# PINs, keys and other secrets

Chris Mitchell

There has been much recent media coverage of announcements by UK banks that within three years or so all credit cards will be smart cards, and transactions will be authorised using PINs instead of signatures. This will hardly be big news for our neighbours in France, who have been using smart cards and PINs since the 1980s! Of course, one difference is that the smart cards already being introduced in the UK will conform to the EMV industry standard, which will enable them to be used in many countries around the world.

However, this article is not about smart credit cards, however interesting they may be. What I want to talk about are the PINs themselves, and also other issues relating to the management of secret values used for security purposes.

Everyone who has ever learnt anything about cryptography and its uses will have been told about the importance of good key management. Cryptographic keys are typically sequences of random-looking bits, of length anything from a handful of bytes to a kilobyte or more. Key management is concerned with managing the generation and distribution of key values, in such a way that only authorised individuals have access to their values.

Another aspect of key management which is often mentioned, but less often taken much notice of, is the need to manage keys after they have been replaced. In particular, if a key has been used to encrypt data, then, even after it is no longer being used, it may need to be kept to decrypt stored versions of encrypted data. When it is no longer required, e.g. because all the stored data has been re-encrypted using replacement keys, then it must be securely destroyed.

Why is this? Well, even though a key is no longer in use, the secrecy of any data which has ever been encrypted using this key is at risk. This is because an unauthorised party may have made a copy of data encrypted using this now obsolete key, and if the key is revealed then this party can recover the data.

This is all well known. Nevertheless, I am not sure that this aspect of key management is always taken as seriously as it should be. There is a tendency to believe that there are very few ‘long term’ secrets – this week’s highly confidential email may be just a boring piece of history a week later. Indeed, even highly confidential government papers are eventually published. However, the suggestion that long-term secrets are few and far between is something I would like to challenge, and this brings us back to PINs and credit cards.

How long have you been using the same PIN with your credit or debit card? Is it five years, ten years, or even longer? Perhaps there are such things as long-term secrets after all! This, of course raises some interesting questions about the use of PINs.

Whenever a PIN for a debit or credit card is entered into a ‘hole in the wall’ (or ATM) the PIN is sent to the card issuer for verification, along with the account number and certain other information. To prevent PINs being disclosed to hackers of the network, PINs are always encrypted before transmission. This precaution has, as far as I know, been rigorously followed from the very beginning.

This nevertheless raises an interesting question. While I imagine banks take care to use encryption algorithms which are believed to be strong, it is not clear what precautions are taken as far as long-term PIN security is concerned. That is, if PINs have a lifetime of ten years or more, we need to be sure that the key used to encrypt

PINs remains secret for at least ten years after it has been taken out of use. This implies that the PIN encryption algorithm should also be chosen to be secure for at least ten years.

The banks have widely used the DES encryption algorithm for many years, and, as is now widely known, DES has been broken. Although most banks have been switching from DES to 'triple DES' (or other more secure alternatives) for a number of years, it does mean that if just one banking network was using single DES to encrypt PINs less than ten years ago then your PIN might be at risk.

Of course, a PIN on its own is no use – to use it you also need the card. On the other hand, most of the information necessary to recreate a card may also be sent across a payment network with the PIN, and this information will not always be encrypted. So forging large numbers of false cards for which the PINs are known may not be so infeasible after all!

However, to do this successfully would require matching current day card information with old card information (and the old encrypted PIN), so the threat is probably not that significant. Even better news is the fact that, with the new EMV smart cards, knowledge of the account number is not sufficient to be able to manufacture operational fraudulent cards. The EMV standard provides a means for a retail card terminal to authenticate the card, which gives an additional layer of protection not present with conventional 'magnetic stripe' cards. So perhaps it is just as well we are being given smart cards!