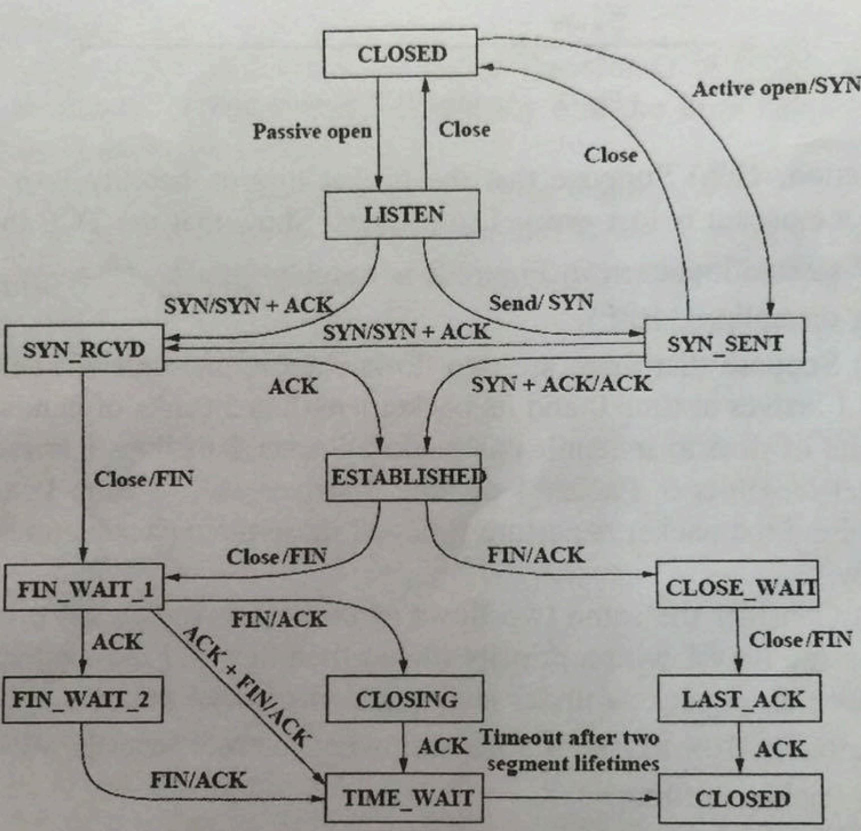
EE 3650 **Introduction to Computer Networks** (Total 100 points.) June 22, 2015.

Student's name:

Student's number:

1) (TCP, 20%) Please be brief in answering the following questions.

   a) (2%) Figure 1 is the state transition diagram of TCP. Please trace the *normal* three-way handshake of both client and server on Figure 1.
   (Please **plot on the graph directly** and **send this sheet back** with you name and your student number.)



1 2 3 4 5 6

Fig. 1. State Transition Diagram of TCP

   b) (2%) In order to support multiple application processes, what are the 4-tuples used as a TCP demux key?

   c) (2%) Show how TCP compute AdvertisedWindow for flow control. (Hint: use the following pointers and parameters: MaxRcvBuffer, MaxSendBuffer, LastByteRead, NextByteExpected, LastByteRcvd, LastByteAcked, LastByteSent and LastByteWritten.)

   d) (2%) Show how TCP uses CongestionWindow, AdvertisedWindow, LastByteAcked, and LastByteSent to compute EffectiveWindow that does both flow control and congestion control.

   e) (2%) Describe how TCP (without fast recovery) adjusts CongestionWindow after a timeout.

   f) (2%) Describe how TCP updates its CongestionWindow when an ACK arrives.

   g) (2%) Give a reason why TCP has to estimate RTT.

h) (2%) Describe how self-clocking is used in Nagle's algorithm and when such an algorithm should be turned off?

i) (2%) Describe how RED is used in conjunction with TCP to avoid synchronized backoff?

j) (2%) Describe fast retransmit and fast recovery in TCP.

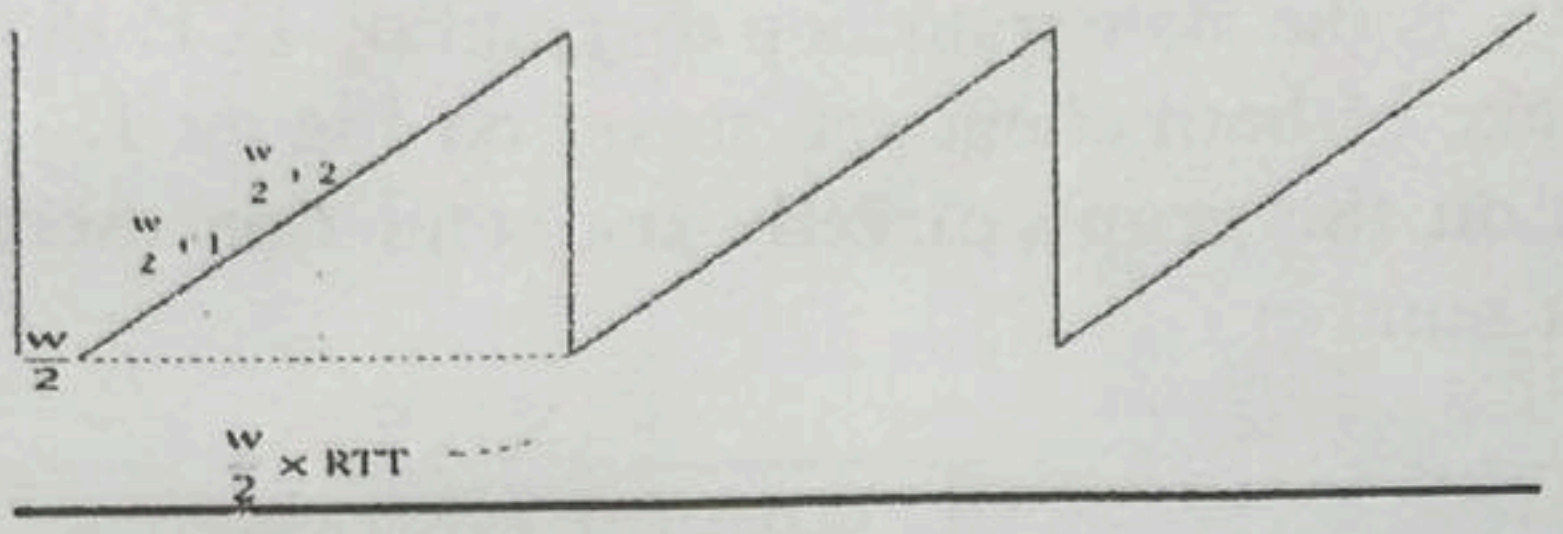


Fig. 2. An ideal TCP sawtooth pattern

F

flow 1

2 0

6 5

1 1

8

10

2) (TCP equation, 10%) Suppose that the packet loss probability is ρ. Consider the ideal case that one packet is lost every $1/\rho$ packets. Show that the TCP throughput under the ideal TCP sawtooth pattern in Figure 2 is roughly $\frac{1}{RTT}\frac{1}{\sqrt{\rho}}\sqrt{\frac{3}{2}} \approx \frac{1.22}{RTT}\frac{1}{\sqrt{\rho}}$.

3) (Queueing disciplines, 10%)

a) (5%) Suppose that there are two flows sharing one unit of bandwidth. Packet 1 of flow 1 arrives at time 0 and its packet length is 5 (units of bandwidths), i.e., it takes 5 units of time to transmit this packet. Packet 2 of flow 1 arrives at time 2 and its packet length is 6. Packet 1 of flow 2 arrives at time 1 and its packet length is 8. Find the packet departure times of these three packets under the *fair queueing* policy.

b) (5%) Consider the same two flows of packets as in the last problem. Suppose that we assign flow 1 with a priority higher than flow 2. Find the packet departure times of these three packets under such a *priority queue* policy.

4) (Security attacks, 10%) Describe the following Internet security attacks.

a) (2%) Packet sniffing.

b) (2%) IP spoofing.

c) (2%) Denial of Service (DOS).

d) (2%) Playback attack.

e) (2%) Man-in-the-middle attack.

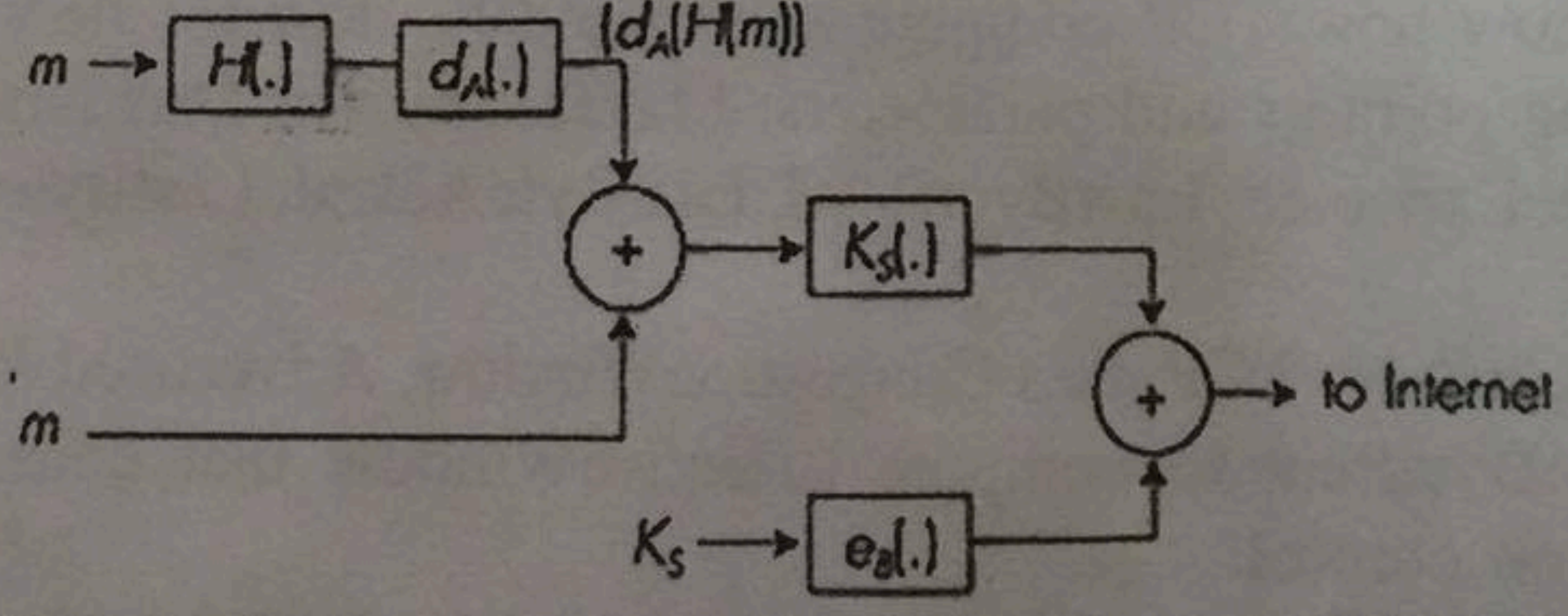


Fig. 3. The operations of sending an PGP email from Alice to Bob

5) (PGP, 6%) In Figure 3, we show the operations of PGP for sending an email from Alice to Bob. Assume that the public keys are available to each other. The email consists of two parts: one is a session key encoded by Bob's public key, and the other part, encoded by the session key, is the message and a digital signature signed by Alice.

   a) (2%) (Confidentiality) Explain briefly why the email is a secret between Bob and Alice.
   b) (2%) (Authentication and non-repudiation) Once the email is decoded by Bob, explain briefly why Bob knows that it is an email sent by Alice.
   c) (2%) (Data integrity) Explain briefly why Bob can be sure that the email has not been altered.

6) (JPEG and MPEG, 6%)

   a) (2%) Consider the DCT(Discrete Cosine Transform) in JPEG, after the transform, it has two parts: the low spatial frequency and the high spatial frequency, which one is more essential? Why?
   b) (2%) In JPEG, which step or steps will lose information?
   c) (2%) Suppose seven frames encoded by MPEG are I, B, B, P, B, B, and I frames. What is the sequence that these seven frames are transmitted? IBBPBBI.

7) (Applications 8%)

   a) (2%) What does a DNS server do?
   b) (2%) What is the main difference between HTTP 1.0 and HTTP 1.1?
   c) (2%) The original design for e-mails only allows transmitting ASCII characters. Describe how base64 encoding is used to transmit binary data in emails. What are the 64 ASCII characters in the base64 encoding?
   d) (2%) What is an overlay network?

8) (Huffman coding, 5%) Consider a sequence contains only three symbols S_1, S_2 and S_3 with probabilities 0.5, 0.3 and 0.2 respectively. Now, for achieving better efficiency, each two symbols are concatenated into a new symbol. Use the Huffman coding to represent these symbols. (Describe every step in details.)

9) (LZ coding, 5%) Consider the following LZ encoded binary sequence, 0000100011001010000000100001100100001111 Suppose the indexes are encoded using 4 bits. Please decode it to find the original sequence.

10) (Diffie-Hellman key agreement 5%)
Consider two (publicly known) parameters 3 and 5 (3 is the generator of the group $\{1, 2, 3, 4\}$), i.e., $3^1 \ mod\ 5 = 3$, $3^2 \ mod\ 5 = 4$, $3^3 \ mod\ 5 = 2$, and $3^4 \ mod\ 5 = 1$. Suppose Bob selects 2 as his secret number and Alice selects 3 as her secret number.

    a) (2%) What number should Bob send to Alice under the Diffie-Hellman key agreement algorithm?
    b) (3%) What is the common secret number (key) between Bob and Alice under the Diffie-Hellman key agreement algorithm?

11) (RSA, 15%)

    a) (5%) Let $\phi(n)$ be the number of positive integers that are less than n and relatively prime to n. Suppose that a is a positive integer relatively prime to n. Show that

$$a^{\phi(n)} \bmod n = 1.$$

b) (5%) Suppose p and q are two prime numbers. Let $n = pq$. Show that

$$\phi(n) = (p-1)(q-1) = \phi(p)\phi(q).$$

c) (5%) Suppose that e is relatively prime to $(p-1)(q-1)$ and $de \bmod (p-1)(q-1) = 1$. Furthermore, suppose M is relatively prime to n and $C = M^e \bmod n$. Show that $M = C^d \bmod n$.