Australian Government

OFFICE OF THE CHIEF SCIENTIST

OCCASIONAL PAPER SERIES

ISSUE 3
JULY 2012

MATHEMATICS IN YOUR WALLET

*Alan Carey**

Do you have a credit card with a chip, or an e-passport? If so, you use mathematics to keep your personal information secret. This paper explains some of the methods that help to keep your money, personal details and identity safe everyday.

Overview

- Encryption[1] technologies protect confidential information used in commerce.
- A common encryption method relies on mathematics to protect information in smart cards and e-passports.
- Encrypted information can be vulnerable to attack by fraudsters.
- More Australians trained in mathematics and related disciplines will be essential to safeguard commerce in the future.

Box 1: Key terms

Cryptography – the science of making and breaking codes.

Encryption – scrambling a message using a code to make it unreadable by those who don't know the code. The message can only be recovered using special knowledge, known as the encryption/decryption key.

Prime number – a number divisible by only 1 and itself. Examples include 2, 3, 5, 7, 11, 13, 17 and 19.

Background

Cryptography is the science of making and breaking codes. It has a long history. Ancient Egyptians, Greeks and Romans used cryptography to send secret messages. The main users of cryptography in more recent times have been governments, military and intelligence organisations. This has changed since the advent of computers and digital technology. Cryptography is now broadly used, particularly in e-commerce. Modern cryptography relies on sophisticated mathematics to protect confidential information.

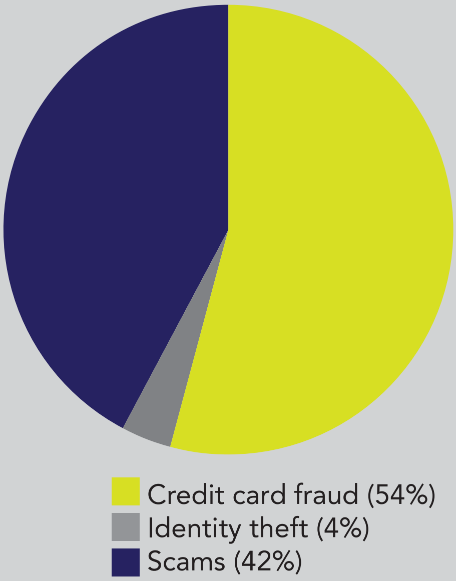
In cryptography, encryption is the process of making information secret, and therefore preventing unauthorised access to that information. Encryption protects confidential information in credit cards, e-passports and other smart cards.

Encryption in most swipe cards uses magnetic technology. The magnetic strip carries coded information, which is decoded when swiped. Fraudsters can use machines to illegally copy information on a magnetic strip, a process called skimming. This can happen during ATM or EFTPOS transactions. Stolen details can then be easily used to create counterfeit cards.

[1] See Box 1 for the definition of key terms used in this paper

The Australian Crime Commission reports that card skimming fraud in Australia is growing. In 2006, card fraud cost Australia close to $100 million. This rose to more than $170 million in 2009.[i] The Australian Bureau of Statistics recently estimated that a total of 1.2 million Australians were victims of at least one incident of personal fraud.[ii] More than 50 per cent of the victims experienced credit card fraud (see Box 2). Clearly, there is a need for more secure credit cards. Smart chip embedded cards or smart cards help to fill this need (Box 3 shows a chip in a smart credit card).

Box 2: Personal fraud in Australia



Personal fraud in Australia by type. Credit card fraud is the most common type of personal fraud. A 2011 survey by the Australian Bureau of Statistics found over a million people were affected by fraud in the previous year. Of these, more than half experienced credit card fraud.

Source: Australian Bureau of Statistics[i]

The most common method for securing information on smart cards is called RSA public key encryption (for inventors Rivest, Shamir and Adleman). The idea behind RSA is relatively simple. Even if you do not have a smart card you might have bought something where the RSA encryption played a role. For example, you may have used PayPal to pay for something you bought online.

This occasional paper describes some of the mathematics that underpins smart cards, and highlights the key role it plays to protect information in our everyday life for banking, shopping and travel. The paper concludes by discussing policy implications for education and training in mathematics and related disciplines.

Prime secrets and two keys

Prime numbers are at the heart of RSA encryption. A prime number is one that can be divided only by 1 and itself to yield a whole number (1 or itself). For example, 2, 3, 5 and 7 are all prime numbers. RSA encryption multiplies two large prime numbers, each typically 300 digits long, to produce an even larger number (see Box 4 for an example of a 300-digit prime number). The resulting very large number is called the 'public key'. The public key codes your private information. As the name suggests, you may give the public key to anyone, but they cannot use it to decode your information. Only the intended recipients who have a private key linked to the two prime numbers you started with can decode your RSA-encrypted information.

So how does RSA encryption hide your credit card details when you shop online? Here's a simple version of how it works: you go to an online shop and choose an item to buy. You add it to your shopping basket then go to the checkout. The address of this page should start with 'https' and, if so, this is when the encryption kicks in. The online shop's computer sets up the security by creating the public and private keys. It keeps the private key to itself and sends the public key to your computer. The keys enable your computer and the shop's computer to share information in a secure way. When you type in your credit card details and press the 'Order' button, your computer encrypts your credit card details before sending them. The online shop's computer then receives and decrypts your details. They are only able to do this because they know the two large primes originally used to create the public key.

RSA is secure because it is incredibly hard to guess the two large prime numbers the online shop started with. While multiplying is comparatively easy for computers, there is no easy way to work in reverse and determine which prime numbers were multiplied to get the public key. Even with a powerful computer, cracking RSA would take billions of years. This asymmetry between the ease of one task and difficulty of its reverse is the key to RSA encryption.

Other features of RSA

Other features of the mathematics underlying RSA are briefly discussed here. One is the challenge to find long prime numbers for setting up the private and public keys. You cannot look at large numbers and easily work out which are prime. There are various ways to test numbers to see if they are prime. Most are far too slow for practical use, especially with very large numbers.

RSA works because finding the two original prime numbers or factors for the public key is difficult. Should someone come up with a practical way to find the factors for the public keys then RSA will no longer be secure. In this case, other encryption techniques will become necessary to secure information.

Another feature is computational cost. Decoding information becomes more difficult as larger prime numbers are used. Every time a smart card is used a computer has to decode the encrypted data. This takes longer and uses more processing power as the prime numbers get larger. Thus, there is a trade-off between the security of using very large prime numbers and the cost that they impose.

Common attacks to access protected information

The chip in your smart card is encrypted by RSA. Card skimming fraud is not yet effective on smart cards. However, during transactions, smart cards interact with terminals or other devices, such as ATMs or EFTPOS machines. Any terminal used during critical transactions must be trustworthy and not copy information from the smart card. Ensuring a terminal presents proper and trustworthy information to a cardholder is called the 'terminal problem'. What is needed is a trusted terminal. There is no perfect solution at the moment and the 'terminal problem' remains a weak point in the security of e-commerce.

Beyond rogue terminals, attacks on smart cards can take the form of direct attempts to extract information from the chips of stolen cards. Such attacks have been effective in defrauding cardholders. One such attack introduces and analyses computational errors into a smart card to completely uncover the encryption keys. Such errors can be introduced by changing the electric signals inside a card.

Box 3: A smart card chip

A chip embedded in a smart credit card.

Source: sxc.hu

More sophisticated attacks require a properly equipped laboratory to reverse-engineer a chip from a stolen card. Unfortunately, such reverse engineering techniques are commonly used. They involve uncovering the layers of a chip by etching and then deducing the chip's information content. The security of smart cards faces an ongoing battle between criminals and designers of encryption technologies.

Training is the key

Right now smart cards and e-passports are very safe. Mathematicians are working to understand potential vulnerabilities of encryption technologies. Many companies are investigating security issues in e-commerce with the aim of preventing fraudulent transactions or frustrating attempts to access secure data. In addition, the business of information security, encryption, accurate storage and transmission of data are vital to Australia's security.

Box 4: An example of a 300-digit prime number

This large number is divisible by only 1 and itself. In RSA cryptography, this and another large prime would be multiplied to produce the public key, which codes your personal information.

203956878356401977405765866929034577280193993314348263094772646453283062722701277632936616063144088173312372882677123879538709400158306567338328279154499698366071906766440037074217117805690872792848149112022286332144876183376326512083574821647933992961249917319836219304274280243803104015000563790123

Source: University of Tennessee[iii]

The Defence Signals Directorate (DSD), an agency within the Defence portfolio, helps keep Australia secure against information fraud, especially where it involves national security. The US counterpart of DSD, the National Security Agency, is the biggest employer of mathematicians in the US. However, recruiting the highly trained specialists who can do this kind of work is difficult.[iv]

Australia has an industry devoted to security and risk management against e-fraud. The people who work to protect our banks and industries are highly trained engineers, computer scientists and mathematicians. Over the period 1995-2005, we lost some of the capacity in Australia to train such people. For example, mathematics departments across the Group of Eight universities shrank by 30 per cent.[v]

The recent *Health of Australian Science* report pointed out that the study of mathematics by 2nd and 3rd year science students at university declined during the 1990s and did not recover in the 2000s.[vi] Today there are too few graduates with the appropriate training to fill the diverse range of essential jobs that demand high level mathematical skills. Importing labour is not a long-term solution as all nations face similar demands to recruit highly trained graduates. The most effective way is to produce a sufficient number of graduates in mathematics and the related disciplines of computer science, statistics and engineering.

Conclusion

Mathematics is arguably the most fundamental of all sciences. It can give us unexpected practical applications with enormous economic value. The development of both Wi-Fi and encryption technologies resulted from an understanding of fundamental mathematics.

Mathematics is expected to play an increasingly important role in protecting personal information and safeguarding e-commerce. The threats to personal information and our economy are a matter of national security. As our economy becomes increasingly reliant on information and knowledge we must ensure that more Australians are trained in mathematics and related disciplines.

References

i) Organised Crime in Australia (2011) Australian Crime Commission.

ii) Australian Bureau of Statistics. Personal fraud, Australia, 2010-11. Catalogue number 4528.0

iii) The Prime Pages. University of Tennessee at Martin. Available at http://primes.utm.edu/lists/small/small3.html
Accessed 29 June 2012.

iv) The NSA: security in numbers. Bloomberg business week (23 January 2006). Available at www.businessweek.com/magazine/content/06_04/b3968007.htm
Accessed 29 June 2012.

v) Australian Academy of Science (2006) Mathematics and statistics: critical skills for Australia's future. The national strategic review of mathematical sciences research in Australia. Available at
www.review.ms.unimelb.edu.au/FullReport2006.pdf

vi) Office of the Chief Scientist (2012) Health of Australian Science. Australian Government, Canberra. Available at www.chiefscientist.gov.au/2012/05/health-of-australian-science-report-2/

Acknowledgements

We thank Brendan McKay and Richard Brent for their review comments.

About this series

These occasional papers from the Office of the Chief Scientist take relevant science from the research world and translate it for a general audience. They aim to bring to the public's attention scientific issues of importance to Australian society. Each issue has been prepared by a multi-disciplinary team and has been through an external review process.

For more information about the series, this issue's topic or to subscribe to future papers, contact the series editor, Ms Sarah White, Office of the Chief Scientist, GPO Box 9839, Canberra ACT 2601, projects@chiefscientist.gov.au.

Papers in this series are available online at chiefscientist.gov.au.

Suggested citation:

Carey, A (2012) Mathematics in Your Wallet,
Occasional Paper Series, Issue 3.
Office of the Chief Scientist, Canberra.

*Alan Carey is Professor of Mathematics at the Mathematical Sciences Institute, The Australian National University.