

**FIȘA DISCIPLINEI****1. Date despre program**

<b>1.1</b> Instituția de învățământ superior	<b>Universitatea “Alexandru Ioan Cuza” din Iași</b>
<b>1.2</b> Facultatea	<b>Facultatea de Informatică</b>
<b>1.3</b> Departamentul	<b>Informatică</b>
<b>1.4</b> Domeniul de studii	<b>Informatică</b>
<b>1.5</b> Ciclul de studii	<b>Studii universitare de Masterat</b>
<b>1.6</b> Programul de studii / Calificarea	Informatica/Licentiat in informatica

**2. Date despre disciplină**

<b>2.1</b> Denumirea disciplinei		<b>Securitatea rețelelor de calculatoare</b>					
<b>2.2</b> Titularul activităților de curs		<b>Prof.Dr. Tiplea Ferucio Laurentiu</b>					
<b>2.3</b> Titularul activităților de seminar		<b>Lect.Dr. Onica Emanuel</b>					
<b>2.4</b> An de studiu	<b>I</b>	<b>2.5</b> Semestru	<b>2</b>	<b>2.6</b> Tip de evaluare	<b>M</b>	<b>2.7</b> Regimul disciplinei*	<b>OB</b>

\* *OB* – Obligatoriu / *OP* – Opțional

**3. Timpul total estimat (ore pe semestru și activități didactice)**

<b>3.1</b> Număr de ore pe săptămână	<b>4</b>	din care: <b>3.2</b> curs	<b>2</b>	<b>3.3</b> seminar/laborator	<b>2</b>
<b>3.4</b> Total ore din planul de învățământ	<b>56</b>	din care: <b>3.5</b> curs	<b>28</b>	<b>3.6</b> seminar/laborator	<b>28</b>
Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și altele					<b>14</b>
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					<b>14</b>
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					<b>28</b>
Tutoriat					-
Examinări					<b>4</b>
Alte activități					-
<b>3.7</b> Total ore studiu individual					<b>56</b>
<b>3.8</b> Total ore pe semestru					<b>114</b>
<b>3.9</b> Număr de credite					<b>8</b>

**4. Precondiții (dacă este cazul)**

<b>4.1</b> De curriculum	-
<b>4.2</b> De competențe	-



## 5. Condiții (dacă este cazul)

5.1 De desfășurare a cursului	Este recomandată prezența la curs
5.2 De desfășurare a seminarului	Prezența la seminar

## 6. Competențe specifice acumulate

Competențe profesionale	<b>C1.</b> Expunerea unor noțiuni și rezultate avansate din domeniul crețelor de calculatoare, în vederea însușirii lor <b>C2.</b> Aplicarea conceptelor asimilate în domenii specializate, precum securitatea informației
Competențe transversale	<b>CT1.</b> Eficientizarea activităților desfășurate în cadru organizat, prin aplicarea regulilor academice de muncă riguroasă și creativă <b>CT2.</b> Utilizarea optimă a surselor informaționale și a resurselor de comunicare din domeniu <b>CT3.</b> Exprimarea unei atitudini responsabile față de înțelegerea rolului domeniului în informatică <b>CT4.</b> Valorificarea eficace a potențialului științific însușit în domeniu

## 7. Obiectivele disciplinei (din grila competențelor specifice acumulate)

7.1 Obiectivul general	Cursul introduce studenților teme avansate în securitatea rețelelor de calculatoare, precum criptografie bazată pe identitate și atribute, și discută modul în care acestea sunt deja utilizate în practica avansată pentru obținerea de tehnici de securitate a informației.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenții vor fi capabili să: <ul style="list-style-type: none"><li>▪ Utilizeze corespunzător concepte de criptografie avansată;</li><li>▪ Înțeleagă corespunzător, la nivel ridicat, securitatea rețelelor de calculatoare.</li></ul>

## 8. Conținut

8.1	Curs	Metode de predare	Observații (ore și referințe bibliografice)
-----	------	-------------------	--



1.	Scurta incursiune in criptografie	Expunere si demonstratii realizate la tabla	2
2.	Criptografie bazata pe identitate (partea I – schema Cocks)	Expunere si demonstratii realizate la tabla	2
3.	Criptografie bazata pe identitate (partea II – schema Cocks)	Expunere si demonstratii realizate la tabla	2
4.	Criptografie bazata pe identitate (partea I – schema BGH)	Expunere si demonstratii realizate la tabla	2
5.	Criptografie bazata pe identitate (partea II – schema BGH)	Expunere si demonstratii realizate la tabla	2
6.	Criptografie bazata pe identitate : anonimizare	Expunere si demonstratii realizate la tabla	2
7.	Criptografie bazata pe identitate : schema Boneh-Franklin	Expunere si demonstratii realizate la tabla	2
8.	Criptografie bazata pe atribute (partea I – scheme bazate pe secret sharing si aplicatii biliniare)	Expunere si demonstratii realizate la tabla	2
9.	Criptografie bazata pe atribute (partea II – scheme bazate pe secret sharing si aplicatii biliniare)	Expunere si demonstratii realizate la tabla	2
10.	Criptografie bazata pe atribute (partea I – scheme bazate pe aplicatii multiliniare)	Expunere si demonstratii realizate la tabla	2
11.	Criptografie bazata pe atribute (partea II – scheme bazate pe aplicatii multiliniare)	Expunere si demonstratii realizate la tabla	2
12.	Constructii de aplicatii multiliniare (partea I)	Expunere si demonstratii realizate la tabla	2
13.	Constructii de aplicatii multiliniare (partea II)	Expunere si demonstratii realizate la tabla	2
14.	Aplicatii la “searchable encryption”	Expunere si demonstratii realizate la tabla	2

**Bibliografie****Referințe principale:**

- L. Martin: Introduction to Identity-based Encryption, Artech House, 2008
- S. Chatterjee, P. Sarkar: Identity-based Encryption, Springer, 2010
- Articole de specialitate

**Referințe suplimentare:**

- F.L. Tiplea. Fundamentele Algebrice ale Informaticii, Ed. Polirom, 2006
- F.L. Tiplea: Introducere in criptografie, Curs Facultatea de Informatica, 2017

<b>8.2</b>	<b>Seminar / Laborator</b>	<b>Metode de predare</b>	<b>Observații</b> (ore și referințe bibliografice)
------------	----------------------------	--------------------------	---



1.	Recapitulare notiuni de baza privind comunicarea in retea. Prezentarea de aplicatii pentru monitorizare si simulare trafic.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
2.	Pregatirea unui mediu controlat pentru simularea de atacuri in retea.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
3.	Exemple de atacuri la nivel legatura de date si internet. Propunerea unei teme aplicative spre rezolvare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
4.	Scurta recapitulare legata de functionarea protocoalelor de transport. Exemple de atacuri asupra TCP bazate pe ICMP.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
5.	Evaluarea temelor propuse spre rezolvare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
6.	Exemple de atacuri asupra TCP bazate pe injectare de pachete la nivel transport (resetarea conexiunii). Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
7.	Exemple de atacuri de tip SYN flood. Detalii privind protectia asupra atacurilor de tip SYN flood si resetare conexiune. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
8.	Discutare de articole stiintifice privind mecanisme de protectie in aria atacurilor la nivel transport.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
9.	Exemple de atacuri bazate pe injectare de pachete cu efect de "deturnare" a sesiunii - session hijacking. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
10.	Scurta descriere SSH ca mecanism de protectie impotriva atacurilor la nivel sesiune si aplicatie. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2



11.	Scurta descriere a diverselor metode de organizare a atacurilor de tip DDoS. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
12.	Chestiuni generale legate de functionarea DNS si DNSSEC. Exemple de atacuri asupra DNS cu acces la mediu si in mod blind. Propunerea unei teme aplicative.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
13.	Evaluare prin exercitii recapitulative.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
14.	Evaluarea temelor propuse spre rezolvare. Prezentarea de tematici de cercetare in domeniul securitatii retelelor de calculatoare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2

**Bibliografie**

- W. Stallings: Cryptography and Network Security, Pearson, 2013
- M. Gregg: The Network Security Test Lab: A Step-by-Step Guide, Wiley 2015
- Wireshark – Online: <https://www.wireshark.org/#learnWS>
- Articole de specialitate

**9. Coroborarea conținutului disciplinei cu așteptările reprezentanților comunității, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului**

Cursul este corelat cu asteptarile moderne in securitatea informatiei (de exemplu, Amazon si-a format recent echipe de securitatea informatiei, multi dintre fostii studenti ai masterului de securitatea informatiei fiind membri ai acestor echipe).

**10. Evaluare**

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Test scris	50%
10.5 Seminar/ Laborator	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu;	Exercitii realizate in clasa de fiecare student, precum si evaluarea de	50%



	Abilitatea de aplicare a lor	implementari	
<b>10.6 Standard minim de performanță</b>			
Minim nota 5 atat la testul scris cat si la activitatea de seminar/laborator			

Data completării

Titular de curs

Titular de seminar

Prof.Dr. Tiplea Ferucio Laurentiu

Lect.Dr. Emanuel Onica

Data avizării în departament

Director de departament