OCR
RECOGNISING ACHIEVEMENT

ADVANCED GCE

MATHEMATICS (MEI) 4754B

Applications of Advanced Mathematics (C4) Paper B: Comprehension

INSERT

Monday 13 June 2011
Morning

Duration: Up to 1 hour

INFORMATION FOR CANDIDATES

- This insert contains the text for use with the questions.
- This document consists of **8** pages. Any blank pages are indicated.

INSTRUCTION TO EXAMS OFFICER / INVIGILATOR

- Do not send this insert for marking; it should be retained in the centre or destroyed.

Card safety

A court case

In a recent (2009) court case, a man claimed that his bank owed him £2100. The money had been taken from his bank account in eight withdrawals from two cash machines, apparently using his bank card, but he said that he had neither made these withdrawals himself nor asked anyone else to make them. His card used chip and PIN technology. The bank had refused to refund his money.

The letters PIN stand for Personal Identification Number and refer to a 4-digit number that is needed to authorise transactions using the card, such as withdrawing money. Some banks do not allow numbers that begin with zero, numbers in which the digits are all the same (such as 5555) or numbers in which the digits are consecutive (such as 2345 or 8765).

When a bank issues you with a card, various security conditions come with it.

- You are not allowed to tell anyone the PIN.
- You are not allowed to write the PIN down; you must remember it.
- You may not lend the card to anyone else.
- If you lose the card, you must report the loss to the bank.

In the 2009 court case, there was no dispute that the withdrawals had taken place. The question was which of the following possible explanations was correct.

1. The man was making a dishonest claim. If so, the man is clearly at fault.
2. The bank had made an error, for example by taking money from this man's account by mistake, and so is at fault.
3. A breach of the card's security conditions, as stated above, had allowed a thief to withdraw the money. If so, the man is legally at fault.
4. A thief had been able to withdraw the money without a breach of the card's security conditions. If so, the fault lies with the bank's systems.

Two of these explanations (1 and 3) say that the man is at fault; the other two (2 and 4) put the blame on the bank.

Explanations 3 and 4 involve successful 'attacks' by a thief.

The judge decided in favour of the bank. His written judgment caused some people concern. Part of it could be read as meaning that chip and PIN technology is absolutely secure; if so, it would imply that it is impossible for a thief to copy, or 'clone', someone else's card or to break a bank's security.

A survey of card users

Following this judgment, MEI conducted a small survey to provide information about the situation, and particularly the four possible explanations. Those taking part were mathematics teachers attending a conference in June 2009; 250 questionnaires were given out and 80 returned. The survey was based on people's experience with their banks.

Banks use software designed to detect suspicious transactions; if one is detected, the bank usually contacts the card-holder to check whether the transaction should go ahead. The survey asked people whether they had been contacted by their banks about a suspicious transaction.

If the answer was Yes, they were then asked to answer a further question as to whether they had

authorised the transaction. An answer of Yes to this further question meant that the transaction was genuine, and an answer of No that an attack had been detected.

- 46 of the 80 respondents had been contacted by their banks, many of them several times.
- Most of the transactions had in fact been authorised, but 11 of the 46 people had been contacted about unauthorised transactions.
- Of the 11 people with unauthorised transactions, 3 could explain them as breaches of card security (typically losing the card) but 9 could not (one person was in both categories).

The survey then went on to ask about cases that had not been picked up by the banks' detection software, resulting in unauthorised withdrawals from people's accounts.

- 21 people reported unauthorised withdrawals.
- Of these, 9 people could explain them as breaches of card security and 13 could not (again one person was in both categories).

In total, 16 out of the 80 people who responded to the survey had been the subject of attacks in which there was no breach of the card's security conditions. Some of the attacks had been stopped by their banks but others had resulted in money being withdrawn from their accounts; some people reported both of these. If the survey results are reasonably representative, they would suggest that, in the course of the $3\frac{1}{2}$ years covered by the survey, 20% of people had suffered an attack without any breach of their cards' security. This may be an overestimate. Only 80 out of 250 people returned the questionnaire; maybe all the 170 who did not return it had nothing to report. In that case the proportion suffering such an attack would be 6.4%.

The conclusion that attacks can happen without breaches of card security is supported by the fact that banks are prepared to bear the considerable costs that must be involved in the process of carrying out checks.

Possible explanations

In a typical court case involving card security, the claimant has had money withdrawn from an account and the bank has refused to refund it. There is no dispute that the withdrawal has taken place. The four possible explanations on the first page apply and the results from the survey make it possible to say something about them.

In the first explanation, it is the claimant who has withdrawn the money and is then saying it was someone else. The survey suggests that the other explanations are also possible. Whether the court judges the claimant to be telling the truth must depend on other evidence.

The next possible explanation is that the bank made an error, and this can happen. One of the responses to the questionnaire said

> *"We went to the bank and spoke at length with the manager. We were fully reimbursed and had a grovelling apology."*

That leaves the two explanations that involve the money being taken by a thief, with or without a breach of the card's security. The survey also identified the number of transactions, as well as the number of people, subject to attacks. There were a total of 42 attacks; several people reported more than one attack. 13 of the attacks could be explained by breaches of card security and 29 could not.

So the data would suggest that, if there has been an attack, the probabilities of the two explanations of breach and no breach of card security are $\frac{13}{42}$ and $\frac{29}{42}$. These figures are based on a small sample and so it would be better to think of them as about $\frac{1}{3}$ and $\frac{2}{3}$. In civil cases, courts decide the outcome on a 'balance of probabilities'. The probabilities of $\frac{1}{3}$ and $\frac{2}{3}$ are so close together that a court would

be unwilling to decide the matter on the basis of them alone, and would look for other evidence before reaching a decision.

The banks

The survey went on to ask those who reported unauthorised withdrawals what happened next. In nearly all cases the bank had refunded the money but in one case this had not happened.

One of the responses to the questionnaire said

> *"The bank described two transactions in the space of 3 or 4 hours. One for about £40 in a shop in London and the other for over £500 at an expensive restaurant/club in London. I was in Paris at the time of these transactions. The bank refunded both amounts after I filled in a form. … I assume that someone had managed to clone my card somehow."*

Clearly fraud can cost the banks a lot of money.

If a bank refuses to pay, the next course of action open to someone who has lost money in this way is to contact the independent Financial Ombudsman. A few of these cases are then taken further and end up in court.

Detecting fraud

The survey provided information about the banks' success in detecting unauthorised transactions. The total number of transactions for those who responded has been estimated as 100 000 for the $3\frac{1}{2}$ years covered by the survey. Table 1 shows data from the survey and, in brackets, figures derived from the estimate of 100 000 transactions.

Transactions	Authorised	Unauthorised	Total
Queried	139	19	158
Not queried	(99 819)	23	(99 842)
Total	(99 958)	42	(100 000)

Table 1

Table 1 illustrates the problems faced by the banks. They check a very large number of transactions, query quite a small proportion of them and succeed in stopping a small number of unauthorised transactions. However, despite all this effort, the figures in Table 1 suggest that they only catch about half of the attacks.

The entries in a table like this are often described using the terms in Table 2.

Transactions	Authorised	Unauthorised
Queried	False positives	True positives
Not queried	True negatives	False negatives

Table 2

A 'positive' is a transaction that is identified by a bank's computer software as suspect and so is queried. The identification is 'false' if the transaction was in fact authorised and it is 'true' if the transaction was unauthorised.

Similarly, a 'negative' is a transaction that is not identified as suspect and this non-identification may be true or false.

So, if the software gives a warning when there is no attack, a false positive results; 139 of these are recorded in Table 1 and, apart from some inconvenience, they are quite harmless. If, however, the software fails to give a warning when there really is an attack, a false negative occurs, resulting in unauthorised withdrawals and these are the serious cases; there are 23 of them in Table 1.

The number of false negatives can be reduced by making the warning criteria in the software more severe, but the effect will inevitably be that the number of false positives rises: the more severe warning criteria will pick out more authorised transactions. Thus the fewer the false negatives, the greater the number of false positives, and vice-versa.

The detection software may be thought of as the front line in the ongoing struggle between thieves and banks. Once thieves learn how it is programmed, they can find ways to defeat it. Consequently the information is considered to be top secret by the banks.

Finally, a piece of advice. Never let anyone else use your card. Legally, your PIN is an electronic signature and so allowing someone else to use it is the equivalent of telling them to forge your signature.

BLANK PAGE

BLANK PAGE