



University of St Andrews

School of Computer Science

DISTINGUISHED LECTURE SERIES 2005/06

Modern Cryptography

By

**Dr Matt Robshaw
France Telecom**

Friday, 2nd December 2005

*2nd Year Laboratory, Jack Cole Building (morning)
Physics Lecture Theatre B,
Physics & Astronomy Building (afternoon)
North Haugh, St Andrews*

Biography

Dr Robshaw graduated from St Andrews in 1988 and completed his PhD At Royal Holloway University of London. During that time his research focused on cryptography in general and stream ciphers in particular. In 1993 he took up a research position with RSA Data Security in California. After more than six years working on a variety of cryptographic projects, he left RSA as Principal Research Scientist and returned to academia. Joining the staff of Royal Holloway University of London in 2000 he became a Reader in Information Security. Recently Dr Robshaw decided to return to industry and took a position at France Telecom Research and Development based in Paris.

Programme

Over the course of three lectures we will look at the development of modern cryptography. We will review the range of techniques available and the much smaller set of algorithms in every-day use. We will also consider some new and developing research directions that are likely to influence our daily life in years to come.

- 10.0 – 11.00** **The Development of Modern Cryptography**
2nd Year Laboratory
Jack Cole Building
- 11.0 – 11.30** *Coffee*
Coffee area
Jack Cole Building
- 11.30 – 12.30** **The Deployment of Modern Cryptography**
2nd Year Laboratory
Jack Cole Building
- 14.30 – 15.30** **New Directions**
Physics Lecture Theatre B
Physics & Astronomy Building
(note change of room for afternoon lecture)