FIŞA DISCIPLINEI*

1. Date despre program

Instituţia de învăţământ superior	Universitatea Lucian Blaga din Sibiu
Facultatea	Ştiinţe
Departament	Departamentul de Matematică şi Informatică
Domeniul de studiu	Informatică
Ciclul de studii	Masterat
Specializarea	Sisteme şi tehnologii Informatice avansate

2. Date despre disciplină

Denumirea disciplinei	**Criptografie**			
Codul cursului	Tipul cursului	An de studiu	Semestrul	Număr de credite
38061003012	DS	2	3	8
Tipul de evaluare	Categoria formativă a disciplinei *(DF=fundamentală.; DD=domeniu; DS=specialitate; DC=complementară)*			
Examen	DS			
Titular activităţi curs	Conf univ. dr. Constantinescu Nicolae			
Titular activităţi seminar / laborator/ proiect	Conf univ. dr. Constantinescu Nicolae			

3. Timpul total estimat

Extinderea disciplinei în planul de învăţământ – număr de ore pe săptămână				
Curs	Seminar	Laborator	Proiect	Total
2	-	2	-	**4**
Extinderea disciplinei în planul de învăţământ – Total ore din planul de învăţământ				
Curs	Seminar	Laborator	Proiect	Total ($NOAD_{sem}$)
28		28		**56**

Distribuţia fondului de timp pentru studiu individual	Nr.ore
Studiul după manual, suport de curs, bibliografie şi notiţe	45
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	45
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	40
Tutoriat:	10
Examinări:	4
Total ore alocate studiului individual ($NOSI_{sem}$)	144
Total ore pe semestru ($NOAD_{sem}$ + $NOSI_{sem}$)	**200**

4. Precondiţii (acolo unde este cazul)

De curriculum	
De competenţe	

Adresa: Str. Ion Raţiu, nr. 5-7
Sibiu, 550024, România
e-mail: dep.matinf@ulbsibiu.ro
http://stiinte.ulbsibiu.ro

Tel: +40 (269) 216 642
Fax: +40 (269) 216 617

5. Condiţii (acolo unde este cazul)

De desfăşurare a cursului	Sală de curs, dotată cu tablă, calculator, videoproiector şi software
De desfăşurare a sem/lab/pr	Sală de laborator dotată cu calculatoare desktop

6. Competenţe specifice acumulate

Competenţe profesionale	• Cunoaşterea şi utilizarea adecvată a noţiunilor teoretice fundamentale legate de criptografie • Capacitatea de a explica modul de constructie a algoritmilor croptografici • Capacitatea de a interpreta rezultatele obtinute • Capacitatea de a implemnta algoritmi criptografici • Capacitatea de a utiliza si modifica conform cerinteleor algoritmii deja implementati • Capacitatea de a proiecta şi realiza aplicaţii complexe care utilizeaza algoritmii si tehnicile invatate
Competenţe transversale	• Dezvoltarea atitudinii pozitive faţă de muncă şi responsabilitate pentru propria pregătire profesională. • Dezvoltarea spiritului de munca in echipa

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	• Insusirea algoritmilor criptografici și a modului în care aceștia pot fi folosiți în diverse situații reale.
Obiectivele specifice	• Insusirea tehnicilor de criptare, codare, identificare respectiv corectie a erorilor si vulnerabilitatilor. • Protectia impotriva atacurilor informatice.

8. Conţinuturi

Curs		Nr. ore
Curs 1	Scurt istoric al criptografiei. Noțiuni de bază. Sisteme simetrice de criptare.	1
Curs 2	Cifruri de substituție. Sisteme de criptare monoalfabetice	1
Curs 3	Cifruri de substituție. Sisteme de criptare polialfabetice	1
Curs 4	Sisteme de criptare fluide. Sisteneme sincronizabile și auto – sincronizabile. Sistemul aditiv fluid de criptare RC4. Securitatea sistemului RC4.	1
Curs 5	Sistemul de criptare DES. Considerații generale. Descrierea sistemului DES. Controverse legate de DES. Moduri de utilizare ale DES-ului. Sisteme de criptare înrudite cu DES.	1
Curs 6	Sistemul de criptare AES. Istoric și scurtă prezentare a sistemelor intrate în finală: Mars, RC6, Serpent, Twofish. Detalii ale sistemului de criptare AES.	1
Curs 7	Criptare cu cheie publica. Considerații generale. Funcții neinversabile. Trapa secretă. Securitatea sistemelor de criptare cu cheie publică. Comparație între criptarea simetrică și cea cu cheie publică.	1
Curs 8	Sistemul de criptare RSA. Implementarea sistemului.	1

Curs 9	Sistemul de criptare El Gamal. Calculul logaritmului discret.	1
Curs 10	Semnături electronice. Protocoale de semnătură. Semnătura El Gamal. Standarde de semnătură electronică	1
Curs 11	Protocoale de distribuire a cheilor. Predistribuirea cheilor. Kerberos. Schimbul de chei Diffie - Hellman	1
Curs 12	Sisteme electronice de plată. Proprietăți de bază. Securitatea plăților electronice. Protocoale de semnătură "bliend'. Scheme de identificare. Problema reprezentării în grupuri.	1
Curs 13	Sistemul electronic de plată Brands. Inițializarea sistemului Brands. Tehnici pentru crearea sistemului. Sistemul de bază Brands. Corectitudinea sistemului de bază.	1
Curs 14	Protocoale de vot electronic. Caracteristicile unui sistem de vot electronic. Protocoale independente de vot. Protocol cu autoritate centrală. Protocolul Mu – Varadharajan. Slăbiciuni ale protocolului Mu – Varadharajan.	1
	Total ore curs:	**14**
Seminar/Laborator		Nr. ore
Sem 1	Implementarea algoritmului lui Cezar	2
Sem 2	Implementarea substituirii monoalfabetice	2
Sem 3	Implementarea cifrurilor de permutare	2
Sem 4	Implementarea sistemului de criptare afin	2
Sem 5	Implementarea sistemului de criptare Polybios	2
Sem 6	Implementarea sistemului de criptare Playfair	2
Sem 7	Implementarea sistemului de criptare Vigenere	2
Sem 8	Implementarea sistemului de criptare Rijndael (AES)	2
Sem 9	Implementarea sisemului de criptare DES	2
Sem 10	Implementarea sistemelor de criptare cu cheie publică – sistemul RSA	2
Sem 11	Implementarea sistemelor de criptare cu cheie publică – sistemul El Gamal	2
Sem 12	Ascunderea informatiei (Steganografia, Filigranarea, Securitatea tiparirii hartiilor de valoare)	2
Sem 13	Atacuri criptografice (forta bruta, text clar (cunoscut, ales, selectat, ...), atac zi de nastere, intalnire la mijloc, om la mijloc, ...)	2
Sem 14	Validarea tranzacţiilor. Securitatea si securizarea tranzacţiilor. Erorile sistemelor, calculatoare moleculare.	2
	Total ore seminar/laborator	28

Metode de predare

Expunerea sistematică a cunoştinţelor (deductivă, inductivă şi formalizată, expuneri ppt); conversaţia frontala; conversaţia euristică, problematizare, studii de caz, modelarea		

Bibliografie

Referinţe bibliografice recomandate	M. Howard, D. LeBlanc, Writing Secure Code, Practical strategies and techniques for secure application coding in a networked world, Second Edition, Microsoft, 2002

Referinţe bibliografice suplimentare	D. Oprea, Protectia si securitatea informatiilor, Ed. Polirom, Iasi, 2003

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Se realizeaza prin contacte periodice cu acestia in vederea analizei problemei.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Ponderea în nota finală	Obs.**
Curs	Însușirea de cunoștințe fundamentale și aprofundate	Examen scris și aplicativ	50%	CEF
Laborator	Prezentare proiect și teme laborator	Evaluare pe parcurs	50%	nCPE
Standard minim de performanţă				
Pentru promovarea examenului, trebuie obținută minim nota 5 la evaluările pe parcurs și la examenul de evaluare finală				

(*) **Fişa disciplinei cuprinde componente adaptate persoanelor cu dizabilităţi, în funcţie de tipul şi gradul acestora.**
(**) CPE – condiţionează participarea la examen; nCPE – nu condiţionează participarea la examen; CEF - condiţionează evaluarea finală;

Data completării: 26.09.2018
Data avizării în Departament:28.09.2018

	Grad didactic, titlul, prenume, numele	Semnătura
Titular disciplină	Conf univ. dr. Constantinescu Nicolae	
Director de departament	Prof.univ.dr. Mugur Acu	