From Algorithms to Cryptography
Tutorial

Fabrizio Luccio and Linda Pagli

Dipartimento di Informatica, Università di Pisa
Corso Italia 40, 56125 Pisa, Italy
luccio,pagli@di.unipi.it

Style and purpose. This is a rather basic set of lectures in algorithms, with an advanced focus. Cryptography and randomization are discussed as non trivial fields of algorithm application.
Contents. Six lectures organized as follows:

1. Coding and encryption of information. Basic concepts on representing numbers, sets, and algorithms. An overview on cryptography and its development in history.
2. Algorithmic paradigms and computational complexity. Iteration and recursion. Lower and upper bounds on time and space.
3. Tractable and intractable problems. The classes P, NP, NP-hard.
4. The role of randomization. Random sources and random number generators. Hash functions. Randomized algorithms.
5. Symmetric and asymmetric cryptography. From DES to AES. Public key cryptosystems and RSA.
6. Cryptography on the Web. Identification, authentication, and digital signatures. Certification Authorities. The protocol SSL.

Prerequisites. Elementary knowledge of algorithm design, data structures, and descrete mathematics is assumed, so the bases of algorithmica will be compressed in a short and partly non conventional resume.

S. Rajsbaum (Ed.): LATIN 2002, LNCS 2286, pp. 15–15, 2002.