CS3235 Tutorial for week 6
(Sept 13-Sept 17, 2004)

September 11, 2004

1. Describe how a digital-signature/checksum/message-digest can be appended to a (plaintext) message, and how such a digital signature can be trusted. (For example - couldn't someone just change the message and then re-create a new changed signature? How could we ensure that this could not happen?)

2. Consider a system which will use a secure web-based transfer of documents, with a secure login system for access to more critical documents. The documents are classified as either top secret, restricted or unrestricted, and the intended users of the system are administrators $(a_1, a_2, \ldots)$, teachers $(t_1, t_2, \ldots)$, students $(s_1, s_2, \ldots)$, and others $(o_1, o_2, \ldots)$. Top secret documents might be ones such as personnel or finance records, and are only available to relevant administrative staff. The restricted documents include various student and research projects which will be available to any of the teaching staff, and to relevant students. Outline the use of the BLP model to model such a system, specifying the subjects, security levels and sample categories, perhaps with brief examples.)

3. Given the security levels `T`, `S`, `C` and `U` (ordered from highest to lowest) and the categories `M`, `N` and `P`, specify what type of access (`read`, `write` or `both`) is allowed in each of the following situations. Assume that access controls allow anyone access unless otherwise specified:

(a) Paul, cleared for `(T,{M,P})` wants to access a document classified `(S,{N,P})`.

(b) Anna, cleared for `(C,{P})` wants to access a document classified `(C,{N})`.

(c) Jesse, cleared for `(S,{P})` wants to access a document classified `(C,{P})`.

4. Some questions on checksums:

(a) What is the overriding reason that we use polynomial long-division to calculate an FCS?

(b) How many extra bits are required to detect a single bit error in a message of 128 8-bit bytes?

(c) How many extra bits are required to detect an odd number of error bits in a message of 128 8-bit bytes?

5. In the discussion on entropy and transmission rate, the received data was corrupted 50% of the time, with each bit of input data being inspected and then either being changed (flipped), or not, with a probability of 0.5. Consider the case where the bit is forced to a 1, or not, with a probability of 0.5. Does this change the situation? Justify your intuition about this by re-working the entropy calculation for $r(X)$.