**UNIVERSITATEA DIN CRAIOVA** Aprobat din anul univ.
**Facultatea de matematică şi informatică** 2008-2009
**Departamentul de matematică**
**Domeniul fundamental : MATEMATICĂ**
**Master 2: Matematici aplicate**
**Forma de învăţământ: cursuri de zi**
**Durata studiilor : 2 ani**

# FIŞA DISCIPLINEI

***Elemente de criptografie***

Titular curs: Lector dr. Christina-Theresia Dan

**Cod**: MA 223
**Ciclul II**: MASTER
Anul II, Semestrul IV, Curs 28 ore, Seminar 28 ore
**Nr. credite** : 6
**Domeniul** : Matematică
**Tip de disciplină** : obligatorie
**Categoria formativă** : disciplină complementară
**Obiective**: Cunoaşterea conceptelor de bază şi a principiilor ce fundamentează criptologia; cunoaşterea principalelor sisteme de criptare cu cheie secretă, a sistemelor DES şi AES; studierea celor mai cunoscute sisteme de criptare cu cheie publică şi a unor posibilităţi de atac asupra acestora; cunoaşterea şi aplicarea noţiunilor matematice necesare în realizarea de algoritmi.
**Discipline anterioare cerute:** Cursurile de teoria elementară a numerelor, algoritmi în teoria numerelor, programarea calculatoarelor, din ciclul de licenţă.
**Forma de evaluare:** Examen (E): Pentru nota finală se iau în calcul activitatea la seminar (20%) şi nota obţinută la lucrarea scrisă ( 80% ).

**Conţinut:**

**$C_1$ :** *Noţiuni introductive*. Securitatea informaţiei si criptografia. Concepte şi noţiuni de bază. Momente principale în istoria criptografiei.

**$C_2$ :** *Clase speciale de funcţii*. Funcţii neinversabile (one-way), trapă secretă, hash. *Detectarea erorii şi metode de corecţie. Generarea de numere aleatoare*.

**$C_3$ :** *Sisteme simetrice de criptare*. Cifruri de substituţie: monoalfabetice (Cezar, afin), polialfabetice (Vigenere, Playfair, Hill). Criptanaliza sistemelor de criptare monoalfabetice şi polialfabetice.

**$C_4$ :** *Sistemul de criptare DES*. Cifru produs. Cifru Feistel. Descrierea sistemului DES. Moduri de utilizare ale DES. Sisteme de criptare înrudite cu DES.

**$C_5$ :** *Modalităţi de atac asupra DES*. Meet in the middle, criptanaliză diferenţială şi liniară.

**$C_6$ :** *Sistemul de criptare AES.* Scurt istoric. Prezentare succintă a sistemelor de criptare finală (Mars, RC6, Serpent, Twofish). Sistemul de criptare AES.

**$C_7$ :** *Criptare cu cheie publică.* Consideraţii generale. Securitatea sistemelor de criptare cu cheie secretă. Criptare simetrică versus criptare cu cheie publică.

**$C_8$ :** *Sistemul de criptare RSA*. Descriere. Implementare. Construcţia unei funcţii trapă eficiente.

**$C_9$ :** *Securitatea sistemului RSA*. Informaţii despre $p$ şi $q$. Exponentul de decriptare.

Informație parțială despre textul clar. Alte tipuri de atac.

**$C_{10}$ :** *Sistemul de criptare El Gamal*. Descriere. Securitatea logaritmilor discreți. Generalizarea sistemului El Gamal.

**$C_{11}$ :** *Criptare cu cheie publică bazată pe problema rucsac*. Criptare Merkle-Hellman. Schema Chor-Rivest.

**$C_{12}$ - $C_{13}$ :** *Semnătură digitală*. Introducere. Noțiuni de bază. Clasificarea semnăturilor digitale şi o scurtă prezentare a acestora. Tipuri de atac la scheme de semnătură. Schema de semnătură RSA şi posibile atacuri. Schema de semnătură El Gamal. Descriere. Variante. Semnătură digitală standard (DSS).

**$C_{14}$ :** *Securitatea bazelor de date şi împărțirea secretelor*.

**Bibliografie**:


1. Bușneag, 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 Cryptography,* 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.