XX10190 Semester 2 Exam FEEDBACK, 2013

For some reason the pink paper tells you ferociously to write down your calculator number. Nobody ever looks at that box. I don't care what your calculator number is. What I do care is that when you are asked to separate sections A and B you should do that, so that we don't have to pass paper back and forth between us when we mark. And please do tick the boxes that say which questions you have attempted, so that I don't have to sift through your script looking for a question you haven't done.

Q3. Well, that was pretty unimpressive, wasn't it? You made a mess of this one. Normally I would say that was my fault, because I can't have got the point across, but you came up with so many different ways to get it wrong that it can't be that.

In any case, some of the mistakes were rather basic. Several of you asserted that $3^3 = 9$ or, less often, 81, which wasn't that serious but obviously didn't help you. A few of you ignored the fact the question asks you about Diffie-Hellmann and wrote about RSA instead, thus scoring zero. Less immediately important, in that I didn't take any marks off, is that far too many of you are native speakers of English and not dyslexic and yet cannot spell the very common word "receive". Yes, I know you usually have a spellchecker (although you may have trouble with predictive text), but the history graduate who cannot multiply 6 by 9 usually has a calculator, and you probably don't have a vey high opinion of him. Put it this way: you don't want to write "recieve" in a job application.

Coming to actual mathematics, quite a few of you wrote about something called $a(m)$ without giving the slightest indication of what it was. The better answers of this type later explained what it might be or what properties it had, but some of you just took no notice of the bit that says $a \in (\mathbb{Z}/m)^*$.

Far more of you took no notice of the bit that says "in G". Read the question: G is just a cyclic group of order n. There are lots of them and I haven't told you which one it is. (It certainly isn't $(\mathbb{Z}/n)^*$, which is of order $\varphi(n)$, not n, and isn't even cyclic usually.) I didn't say G is the integers mod n, although it is automatically *isomorphic to* the integers mod n.

The elements of G could be matrices or complex numbers (very likely) or anything else you can multiply together. It doesn't make sense to talk about m^a mod n, because that means "take the remainder when you divide m^a by n". Now $m \in G$, so $g^a \in G$, not $\mathbb{Z}/n$ or $(\mathbb{Z}/n)^*$; and I don't know how to divide m by n, because I don't know what m is. All I know about m is that it's a member of G, so all I can do with it is multiply it by other elements of G or take its inverse.

There was a lot of failing to read the question. Later on, it says $\mathbb{F}_{47}^*$, not $(\mathbb{F}_{47}^*)^2$. Yes, I know that $(\mathbb{F}_p^*)^2$ and Sophie Germain primes turned up in the lectures. So did Fred Flintstone. It doesn't make them the answer to the question.

It also doesn't mention anything called p, so if you mention something called p you have to say what it is. My solution does not have anything called p in it.

If you are going to say that Alice calculates a^{-1}, you need to say why she can do that, as the system wouldn't work if she couldn't.

You don't actually have to recalculate s for Agatha and Bertie, but if you did do that successfully you got the marks. I could have prevented you from doing the question that way, by asking you to show that if they and Alice and Bob (using the keys I gave you) each start with the same m then both pairs end up with the same secret, whatever m is, not just $m = 3$. Many of you did do that, but doing it for $m = 3$ was good enough.

On the other hand you then have to be able to work out 3^{125} and 3^{33} mod something, let's say mod k There were three separate ways to get this wrong. The commonest was to work mod the wrong k. I'm not telling you the answers here so you should think what the right number is. A second way, which was surprisingly common, was to use a calculator (number carefully written on the pink paper) to compute 3^{125} and then say that was the answer. In other words, just ignore that mod k stuff and hope it goes away. It doesn't, of course. Look, if I ask you whether 123^{565} is even or odd, you can tell me instantly, but if I ask you what it is, you can't. The third way of getting it wrong was not to know how exponentiation works. $3^{5\times5\times5}$ is not the same as $3^5 \times 3^5 \times 3^5$, and 3^{33} is not 3^{11^3}.

Several of you set up a shared secret by having Alice send Bob m^a and having Bob compute m^{ab} and then either stop, or send m^{ab} back to Alice. The first of these produces a secret, m^{ab}, but it isn't shared (Alice

doesn't know it); the second produces something shared, but it isn't secret (Eve saw it when Bob sent it to Alice). A subtler mistake was one that ended up with the common secret being m^b. That's almost all right, but it allows Bob some control over it because he can change b. He can't make it be anything he likes unless he can solve the discrete log problem, but he can avoid anything he doesn't like.

The main trouble, though, was writing stuff that made no sense at all. Things like "solve g^r", for instance; and you didn't mean "find g^r". You solve an equation or a problem, and you solve it for something. Otherwise you might as well write "solve 17". Or you used $\Longrightarrow$ to mean "I need to put some symbol here", as in "$3^3 = 27 \Longrightarrow 27^{11} \bmod k$". This means nothing. Suppose 27^{11} happens to be 14 mod k: you have written "27 implies 14". Statements that mean nothing do not get any marks. Here is a more extended example. It is from a real script, because I find it hard to make this stuff up – I apologise to whoever wrote it, but this was fairly typical and he or she is not being singled out.

"discrete log problem of G is given $x \in G$ $x = \log p^x$ find x is very hard to solve"

I think that if I had written that on the board in the lectures you would not have let me go on, particularly if I hadn't said anything about anything called p. So you give me x, and then I multiply p, whatever that is, by itself x times, although x isn't a number, and take the log (doesn't that give me $x \log p$?) and that's equal to x. And then I find x, which should be easy because you just gave me x, but "it", whatever "it" is, is very hard to solve. No marks: and before you laugh, there is an even chance that your answer wasn't any better.

Q4. This was a bit better. Quite a few people scored very little because they hadn't learnt the bookwork. If you have no idea what a cyclic group is, for example, then you are in trouble, which is not surprising as you weren't paying attention either in this course or in algebra. Some of you seemed to think that it's a group in which $g^{|G|} = 1$, although that is true for any g in any finite group. Some of you may have known what it is but expressed the thought by using words like "create", without explaining what you meant by them. Again, you wouldn't be happy if I did that.

A lot of you assumed, either explicitly or implicitly, that n is the product of two primes or, only slightly better, is squarefree, and gave arguments that fail for $n = 1$, $n = 100$ or simply $n = 4$. Some of you stated the formula for $\varphi(n)$, as asked, but used it to show that $\varphi(p) = p - 1$: of course this is no good, because unless you prove the formula you haven't shown anything.

Your attempts to prove that a finite subgroup of K^* is cyclic were mostly of the Eric Morecambe (ask your dad, or perhaps your grandad) school of mathematics: all the right words, but not necessarily in the right order. Incidentally, it doesn't say in the question that K is finite. Some of you talked about "the field $\mathbb{Z}/m$", although it's only a field if m is prime, and a few talked about "the field $(\mathbb{Z}/m)^*$, which it never is. You have to understand that words like "group" and "field" have precise meanings and you mustn't say them if you mean something else. The empty set is not a group or a field, so it certainly isn't a cyclic group.

Then there is the myth that you need two base cases for strong induction. You don't. Epp uses two base cases (I have no idea why), but she doesn't say they are different and they nearly always aren't. If you had come to the problems classes you would have known that, because I told you. It's harmless to do more base cases than you need, but it shows that you don't really know what's going on.

A few rarities occurred hereabouts. When a question says "hence or otherwise" it nearly always means "hence, but if you do think of something different you'll get the marks", and it is quite unusual for people to try "otherwise", let alone succeed. But this time three people did succeed, and they didn't all do the same thing either. The other rarity was the symbol $\div$, which you last saw in primary school but a few people found convenient here. There is nothing wrong with that. Finally, one of you, having crossed out something and then realised you did mean it after all, wrote the word "stet" next to it. I am impressed, firstly that you know the meaning of this word (it is a Latin subjunctive, for goodness' sake, used by proofreaders) and secondly that you assumed, correctly, that I do.

You were supposed to give reasons for the last part (this is what you are supposed to do in mathematics exams) and a lot of you guessed. If you guessed both parts right you got half marks, so guessing as a strategy scores you one-eighth. You can do better than that. Not, though, by claiming that because $(\mathbb{Z}/p)^*$ is cyclic and 24 and 9 aren't prime, $(\mathbb{Z}/24)^*$ and $(\mathbb{Z}/9)^*$ can't be cyclic. That argument scored zero, which is generous.

Finally, some notation. $\mathbb{R}$ means the real numbers, not the rational numbers (which are $\mathbb{Q}$, for "quotient"). In any case, neither has anything to do with this question. You may write the integers modulo 9 as $\mathbb{Z}/9$ (my personal preference) or $\mathbb{Z}_9$ (also very common) or $\mathbb{Z}/9\mathbb{Z}$ but not $\mathbb{Z} \setminus 9$, which, if it means anything, would mean all the integers except 9. The symbols ϕ, φ, ψ, $\oslash$ and $\emptyset$ are all different. The first two are alternative forms of the Greek letter phi: you should pick one and stick to it, but it doesn't matter much. The third is the Greek letter psi, which is different. The fourth is a Norwegian o-slash, and is used for writing Norwegian. The fifth is the empty set symbol: I believe it is derived from the Norwegian one. The main point is that $\emptyset \neq \phi$.

Q5. Much better. The bookwork was a giveaway, gratefully accepted by most of you. One of you, however, complained (but, to be fair, crossed the complaint out) that he or she couldn't remember what a code was and that "it is outrageously unfair, as the rest of the question relies on this little thing". Personally, I think it entirely fair that if you are going into an exam on a course partly about codes you should know what a code is, which is not exactly a little thing; but the writer appears not to have noticed the book with the answer in that you were allowed to bring to the exam. In fact that made quite a lot of the question rather easy, so it was more of an initiative test really.

There are lots of checks built in: for example you should have $HG = 0$ and $DG = I$. In particular you have to be able to do those matrix multiplications: if you can't, because the matrices aren't the right sizes, then one of the matrices you have written is the wrong size and is therefore wrong.

Remember that we are working in $\mathbb{F}_2$, so $-1 = 1$ and $2 = 0$. Some of you did unnecessary calculations, carrying 2s around with you.

Don't assume that notation is absolutely fixed. You have to accept that what is called m in one book or lecture course may be called n somewhere else, and think what the notation means. Similarly, your method of finding $\ker H$ may (as one of you pointed out) be different from mine, which is no problem.

In the last part you got marks for giving D even if your G was wrong. Some people simply wrote D straight down, which was all right. It is H, not D, that is the check matrix. (D for Decoder; H for cHeck: not C for Check because of C for Code.)

$d(C)$ is NOT the rank of H. Two years ago I mentioned them both in the same sentence in a way that suggested that they were, and although I explained immediately what I had meant to say I still see this being written in exams.

You may not simply write $d(x, y)$ without giving any explanation of what it means.

In the last part, you do have to calculate the rank of H. Row rank and column rank are always the same. You aren't asked to calculate $d(C)$, although it is easy to see what it is; but just because the given word has weight equal to $d(C)$ it doesn't mean it's a valid codeword, and I didn't give any marks for guesses either. $d(C)$ is the weight of the smallest valid nonzero codeword, but other invalid codewords might also have that weight.