PROGRAMMING AND DISCRETE MATHEMATICS (XX10190): EXAM COMMENTS

These are some comments on the exam (not the class test) at the end of XX10190. They relate only to the questions set by me (GKS), and are supposed to be useful feedback for those who sat the exam and guidance for those who are taking the course in the future.
I normally produce these soon after the exam has been sat. This year personal reasons prevented me from doing that. I apologise, but I hope that they will still be useful.

First of all, a couple of general comments, mostly repeated from comments I made about other courses in earlier years.
A few people, but not as many as last year, were puzzled by the cover sheet. You didn't lose marks for getting it wrong, but people who did get it wrong mostly didn't do very well. I suppose that if you have just been defeated by a small piece of pink paper you haven't much chance when it comes to mathematics.
You do not tear of the bit that says "FOR EXAMINER'S USE ONLY, CAREFULLY TEAR OFF PERFORATED SLIP" because you are not the examiner. I am, but as a matter of fact I don't tear that off either. You write your name where it tells you to write your name: then you remove the white strip, revealing a sticky bit, and you fold the bit you've just written your name on over and stick it down. Now I can't see who you are and you can still put your script neatly inside the pink folder and fasten it with a treasury tag (one of those green things). Some of you carefully did all this and then wrote your name on your answers, which doesn't really matter.
Please don't put all the unused paper on your desk in with your script. I have to go through it page by page to check that it really is unused.
Whatever it says on the front you will not be disciplined if you fail to write your calculator number on the cover sheet. I have no idea why the cover sheet makes this absurd threat.
Please, please do fill in the bit where it asks you to tick the questions you did. Otherwise, instead of just putting your script on the pile when I get to a question you didn't do, I have to go right through your script looking for the answer that isn't there.
It is also really important to divide the answers up correctly into Part A and Part B, because they are marked by different people at the same time. Almost everybody got that right: thank you.

Next, some other generalities. Most people's writing was easily legible and you are, after all, in a hurry so I do not expect anything very tidy. For the same reason, and because English is not the first language of all of you, I don't expect perfectly polished sentences. You should know by now, though, that there are two o's in "proof" but only one in "prove";

and you shouldn't still be using "times" as a verb, as in "we times z by $\bar{z}$" because you are no longer in the reception class and you can use long words like "multiply" without having to go and sit in the quiet corner afterwards to get over it.

Q4. This was mostly fairly well done. A few people do not know which one is Diffie-Hellman and which is RSA, and carefully described the wrong one. Apart from that most people got quite a long way through the question. In part (a) I do not much mind whether you tell me that a and b are integers or integers mod p, but you do have to understand that they need to be not divisible by p. They shouldn't be ± 1 mod p either if you want anything worthwhile to happen, but the algorithm still works if you take $a = 1$: it just doesn't do anything useful. In part (b) you need to understand what is mod p and what is mod q. The point is that a and b are mod p, and one of the things that Alice has to do is compute an inverse of a mod p, using Euclid's algorithm – you needed to say that. m, on the other hand, is mod q: we are insisting that m should be a square, simply so as to have p possibilities rather than $2p$. The biggest trouble came in part (c). Some of you seem to think that Eve's problem is that she doesn't know q. But she does: she must do, because Alice has told Bob that if he wants to send her a message he must put it in the form of a (square) integer mod q, and Eve heard her say that. Alice and Bob have not agreed anything secretly in advance: indeed, they don't have to know each other and they don't necessarily even trust each other. For all Alice knows, Bob and Eve are the same person. The fundamental problem for Eve, and this is what you had to say, is that she can't take discrete logs quickly enough; so even though she sees m^a and $m^{ab} = (m^a)^b$ she can't work out what b is. Part (d) caused little trouble.
You are warned that there are other uses of Diffie-Hellman. If you are unwise enough to rely on Wikipedia you will be told about a slightly different application of the same idea. It's not wrong (a lot of things on Wikipedia are wrong): it simply isn't what we were teaching you about.

Q5. You know what the Euler φ function is. Mostly you also know why it takes the value it does take: all I wanted was the observation that of the numbers less that n, one-pth are divisible by p and therefore don't count, and that doesn't depend on whether they are divisible by other primes. But it's not much harder to give a proper proof, and many of you did. Mostly you know what a cyclic group is, too; but you fell off the cycle in part (d). Far too many of you offered proofs that didn't use the fact that you are in a field at all. It depends critically on being able to factorise the polynomial $x^d - 1$ uniquely and on the remainder theorem. There was a full proof in the lectures, which you should have learnt. Answers to the last part were often confused, suggesting that although you can recite the

definition of a cyclic group you don't all know what it means. Both $(\mathbb{Z}/10)^*$ and $(\mathbb{Z}/12)^*$ have four elements, so they are cyclic if yo can find an element of order 4. So you just try them all, and in one case you succeed and in the other you don't. It takes about thirty seconds.

Q6. People found ingenious ways to get this one wrong. You do have to get the matrices the right way round: an $n \times m$ matrix is not just as good as an $m \times n$ one. And if you assert that $HG = 0$ and you have written them both down, it's a good idea to check that you do actually get zero when you do the multiplication. I also found an ingenious way to get this question wrong, because in one of the lectures I mistakenly mentioned the rank of H as having something to do with computing $d(C)$. You dutifully wrote that down, which is fair enough. Ten minutes later I realised what I had done and I emailed everybody on the course telling them to remove that bit. At the beginning of the next lecture I said it again, and apologised. But the mistake was ineradicable, like bindweed; dozens of you repeated it, showing that you had ignored my email and not understood the notes.

GKS, 2/9/10