WMC 2006

Workshop on Mathematical Cryptology

MINISTERIO DE EDUCACIÓN Y CIENCIA

UC UNIVERSIDAD DE CANTABRIA

TOPICS include:

- Primality and integer factorization.
- Secure encryption schemes based on group theory.
- Multivariate polynomial cryptosystems. Groebner bases.
- Elliptic and hyperelliptic curves cryptosystems.
- Computational complexity.
- Lattice-based cryptosystems.
- Pseudorandom sequence generators for stream ciphers.
- Public key cryptosystems based on algebraic coding theory.
- Information security with mathematical emphasis.
- Quantum Cryptography

Invited Speakers

Simon R. Blackburn,
Royal Holloway, London.

Antonio Campillo,
Universidad de Valladolid.

Jean-Charles Faugère,
CNRS-INRIA, Paris.

Mª Isabel González,
Universidad Rey Juan Carlos, Madrid.

Llorenç Huguet,
Universitat de les Illes Balears.

Harald Niederreiter,
National University of Singapore.

Franceso Pappalardi,
Università degli Studi Roma III.

Emilio Santos,
Universidad de Cantabria.

Igor Shparlinski,
Macquarie University, Sydney.

Organizers

Jaime Gutierrez,
Universidad de Cantabria.

Álvar Ibeas,
Universidad de Cantabria.

Santander, SPAIN
June 29-30 2006

The workshop will be held at the Faculty of Sciences, in the University of Cantabria.
For contributions or further information, contact the organizers:

http://grupos.unican.es/amac