Course in Cryptography (Crittografia) - 2009-2010

A. Languasco
University of Padova, Italy
Faculty of di Mathematics, Physics and Natural Sciences
Computer Sciences Master's Degree course (Laurea Magistrale)

It is also open to students of the **Mathematics Master's Degree (Laurea Magistrale)**, and of the **Erasmus Master Mundus ALGANT program**.

When: first trimester; six hours per week.

Where: Room 2BC/60 of the "Torre Archimede", via Trieste, 63, Padova.

Total number of hours: about 48 (6 credits).

Examination: oral trial.

Description of the course

The main goal of the Cryptography course is to give an overview of the theoretical basis of the field in order to allow a critical study of the cryptographic protocols used in many applications (authentication, digital commerce). In the first part we will give the mathematical basic tools (essentially from elementary and analytic number theory) that are required to understand modern public-key methods. In the second part we will see how to apply this know-how to study and criticize some protocols currently used.

Program

First Part: Basic theoretical facts.

Modular arithmetic. Prime numbers. Divisibility and Euclidean algorithm. Little Fermat Theorem. Euler φ function. Chinese remainder theorem. Finite fields: order of an element and primitive roots. Primality tests: Fermat. Pseudoprimality. Carmichael numbers. Quadratic residues and the Legendre symbol. Jacobi Symbol. Euler's theorem. Euler pseudoprimality test. Miller-Rabin test. Jaeschke numbers. Agrawal-Kayal-Saxena's test. RSA method: first description, attacks. Rabin's method and its connection with the integer factorization. Discrete logarithm methods. How to compute the discrete log in a finite field. Elementary factorization methods. Some remarks on Pomerance's quadratic sieve.

Second Part: Protocols and algorithms.

Fundamental crypto algorithms. Symmetric methods (historical ones, DES, AES) . Asymmetric methods. Attacks. Digital signature. Pseudorandom generators (remarks). Authentication protocols (Kerberos, Needham-Schroeder). Key exchange, Key exchange in three steps, secret splitting, secret sharing, secret broadcasting, timestamping. Signatures with RSA and discrete log.

References

1) A.Languasco, A.Zaccagnini - Introduzione alla Crittografia - Hoepli Editore, 2004. (italian).
2) N.Koblitz - A Course in Number Theory and Cryptography, Springer, 1994.
3) R.Crandall, C.Pomerance, - Prime numbers: A computational perspective - Springer, 2001.
4) B. Schneier - Applied Cryptography - Wiley, 1994.