Programma di Crittografia, a.a. 2018–19

Versione italiana.

Elementi di aritmetica di base e di teoria dei numeri elementare. In particolare, aritmetica modulare e campi finiti, numeri primi e cenni sulla loro distribuzione, test di primalità, fattorizzazione, logaritmi discreti. Operazioni elementari e loro complessità.

Principali sistemi crittografici (classici e a chiave pubblica) e algoritmi che permettono di risolvere problemi computazionali correlati.

English version.

Basic elements of arithmetics and elementary number theory. In particular, modular arithmetic, finite fields, prime numbers and their distribution, primality tests, discrete logarithms.

Main (classic and public key) cryptographic systems and algorithms which allow to solve computational related problems.

Obiettivi formativi.

Apprendimento delle nozioni basilari di aritmetica, teoria dei numeri e applicazioni alla crittografia nell'ambito della sicurezza delle informazioni.

Testi base:

W. M. Baldoni, C. Ciliberto, G. M. Piacentini, Aritmetica, crittografia e codici, Ed. Springer Italia, Unitext.

Modalità e calendario di esami.

L'esame consiste di una prova orale, che verterà su *tutto* il programma svolto.

Il calendario di esami verrà fissato in accordo con le deliberazioni del Consiglio di Corso di Laurea. Non verranno concessi appelli straordinari.