

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Babeș-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematica și Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Licența
1.6 Programul de studii / Calificarea	Informatică – limba română

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Securitatea Informației</b>						
2.2 Titularul activităților de curs	<b>Lect. univ. Dr. Christian Sacarea</b>						
2.3 Titularul activităților de seminar	<b>Lect. univ. Dr. Christian Sacarea</b>						
2.4 Anul de studii	<b>4</b>	2.5 Semestrul	<b>7</b>	2.6. Tipul de evaluare	<b>E</b>	2.7 Regimul disciplinei	<b>Optionala</b>

### 3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	<b>3</b>	Din care: 3.2 curs	<b>2</b>	3.3 seminar/laborator	1 lab
3.4 Total ore din planul de învățământ	<b>42</b>	Din care: 3.5 curs	<b>28</b>	3.6 seminar/laborator	<b>14</b>
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					50
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					30
Tutoriat					20
Examinări					13
Alte activități: .....					-
3.7 Total ore studiu individual		133			
3.8 Total ore pe semestru		175			
3.9 Numărul de credite		7			

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	<ul style="list-style-type: none"> <li>Algebra liniară</li> </ul>
4.2 de competențe	<ul style="list-style-type: none"> <li>Competențe medii de programare, capacitate de sinteză și analiză</li> </ul>

### 5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	<ul style="list-style-type: none"> <li></li> </ul>
5.2 De desfășurare a	<ul style="list-style-type: none"> <li>Laborator dotat cu calculatoare</li> </ul>

**6. Competențele specifice acumulate**

<b>Competențe profesionale</b>	C6.2 Identificarea și explicarea arhitecturilor de bază pentru organizarea și gestiunea sistemelor
<b>Competențe transversale</b>	<p>CT1 Aplicarea regulilor de muncă organizată și eficientă, a unor atitudini responsabile față de domeniul didactic-științific, pentru valorificarea creativă a propriului potențial, cu respectarea principiilor și a normelor de etică profesională</p> <p>CT3 Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională</p>

**7. Obiectivele disciplinei** (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	<ul style="list-style-type: none"> <li>• Studentii trebuie să stăpânească elementele definitorii ale securității informației, elemente de criptografie și de atac criptanalitic;</li> </ul>
7.2 Obiectivele specifice	<ul style="list-style-type: none"> <li>• Modalitățile de identificare a vulnerabilităților unui sistem informatic</li> <li>• Cunoașterea elementelor de bază ce asigură securitatea informației din punct de vedere criptografic</li> <li>• Modalități specifice de atac criptografic</li> </ul>

**8. Conținuturi**

8.1 Curs	Metode de predare	Observații
Cursul 1. Sisteme de securizare a informației. Un scurt istoric, introducere în criptografie, prezentarea unor algoritmi simpli.	Discuții, prelegeri, studii de caz	
Cursul 2. Algoritmi criptografici cu cheie simetrică. Evoluția acestor algoritmi. Vulnerabilități. Generarea și alegerea cheii. Metode de atac.	Discuții, prelegeri, studii de caz	
Cursul 3. Generatoare de numere pseudoaleatoare. Trecere în revistă a principalelor generatoare de numere pseudoaleatoare, inclusiv arii de aplicabilitate. Vulnerabilități și atacuri.	Discuții, prelegeri, studii de caz	

Cursul 4. Generatoare de numere real aleatoare. Prezentarea problematicei. Necesitatea acestor generatoare pentru aplicatii criptografice. Exemple.	Discutii, prelegeri, studii de caz	
Cursul 5. Sistemul one-time-pad	Discutii, prelegeri, studii de caz	
Cursul 6. Criptarea in retele de telefonie mobila. Cifrul A5/1, A5/2. Prezentarea algoritmilor.	Discutii, prelegeri, studii de caz	
Cursul 7. Vulnerabilitatile cifrului A5/1, A5/2.	Discutii, prelegeri, studii de caz	
Cursul 8. Atacul asupra cifrului A5/1, A5/2.	Discutii, prelegeri, studii de caz	
Cursul 9. Protocolul Bluetooth. Cifrul A5/3.	Discutii, prelegeri, studii de caz	
Cursul 10. Atacul asupra protocolului Bluetooth.	Discutii, prelegeri, studii de caz	
Cursul 11. Retele wireless. Prezentare generala a principiilor de securitate informatica.	Discutii, prelegeri, studii de caz	
Cursul 12. Retele wireless. Protocele, algoritmi, vulnerabilitati.	Discutii, prelegeri, studii de caz	
Cursul 13. Atacul asupra protocolului wireless.	Discutii, prelegeri, studii de caz	
Cursul 14. Atacul unui protocol wireless	Discutii, prelegeri, studii de caz	
<b>8.2 Seminar / laborator</b>		
<b>8.2 Seminar / laborator</b>	<b>Metode de predare</b>	<b>Observații</b>
Laborator 1: Analiza unui algoritm criptografic. Metode si sisteme software.	Expunere, dialog, studii de caz	2 ore în doua saptamâni – 7 laboratoare
Laborator 2: Atacul unor texte criptate.	Expunere, dialog, studii de caz	
Laborator 3: Implementarea unor generatoare de numere pseudoaleatoare. Discutii pe aceasta tema.	Expunere, dialog, studii de caz	
Laborator 4. Sistemul one-time-pad	Expunere, dialog, studii de caz	
Laborator 5. Criptarea in retele de telefonie mobila. Implementarea algoritmilor.	Expunere, dialog, studii de caz	
Laborator 6. Criptarea in retele de telefonie mobila. Implementarea algoritmilor.	Expunere, dialog, studii de caz	
Laborator 7. Atacul cifrului A5/1.	Expunere, dialog, studii de caz	

## **9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului**

- Cursul exista in programa universitatilor reprezentative din lume

- Continutul cursului este considerat important pentru securizarea sistemelor informatice

## 10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoasterea principiilor fundamentale	Examen scris	40%
	Aplicarea metodelor invatate in rezolvarea problemelor		
10.5 Seminar/laborator	Implementarea conceptelor si algoritmilor predate la curs	Proiect	40%
	Inovare, spirit de initiativa, munca in echipa	Examinare, portofoliu, observare continua	20%
10.6 Standard minim de performanță			
<ul style="list-style-type: none"> <li>• Minim nota 5 in urma evaluarilor globale</li> </ul>			

Data completării

Titular de curs

Titular de seminar

30.4.2014

Lect. univ. Dr. Christian Sacarea

Lect. univ. Dr. Christian Sacarea

Data avizării în departament

Director de departament

.....

Prof. Univ. Dr. Bazil Parv