FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea „Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Informatică**
1.3 Departamentul	**Informatică**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Master**
1.6 Programul de studii / Calificarea	**Securitatea informației**

2. Date despre disciplină

2.1 Denumirea disciplinei			**Logici de încredere în securitatea informației**				
2.2 Titularul activităţilor de curs			**Prof. Dr. Cristian-Dumitru Masalagiu**				
2.3 Titularul activităţilor de seminar			**Prof. Dr. Cristian-Dumitru Masalagiu**				
2.4 An de studiu	**2**	**2.5** Semestru	**2**	**2.6** Tip de evaluare	**E**	**2.7**Regimul disciplinei	**OB**

** OB – Obligatoriu / OP–Opţional*

3. Timpul total estimat(ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**4**	din care:**3.2**curs	**2**	**3.3**seminar	**2**
3.4 Total ore din planul de învăţământ	**56**	din care:**3.5** curs	**28**	**3.6**seminar	**28**
Distribuţia fondului de timp					ore
Studiu după manual, suport de curs, bibliografie şi altele					**14**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					**28**
Pregătire seminarii/laboratoare,teme, referate, portofolii şi eseuri					**138**
Tutoriat					**0**
Examinări					**2**
Alte activităţi					**2**

3.7 Total ore studiu individual	**180**
3.8 Total ore pe semestru	**240**
3.9 Număr de credite	**8**

4. Precondiţii

4.1 De curriculum	**Absolvirea unui curs de „Logică pentru informatică”**
4.2 De competenţe	**-**

5. Condiţii

5.1 De desfăşurare a cursului	-
5.2 De desfăşurare a laboratorului	**-**

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.** Cunoaște conceptele de bază legate de sistemele de securitate și comunicarea prin protocoale specifice în sistemele multiagent. **C2.**Înțelege modalitatea de a construi logici noi pentru a analiza protocoalele de securitate și a demonstra corectitudinea funcționării acestora. **C3.**Stăpânește logicile clasice (**LP**, **LP1**) precum și câteva logici neclasice cum ar fi: logica modală (**MD**), logicile temporale cutimp liniar și ramificat (**LTL, CTL, CTL***). **C4.**Și-a însușit conceptele de bază legate de logicile epistemice în general și logicile de încredere în particular (cum ar fi **BAN**, **GNY** sau **SvO**). **C5.**Este capabil să folosească practic, pentru demonstrații într-un sistem deductiv sau pentru a arăta satisfiabilitatea unei formule, undemonstrator automat (**Isabelle**sau **HOL**), un model-checker (**MCMAS** sau **TLC**), sau un **SMT**-solver (de exemplu, **Z3**).
Competenţe transversale	**CT1.**Colaborează în echipă pentru atingerea unui obiectiv comun. **CT2.** Utilizeazacompetent atât softuri comerciale dedicate, cât și instrumente formale pentru dezvoltarea de noi competențe. **CT3.** Prezintă coerent în fața unui public soluțiile propuse.

7. Obiectivele disciplinei

7.1Obiectivul general	Capacitatea de a analiza și de a demonstra corectitudinea funcționării, cu ajutorul logicii formale, a oricărui protocol criptografic de securitate utilizat pentru comunicare într-un sistem multiagent.
7.2Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Explicediferențele dintre diverse logici care pot fi utilizate în scopul amintit. ▪ Utilizeze, fără implicarea directă a unui computer, sistemele deductive specifice (de exemplu**SD-BAN** sau**SD-GNY**). ▪ Analizeze, cu ajutorul logicii, vulnerabilitățile unor protocoale existente; să creeze noi protocoale sau chiar noi logici pentru analiza acestora. ▪ Utilizeze demonstratoare automate, model-checker-e, **SMT**-solver-e comerciale existentepentru raționamentele specifice logicilor de încredere trecute în revistă la curs. ▪ Descrie și să traducă din limbaj natural într-un limbaj intermediar și în unul formal bazat pe logică un protocol de securitate și specificațiile funcționării corecte a acestuia.

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii**
1.	Recapitulare: logica aristotelică (**LP**, **LP1**), sisteme de securitate, protocoale criptografice de comunicare în sisteme multiagent	Expunere, demonstrație, exemplificare	2 ore
2.	Logica modală clasică (**MD**), logica temporală cu timp liniar (**LTL**) și ramificat (**CTL**, **CTL***)	Expunere, demonstrație, exemplificare	2 ore
3.	Logici epistemice, cunoștințe (**K***noledge*) și credințe (**B***eliefs*)	Expunere, dezbatere, exemplificare	2 ore

4.	Măsuri ale „distanței” dintre **K**-**B**	Expunere, dezbatere, demonstrație	2 ore
5.	Logica justificărilor plauzibile (**L***ogic of***P***lausible***J**ustification*) în sistemele multiagent	Expunere, dezbatere, demonstrație	2 ore
6.	Logici calitative și cantitative; proprietăți de securitate (*authenticity, anonimity, observability* etc.)	Expunere, demonstrație	2 ore
7.	Protocoale criptografice de securitate în sisteme multiagent (generice, didactice, dedicate); *forma abstractă* a protocoalelor	Expunere, dezbatere	2 ore
8.	Logica **BAN** (**B***urrows*, **A***badi*, **N***eedham*) în contextul dat de modelul Dolev-Yao (**MDY**)	Expunere, dezbatere, exemplificare	2 ore
9.	Sintaxa **BAN** în **BNF** (**B***ackus-***N***aur***F***orm*); *formule* și *propoziții*	Expunere, exemplificare	2 ore
10.	Sistemul deductiv **SD-BAN**; *axiome* și *reguli de inferență*	Expunere, demonstrație, exemplificare	2 ore
11.	Protocoalele **N***eedham-***S***chröder*(**NS**) cu *shared-key* și cu *public-key*; sistemul deductiv extins **SD-BAN+**	Expunere, dezbatere, demonstrație, exemplificare	2 ore
12.	Vulnerabilitățile logicii **BAN** și posibilitatea unor *replay attacks*; logica **GNY** (**G***ong*, **N***eedham*, **Y***ahalom*)	Expunere, dezbatere, exemplificare	2 ore
13.	Sintaxa (**BNF**) **GNY**, sistemele **SD-GNY** și (pentru protocoale specifice) **SD-GNY+**	Expunere, dezbatere, exemplificare	2 ore
14.	Analiza bazată pe logică (**GNY**) a unor protocoale **RFID** (**R***adio***F***requency***ID***entification*); vulnerabilități și extensii **GNY**	Expunere, dezbatere, exemplificare	2 ore

Bibliografie
Referinţe principale:

- D. Monniaux – Analysis of Cryptographic Protocols Using Logics of Belief: An Overview, J. T. I.T., 2006.
- R. Stalnaker – On Logic of Knoledge and Belief, Springer Verlag, 2006.
- P.C. van Oorschot – Handbook of Applied Cryptography, Carleton University, 2002.
- M. Benerecetti, et al. – A Logic of Belief and a Model Checking Algoritm for Security Protocols, 2000.
- L. Gong, R. Needham, R. Yahalom – Reasoning about Belief in Cryptographic Protocols, Proc. of the IEEE 1990 Symposium on Security and Privacy, p.234-248.

Referinţe suplimentare:

- Site-uri INTERNET care vor fi precizate la primul curs, accesibile din pagina mea web.
- T. Kwon, S. Lim – Automation-Considered Logic of Authentication and Key Distibution, Spinger Verlag, 2003.
- D. Yiqiang – An Improvement of **GNY** Logic for the Reflection Attacks, Springer Verlag, 1999.
- R. Fagin, et al. – Reasoning about Knoledge, M. I. T. Press, 2003.

8.2	**Seminar**	**Metode de predare**	**Observaţii**

1.	Sisteme deductive în **LP** și **LP1**; deducția naturală; satisfiabilitate, teorii logice și teoreme de corectitudine și completitudine	Exemplificare, exerciții	2 ore
2.	Stări, drumuri, structuri Kripke modale și temporale	Exemplificare, exerciții	2 ore
3.	**K**-logica, **B**-logica, sitem multiagent formalizat (**MAS**); stări locale ale agenților, protocoale, drumuri, π-structuri	Exemplificare, exerciții	2 ore
4.	**KB**-logica	Exemplificare, exerciții	2 ore
5.	O variantă de formalizare simultană a logicilor (care *justifică* „cantitatea” de *încredere acordată unui agent*) și **MAS**	Exemplificare, exerciții	2 ore
6.	Aspecte calitative și cantitative ale verificării anonimității și autenticității pentru participanții la comunicare în sistemele multiagent	Exemplificare, exerciții	2 ore
7.	Studiul generic al unor protocoale didactice simple (**W***ide*-**M***outh*-**F***rog* sau *vot electronic*)	Exemplificare, exerciții	2 ore
8.	Studiul generic al unor proprietăți de securitate pentru agenți exprimate prin analiza unor protocoale tratate cu logica **BAN**	Exemplificare, exerciții	2 ore
9.	Semantica „prinsă” în sintaxa **BAN** și propoziții de *adnotare* a textului	Exemplificare, exerciții	2 ore
10.	Demonstratorul **Isabelle/HOL**; concepte de bază și utilizare	Exemplificare, exerciții	2 ore
11.	Analiza protocoalelor **NS** cu **Isabelle**	Exemplificare, exerciții	2 ore
12.	Exemple de vulnerabilități **BAN**; protocoale **NS** modificate; semantică „înglobată” (în sintaxă) și „embrion” de semantică formală (pentru propozițiile **GNY**)	Exemplificare, exerciții	2 ore
13.	Exemple de folosire a **MCMAS** în cazul sistemului deductiv **SD-GNY+**	Exemplificare, exerciții	2 ore
14.	Logica **SvO** (**S***yverson*,**v***an***O***orschot*), extensie pentru **BAN** și **GNY**	Exemplificare, exerciții	2 ore

Bibliografie suplimentară pentru seminar

- Lomuscio, H. Qu, F. Raimondi, MCMAS v1.0.0: User Manual, 2009.
- M. Wenzel, The Isabelle/Isar Reference Manual, 2013, url: http://isabelle.in.tum.de/documentation.html.

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

Masterul de Securitatea Informației este un master dedicat formării unor specialiști în domeniul corespunzător. Disciplina în sine se încadrează în contextul programei analitice a masterului. În privința legăturii cu comunitatea, asociațiile profesionale și angajatorii putem spune că facultatea a creat o legătură directă cu foruri reprezentative ale statului, cum ar fi SRI, STS și SIE. Am participat la organizarea de simpozioane, avem absolvenți angajați de curând (de exemplu la BITDEFENDER Iași) și avem personalități angajate în programe internaționale de profil.

10. Evaluare

Tip activitate	**10.1 Criterii de evaluare**	**10.2 Metode de evaluare**	**10.3 Pondere în nota finală (%)**
10.4 Curs	Atât testul scris cât și referatul vor fi evaluate cu note de la 1 la 10.	Test scris +prezentare referat cercetare	50% + 25%
10.5 Seminar	Se vor evalua activități specifice „pe parcurs”; fiecare activitate va fi apreciată cu note de la 1 la 10; se ia în calcul media lor aritmetică	Rezolvări sarcini concrete	25%
10.6 Standard minim de performanţă: media ponderată a celor 3 activități principale trebuie să fie ≥ 5. Aceasta este și condiția de promovare.			

Data completării Titular de curs Titular de seminar

Data avizăriiîn departament Director de departament