Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets if necessary.

Total Marks: **30**

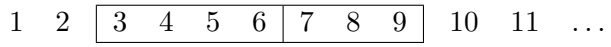
[10] 1. This question refers to the article *Peer-to-Peer Systems*, by by Rodrigo Rodrigues and Peter Druschel. As the authors say, the term P2P has been defined in different ways; list, and briefly explain, three properties of a P2P system.

Solution: Any three of the following, defined on pp. 72 and 74 of the article.

- High degree of decentralization
- Self-organization
- Multiple administrative domains
- Low barrier to deployment
- Organic growth
- Resilience to faults and attacks

[10] 2. The TCP sliding window mechanism operates at the octet level; it solves two important problems: efficient transmission and flow control.

Consider the following window, where 1 through 11 are octets:



Let "ack" abbreviate "acknowledged."

(a) Explain what is the status (sent/ack) of the octets in this example.

(b) How does the sliding window improve the efficiency of transmission?

(c) How does it improve flow control?

Solution: (a) 1 and 2 have been sent and ack; 3–6 have been sent but 3 has *not* been ack yet (while 4–6 might, or might not, have been ack); 7–9 may be sent, but they have not been sent yet; 10–11 cannot be sent at this point. (b) The sliding window allows several octets to be sent before an ack arrives, increasing the throughput by keeping the network busy. (c) The sliding window protocol also solves the end-to-end flow control problem, by allowing the receiver to restrict transmission until it has sufficient buffer space to accommodate more data (the receiver controls the size of the window).

[10] 3. Recall that an Apache HTTP server password scheme uses a function `crypt()` which in turn computes a number of DES rounds.

For example,

```
eYZUcvy1BSUak == crypt("2c8c2e49","eY")
```

On the other hand, DES takes as input a 64-bit string and a 56-bit string, and `crypt()` computes rounds of DES.

Explain how the input to `crypt()` is related to the input to DES.

Solution: In the above example, `crypt()` has two arguments:

`2c8c2e49` and `eYZUcvy1BSUak`

Call the first argument the "password" and the second the "salt." The password can be of any length, but only the first 8 ASCII characters are used; an ASCII character requires 7 bits, and so it takes $7 \cdot 8 = 56$ bits to encode the password. When `crypt()` invokes DES for the different rounds, it starts the first round with an input consisting of a string of 64 zero bits, and a string of 56 bits which encodes the password. It feeds each round with the output from the previous round slightly perturbed by the salt. In fact, only the first two characters of the salt are used (and only the lower case letters, the upper case letters, and the digits, are allowed as characters for the salt). These two characters can be encoded with 6 bits each, as in Base64, and hence they yield 12 bits (which, as mentioned, are used for the perturbation). Finally, the output of `crypt()` is a 13 characters long string, where the first two characters are the salt, and the remaining 11 characters are a Base64 encoding of the output of the rounds. Why 11 characters? Because the output of DES is 64 bits, which is not divisible by 6; so 64 bits are padded (with 00) to be 66 bits, which when divided by 6 yields 11 Base64 symbols.