1. Let $X$ represent a 2-bit string that can have the values 00 (= 0), 01 (= 1), 10 (= 2) or 11 (= 3) with equal probability, and then assume that this string is corrupted by a signal, giving a result $Y$.

   (a) if the corruption signal *sets* each bit to a 1 with probability 50%, calculate $p(X = 1 \mid Y \geq 1)$ (The probability that $X$ was 01 given that $Y$ is now greater than or equal to 01, i.e. it is 01 = 1, 10 = 2 or 11 = 3).

   (b) if the corruption signal *flips* each bit with probability 50%, calculate $p(X = 1 \mid Y \geq 1)$ (The probability that $X$ was 01 given that $Y$ is now greater than or equal to 01, i.e. it is 01 = 1, 10 = 2 or 11 = 3).

2. Hugh got completely lost in the lecture last Thursday when he attempted to explain how to use CRT to quickly calculate the number $x$. Put him out of his misery, by clearly explaining how to use CRT to quickly calculate the number $x$ with a worked example.

3. Calculate the entropy of a source transmitting 128 different characters, with the probabilities of E, T, A, O, N, S, H, R being $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$, $\frac{1}{12}$ respectively and the other 120 characters being evenly distributed. Estimate the average size of a 128 character message if you could use the best encoding scheme.

4. What is the unicity distance of the one-time pad? Justify your reasoning using the unicity distance equation.

5. Choose values $a$, $c$, and $m$ for a linear congruential random number generator that will generate a random looking sequence that repeats after 15 values.