Name _____ Student No. _____

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

Total Marks: **30**

[10] 1. Define the following terms:

(a) Iterative versus concurrent server.

(b) Encapsulation versus demultiplexing.

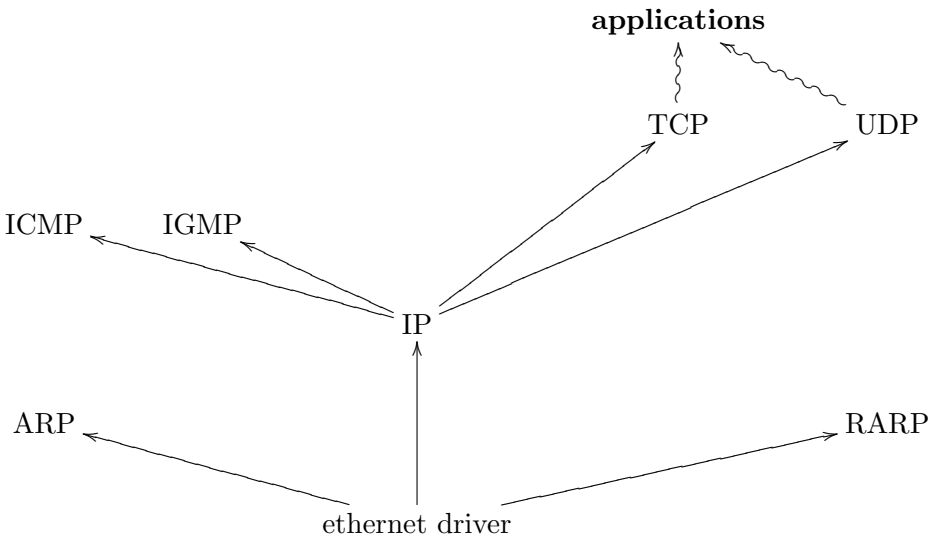
(c) Electronic code book versus cipher block chaining.

Solution: An iterative server can process only one client at a time; a concurrent server can service several clients simultaneously (by spawning new processes, tasks or threads).

As data is sent down the protocol stack, each layer add information to the data by prepending headers and/or trailer information to the data that it receives, until the whole thing is sent as a stream of bits across the network. Demultiplexing is the reverse operation, up the protocol stack, as data arrives at its destination.

In ECB a long message is broken up into message chunks, and then each chunk is encrypted (with the same key). In particular, if chunk i and chunk j are identical, so are cipher blocks i and j. In CBC, each block (except the first one for which we need an explicit "initial value") is xor'ed first with the result of encrypting the previous block *before* it is itself encrypted (with the same key).

[10] 2. Explain the following diagram; concentrate on the "data flow." Be brief.



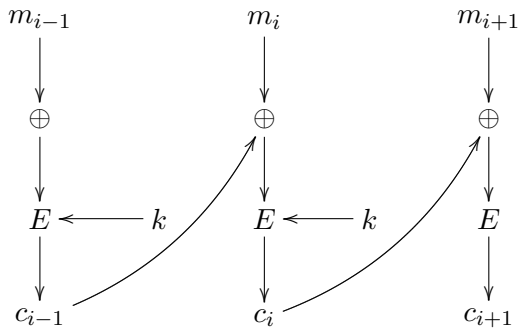
Solution: This diagram portrays a (somewhat simplistic) view of demultiplexing as data travels up the protocol stack.

First the bits arrive "on the wire" into the ethernet driver. There are three layers of arrows: in the bottom layer we have demultiplexing based on frame type in the ethernet header. In the second (middle) layer we have demultiplexing based on protocol value in IP header. In the third (top) layer we have demultiplexing based on destination port number in the TCP & UDP header.

Full names given below for completeness:

ARP: Address Resolution Protocol
RARP: Reverse Address Resolution Protocol
IP: Internet Protocol
ICMP: Internet Control Message Protocol
IGMP: Internet Group Management Protocol
TCP: Transmission Control Protocol UDP: User Datagram Protocol

[10] 3. Consider a portion of cipher block chaining (CBC), depicted in the figure below.



(a) Suppose that an adversary intercepts the message, and wants to flip the 7-th bit of message block m_i, that is, he wants to change the ciphertext in such a way that the 7-th bit of message block m_i is flipped. How would he go about it? Justify your answer.

Solution: All he needs to do is to flip the 7-th of c_{i-1}. The reason is that c_i is xor'ed with the result of decrypting c_i with key k; call the result of this decryption d_i. Then, $m_i = d_i \oplus c_{i-1}$, and if $x \oplus y = y$, then $\bar{x} \oplus y = \bar{z}$.

(b) How could the legitimate recipient of the message detect the tampering?

Solution: By changing one bit of c_{i-1}, the attacker is forced to change m_{i-1}. Further, if the encryption/decryption algorithm has a good "mixing property," by changing one bit of c_{i-1} the attacker is likely to change many bits of m_{i-1} in a way that he has no control over. This could be detected by the recipient, especially if a CRC is used.