UNIVERSITY OF CRAIOVA Approved with academic year
Faculty of Mathematics and Informatics 2008-2009
Departament of Mathematics
Fundamental domain : MATHEMATICS
Master 2: APPLIED MATHEMATICS
Duration of studies : 2 years

Elements of cryptography

Instructor : Lector dr. Christina-Theresia Dan

Cod: MA 223
Cycle II: Master
Second Year , Semester IV, Cours 28 hours, Seminar 28 hours
Nr. of credits: 6
Domain: Mathematics
Type : fundamental
Category : specialized discipline
Objectives: To have a knowledge of the basic notions and principles of cryptology; to know the major cryptosystems with secret key, DES and AES; to study the most popular public-key cryptosystems and their security; to apply mathematical notions in solving applicative problems.
Necessary background: The courses of: elementary number theory, algorithms in number theory, algebra (I, II and III), computer programming.
Evaluation form : Exam (E)

Contents:

- **C_1 :** *Basic notions***.** Information security and cryptography. Basic concepts. Breaf history of cryptography.
- **C_2 :** *Special classes of functions*: One way functions, trapdoor, hash. *Detecting error and methods of correction. Generating random numbers.*
- **C_3 :** *Symmetric-key encryption*. Substitution cyphers: monoalphabetic (Cezar, affine), polialphabetic (Vigenere, Playfair, Hill). Cryptanalisis of such ciphers.
- **C_4 :** *Data Encryption Standard* (*DES*). Product ciphers. Feistel cipher. Description of the cryptographic scheme DES. Utility of DES. Cryptosystems related with DES.
- **C_5 :** *Various attacks on DES*. Meet in the middle, differential and linear cryptanalisis.
- **C_6 :** *Advanced Encryption Standard* (*AES*). History. Description of the finalist crypto-systems for AES (Mars, RC6, Serpent, Twofish). AES.
- **C_7 :** *Public-key cryptography.* Basic notions. The security of secret-key cryptosystems. Symmetric-key vs public-key cryptography.
- **C_8 :** *RSA public-key cryptosystem.* Description. Implementation. *RSA* encryption in practice.
- **C_9 :** S*ecurity of RSA*. Relation to factoring. Small encryption exponent *e*. Message concealing. Another attacks.
- **C_{10} :** *El Gamal public-key cryptosystem*. Description. Security of discrete logarithms. Generalalized El Gamal encryption.

C_{11} : *Knapsack public-key encryption*. Merkle-Hellman encryption. Chor-Rivest public-key encryption.

C_{12} - C_{13}: *Digital signature.* Introduction. Basic notions. A classification of digital signature schemes and short presentation. Types of attacks on signature scheme. *RSA* signature and possible attacks. El Gamal signature. Digital standard signature (*DSS*).

C_{14} : *Data base security and secret sharing*.

Bibliography:

1. Buşneag, D., Boboc, F., Piciu, D., *Aritmetică şi teoria numerelor*, Editura Universitaria, Craiova, 1999.
2. Dan, C., *Algoritmi în teoria numerelor*, Editura Universitaria, Craiova, 2005.
3. Koblitz, N., *A Course in Number Theory and Crzptography,* ed. a II-a, Springer-Verlag, Berlin, 1994.
4. Knut, D.E., *The Art of Computer Programming*, vol. I, ed. a II-a, Addison-Wesley, 1973.
5. Menezes, A., Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1998.
6. Yan, Song Y., *Number theory for computing*, ed. a II-a, Springer Verlag, 2002.