CS3CN3/SE4C03 Test 1 Winter 2011

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) Active vs. Passive attacks
Defined on pg 15 in textbook

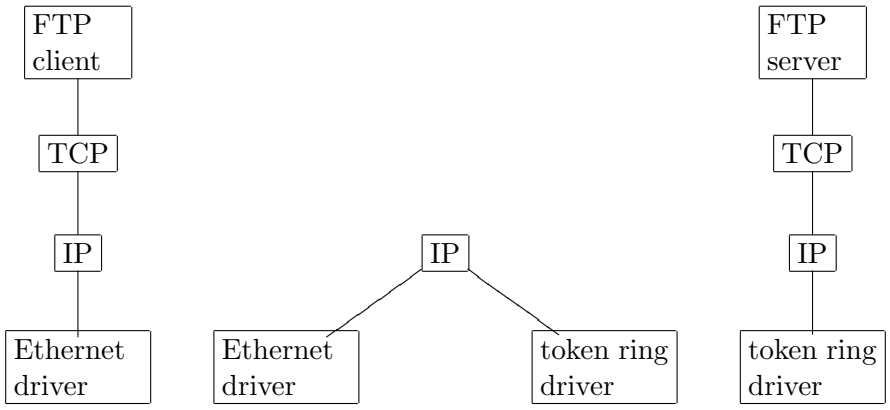
(b) Covert channel
Define on pg 30

(c) Symmetric vs. Asymmetric cryptography
Defined on pg 47 & pg 50

(d) Message digest
Defined on pg 54

(e) Substitution vs. permutation (as in "data transformation")
Define on pg 61

[10] 2. Suppose that we have two networks, an *ethernet* and a *token ring* connected into an internet by a router as in the following diagram:



(a) Which layers are *end-to-end* and which layers are *hop-by-hop*?

Top two layers (FTP and TCP are end-to-end. Bottom two are hop-by-hop.

(b) What is the difference between the TCP layer and the IP layer?

The TCP layer provides data flow between two hosts. In particular, TCP provides reliable flow of data: it divides the data into chunks; it does acknowledging of received packages; it sets timeouts to acknowledgments from the other side. The IP layer handles the movement of packets around the network; so it does routing, and it is aware of the network topology, while TCP is not.

(c) In the above diagram, indicate the missing connections and label the two networks and the router.

The ethernet network is described by the left column; the token-ring network is described by the right-most column; the middle "triangle" is the router. The two ethernet drivers are connected; the two token drivers are connected. There is a connection between left IP box and the middle IP box, and a second connection between the middle IP box and the right IP box. FTP and TCP boxes are connected directly to each other.

[10] 3. Suppose that we wish to encode (transform) blocks of k-bits. Explain:

(a) $k(2^k - 1)$ bits are sufficient to describe a mapping that is a *reversible substitution.*
There are 2^k k-bit blocks. Each such block is mapped to another k-bit block; this can be described with $k2^k$ bits. But block number 2^k, the "last block" does not have to be specified in a reversible substitution, as it has to go to the last remaining unused k-bit block.

(b) $(k-1)\lceil \log_2 k \rceil$ bits are sufficient to describe a mapping that is a *permutation.*
Same rational as above, except that we require $k\lceil \log_2 k \rceil$ bits to describe a permutation from k elements to k elements; each of the k elements in the domain have to be mapped to a new location; each such location can be described with $\lceil \log_2 k \rceil$ bits. Again, we can "shave-off" the last element, since there is no choice as far as where it goes.

(c) What are the advantages/disadvantages of each?
The advantage of a substitution is that it performs stronger mixing, while it requires a lot of bits to give explicitly. The advantage of a permutation is the efficiency of description, while from an "information theoretic" point of view it does not mix very well—for example, it preserves the number of zeros and ones.