UNIVERSITY OF CRAIOVA
Faculty of Mathematics and Computer Science
Department of mathematics
Fundamental domain : Exact sciences
Domain: Mathematics
Master: Applied mathematics
Form: Day classes
Duration of studies: 2 years
Approved with academic year 2009-2010

Topics on criptography
Syllabus

Course coordinator: Assoc. Prof.dr. Dana Piciu
Code :MA 224
Second Cycle: MASTER
Second Year , Semester 2, Course 28 hours, Seminar 14 hours
Nr. of credits: 6
Domain: Mathematics
Type : compulsory
Category: complementar
Objectives : To enable the students with the basis elements in theory of criptography.
Necessary background: All courses in algebra from Licence cycle and Arithmetic and Elementary Theory of numbers .
Evaluation : Exam (E)

Contents :
Basis notions in criptography
Ciphers of substitution
Mecanical systems of encryption
Fluide systems of encryption
Systems of encryption DES
Modality of atac angaist DES
Systems of encryption AES
Encryption with public key
Systems of encryption RSA
Security of systems RSA
Systems of encryption El Gamal
Another systems of encryption with public key.

Bibliography
1. A. Atanasiu: *Teoria Codurilor*, Ed. Universităţii Bucureşti, 2002.
2. T.El Gamal: *A public key cryptosystem and a signature scheme based on discrete algorithms*, IEEE Transactions on information Theory, 31 (1985), 469-472.
3. A. Salomaa : *Criptografie cu chei publice*, Ed. Militară, 1994.
4. N.Koblitz: *A course in number theory and criptography*,Springer, Second edition,1994