„FIŞA DISCIPLINEI

Universitatea	„1 DECEMBRIE 1918”
Facultatea	DE ŞTIINŢE
Specializarea	INFORMATICA

I.

Denumire disciplină	SECURITATE SOFTWARE	**Categoria** (DF/DD/DS/DC):

II.

Structură disciplină (Nr. ore săptămânal)				
Semestrul	Curs	Seminar	Laborator	Proiect
	28	-	14	14

III.

Statut disciplină	Obligatorie	Opţională	Facultativă
	X		

IV.

Titular disciplină				
	Curs	Seminar	Laborator	Proiect
Numele şi prenumele	INCZE ARPAD		INCZE ARPAD	
Instituţia	U. 1 DECEMBRIE 1918			
Catedră / Departament	DSEI			
Titlul ştiinţific	DOCTOR			
Gradul didactic	LECTOR			
Încadrarea (norma de bază/ asociat)	NB			
Vârsta	46			

V.

OBIECTIVELE DISCIPLINEI **(CURS ŞI APLICAŢII):** Cunoasterea conceptelor de bază si a principiilor ce fundamentează criptologia; cunoasterea principalelor sisteme de criptare cu cheie secretă, a sistemelor DES si AES; studierea celor mai cunoscute sisteme de criptare cu cheie publică si a unor posibilităţi de atac asupra acestora; cunoasterea si 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 (50%) si nota obţinută la lucrarea scrisă (50%).

VI.

Conţinutul disciplinei	
C1 : Noţiuni introductive. Securitatea informaţiei si criptografia. Concepte si noţiuni de bază. Momente principale în istoria criptografiei. C2 : Clase speciale de funcţii. Funcţii neinversabile (one-way), trapă secretă, hash. Detectarea erorii si metode de corecţie. Generarea de numere aleatoare. C3 : Sisteme simetrice de criptare. Cifruri de substituţie: monoalfabetice (Cezar, afin), polialfabetice (Vigenere, Playfair, Hill). Criptanaliza sistemelor de criptare monoalfabetice si polialfabetice. C4 : Sistemul de criptare DES. Cifru produs. Cifru Feistel. Descrierea sistemului DES. Moduri de utilizare ale DES. Sisteme de criptare înrudite cu DES. C5 : Modalităţi de atac asupra DES. Meet in the middle, criptanaliză diferenţială si liniară. C6 : Sistemul de criptare AES. Scurt istoric. Prezentare succintă a sistemelor de criptare finală (Mars, RC6, Serpent, Twofish). Sistemul de criptare AES. C7 : Criptare cu cheie publică. Consideraţii generale. Securitatea sistemelor de criptare cu cheie secretă. Criptare simetrică versus criptare cu cheie publică. C8 : Sistemul de criptare RSA. Descriere. Implementare. Construcţia unei funcţii trapă	

eficiente. C9 : Securitatea sistemului RSA. Informaţii despre p si q. Exponentul de decriptare. Informaţie parţială despre textul clar. Alte tipuri de atac. C10 : Sistemul de criptare El Gamal. Descriere. Securitatea logaritmilor discreţi. Generalizarea sistemului El Gamal. C11 : Generatoare de numere aleatoare. Generarea cheilor de criptare. C12: Semnătură digitală. Introducere. Noţiuni de bază. Clasificarea semnăturilor digitale si o scurtă prezentare a acestora. Tipuri de atac la scheme de semnătură. Schema de semnătură RSA si posibile atacuri. Schema de semnătură El Gamal. Descriere. Variante. Semnătură digitală standard (DSS). C13: Scheme de partajare a secretelor. Criptografie vizuală C14: Securitatea bazelor de date
VI.2. Seminar (dacă este cazul)
-
VI.3. Lucrări de laborator (dacă este cazul)
Lucrările de laborator vor conţine aplicaţii practice pentru subiectele tratate la curs.
VI.4. Tematică proiect (dacă este cazul)
Realizarea unei aplicaţii pentru criptarea fişierelor Realizarea unei aplicaţii care să utilizeze o schemă de partajare a secretului

VII.

Bibliografie
1. Busneag, D., Boboc, F., Piciu, D., *Aritmetică si 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. 1. 6. Yan, Song Y., *Number theory for computing*, ed. a II-a, Springer Verlag, 2002.

VIII.

Forme de activitate	**Metode didactice folosite**
Curs	Cursul se va preda utilizând prezentări Power Point cu ajutorul videoproiectorului
Seminar	
Laborator	La laborator se vor face aplicaţii ale noţiunilor predate la curs, astfel încât studenţii să înţeleagă, să aprofundeze şi mai ales să-şi formeze deprinderi de a aplica practic cunoştinţele achiziţionate.
Proiect	

IX.

Forme de activitate	**Evaluare** (scris, scris şi oral, oral, test, aplicaţie practică, altele)	**Procent din nota finală**
Examen	aplicaţie practică	**50%**
Colocviu	-	**-**
Seminar	-	**-**
Laborator	aplicaţii practice	**50%**
Proiect	-	**-**

Data: Titular curs,