UNIVERSITATEA TITU MAIORESCU
Facultatea de Informatică
Catedra de informatică

APROB
DECAN
Prof. dr.
Emil CREŢU

PROGRAMĂ ANALITICĂ

An universitar: 2011-2012

Denumirea disciplinei	**Bazele matematice ale criptografiei**						
Codul disciplinei	**I.1.1.1.**	Numărul de credite	8	Numărul ore pe semestru / activităţi			
				Total	C	S	S/L/P
				56	28	28	28
Facultatea beneficiară	**Facultatea de Informatică**			Anul			2
				Semestrul			4
Specializarea	**Masterat: Securitatea sistemelor informatice şi reţelelor informaţionale**						

Obiective

1. Cunoaşterea unor instrumente matematice pe care se bazează sistemele criptografice moderne.
2. Exemplificarea folosirii bazelor matematice în elaborarea unor sisteme de încriptare şi de decriptare.
3. Insuşirea principiilor analizei criptografice, metode şi procedee de evitare a vulnerabilităţilor unor sisteme criptografice

Conţinut (Descriptori)

Cap.1 Grupuri abeliene finite.

Subgrupuri, grupuri ciclice, generatori. Problema logaritmilor discreţi. Definiţii, exemple, algoritme.

Teorema chineză a claselor de resturi. Structura grupurilor abeliene finite. Grupul unităţilor inelului Z_n. (**4 ore curs, 4 ore seminar**).

Cap.2 Corpuri finite.

Caracteristica unui corp. Corpul definit de un polinom ireductibil. Corpuri Galoisiene. Isomorfismul corpurilor definite de polinoamele ireductibile de gradul n peste corpul Z_p. Laticea corpurilor finite de caracteristică p.

Generatori multiplicativi ai unui corp Galoisian. Polinoame primitive. (**4 ore curs, 4 ore seminar**).

Cap.3 Sisteme criptografice.

Definiţia unui sistem criptografic. Sistemul criptografic Rivest-Shamir-Adleman. Criptarea, decriptarea, analiza sistemului. Algoritme de descompunere în factori.

Sistemul criptografic ElGamal. (**4 ore curs, 4 ore seminar**).

Cap.4 Rădăcina pătrată într-un inel de clase de resturi.

Simbolul lui Legendre: definiţie, proprietăţi, exemple. Simbolul lui Iacobi. Algoritmul de rezolvare a ecuaţiei $x^2 = a$ în corpul Z_p.

Sistemul criptografic al lui Rabin. (**4 ore curs, 4 ore seminar**).

Cap.5 Curbe eliptice

Grupul abelian al unei curbe eliptice definite peste un corp finit. Exemple. Teorema lui Hasse privind ordinul grupului unei curbe eliptice.

Algoritmul de calculare a ordinului unui punct al unei curbe eliptice. (**4 ore curs, 4 ore seminar**).

Cap.6 Sisteme criptografice bazate pe curbe eliptice.

Avantajele folosirii curbelor eliptice în sistemele criptografice. Clase de curbe eliptice întrate în uz în criptografie. (**4 ore curs, 4 ore seminar**).

Ca.7 Semnături digitale.

Cerinţele semnăturii digitale. Câteva exemple de sisteme de semnături digitale. (**4 ore curs, 4 ore seminar**).

Forma de evaluare (E – examen, V – verificare pe parcurs, C – colocviu)		E
Stabilirea notei finale (procentaje)	examinare finală	50%
	activităţi aplicative atestate/laborator/lucrări practice/proiect, teste pe parcursul modulului, teme de control	50%
Bibliografia	1. Constantin DOCHIŢOIU, *Instrumente algebrice ale criptografiei*, Ed. Academiei Tehnice Militare, Bucureşti, 2009 2. Neal KOBLITS, *A Course in Number Theory and cryptography*, Springer-Verlag, New York, 1988. 3. Neal KOBLITS , *Algebraic aspects of Cryptography*, Springer-Verlag, New York, 1999 4. Alfred MENEZES, Paul C. van OORSHOT, Scot. A. VANSTONE, *Handbook of Applied Cryptography*, CRC Press, 2001	
Titular (titulari)	Grad didactic, titlu, prenume, numele	
	Conf. dr. Constantin DOCHIŢOIU	