uc3m | Universidad Carlos III de Madrid

COURSE CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UNIVERSIDAD CARLOS III DE MADRID |

PRESENTATION PART 1

The first block of the course introduces the discipline of cryptography and its fundamentals, in four modules.

- In Module 1 the students will learn the mathematical principles of cryptography, learning the basic operations of modular arithmetic in finite groups of integers and polynomials with binary coefficients.

- In Module 2 the basic concepts of cryptography are introduced, including what a cryptosystem is and what its main characteristics are, as well as how the security of cryptographic algorithms is based on their cryptanalysis.

- In Module 3 it is explained how information theory is the base of modern cryptography, specially through the concepts of entropy and conditioned entropy. Other concepts intrinsically linked to cryptography and its security, such as randomness and algorithmic complexity, are also explained.

- Finally, in Module 4 the main classical cryptography algorithms and their cryptanalysis are studied, as they allow to illustrate in an accessible manner the concepts and techniques used in modern cryptography.

Associated material

The material associated with this topic includes lecture notes slides and a collection of proposed exercises on the aspects covered in these modules with their solution. In addition, a set of objective answer quizzes are offered, with solutions, which allow students to verify their learning in these modules.