_{hex}$	$= 3_{dec}$	=	0	0	1	1
$\mathbf{4}_{hex}$	$= 4_{dec}$	=	0	1	0	0
$\mathbf{5}_{hex}$	$= 5_{dec}$	=	0	1	0	1
$\mathbf{6}_{hex}$	$= 6_{dec}$	=	0	1	1	0
$\mathbf{7}_{hex}$	$= 7_{dec}$	=	0	1	1	1
$\mathbf{8}_{hex}$	$= 8_{dec}$	=	1	0	0	0
$\mathbf{9}_{hex}$	$= 9_{dec}$	=	1	0	0	1
$\mathbf{A}_{hex}$	$= 10_{dec}$	=	1	0	1	0
$\mathbf{B}_{hex}$	$= 11_{dec}$	=	1	0	1	1
$\mathbf{C}_{hex}$	$= 12_{dec}$	=	1	1	0	0
$\mathbf{D}_{hex}$	$= 13_{dec}$	=	1	1	0	1
$\mathbf{E}_{hex}$	$= 14_{dec}$	=	1	1	1	0
$\mathbf{F}_{hex}$	$= 15_{dec}$	=	1	1	1	1

Try by yourself

Convert $(FFFF)_{hex}$ to Decimal and binary

Bit: one binary number
Byte: 8 bits, two hex numbers. 4 3 2

The following shows a packet captured by Wireshark, what is the size of the packet?

```
b8 ee 0e 69 85 f4 88 e9  fe 85 1d 22 08 00 45 00
00 28 90 c5 00 00 40 06  aa ea c0 a8 00 08 c0 e5
bd 8a d5 f9 01 bb 97 48  c5 77 5b 50 80 76 50 10
08 00 58 78 00 00
```

Easy

2. Basic probability

We transmit 1 byte data from the sender to the receiver, each bit is flipped by the channel with probability 0.1 independently. What is the probability that there are exactly 2 bits flipped?

3. Traceroute to sydney.edu.au.

Which hop shows the router in your home?

Which hop shows sydney.edu.au? What is the IP address of sydney.edu.au?

COMP 9121 Week 2

Data-Link Layer

Easy

Exercise 1. CRC

(1) Consider the following information bits 1010101 and CRC generator 1101. What are the coded bits to be transmitted? Show that the coded bits are divisible by 1101.

(2) The system can be shown in the following figure.

Received bits – (minus) coded bits is called the error pattern (note that here "–" is equivalent to XOR). Obviously, all "0" error pattern means "no error".

Please show

(a) Error pattern 0000100 can be detected by the receiver.

(b) Error pattern 0001101 cannot be detected by the receiver.

(c) Could you find another error pattern which cannot be detected by the receiver?

Normal

Exercise 2. Slotted ALOHA

Consider two nodes, A and B, that use the slotted ALOHA protocol to contend for a channel. Suppose node A has more data to transmit than node B, and node A's retransmission probability p_A is greater than node B's retransmission probability, p_B.

(1) Provide a formula for node A's average throughput. What is the total efficiency of the protocol with these two nodes?

(2) If $p_A = 2p_B$, is node A's average throughput twice as large as that of node B? Why or why not? If not, how can you choose p_A and p_B to make that happen?

(3) In general, suppose there are N nodes, among which node A has retransmission probability $2p$ and all other nodes have retransmission probability p. Provide expressions to compute the average throughputs of node A and of any other node.

Exercise 3. More on Slotted ALOHA

Suppose four active nodes—nodes A, B, C and D—are competing for access to a channel using slotted ALOHA. Assume each node has an infinite number of packets to send. Each node attempts to transmit in each slot with probability p. The first slot is numbered slot 1, the second slot is numbered slot 2, and so on.

(1) What is the probability that node A succeeds for the first time in slot 5?

(2) What is the probability that some node (either A, B, C or D) succeeds in slot 4?

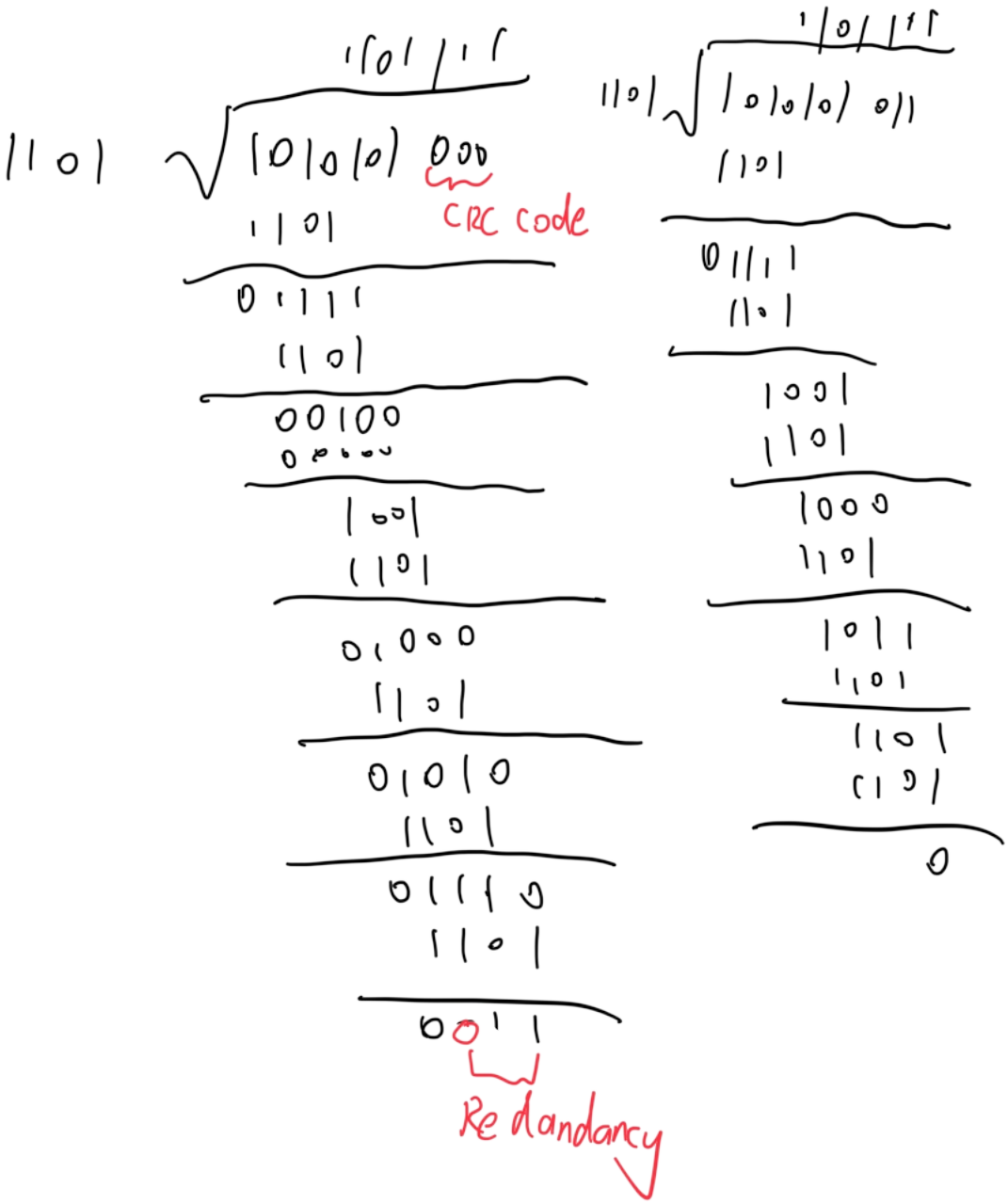
(3) What is the probability that the first success occurs in slot 3?

(4) What is the efficiency of this four-node system?

$G(x) = 1101$

res: 1010100 011

(1) Consider the following information bits 1010101 and CRC generator 1101. What are the coded bits to be transmitted? Show that the coded bits are divisible by 1101.



(2) The system can be shown in the following figure.

Received bits – (minus) coded bits is called the error pattern (note that here "–" is equivalent to XOR). Obviously, all "0" error pattern means "no error".

$G(x) = 1101$

Please show

(a) Error pattern 0000100 can be detected by the receiver.

(b) Error pattern 0001101 cannot be detected by the receiver.

(c) Could you find another error pattern which cannot be detected by the receiver?

(a) $E(x) = 100$

(b) $E(x) = 1101$ $1101\overline{)1101}$

(c) 1101 1101

Normal

Exercise 2. Slotted ALOHA

Consider two nodes, A and B, that use the slotted ALOHA protocol to contend for a channel. Suppose node A has more data to transmit than node B, and node A's retransmission probability p_A is greater than node B's retransmission probability, p_B.

(1) Provide a formula for node A's average throughput. What is the total efficiency of the protocol with these two nodes?

(2) If $p_A = 2p_B$, is node A's average throughput twice as large as that of node B? Why or why not? If not, how can you choose p_A and p_B to make that happen?

(3) In general, suppose there are N nodes, among which node A has retransmission probability $2p$ and all other nodes have retransmission probability p. Provide expressions to compute the average throughputs of node A and of any other node.

X: no. of packets attempted for transmission in one timeslot.

Normalized throughput = $P(X=1)$ # N is all nodes which want to use this chanel

$= Np(1-p)^{N-1}$ # we need do binomial for p

(1). throughput: 吞吐量

A's efficiency: $P_A(1-P_B)$

$Np(1-p)^{N-1} = 2p(1-p) = p(1-p) + p(1-p)$

(!! why! 我们需要所有点的组合可能)

Total Efficiency: $P_A(1-P_B) + P_B(1-P_A)$

(2) Assume $P_A = 2P_B$

A's: $P_A(1-P_B) = 2P_B - 2P_B^2$

$\Rightarrow$ A's ≠ 2B's

B's: $P_B(1-P_A) = P_B - 2P_B^2$

In order to make it happen, we have

$A's = 2B's$

$P_A - P_A P_B = 2P_B - 2P_A P_B \Rightarrow P_A + P_A P_B = 2P_B \Rightarrow P_A = \frac{2P_B}{1+P_B}$

---

(1) [notes]

If $N=3$, there are A, B, C Nodes

$$Np(1-p)^{N-1} = 3p(1-p)^2$$

$$\Downarrow$$

$$P_A(1-P_B)(1-P_C) + P_B(1-P_A)(1-P_C) + P_C(1-P_B)(1-P_A)$$

---

(3)

A's average throughput:

$P_A = 2p \qquad P_{other} = p$ (i.e. $P_B = P_C = \cdots P_N = p$)

Hence it's average throughput $= P_A(1-P_{other})^{N-1}$

$$= \boxed{2p(1-p)^{N-1}}$$

Other's average throughput $= P_{other}(1-P_A)^{N-2}(1-P_A)$

$$= \boxed{p(1-p)^{N-2}(1-2p)}$$

X

Normal

Exercise 3. More on Slotted ALOHA

Suppose four active nodes—nodes A, B, C and D—are competing for access to a channel using slotted ALOHA. Assume each node has an infinite number of packets to send. Each node attempts to transmit in each slot with probability p. The first slot is numbered slot 1, the second slot is numbered slot 2, and so on.

(1) What is the probability that node A succeeds for the first time in slot 5?

(2) What is the probability that some node (either A, B, C or D) succeeds in slot 4?

(3) What is the probability that the first success occurs in slot 3?

(4) What is the efficiency of this four-node system?

(1) let $P(A)$ represent the probability node A succeeds in a slot

$$P(\text{A firstly succeed in slot 5}) = [1-P(A)]^4 P(A)$$

前4次A都失败　第5次成功

(2) $P(\text{some node succeed in slot 4})$ # in any slot is the same answer

$$= P(\text{A succeed in slot 4}) + \cdots + P(\text{D succeed in slot 4})$$

$$= (1-p)^3 p + \cdots + (1-p)^3 p \quad \#\ (1-p)^3$$：其它3个node都失败 p：指定node成功

$$= 4(1-p)^3 p = P(X=1)$$

(3) $P(\text{first success in slot 3})$

$$= P(\text{No node succeed in first 2 slots}) \cdot P(\text{some node success in slot 3})$$

$$= [1 - P(\text{some nodes succeed in a slot})]^2 \cdot P(\text{some nodes succeed in slot 3})$$

$$= [1-(4(1-p)^3 p)]^2 \cdot (4(1-p)^3 p)$$

前2个node　3rd

(4)

Efficiency = Normalized Throughput

$= P(X=1)$

$= \binom{N}{k} p^k (1-p)^{N-k}$

$= \binom{4}{1} p^1 (1-p)^3$

$= \frac{4!}{3!\,1!} p(1-p)^3$

$= \frac{4\times3\times2\times1}{3\times2\times1\times1} \times \cdots$

$= 4p(1-p)^3$

IV $p(1-p)^{N-1}$

#会发现其实就是(2)所求的

COMP9121 Week 3

Parity-Check Code Simulation

In this lab, you are going to understand a simulator of parity-check code and test its performance. The almost-ready skeleton code is provided at Paritycheckskeleton.py. You task is to understand each line of the codes.

The simulator is summarized as follows:

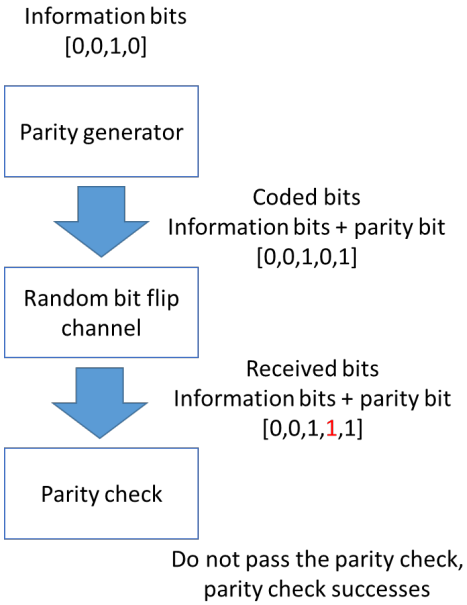


Fig. 1 parity-check code simulation

(1) Randomly generate an N-bit information stream. (Feel free to choose N. You are recommended to choose N=4 or 5. N=5 in the skeleton code. The variable name is infolength). This is done in the skeleton code. You need to locate the lines in the skeleton code.

(2) Generate the parity bit and you can derive an (N+1)-bit coded stream. This is done in the function def GenerateParity(information) in the skeleton code. You need to locate the lines in the skeleton code.

(3) Send the coded stream into a random flipping channel with bit-flip probability p=0.1. For each bit, you need to randomly flip it. The resultant bit stream is received by the receiver. This is done in the function def ErrorChannel(coded) in the skeleton code. You need to locate the lines in the skeleton code.

(4) The receiver checks the received bits. This is done in def CheckParity(received) in the skeleton code. Then, there will be three possibilities:

   A) None of the bits are flipped.
   B) Some of the bits are flipped, and this is detected by the parity check (Shown in Fig. 1).
   C) Some of the bits are flipped, but this is not detected by the parity check.

   You need to locate the lines in the skeleton code.

(5) Repeat the above procedure many times (e.g., 10000). Find out the probabilities of A), B), and C). You need to locate the lines in the skeleton code.

Easy

Questions

include parity bit

1. Theoretically, let N denote the bit length of the original information (N+1 is the length of the coded bits), and p denote the probability of bit-flip. Then, Event A) happens with a probability

$$(1-p)^{N+1}$$

Could you verify this theoretical result by your simulator?

2. What are the theoretical probabilities of events B) and C)? Could you verify them by your simulator?

3. Let $p = 0.05$ and N=6. Modify the skeleton code to find out the simulated probabilities of events A, B, and C.

A) $(1-p)^{N+1}$ # All success, N=6

B) $\binom{7}{1}(1-p)^{6}p^{1}$ # 1 incorrect

$+\binom{7}{3}(1-p)^{4}p^{3}$ # 3 incorrect

$+\binom{7}{5}(1-p)^{2}p^{5}$ # 5 incorrect

$+\binom{7}{7}(1-p)^{0}p^{7}$ # 7 incorrect

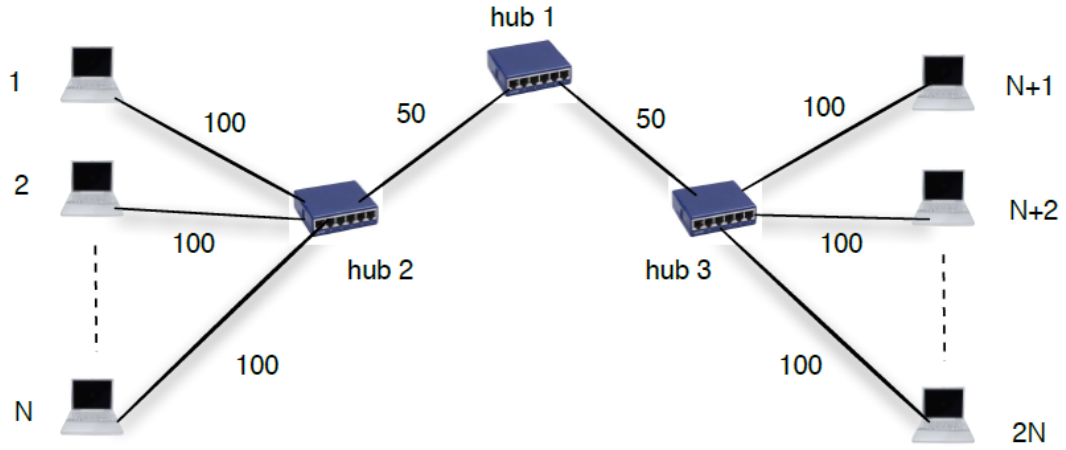
C) 1 - res of (A) - res of (B)

week3 lec learn

COMP9121 Tutorial Week 4

1. CSMA-CD Performance

2N computers have been connected in a network as illustrated. The length of each link is written in meters. Each computer generates 1000 packets per second with each packet being 500 bytes. The maximum rate of all links is 1 Gbps. The propagation speed in the medium is 2.0×10^8 meters/second.



(1) What is the maximum number of nodes supported in the network if CSMA-CD is used on the shared medium? (Recall that the CSMA-CD efficiency is $\frac{1}{1+5\frac{t_{prop}}{t_{trans}}}$)

(2) Assume that hub1 is replaced with a switch. Find the maximum number of nodes supported in the network if CSMA-CD is used on the shared medium. Assume that half of the traffic is kept in its own side and half of the traffic goes to the other side.

2. Routing Table

A company has been granted a block of IP addresses starting with 150.12.16.0/24. The address space should be allocated to four subnets A, B, C and D. Subnet A needs 9 addresses, subnet B needs 18 addresses, subnet C needs 28 addresses, and subnet D needs 12 addresses. The IP addresses have been assigned in the following order A, B, C, and D (subnet A has the smallest IP addresses and subnet D has the largest IP addresses). What is the starting IP address of subnet C?

3. Routing Table

A router has the following CIDR entries in its routing table (Table **1):**
Table **1:** Routing table

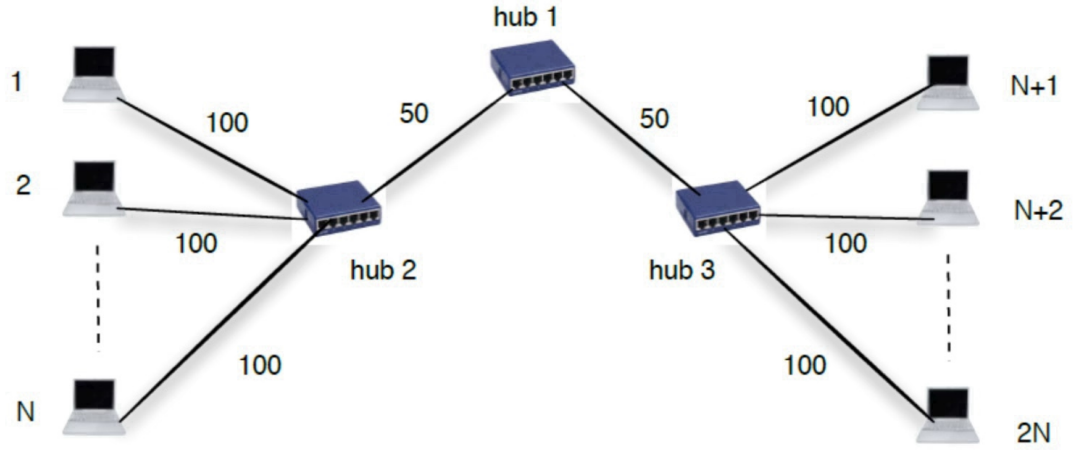
Address/ mask	**Interface**
150.12.192.0/19	Interface 1
150.12.0.0/16	Interface 2
150.12.216.0/21	Interface 3
Default	Interface 4

A packet with address 150.12.218.51 arrives. Which interface would the packet be forwarded to?

1. CSMA-CD Performance

frame = packet

2N computers have been connected in a network as illustrated. The length of each link is written in meters. Each computer generates 1000 packets per second with each packet being 500 bytes. The maximum rate of all links is 1 Gbps. The propagation speed in the medium is 2.0×10^8 meters/second.



(1) What is the maximum number of nodes supported in the network if CSMA-CD is used on the shared medium? (Recall that the CSMA-CD efficiency is $\frac{1}{1+5\frac{t_{prop}}{t_{trans}}}$)

(2) Assume that hub1 is replaced with a switch. Find the maximum number of nodes supported in the network if CSMA-CD is used on the shared medium. Assume that half of the traffic is kept in its own side and half of the traffic goes to the other side.

(1) $t_{trans} = \frac{500 \times 8}{1\,Gb} = \frac{500 \times 8}{10^9\,bps} = 4 \times 10^{-6}$

$t_{prop} = \frac{100 \times 6 + 50 \times 2 + 100 \times 2}{2.8 \times 10^8}$ longest distance = 300

Effi $= 0.3478$

$\frac{1}{1+5\frac{t_{prop}}{t_{trans}}}$

$$2N = \frac{0.3478 \times 10^9}{\text{traffic of each node}}$$

$$\left(1000 \times 500 \times 8\right)$$

$$= \lfloor 86.95 \rfloor = 86$$

(2) ① hub ⇒ switch means the cable length is cut in half

~~② 2N become N in each subnet~~

longest distance = computer – hub – computer
(they in same subnet)

$$= 200$$

$$t_{prop} = \frac{200}{2\times10^8} = 1\,\mu s$$

$$t_{tran} = same = 4\,\mu s = 4\times10^{-6}$$

$$efficiency = 0.444$$

$$\frac{N}{2}tN = \frac{0.444\times10^9}{1000\times500\times8} = 111$$

因题目中给定该condition

$N = 74 \Rightarrow 2N = 148$

这个提所有computer

Week 6 Normal

这是子网掩码

2. Routing Table

A company has been granted a block of IP addresses starting with 150.12.16.0/24. The address space should be allocated to four subnets A, B, C and D. Subnet A needs 9 addresses, subnet B needs 18 addresses, subnet C needs 28 addresses, and subnet D needs 12 addresses. The IP addresses have been assigned in the following order A, B, C, and D (subnet A has the smallest IP addresses and subnet D has the largest IP addresses). What is the starting IP address of subnet C?

150.12.16. (8 bits) ← 0-255

A 9-size need 4 bits
- 150.12.16.0000.0000
- 150.12.16.0000.1111
- begin with all 0
- end with all 1

B 18 need 5 bits
- 150.12.16.0001.0000 ✗ 不是以0开头
- 150.12.16.0010.0000 ✓ 是以0开头
- 150.12.16.0011.1111

C 28 need 5 bits
- 150.12.16.0[00].0000 在开始加1，进2-Base计算
- 150.12.16.0101.1111

Note:

# of elements		num of address
1 bit	2 {0,1}	2-2=0
2 bit	4 {00,01,10,11}	4-2=2
3 bit	8 ...	8-2=6

之所以减2是因为不能有 all 0 or all 1 addr

Easy

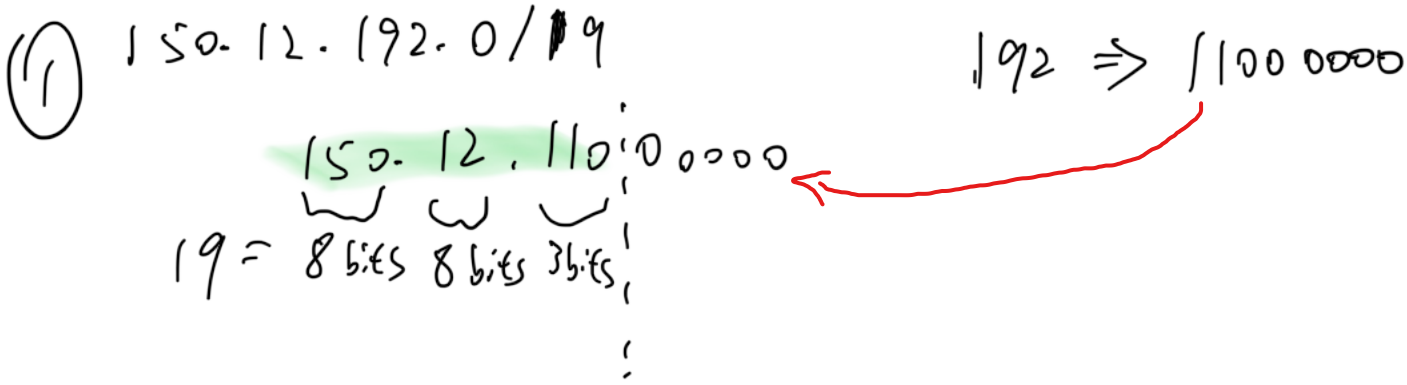
3. Routing Table

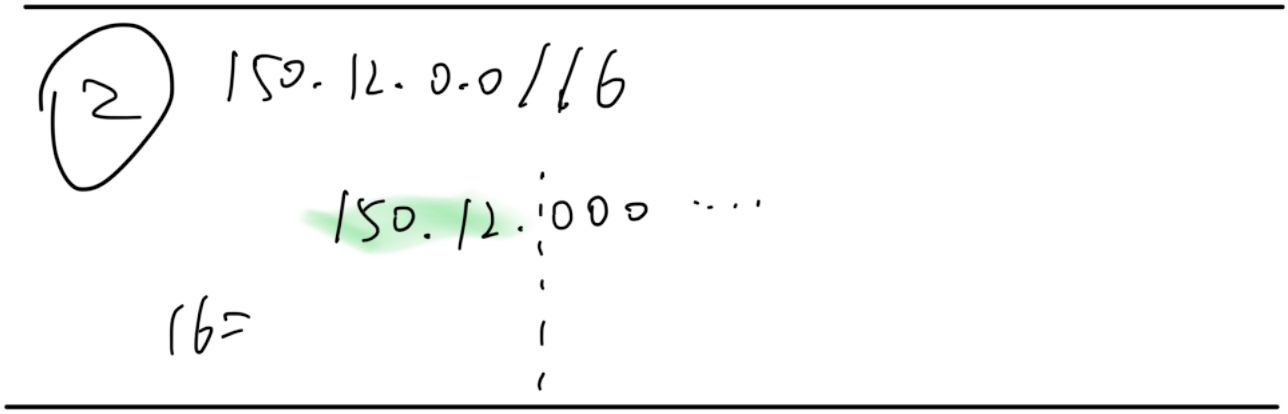
A router has the following CIDR entries in its routing table (Table **1):**

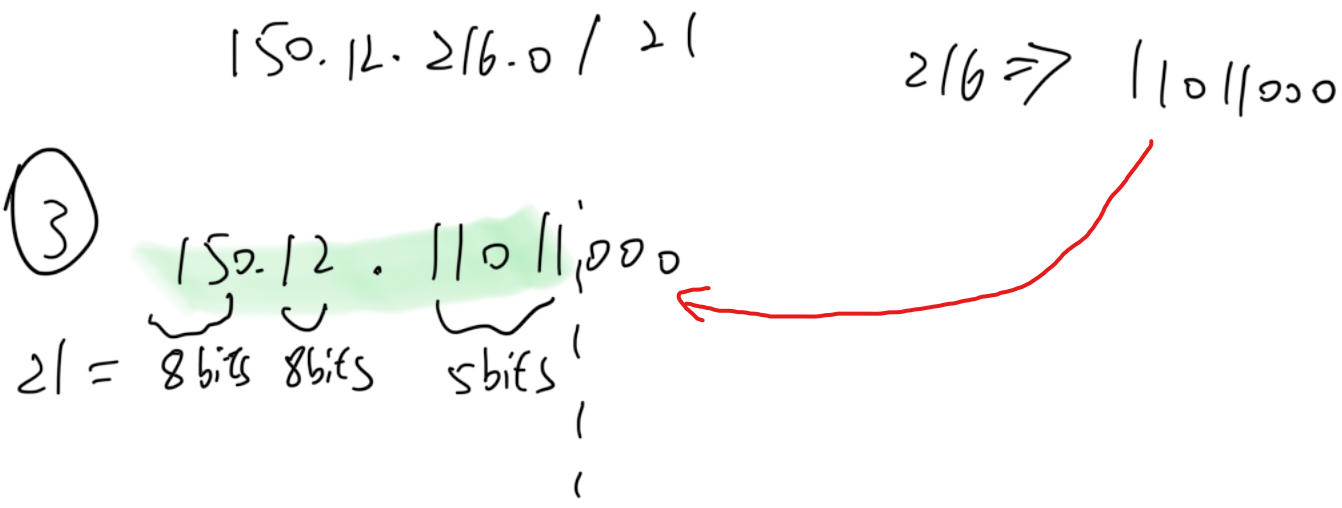
Table **1:** Routing table

Address/ mask	**Interface**
150.12.192.0/19	Interface 1
150.12.0.0/16	Interface 2
150.12.216.0/21	Interface 3
Default	Interface 4

A packet with address 150.12.218.51 arrives. Which interface would the packet be forwarded to?







150.12.218.51

218 → 11011010

51 → .....

150.12.11011010.....

8bits 8bits

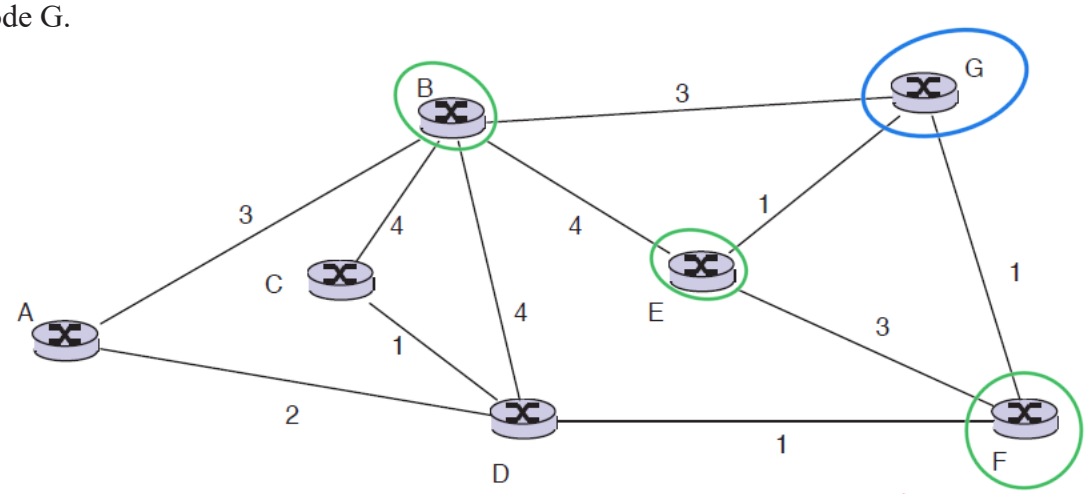
使用 longest prefix matching

we goto interface 3

Normal

COMP 9121 Week 5

(1) In the graph below, use the Distance Vector routing (without split horizon or reverse poisoning) to find the minimum distance from each node to node G. Assume that exchanges of routing information and routing table updates are synchronous (i.e., they happen at the same time at all nodes). Fill out the table below to find the shortest distance from each node to node G.



Next Node

distance to G

	A	B	C	D	E	F
Initial	-1, ∞	-1, ∞	-1, ∞	-1, ∞	-1, ∞	-1, ∞
1	-1,∞	G,3	-1,∞	-1,∞	G,1	G,1
2	B,6	G,3	B,7	F,2	G,1	G,1
3	D,4	G,3	D,3	F,2	G,1	G,1
4	D,4	G,3	D,3	F,2	G,1	G,1

End when our answer → same to previous one

(2) Following (1), assume that the link between nodes F and G is disconnected. Do NOT use split horizon or reverse poisoning. Fill out the table below to find the shortest distance from each node to node G.

Normal

	A	B	C	D	E	F
Initial	D,4	G,3	D,3	F,2	G,1	G,1
1	D,4	G,3	D,3	F,2	G,1	E,4 X
2	D,4	G,3	D,3	F,4	G,1	E,4 X
3	D,6	G,3	D,5	F,4	G,1	E,4
4	D,6	G,3	D,5	F,5	G,1	E,4
5	B,6	G,3	D,6	F,5	G,1	E,4
6	B,6	G,3	D,6	F,5	G,1	E,4 ✓
7						
8						

F的neighbour有E D

因为只参考上一行

D,3

D,3

又因为不进行下面的判断，所以为 D,3

D的最短路径已含F，所以F不能再从D学习最短路径

Hard

(3) Following (1), assuming that the link between nodes F and G is broken, use split horizon with reverse poisoning to find the shortest distance from all nodes to G.

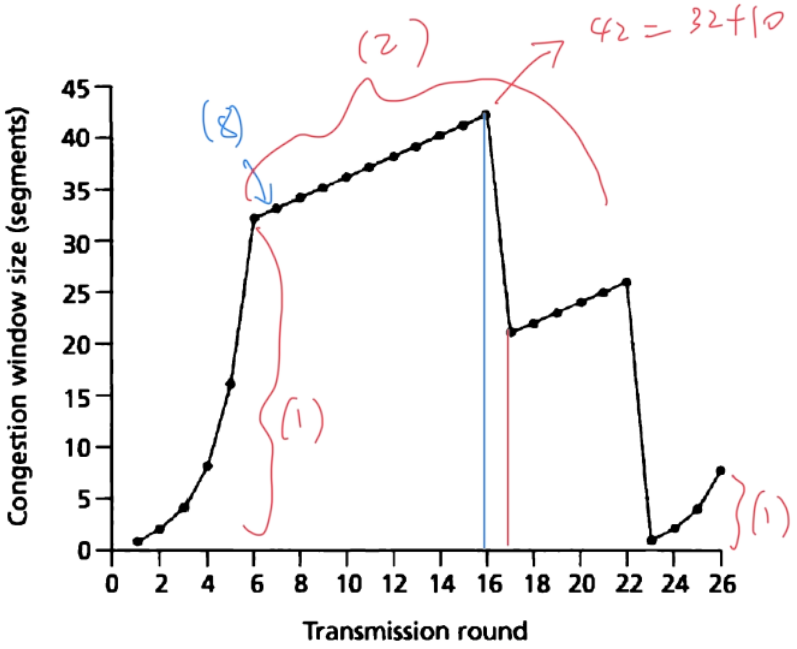
因为不允许reverse

	A	B	C	D	E	F
Initial	D,4	G,3	D,3	F,2	G,1	G,1
	D,4	G,3	D,3	F,2	G,1	E,4
	D,4	G,3	D,3	F,5	G,1	E,4
	B,6	G,3	D,6	F,5	G,1	E,4
	B,6	G,3	D,6	F,5	G,1	E,4 ✓

COMP 9121 Week 9 Tutorial

1. TCP

Normal



Consider the above figure. Assuming TCP Reno is the protocol experiencing the behavior shown above, answer the following questions. In all cases, you should provide a short discussion justifying your answer.

(1). Identify the intervals of time when TCP slow start is operating. (0-5), (22-26) include 26 because there is a trend

(2). Identify the intervals of time when TCP congestion avoidance is operating. (6-22)

(3). After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout? triple duplicate

(4). After the 22nd transmission round, is segment loss detected by a triple duplicate ACK or by a timeout? timeout

(5). What is the initial value of ssthresh at the first transmission round? 32 1->2->4...->32

(6). What is the value of ssthresh at the 18th transmission round? 21 = 42/2

(7). What is the value of ssthresh at the 24th transmission round? 26/2 = 13

(8). During what transmission round is the 70th segment sent? 7

(9). Suppose TCP Tahoe is used (instead of TCP Reno), and assume that triple duplicate ACKs are received at the 16th round. What are the ssthresh and the congestion window size at the 19th round? ssthresh = 21; window: 1, 2, 4, so it is 4

(10). Again suppose TCP Tahoe is used, and there is a timeout event at 22nd round. How many packets have been sent out from 17th round till 22nd round, inclusive?

Cond 1 + 2 + 4 + 8 + 16 + ~~32~~ 21 = 52

round 17th 18th 19th 20th 21th 22nd

ssthreth 21 21 21 21 21 21

notice 23rd should be 1 again

Hard

2. Cross-layer (HTTP, TCP, Routing)
Consider the network shown below. Assume that the one-way delay through each "cloud" in the figure is 1 ms (for example, it takes 1 ms from C to LC). In the system, RIP routing protocol is used. The cost of each "cloud" is 1.

Client C wishes to see a webpage on Web server. The size of the main web page is small. After obtaining the main page, C finds that there are 2 small objects to be fetched. One object is stored in Server A, the other object is stored in Server B. Suppose that persistent HTTP is used.

(1) How long in total does it take for C to successfully obtain the webpage (including the main page and two objects). Suppose that C can start to connect to server A after the main page is fully downloaded. C can start to connect to server B after object 1 is fully downloaded.

16+12+12

Connect

For

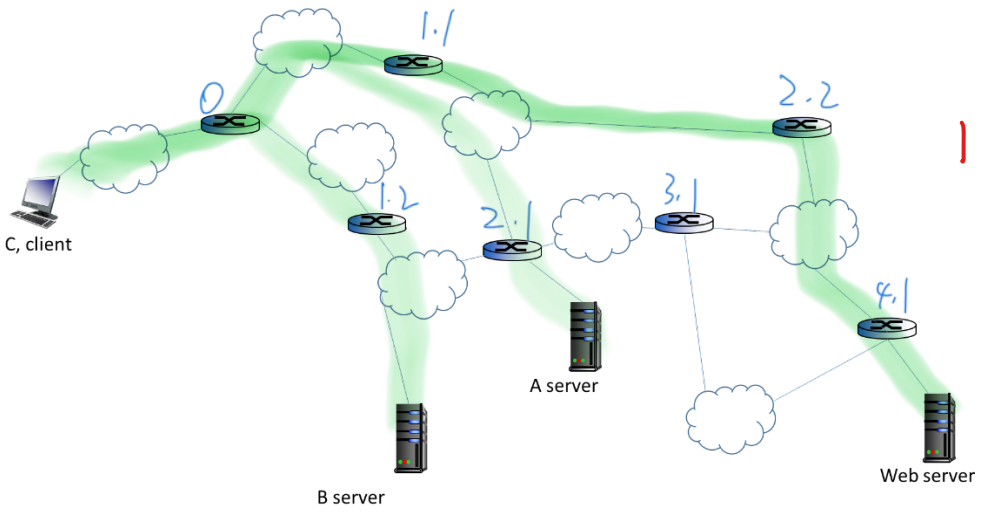
(2) Re-do the problem if the two objects are not small. Each object fits into 10 TCP segments. ssthresh=4 segments. Ignore transmission delay. No packet is lost.

16+3×10+3×10 +1RT

4RTT

1 2 4 5

Finish transfer



(1) take 2x(4+4) ms to get main page from web server

take 2x(3+3) ms to get from A

2x(3+3) client ack 3

(2) 2x(4+4) for host

web send segment 1 to client

segment 2,3

since receive all

Done

A: 3 +3 +3 +3 +3 +3 +3 +3 +3 +3 +3

establish connection

1 cwnd 2cwnd 4 cwnd 5cwnd

4次到ACK, web才能再发, By TCP

16+10+30= 76

COMP 9121 Week 11

1. Bitcoin mining.

In this question, you will need to understand "mining" of bitcoins. It is based on the fact that nobody can find the input value that results a given hashed value. However, given the input, it is easy to verify its hashed value.

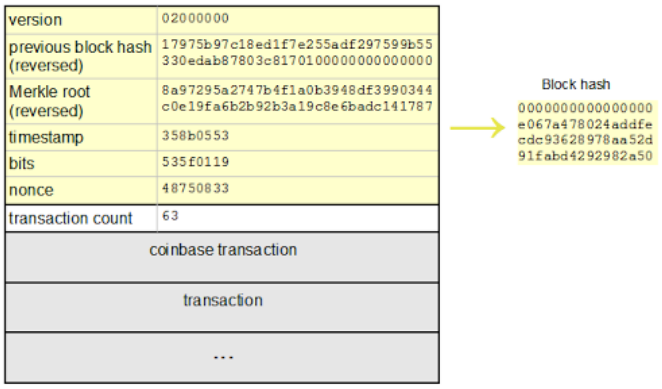
Bitcoin mining can be regarded as "proof of work" [1]. "Proof of work" is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.

Let's say the base string that we are going to do work on is "Hello, world!". Our target is to find a variation of it that SHA-256 hashes to a value beginning with '000' (12-bit '0's). We vary the string by adding an integer value to the end called a nonce and incrementing it each time. Finding a match for "Hello, world!" takes us 4251 tries (but happens to have zeroes in the first four digits):

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

(Note: the hashed value is in hexadecimal format, each hexadecimal number is equivalent to 4 bits.)

4251 hashes on a modern computer is not very much work (most computers can achieve at least 4 million hashes per second). Bitcoin automatically varies the difficulty. A successful hash requires a value beginning with 64-bit '0's.



The figure above shows a transaction block. You need to "guess" the nonce so that the hash of the yellow field begins with 64-bit '0's. There is no fast way to guess the nonce. All you can do is exhaustive search. You can assume that other fields are given in this example.

Figure source http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

Question.
(1) What is the successful probability if you guess once?
(2) What is the successful probability if 10^7 computers guess and each guesses 10^{11} times?

[1] https://en.bitcoin.it/wiki/Proof_of_work

2. Private Key.
In this experiment, you will need to check public and private keys in a Linux system.
Use your Linux/MacOS/Windows system. Use the following command to generate a pair of public and private keys.

```
ssh-keygen -b 1024 -t rsa
```

If you are using the latest version of MacOS or Windows, you need to use the following command.

```
ssh-keygen -b 1024 -t rsa -m PEM
```

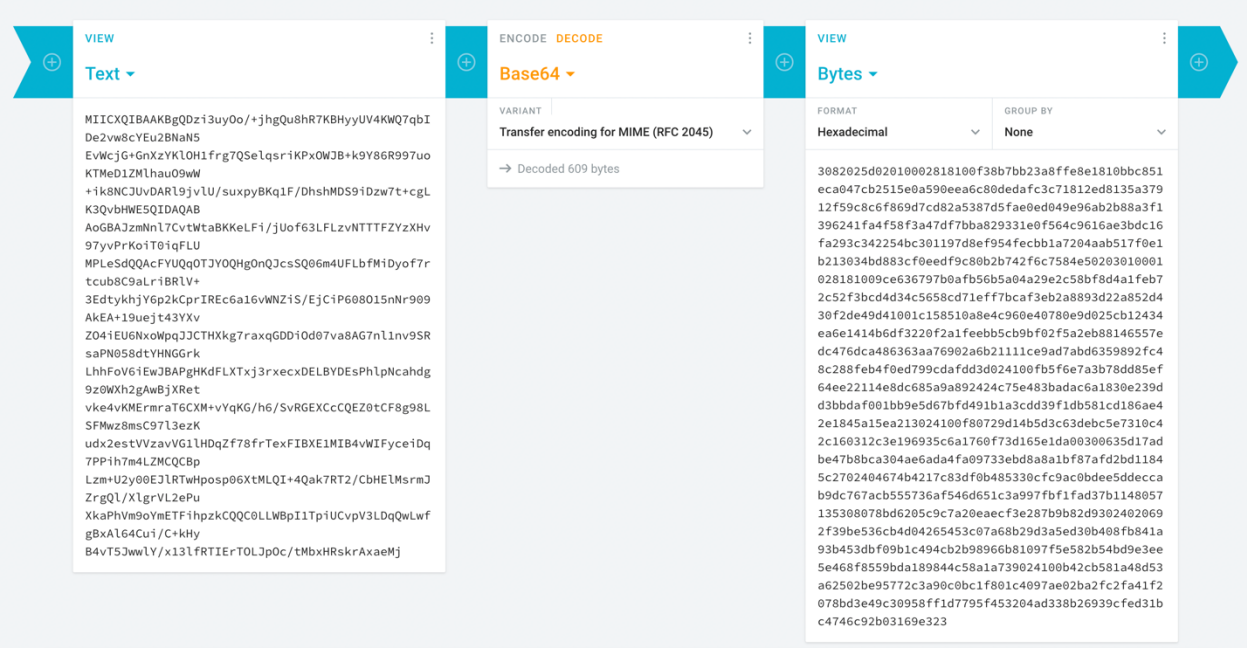
Enter "testfile" for file name. (You can choose any name you like.)
Do not enter anything for passphrase. (Otherwise, you need password to access the private key.)
Then, your public key is stored in testfile.pub and your private key is stored in testfile.
Use the following command to check your private key

```
Cat testfile
```

Then it will show something like

```
david@david-Latitude-E5570:~/keytry$ cat testfile
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDzi3uyOo/+jhgQu8hR7KBHyyUV4KWQ7qbIDe2vw8cYEu2BNaN5
EvWcjG+GnXzYKlOH1frg7QSelqsriKPxOWJB+k9Y86R997uoKTMeD1ZMlhauO9wW
+ik8NCJUvDARI9jvlU/suxpyBKq1F/DhshMDS9iDzw7t+cgLK3QvbHWE5QIDAQAB
AoGBAJzmNnl7CvtWtaBKKeLFi/jUof63LFLzvNTTTFZYzXHv97yvPrKoiT0iqFLU
MPLeSdQQAcFYUQqOTJYOQHgOnQJcsSQ06m4UFLbfMiDyof7rtcub8C9aLriBRlV+
3EdtykhjY6p2kCprIREc6a16vWNZiS/EjCiP608O15nNr909AkEA+19uejt43YXv
ZO4iEU6NxoWpqJJCTHXkg7raxqGDDiOd07va8AG7nl1nv9SRsaPN058dtYHNGGrk
LhhFoV6iEwJBAPgHKdFLXTxj3rxecxDELBYDEsPhlpNcahdg9z0WXh2gAwBjXRet
vke4vKMErmraT6CXM+vYqKG/h6/SvRGEXCcCQEZ0tCF8g98LSFMwz8msC97l3ezK
udx2estVVzavVG1IHDqZf78frTexFIBXE1MIB4vWIFyceiDq7PPih7m4LZMCQCBp
Lzm+U2y00EJIRTwHposp06XtMLQI+4Qak7RT2/CbHEIMsrmJZrgQl/XlgrVL2ePu
XkaPhVm9oYmETFihpzkCQQC0LLWBpI1TpiUCvpV3LDqQwLwfgBxAI64Cui/C+kHy
B4vT5JwwlY/x13IfRTIErTOLJpOc/tMbxHRskrAxaeMj
-----END RSA PRIVATE KEY-----
```

The above red string is coded by BASE64. You need to decode it by BASE64-HEX (RFC2045) to convert it to hexadecimal numbers. Use the following website.
https://cryptii.com/pipes/base64-to-hex



This will show the private key in hexadecimal format:
3082025d02010002818100f38b7bb23a8ffe8e1810bbc851eca047cb2515e0a590eea6c80de
dafc3c71812ed8135a37912f59c8c6f869d7cd82a5387d5fae0ed049e96ab2b88a3f1396241fa
4f58f3a47df7bba829331e0f564c9616ae3bdc16fa293c342254bc301197d8ef954fecbb1a720
4aab517f0e1b213034bd883cf0eedf9c80b2b742f6c7584e5020301000102818100 9ce63679
7b0afb56b5a04a29e2c58bf8d4a1feb72c52f3bcd4d34c5658cd71eff7bcaf3eb2a8893d22a85
2d430f2de49d41001c158510a8e4c960e40780e9d025cb12434ea6e1414b6df3220f2a1feeb
b5cb9bf02f5a2eb88146557edc476dca486363aa76902a6b21111ce9ad7abd6359892fc48c2
88feb4f0ed799cdafdd3d024100fb5f6e7a3b78dd85ef64ee22114e8dc685a9a892424c75e48
3badac6a1830e239dd3bbdaf001bb9e5d67bfd491b1a3cdd39f1db581cd186ae42e1845a15
ea213024100f80729d14b5d3c63debc5e7310c42c160312c3e196935c6a1760f73d165e1da0
0300635d17adbe47b8bca304ae6ada4fa09733ebd8a8a1bf87afd2bd11845c2702404674b4
217c83df0b485330cfc9ac0bdee5ddeccab9dc767acb555736af546d651c3a997fbf1fad37b11
48057135308078bd6205c9c7a20eaecf3e287b9b82d93024020692f39be536cb4d04265453c
07a68b29d3a5ed30b408fb841a93b453dbf09b1c494cb2b98966b81097f5e582b54bd9e3ee
5e468f8559bda189844c58a1a739024100b42cb581a48d53a62502be95772c3a90c0bc1f801
c4097ae02ba2fc2fa41f2078bd3e49c30958ff1d7795f453204ad338b26939cfed31bc4746c92
b03169e323

They are ordered in a predefined format. It will tell the values of n, e, d, p, q, and a few other values. (Please review the slides to check the meanings of n, e, d, p, q).

The above "predefined format" is called Abstract Syntax Notation One (ASN.1). It is a standard way to define data structure used in telecommunications and computer networking, and especially in cryptography. You can use the following website to see what it represents for

https://holtstrom.com/michael/tools/asn1decoder.php

(This website can translate directly from BASE64 to ASN.1, but you should know there are two stages: BASE64->HEX->ASN.1)

The translated numbers are actually in the following order.

```
RSAPrivateKey ::= SEQUENCE {
    version           Version,
    modulus           INTEGER,  -- n
    publicExponent    INTEGER,  -- e
    privateExponent   INTEGER,  -- d
    prime1            INTEGER,  -- p
    prime2            INTEGER,  -- q
    exponent1         INTEGER,  -- d mod (p-1)
    exponent2         INTEGER,  -- d mod (q-1)
    coefficient       INTEGER,  -- (inverse of q) mod p
    otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
```

In the class, we know that the large number n can be factorized as p*q. This is a secret only known from the private key. The first "purple" part shows the value of n and the second and third purple parts show the values of p and q.

Question:
(1) How long is n, p, and q.
(2) Verify n is the product of p and q using Python.
(3) Re-do the experiments by generating your own keys.

(1)

```
34 22 54 bc 30 11 97 d8 ef 95 4f ec bb 1a 72 04 aa b5 17 f0 e1 b2 13 03 4b d8 83 cf 0e ed f9 c8 0b
2b 74 2f 6c 75 84 e5 02 03 01 00 01 02 81 81 00 9c e6 36 79 7b 0a fb 56 b5 a0 4a 29 e2 c5 8b f8 d4
a1 fe b7 2c 52 f3 bc d4 d3 4c 56 58 cd 71 ef f7 bc af 3e b2 a8 89 3d 22 a8 52 d4 30 f2 de 49 d4 10
01 c1 58 51 0a 8e 4c 96 0e 40 78 0e 9d 02 5c b1 24 34 ea 6e 14 14 b6 df 32 20 f2 a1 fe eb b5 cb 9b
f0 2f 5a 2e b8 81 46 55 7e dc 47 6d ca 48 63 63 aa 76 90 2a 6b 21 11 1c e9 ad 7a bd 63 59 89 2f c4
8c 28 8f eb 4f 0e d7 99 cd af dd 3d 02 41 00 fb 5f 6e 7a 3b 78 dd 85 ef 64 ee 22 11 4e 8d c6 85 a9
a8 92 42 4c 75 e4 83 ba da c6 a1 83 0e 23 9d d3 bb da f0 01 bb 9e 5d 67 bf d4 91 b1 a3 cd d3 9f 1d
b5 81 cd 18 6a e4 2e 18 45 a1 5e a2 13 02 41 00 f8 07 29 d1 4b 5d 3c 63 de bc 5e 73 10 c4 2c 16 03
12 c3 e1 96 93 5c 6a 17 60 f7 3d 16 5e 1d a0 03 00 63 5d 17 ad be 47 b8 bc a3 04 ae 6a da 4f a0 97
```

Convert | HEX to ASN.1 | Swap(In,Out) | Z | HEX to ASCII | ASCII to HEX | HEX to B64 | B64 to HEX

print (len("green part")x4)

= 1024

Output

```
U.P.SEQUENCE {
   U.P.INTEGER 0x00 (0 decimal)
   U.P.INTEGER                                                    n
0x00f38b7bb23a8ffe8e1810bbc851eca047cb2515e0a590eea6c80dedafc3c71812ed8135a37912f59c8c6f869d7cd82a5387d5fae0ed049e96ab2b88a3f13962
41fa4f58f3a47df7bba829331e0f564c9616ae3bdc16fa293c342254bc301197d8ef954fecbb1a7204aab517f0e1b213034bd883cf0eedf9c80b2b742f6c7584e5
   U.P.INTEGER 0x010001 (65537 decimal)
   U.P.INTEGER
0x009ce636797b0afb56b5a04a29e2c58bf8d4a1feb72c52f3bcd4d34c5658cd71eff7bcaf3eb2a8893d22a852d430f2de49d41001c158510a8e4c960e40780e9d
025cb12434ea6e1414b6df3220f2a1feebb5cb9bf02f5a2eb88146557edc476dca486363aa76902a6b21111ce9ad7abd6359892fc48c288feb4f0ed799cdafdd3d
   U.P.INTEGER  P
0x00fb5f6e7a3b78dd85ef64ee22114e8dc685a9a892424c75e483badac6a1830e239dd3bbdaf001bb9e5d67bfd491b1a3cdd39f1db581cd186ae42e1845a15ea2
13                                                                                                                              512
   U.P.INTEGER  Q
0x00f80729d14b5d3c63debc5e7310c42c160312c3e196935c6a1760f73d165e1da00300635d17adbe47b8bca304ae6ada4fa09733ebd8a8a1bf87afd2bd11845c
27                                                                                                                              512
   U.P.INTEGER
0x4674b4217c83df0b485330cfc9ac0bdee5ddeccab9dc767acb555736af546d651c3a997fbf1fad37b1148057135308078bd6205c9c7a20eaecf3e287b9b82d93
   U.P.INTEGER
0x20692f39be536cb4d04265453c07a68b29d3a5ed30b408fb841a93b453dbf09b1c494cb2b98966b81097f5e582b54bd9e3ee5e468f8559bda189844c58a1a739
   U.P.INTEGER
0x00b42cb581a48d53a62502be95772c3a90c0bc1f801c4097ae02ba2fc2fa41f2078bd3e49c30958ff1d7795f453204ad338b26939cfed31bc4746c92b03169e3
23
}
```

(2) n = real part (直接复制就好，都变第1

p = ...

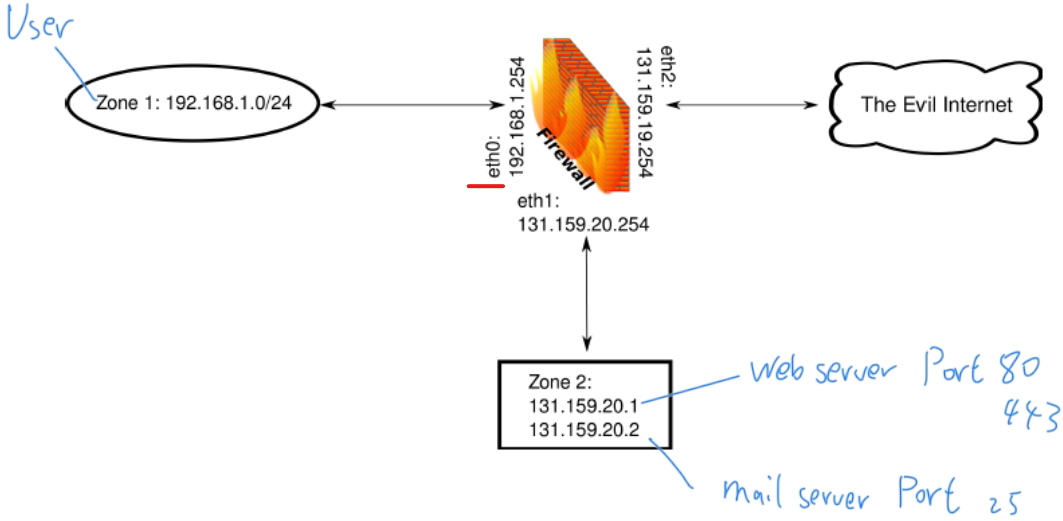
q = ...

print (n == p x q)

Normal

COMP9121 Week 12

1. We will practice firewall configuration in this task. The figure below shows the configuration you want to achieve. In Zone 2, you've got one Web server (131.159.20.1) on TCP ports 80 and 443, and one mail server (131.159.20.2) on TCP port 25. Your home users reside in Zone 1.



Your security policy is as follows:

1. Your home users may freely access any Web service, anywhere, on ports 80 and 443, but only if they initiate the connection themselves (i.e. they are allowed to browse the Web). No-one outside Zone 1 can initiate connections to Zone 1, on any port.

2. Everyone, including the Evil Internet, can access the web server (both ports) and mail server in Zone 2. However, no host in Zone 2 can initiate connections anywhere else.

To save you some writing, you can refer to the IP ranges (source and destination) by their 'zone names'. Use 'Ext' if you want to refer to the Evil Internet, 'Zone 1' if you want to refer to the IP range of Zone 1 etc.

Complete the table to define a stateless firewall configuration for the given scenario.

Interface	Source IP	Destination IP	Source Port	Destination Port	ACK	Action
Eth0	Zone1	*	*	80, 443	Any	allow
Eth1	Zone2	Zone1	80, 443	*	Set	allow
Eth2	Ext	Zone1	80, 443	*	Set	allow
Eth2	Ext	131.159.20.2	*	25 mail	Any	allow
Eth1	131.159.20.2	Ext	25 mail	*	Set	allow
Eth2	Ext	131.159.20.1	*	80,443 web	Any	allow
Eth1	131.159.20.1	Ext	80, 443 web	*	Set	allow
Eth0	Zone1	131.159.20.2	*	25 mail	Any	allow
Eth1	131.159.20.2	Zone1	25 mail	*	Set	allow
*	*	*	*	*	*	Deny

Z1 -> Z2 & Ext
Z2 -> Z1
Ext -> Z1
Ext -> Z2
Z2 -> Ext
Ext -> Z2
Z2 -> Ext
Z1 -> Z2
Z2 -> Z1

Q1
Q2

Any: Can establish connection
Set: Cannot establish connection by itself, can only reply

Fire wall interface