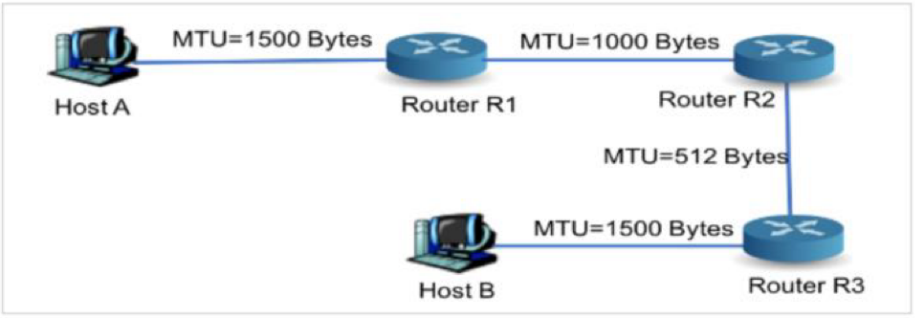
ip分段

这道题，没说明一定要用满mtu，所以，data要保证是8的倍数，才能够实现每个段的整除。

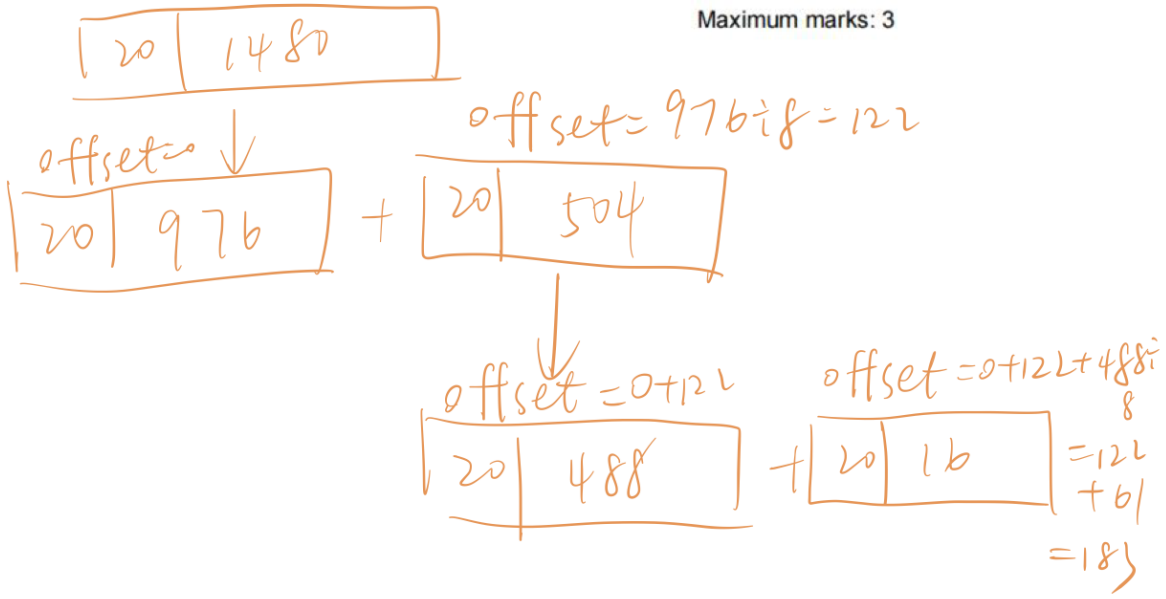
5



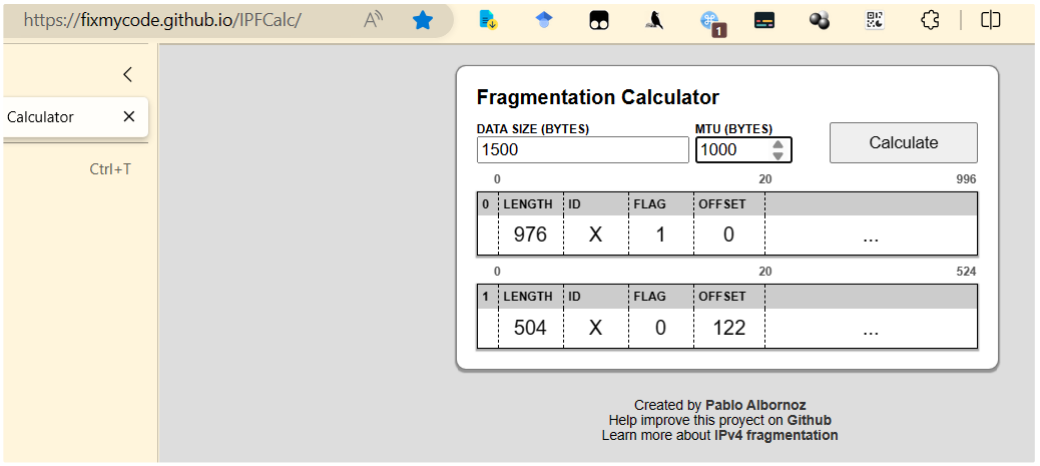
Consider the network in the illustration. Now suppose that the IP layer of Router R1 receives a datagram of size 1500 Bytes, including 20 bytes of IP header, from Host A. What would be the value in Fragment Offset field of the last fragment received at Host B? [ ] .

Maximum marks: 3

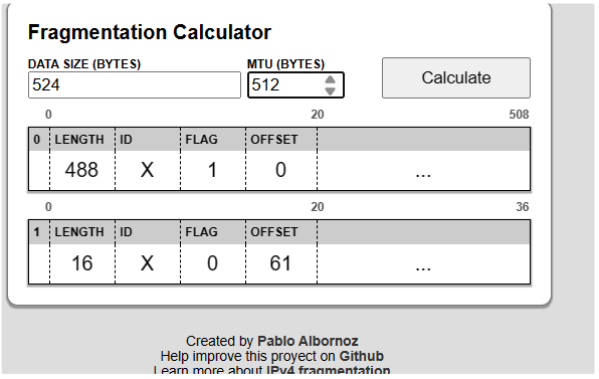
184



用计算器，data size是总的大小，包含头的。



直接划分第二段，是61，加上第一次划分得到的122，122+61=183



ed论坛上老师给的原因：

Dear Tutor,

In Q7, F3 (F3: 28 + 20 = 48 Bytes :: Offset=124, MF=0)
The last fragment's length "28" is NOT a multiple of 8, while "Offset should be expressed as multiple of 8 bytes"

Does it mean that we have to accept that the LAST fragment's length could not be a multiple of 8. Also we have to make sure every previous fragmentations' lengths are multiples of 8, so that the offset should be expressed as multiple of 8 bytes.

♡ Reply Edit Delete ···

Tim Arney STAFF 22h

It isn't necessary for the last fragment, *because* there are no fragments that come after it. Whether or not it contains a multiple of 8 bytes won't affect the reassembly.

However, all fragments that come before it *must* carry a multiple of 8 bytes, to ensure the correct reassembly. Otherwise the offset of the last fragment won't be correct.

length,

5 Suppose that a 5700-byte IPv4 datagram (including IP headers) arrives at a router R1. R1 determines that the datagram is to be forwarded on an outgoing link with MTU of 2020 bytes. R1 creates the necessary IPv4 fragments and forwards them on the outgoing link. All fragments arrive in the correct order at the next hop router R2. R2 determines that all fragments are to be forwarded on an outgoing link with MTU of 1220 bytes. How many IPv4 fragments does R2 forward on the outgoing link? For each transmitted fragment indicate the following IPv4 header fields: length, MF flag and offset. No explanation is required.

Fill in your answer here

1.mf为1，表示后面还有包
2.算offset的时候要除以8
3. payload + header = MTU

Fragment 1: 1220, 1, 0;
Fragment 2: 820, 1, 150;
Fragment 3: 1220, 1, 250;
Fragment 4: 820, 1, 400;
Fragment 5: 1220, 1, 500;
Fragment 6: 500, 0, 650;
0.5 mark for the correct fields for each fragment.

offset计算公式：前一个包的offset + 前一个包的payload / 8

fragment length MF offset
Fragment 1220, 1, 0;
Fragment 820, 1, 150;
Fragment 1220, 1, 250;
Fragment 820, 1, 400;
Fragment 1220, 1, 500;
Fragment 500, 0, 650;

写length的时候，把头算上。是头加上数据。

Words: 24

写length的时候，把头算上。是头加上数据。header fields的时候

网络地址划分

34=0010 0010，这里的描述有点问题。一个地址块的地址应该是主机全为0的。

9 The XYZ Company has requested a block of IP addresses from an ISP. The block that was allocated to XYZ was **191.56.125.34/25**. 新描述：该公司的子网号是25位，其中一个主机的ip地址是191.56.125.34

Calculate the number of addresses in this block. 2^7 = 128

Find the network address. **Answer in the a.b.c.d/x format.** 191.56.125.0/25 主机号全为0

Find the broadcast address. **Answer in the a.b.c.d/x format.** 191.56.125.127/25

Find the range of addresses that would be available for use by hosts. **Answer in the a.b.c.d/x format** from 191.56.125.1/25 to 191.56.125.126/25

比网络地址加1 比广播地址少一

Maximum marks: 3

交互机，数据链路层的大题

网络安全

Suppose *N* people want to communicate with each of *N* – 1 other people using symmetric key encryption. All communication between any two people, *i* and *j*, is visible to all other people in this group of *N*, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole?

Now suppose that public key encryption is used. How many keys are required in this case?

Provide a short explanation for your answers in the space below.

Fill in your answer here

网络安全的题不考了。

Maximum marks: 2

Answer:

Symmetric Key Encryption: A symmetric key would be required between each pair of people. So Person 1 would require (N-1) keys to communicate with others. Person 2 would require (N-2), Person 3 would require (N-3) and so on. Thus total keys required = (N-1) + (N -2) + (N-3) .... + 1 = N(N-1)/2.

Public Key Encryption: Each person would only require a public, private key pair. So the total keys required = N pairs of public, private key pairs.

26 What is the role of a Certification Authority (CA) in Public Key Infrastructure (PKI)?

Select one alternative:

网络安全的题不考了。

- CA's are not used in PKI
- Issues a session key to both end parties for communication
- Maintain private keys of all authenticated users
- Guarantee that the public key of the registered user is authenticated by issuing a digital certificate

27 SuperMail wants every email to be authenticated and protected from modification or tampering while it is transit from the sender to the receiver. Suppose Alice is sending an email *M* to Bob. Assume that a SuperMail employee proposes the following solution: Alice's software should encrypt M using Bob's public key. In other words, Alice's software should send E_{KB+} (M) to Bob. Can you comment on whether the employee's solution meets the requirement stated above. Justify your answer.

网络安全的题不考了。

Fill in your answer here

Maximum marks: 1

Answer:

Encryption does not provide authenticity/integrity. Anyone can send such a ciphertext.

Ayda wants to transmit the assignment marks from her home computer to Salil at UNSW. She is worried that an enterprising COMP3331/9331 student may have hacked a router along the path and might modify the message to improve their mark. So when Ayda sends a message M to Salil, she also calculates H = Hash(M) and appends H to the message. Salil receives M and H, and calculates H' = Hash(M), only accepting the message as valid if H' = H. You can assume that Hash is a well-known secure hash function that is one-way and collision resistant.

Could an enterprising COMP3331/9331 succeed in changing their mark? If yes, then explain how the attack can be launched. If not, then explain how the approach mentioned above is secure. If the attack is possible, also propose a modification to the way marks are transmitted between Ayda and Salil that would prevent the attack and ensure message integrity in a more general sense.

如何修改：截取了信道，直接扔掉ayda的信息，然后生成新的对应的哈希。（因为这个哈希算法，所有人都知道）

提出新方法：1. 对称密钥，提前约定好了一个密码。互相知道。用这个密码加密

2. 数字签名。digital signature，Ayda可以将她的数字签名(使用她的私钥生成)固定在消息上。sall可以使用她的认证公钥验证签名，以检查消息在整个过程中没有被修改。

Salil has put up his public key on his webpage. He has included a certificate from a certification authority called VeriSign. You wish to download his public key and confirm that it indeed belongs to him. For this verification, you will need to use the following key on the certificate:

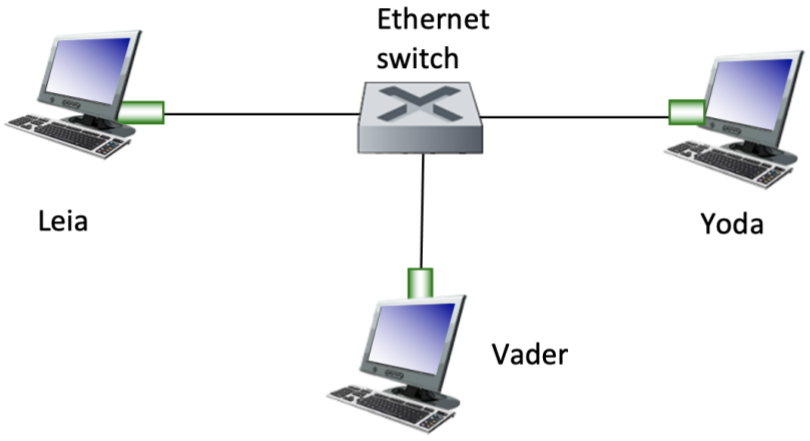
Select one alternative:

- Salil's private key
- Your public key
- Verisign's private key
- Your private key
- Versign's public key

```
Versign's public key
```

Authentication Switch Network

Consider the network depicted below where Leia, Yoda and Vader are connected through an Ethernet switch. The switch is assumed to be functioning correctly (i.e. it is not compromised) and only forwards the frames to the intended destination as per the destination MAC address (i.e., it has learnt of the network topology and its switch table is correctly populated).



Leia sends a message to Yoda. Yoda knows Leia's true IP address. In each scenario, explain why or why not authenticity is guaranteed - i.e., Yoda can tell for sure that the the message is indeed coming from Leia and not from Vader.

Scenario 1: Leia sends the message to Yoda over UDP

Scenario 2: Leia sends the message to Yoda over TCP: Leia establishes a TCP connection with Yoda, sends the message and then closes the TCP connection.

1）不能保证真实性，因为Vader可以使用Leia的IP地址作为IP数据段的IP。

2）通过以下意义保证了真实性：要通过TCP发送消息，Vader必须首先与YODA建立TCP连接，即发送SYN并接收SYN ACK。如果Vader假冒Leia的IP地址，Yoda将把他的Syn Ack发送给Leia（不是Vader）。

该交换机不会将包含此SYN ACK段的包转发给Vader，Vader无法看到Yoda的Syn Ack。因此，Vader很难用最终的ACK做出响应来完成TCP连接设置，因为他需要猜测YODA的初始序列编号（这是0到2^32 -1之间的随机值）。

如果Vader试图完成3次握手，但ACKS错误的序列编号，YODA将无法完成TCP连接设置，因此Vader无法发送消息。

Alice wants to send a message *m* to Bob and prove that the message is from her. Appending which of the following to *m* would achieve this goal?

Select one alternative:

- *m* encrypted with Alice's public key
- *m* encrypted with some random number only known to Alice
- *m* encrypted with Bob's public key
- *m* encrypted with Alice's private key ✓
- *m* encrypted with a Certificate Authorities public key

Consider a setting where Vader, an adversary has full access to the communication channel between Yoda and Leia. Yoda wants to send a message to Leia.

In each scenario below, explain whether or not Leia can always verify the authenticity of the received message *m*, i.e., verify that the message *m* is indeed sent by Yoda (and not by Vader claiming to be Yoda).

K^+_L and K^+_Y are the public keys of Leia and Yoda, respectively. H is a cryptographic hash function which is known to everyone, i.e., Leia, Yoda and Vader.

Scenario 1: Leia receives a message [m, $K^+_Y(H(m))$]

Scenario 2: Leia receives a message [m, $K^+_L(H(m))$]

You must provide justifications for your answers for both scenarios.

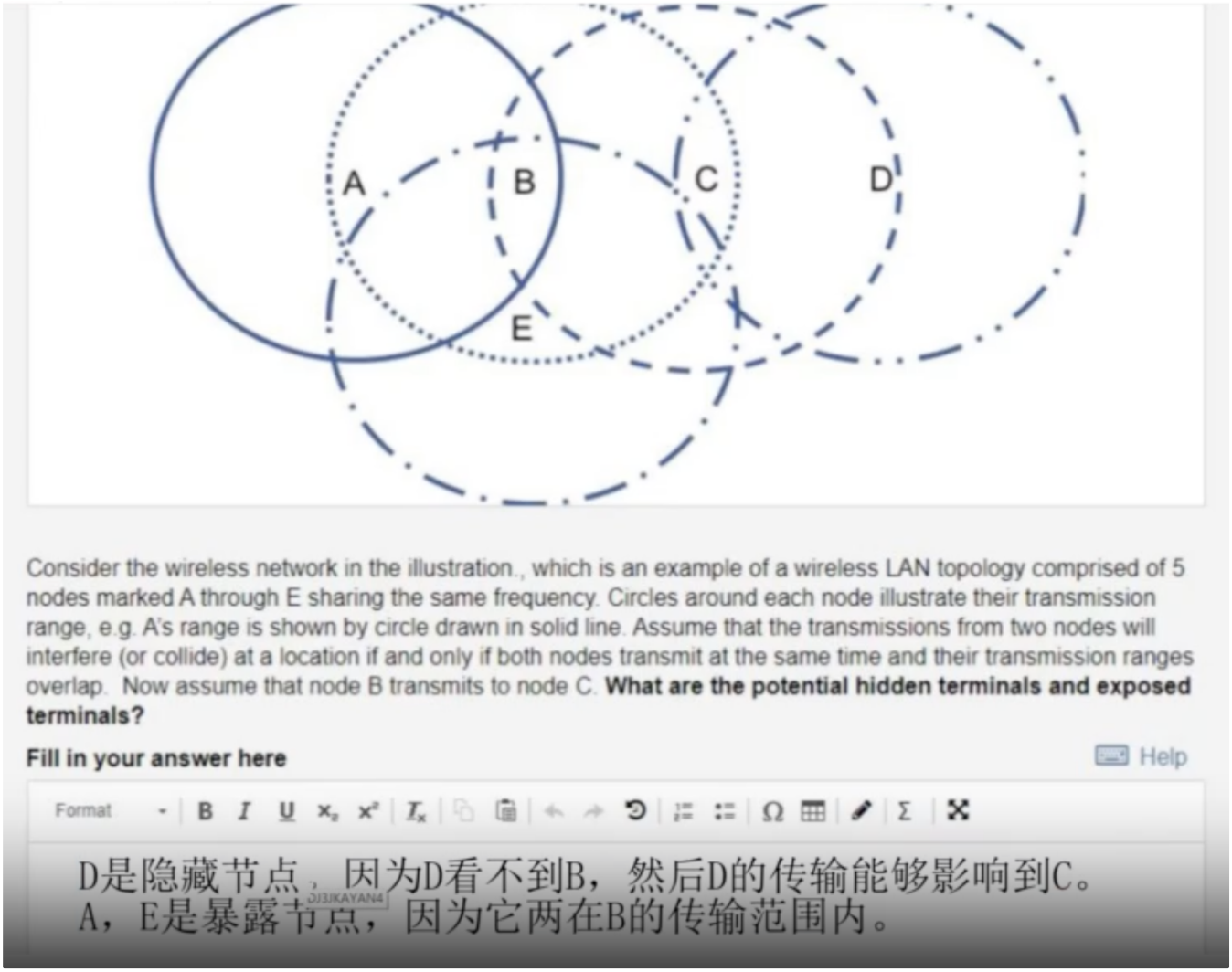
Fill in your answer here for both scenarios:

这两都不行

情景1：哈希函数是广为人知的。Y的公钥也是广为人知的。

情景2：哈希函数是广为人知的。L的公钥也是广为人知的。

wifi



B给C发的时候，C不算暴露节点。因为，暴露节点，就是指那些原本能发，也打算发，但听到了B以后，不发了的节点。C是正常通信的节点。

crc在线计算器