Crittografia
(Laurea Magistrale in Matematica)
Programma del Corso
A.A. 2016-2017

Docente: Prof. Roberto La Scala
II semestre

Argomenti del corso:

- Crittografia classica, crittoanalisi;
- Teoria dell'informazione di Shannon, segretezza perfetta, entropia, crittosistemi prodotto;
- Cifrari a blocchi, Data Encryption Standard, Advanced Encryption Standard;
- Crittografia a chiave pubblica, crittosistemi RSA, test di primalità, radici quadrate modulo n, algoritmi di fattorizzazione;
- Logaritmi discreti, crittosistema di ElGamal, calcolo di logaritmi discreti, campi finiti;
- Cifrari a flusso, generatori di numeri pseudo-random.

Testi consigliati:

1. D. Stinson, Cryptography: theory and practice, 3rd Edition
2. S. Vaudenay, A classical introduction to cryptography, Springer, 2006
3. T. Baigèneres, Y. Lu, S. Vaudenay, P. Junod, J. Monnerat, A classical introduction to cryptography, exercise book, Springer 2006
4. R. Lidl, H. Niederreiter, Finite Fields, 2nd Edition