CS3235 Tutorial for week 5
(Sept 8-Sept 12, 2003)

6th September 2003

1. **Question 1, Chapter 32 in textbook:** Let X represent the roll of a red die, and let Y represent the sum of the values from rolling a red die and a blue die. Prove that $p(X = 3 \mid Y = 8) = \frac{1}{5}$.

2. An essential component of the RSA cryptographic scheme is raising a large number x to a large power y (modulo some other number n). We could do this by just multiplying x by itself $y - 1$ times (we will call this method A), but as pointed out in the notes (page 31) this is not fast. The notes suggest techniques (methods B and C) for calculating x^y.

   (a) Estimate the time complexity of method A and method B using big O notation.

   (b) Given that a multiplication takes 1mS, and assuming that all other operations are instantaneous, estimate the time to calculate x^y using each method, where y is a randomly generated 100 digit number.

3. Calculate the entropy of a source transmitting 64 different characters, with the probabilities of E, T, A, O, N, S, H, R being $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{16}$, $\frac{1}{16}$, $\frac{1}{16}$, $\frac{1}{16}$, $\frac{1}{16}$ and $\frac{1}{16}$ respectively and the other 56 characters being evenly distributed.

4. Devise a Huffman encoding for the above data.

5. What is the unicity distance of the one-time pad?