UNIVERSITATEA DIN BUCUREŞTI
FACULTATEA DE MATEMATICĂ ŞI INFORMATICĂ
Str. Academiei 14, Bucureşti, ROMÂNIA
Tel/Fax: (401) 315 6990; Tel: (401) 314 8507, Cod poştal 010014

Tematica și bibliografia lecției deschise pentru ocuparea postului de LECTOR poziția 38 – Departamentul de Matematică

Elemente de algebră modernă

TEMATICĂ
1. Teorie Galois
2. Extinderi algebrice normale, extinderi algebrice separabile.
3. Teorema elementului primitiv.
4. Grup Galois. Teorema fundamentala a teoriei Galois.
5. Radacinile unitatii. Polinoame ciclotomice.
6. Grupuri rezolubile. Criteriul de rezolvabilitate al lui Galois.

BIBLIOGRAFIE
1. I.D. Ion, N. Radu, Algebra, Ed.Didactica si Pedagogica, Bucuresti, 1991
2. C. Ionescu, Ecuatii algebrice, Ovidius University Press, Constanta, 2005
3. I.D. Ion, C. Nita, D. Popescu, N. Radu, Probleme de algebra, Ed. Didactica si Pedagogica, Bucuresti, 1981
4. J. Rotman, Galois Theory, 2nd edition, Springer-Verlag, New York, 1998.

Criptografie aplicată / *Applied cryptography*

TEMATICĂ / *THEMATICS*
1. Semnături digitale (Protocoale pentru semnături digitale; RSA, ElGamal, DSA. Funcții Hash. Semnături digitale GGH cu latice. Semnături digitale NTRU. Semnături digitale de tip fail-stop) / *Digital Signatures (Digital Signature Protocols; RSA, ElGamal, DSA. Hash Functions. GGH lattice-based digital signatures. NTRU digital signatures. Fail-stop digital signatures)*.
2. Comerț electronic (Certificate digitale. Protocolul Schnorr. Protocolul Cash. Securitatea tranzacțiilor electronice: protocoale SET. Carduri smart) / *Electronic Commerce (Digital Certificates. Schnorr protocol. Cash Protocol. The security of the electronic transactions: SET protocol. Smart Cards)*.
3. Vot electronic (Protocoale de vot electronic. Criptare homomorfă. Semnături oarbe. Securitatea votului electronic) / *Electorning Voting (Electronic voting protocols. Homomorphic Encryption. Blind Signatures. The security of the Electronic voting)*.
4. Securitatea e-mail / *The security of e-mail*.

BIBLIOGRAFIE
1. B. Schneier, Applied Cryptography: John Wiley and Sons, 1996
2. A. Menezes, P. VanOorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 2001.

NOTĂ
Lecțiile din tematica disciplinei Criptografie aplicată / Applied cryptography se susțin în limba engleză.