Careers using Mathematics: Cryptography

Chris Mitchell
Royal Holloway, University of London
www.isg.rhul.ac.uk/~cjm

My career

- A level Maths (1972)
- BSc (1975) and PhD (1979) in Maths – University of London.
- Racal Comsec (Salisbury): 1979-1985.
- HP Laboratories (Bristol): 1985-1990.
- Royal Holloway, University of London (near Windsor): 1990-present.

Uses of Maths

- Although I am a Professor of Computer Science, Maths has played a central part in my 30 year working life.
- Even when not using Maths directly, the training in thinking I received as a pure mathematician has been invaluable to me.

Cryptography

- Cryptography is the science of secret writing, i.e. ways of **encrypting** data to conceal it.
- It has a very long history (thousands of years).
- It is a branch of Mathematics, and modern cryptography (and cryptanalysis) uses a wide variety of types of mathematics.

Uses of crypto

- Cryptography is used very widely in:
  - mobile phones (protecting calls and texts);
  - banking (chip and PIN cards);
  - Internet (protecting transaction details using SSL, SSH, ...);
  - corporate computer security;
  - home computing (Windows and other OSs come with a set of crypto algorithms);
  - satellite TV (e.g. Sky); ...

RSA

- RSA was invented in the 1970s by **R**ivest, **S**hamir and **A**dleman (working at MIT).
- It was the first practical and secure example of a public key cryptosystem.
- Now very widely used, e.g. on chip and PIN credit cards, and to protect Internet e-commerce transactions.

RSA – background

- RSA uses Mathematics going back hundreds of years, and which was originally invented purely for the love of the subject.
- Prime numbers: 2, 3, 5, 7, 11, ...
- RSA relies on fact that every number can be **uniquely** composed into prime factors, but that doing it is hard!

Primes and factoring

- If I give you two very large prime numbers, it is not so hard to multiply them together, even of they are very large (e.g. hundreds of digits long).
- However, if I give you their product, then finding the prime factors can be very hard.

Examples

- 53 and 61 are primes
- $53 \times 61 = 3233$ (easy to do on paper – or in your head).
- Find the factors of 3233 – well, you could try every prime in turn, e.g. divide 3233 by 2 (do you get a whole number answer?), then by 3, then by 5, and so on ...
- But for very large numbers this will be infeasible!

Primes and RSA

- RSA works because of the hardness of factoring.
- Can you find a new method ...?
- If so, then it would revolutionise the way we so everyday security for banking, computer communications, ...