Summer School 2006

The Faculty of Mathematics and Computer Science from the University of Bucharest (FMI UNIBUC), the Institute of Mathematics of the Romanian Academy (IMAR) and the Romanian Mathematical Society (SSMR) organize a

Summer school on
Cryptography and Cryptology

August 20-26, 2006

Vatra Dornei, Romania

Cryptography - literally, "hidden writing," from the Greek - is probably as old as writing itself. Whether it is a crucial military dispatch or a secret love letter, people have been attempting to hide their private messages from prying eyes throughout history.

The workshop is intended for those interested in learning the background of cryptography and cryptology. The intention of this summer school is at least two folded: 1) To give a broader picture on standard cryptography methods. 2) To present how the security of different kind of cryptographic systems can be proved by using mathematics. Some of the topics to be considered are the RSA public-key cryptosystem, hash functions, signature schemes etc. An overview of mathematics needed for this course will be given as well.

The website of the Summer school is:

http://rms.unibuc.ro