XX10190 FEEDBACK: May exam, Section B

The first good sign was that everybody had followed the instructions. Nobody had torn off the bit of paper that says "For Examiner's Use Only". Nobody had attached their script to the back of the paper. Nobody had written on the wrong side of the paper and had to make a new hole in the top right corner instead of using the punched hole in the top left. Nobody tried to tie a knot in the treasury tag (that little bit of green string). And nobody wrote the answers to Section A and Section B questions on the same bit of paper and then couldn't hand them to different examiners.

Once I started marking the exam, though, some difficulties became apparent.

Q3. This begins "Define the field $\mathbb{F}_p$". So you should start by writing "The field $\mathbb{F}_p$ is…", and if you don't you will probably lose a mark, and a very easy mark at that. Part (b) asks you to show that $(\mathbb{F}_p^*)^2$ is a subgroup of $\mathbb{F}_p^*$, so you should do that: the hard (well, not very hard) part is "group", not "sub". Many of you pointed out that $(\mathbb{F}_p^*)^2 \subset \mathbb{F}_p^*$ and stopped, scoring nothing.

Part (c) divided you three ways: those who knew what $\left(\frac{a}{p}\right)$ is but knew nothing about it (the largest group); those who didn't even know that (not very many); and those who could do the question. These last, and a few from the other two groups, could do (d) as well. It was (e) that produced the widest variation. Many of you chose to ignore the bit that says "you should state carefully any general facts that you use" and just used them anyway. This cost you marks.

Too many of you thought that $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$ (with the exception, which you did know), ignoring the fact that the second of these makes no sense unless a is prime too.

It says at the beginning of the question that p is an odd prime. You are not allowed to write about $\mathbb{F}_n$ or about $\left(\frac{a}{n}\right)$ is n is not prime. The following numbers, NONE OF WHICH IS PRIME, were treated as if they were prime (and in some cases actually stated to be prime) by at least some of you:

$$3591;\ 1053;\ 900;\ 552;\ 513;\ 399;\ 370;\ 276;\ 243;\ 215;\ 185;\ 153;\ 138;$$
$$133;\ 91;\ 82;\ 69;\ 46;\ 30;\ 27;\ 24;\ 20;\ 12;\ 8;\ 6;\ 4;\ 1;\ 0;\ -1.$$

There are three questions in Section B of this exam, each carrying 23 marks, for a total of $\ldots 69 = 3 \times 23$. Michaelmas Day (September 25th) and Christmas Day fall on the same day of the week because September, October and November have $91 = 7 \times 13$ days between them so that's 13 weeks exactly.

Q4. Some of you did not bother to learn which is RSA and which is Diffie-Hellman before entering the examination room. I do not have much sympathy with that level of preparation. The accounts of Diffie-Hellman given by such people when they were asked for an account of RSA scored zero, but they were as confused as you might expect anyway.

There was also a strangely widespread belief that Bob's message is "HI". It isn't: it says in the question that it is "6". This confusion was usually combined with a ramble about breaking messages up into letters encoded by A=1, B=2 and so on (google ASCII to find out how it is really done; but this has nothing to do with RSA). Epp, incorporated in the course book, uses that simplification and uses the message "HI" as an example, because she is American. Some of you had memorised this example and wrote it out, regardless of the fact that you had not been asked that question. Of course you scored zero.

The meaningless phrase "positive inverse" was widely used and cost everybody who used it one mark. I wrote "multiplicative inverse", which does mean something. Is it also in Epp somewhere? These are integers mod something and it doesn't make sense to talk about them as positive or negative.

Some of you are unable to distinguish between Euler (Swiss, 300 years ago) and Euclid (Greek, 2500 years ago), probably because they both have names beginning "Eu-". This did not cost a mark, but isn't impressive.

Generally, though, this question was pretty well done. Some people, but not very many, got confused between messages (which are read mod N) and keys (which are read mod $\varphi(N)$): this led to disaster in the final part. Lots of people missed the point that the system breaks down if Bob tries to send a message divisible by p or q, but these numbers are so large that that never happens. Not everybody was very clear

about what Eve's difficulty is, but most people had some idea. A significant number of you scored full marks on this question.

Q5. Much better. Nearly all of you knew the basic definitions, although many of you cannot spell "kernel" or "independent". The latter is on display in inch-high letters in every newsagent. A good many knew how to calculate the minimal distance from the check matrix. Some then spoiled the effect by asserting that it is equal to the rank or to the minimal weight of a row. You did not try to prove these things, which is just as well as they aren't true. There was then a sharp division between those who worked out what the size of the generating matrix in the last part should be and those who guessed. Few guessed right. Those who didn't guess usually got most of the rest of the question out.