Cr1 - Crittografia 1

Programma

Crittografia a chiave pubblica: RSA e schema di Rabin. Test di primalità probabilistici. Logaritmi discreti. Dieffie-Hellmann. El-Gamal. Baby steps, Giant steps. Firme digitali e cenni di crittografia a chiave simmetrica.

Materiale Didattico

[1] Neal Koblitz, A Course in Number Theory and Cryptography. Springer, (1994). GraduateTexts in Mathematics, No 114.[2] Douglas R. Stinson, Cryptography: Theory and Practice. CRC Pr, (1995).[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] F. Pappalardi, NOTE DI CRITTOGRAFIA A CHIAVE PUBBLICA . Fascicolo 1. Prerequisiti di Matematica, (2003).[5] A. Susa, NOTE DI CRITTOGRAFIA A CHIAVE PUBBLICA . Fascicolo 3. Campi finiti,Logaritmi discreti e Crittosistemi derivati., (2003).[6] Richard Crandall, Carl Pomerance, Prime numbers, a computational Perspective. Springer,(2001).