Cr1 - Crittografia 1

Programma

Crittografia a chiave pubblica: RSA e schema di Rabin. Fattorizzazione di un intero: studio di alcuni algoritmi di fattorizzazione. Numeri pseudonimi (numeri di Carmichael, basi euleriane, basi forti). Test di primalità probabilistici. Calcolo del logaritmi discreto in un gruppo. Crittosistemi di Dieffie-Hellmann. El-Gamal. Baby steps, Massey Omura. Cenni sui crittosistemi ellittici.

Materiale Didattico

[1] Neal Koblitz, A Course in Number Theory and Cryptography. Springer, (1994). GraduateTexts in Mathematics, No 114. [2] A. Languasco -A. Zaccagnini, Introduzione alla crittografia, Hoepli. [3] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of appliedCryptography, CRC Press Series on Discrete Mathematics and its Applications. CRC Press,Boca Raton, FL, (1997) [4] Richard Crandall, Carl Pomerance, Prime numbers, a computational Perspective. Springer,(2001). [5] D. Stnson, Cryptography- Theory and practice. CRC Press (2nd edition).