1. *When the Domain Name System resolves a machine name, it returns a set of one or more IP addresses. Explain why.*

If the site you are look for only has one location for the directory, and which is being accessed by countless people on the world at the same time, users will have to wait for too long since they are in the same queue. So, the purpose of having one domain name corresponds to multiple IP addresses is to avoid overloading.

1. *Can you configure your browser to open multiple simultaneous connections to a Website? What are the advantages and disadvantages of having a large number of simul-taneous TCP connections?*

Yes, multiple concurrent TCP connections is possible.

Advantages:

Since multiple concurrent connections is possible, it enhances the performance of the connection such as downloading all different 313 videos from Ecampus at the same time.

Using TCP has great reliability.

Multi-concurrent connections also lower the rate of failure of transmission like package missing.

Disadvantages:

Since congestion method is applied, a sudden slowdown of data transfer might lead to blocks of connections.

1. *Is it always crucial to know that the message you have sent has arrived at its destination safely? If your answer is “yes”, explain why. If your answer is “no”, give appropriateexamples.*

No, it is not crucial to know. Most of the programs assumes the message might not be received by its destination. I think this is because waiting for reply from the receiver is too pricey. Since the program usually deliver packets to many systems, it is assumed that some of the systems will receive message from it. For example, when testing if a remote system is available for connections over the network, the deliver program will not receive any reply if something goes wrong, then it knows error has occurred.

1. *The original HTTP protocol uses TCP/IP as the underlying network protocol. Foreach page, graphic, or applet, a separate TCP session was constructed, used, and torndown. Because of the overhead of building and destroying TCP/IP connections, therewere performance problems with this implementation method.*
2. *Would using UDP rather than TCP be a good alternative? List the pros and cons.*

|  |  |
| --- | --- |
| TCP | UDP |
| Connection-oriented protocol | Datagram oriented protocol |
| Guarantees the delivery of the data | Does not guarantee the delivery of the data |
| Has flow control | Does not have flow control |
| Ensures in-order delivery | Does not ensure in-order delivery |
| Slower | Faster |

UDP is better for sending small packages while TCP is better to deliver huge amount of data which requires a stable connection.

1. *What other changes could you make to improve the performance of the original HTTP?*

Before the delivery of the data, predict and evaluate if this delivery is large enough that needs a reliable connection, and choose between UDP and TCP.

1. *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 awhole? Now suppose that public key encryption is used. how many keys are required in this case?*

In the case of SYE, if sender and receiver use different key to communicate:

1 secret key is required for every single connection. Since N people needs to talk to N-1 other people, there will be N(N-1) connections in total, thus N(N-1) keys.

If sender and receiver use the same key to communicate:

The total number of keys required will be divided by 2, which is N(N-1)/2 keys.

In the case of PYE, since every person has 2 keys, one public key and one private key, where public key for encryption and private key for decryption, the total number of keys is 2\*N.

1. *Using the RSA public key encryption algorithm discussed in class, choose p=5 and q=11 to encrypt the word “hello”. (Represent the plaintext as a sequence of integer codes of the characters in the string, where ’a’ has code 1, ’b’ has code 2, etc..) Apply the decryption algorithm to recover the original plaintext message. To make the grader’swork simpler, pick k\_e= 7.*

n = p\*q = 55

f(n) = (p-1)\*(q-1) = 40

k\_d \* 7 mod 40 = 1

k\_d = 23

Then:

d = e^(-1) mod (f(n))

= -13 mod 40

= (27 – 40) mod 40

d = 27

Since a=1, b=2….

H = 8

E = 5

L = 12

L = 12

O = 15

8^7 mod 55 = 2

5^7 mod 55 = 25

12^7 mod 55 = 23

12^7 mod 55 = 23

15^7 mod 55 = 5

Thus 2, 25, 23, 23, 5 are encrypted values

To decrypt the value, we then use:

2^23 mod 55 = 8

25^23 mod 55 = 5

23^23 mod 55 = 12

23^23 mod 55 = 12

5^23 mod 55 = 15

8 = H

5 = E

12 = L

12 = L

15 = O

The decrypted message is hello.