Programma di Crittografia, a.a. 2017–18

Elementi di aritmetica di base e di teoria dei numeri elmentare. Operazioni elementari, algoritmi e loro complessità. Aritmetica modulare e campi finiti, numeri primi e cenni sulla loro distribuzione, test di primalitá, fattorizzazione, logaritmi discreti.

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

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.