Babeş–Bolyai University, Cluj–Napoca
Faculty of Mathematics and Computer Science
Academic year 2005-2006
Semester 4

I. General information on the course, seminar

Title: Computational Algebra (Computer Science - English)
Code: MML0007
Number of credits: 5
Place:
Schedule:

II. Information on the teacher

Name, position: Septimiu Crivei, assoc. prof. dr.
Contact information: crivei@math.ubbcluj.ro
Wednesday 10-12 Chair of Algebra, Str. Ploiesti 25.

III. Description of the course

Aims:
The course presents the mathematical algorithms used in public key cryptography. Students will be able to compare classical cryptography and public key cryptography. Number-theoretic and abstract algebra algorithms will be studied and will be implemented in projects.

Contents:

1. Public key cryptography.
2. Notions of algorithm complexity.
3. Elements of number theory.
4. Algorithms for testing primality.
5. Factorization algorithms for integers.
6. Polynomials and finite fields.
7. Algorithms for discrete logarithms and factorization of polynomials.
8. Practical aspects of public key cryprosystems.

IV. Compulsory bibliography

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational Algebra with Applications to Coding Theory and Cryptography, Editura EFES, Cluj-Napoca, 2006.
2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997.
(available at http://www.math.uwaterloo.ca/~ajmeneze)

V. Materials used during the teaching process:

N/A

VI. Schedule of lectures:

Week 1: Classical cryptography. Examples.
Key words: cryptosystem, cryptanalysis.
Week 2: Public key cryptography.
Key words: public key, one-way function, RSA cryptosystem.
Week 3: Algorithm complexity.
Key words: big O notation, polynomial (exponential) time algorithm, complexity.
Week 4: Congruences.
Key words: congruence, Euler's function, repeated squaring algorithm.
Week 5: Primes, quadratic residues.
Key words: prime, quadratic residue, Legendre (Jacobi) symbol.
Week 6: Algorithms for testing primality.
Key words: prime, pseudoprime, Fermat algorithm, Solovay-Strassen algorithm, Miller-Rabin algorithm.
Week 7: Agrawal-Kayal-Saxena-Lenstra algorithm.
Key words: prime, polynomial.
Week 8: Factorization algorithms for integers I.
Key words: factorization, Pollard's rho algorithm, Pollard's p-1 algorithm, Fermat's algorithm.
Week 9: Factorization algorithms for integers II.
Key words:factorization, factor base, continued fraction, continued fractions algorithm, quadratic sieve algorithm.
Week 10: Rabin public key cryptosystem.
Key words: Rabin cryptosystem, modular square root, square root.
Week 11: ElGamal public key cryptosystem, finite fields.
Key words: ElGamal cryptosystem, polynomial, finite field.
Week 12: Factorization of polynomials: Berlekamp's algortihm.
Key words: factorization, polynomial, vector space, Berlekamp's algorithm.
Week 13: Discrete logarithm.
Key words: discrete logarithm, Silver-Pohlig-Hellman algorithm, index calculus algorithm.
Week 14: Practical aspects of public key cryptosystems.
Key words: security, attack, hash function, digital signature.

VII. Evaluation:

Homework and project. The grade is computed as follows: N=1+H+P, where N= the final grade, H= the points for the homework problems (max. 6), P= the grade for the project (max. 3).

VIII. Organizing details, exceptional situations:

There will be strict deadlines for the homework. The project will be done in teams of 2-3 students.

IX. Optional bibliography:

1. T.H. Cormen, C.E. Leirson, R.L. Rivest, Introduction to Algorithms. MIT, 1990.
2. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
3. D.E. Knuth, The Art of Computer Programming. Addison Wesley Longman, 1998.
4. N. Koblitz, Introduction to Number Theory and Cryptography. Springer-Verlag, New York, 1987.
5. B. Schneier, Applied Cryptography. John Wiley & Sons, 1996.