COMP3260/6360 Supplementary Midterm Test 1 Feedback

Question 1 (average mark 8.32 out of 20)

Mistakes included:

- Forgetting to invert the probability inside the log. (E.g., when $P(X) = \frac{1}{5}$ then $P(X)\lg\frac{1}{P(X)} = \frac{1}{5}\lg 5$ and not $\frac{1}{5}\lg\frac{1}{5}$).
- Constructing an efficient encoding of the message X, even though the question didn't ask for it.
- Not knowing how to calculate the equivocation $H_Y(X)$.
- Not calculating the conditional probabilities correctly.

Question 2 (average mark 12.88 out of 28)

This question was marked as follows:

- 0 points for incorrect true/false answer (regardless of explanation).
- 1 point for correctly indicating true or false with no explanation or an incorrect explanation.
- 2 points for correct true/false answer with a partially correct explanation.
- 3 marks for a correct true/false answer with mostly good explanation.
- 4 marks for correct true/false with good explanation.

With that in mind most marks were lost to either not providing an explanation or providing an incorrect answer.

Common mistakes were:

- Part (a) Stating that 27 was prime (and thus incorrectly answering true). 27 is, in fact, *not* prime (it is 3^3).
- Part (b) Finding gcd(15,5), but not knowing what to do with it.
- Part (c) Not stating any reason why bitwise exclusive OR is more efficient than $GF(p)$ computations.
- Part(d) Not stating which algorithm is efficient for computing multiplicative inverses (i.e., simply stating that there is one).
- Part(g) Misunderstanding the difference between unconditionally secure, and perfect secrecy.

Question 3 (average mark 20.12 out of 32)

Typical problems were:

a. • Not computing n correctly
   • Not computing $\phi(24)$ correctly
b. Not finding d_1 and d_2
c. Most students did well

Question 4 (average mark 12.20 out of 20)

This question was well done, and I think most students did better in it than in the original midterm test. Most points were lost to not attempting the question

Some common small mistakes were:

- Not knowing the difference between $\phi(p(x))$ and $\phi(2^3)$.
- Not fully understanding that the inverse was given by $a^{\phi(p(x))-1}$.
- Small arithmetic mistakes.