FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informaţiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informaţiilor și Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	14.2

2. Date despre disciplină

2.1 Denumirea disciplinei				Criptografie Aplicată	
2.2 Titularul de curs				Prof.dr.ing. Alin Suciu - asuciu@cs.utcluj.ro	
2.3 Titularul activităţilor de seminar / laborator / proiect				Prof.dr.ing. Alin Suciu - asuciu@cs.utcluj.ro	
2.4 Anul de studiu	2	2.5 Semestrul	2	2.6 Tipul de evaluare	E
2.7 Regimul disciplinei	Categoria formativă				DA
	Opționalitate				DOp

3. Timpul total estimate

3.1 Număr de ore pe săptămână	4	din care:	3.2 Curs	2	3.3 Seminar	2	3.3 Laborator		3.3 Proiect	
3.4 Număr de ore pe semestru	56	din care:	3.5 Curs	28	3.6 Seminar	28	3.6 Laborator		3.6 Proiect	

3.7 Distribuţia fondului de timp (ore pe semestru) pentru:	
(a) Studiul după manual, suport de curs, bibliografie şi notiţe	24
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren	10
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri	32
(d) Tutoriat	0
(e) Examinări	3
(f) Alte activităţi:	0
3.8 Total ore studiu individual (suma (3.7(a)...3.7(f)))	69
3.9 Total ore pe semestru (3.4+3.8)	125
3.10 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	NU SUNT
4.2 de competenţe	Programare in limbajul C

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50%
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la seminar obligatorie 90%

6. Competenţele specifice acumulate

Competențe profesionale	C2 - Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament • C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior • C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare • C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității C5 - Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • C5.2 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • C5.3 – Aplicarea unor modele matematice și informatice teoretice sau cu o arie mai generală de aplicabilitate pentru a analiza, evalua și rezolva probleme diverse de securitate/confidențialitate din lumea reală • C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate
Competențe transversale	N/A

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

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale criptografiei, precum și cu folosirea și înțelegerea celor mai reprezentative și pe larg folosite primitive criptografice, cu accent pe aplicarea acestora in sistemele actuale. Se urmărește dobândirea de către studenți a capacității de folosire a diverselor metode și tehnici criptografice și de apreciere a valorii și implicațiilor acestora din punctul de vedere al securității informației.
7.2 Obiectivele specifice	1. Înțelegerea primitivelor și metodelor criptografice existente, 2. Înțelegerea și evaluarea securității unor primitive criptografice, 3. Însușirea abilității de a folosi în mod corespunzător primitive criptografice în aplicațiile proprii, 4. Însușirea abilității de a analiza cerințele și necesitățile unor proiecte

	software din punct de vedere criptografic.

8. Conţinuturi

8.1 Curs	Nr. ore	Metode de predare	Observaţii
Elemente introductive și noțiuni fundamentale de criptografie	2	Expunere la tablă, prezentare cu video-proiectorul, discuții.	
Cifruri fundamentale: transpozitie, substitutie monoalfabetica	2		
Cifruri fundamentale: substitutie polialfabetica, cifrul Vigenere	2		
Cifruri fundamentale: substitutie poligramica, cifrul Playfair si cifrul Hill	2		
One Time Pad, Generatoare de numere aleatoare (TRNG, PRNG)	2		
Cifruri de tip Stream (flux de date)	2		
Cifruri de tip bloc, cifrul DES	2		
Cifruri de tip bloc, cifrul AES	2		
Cifruri de tip bloc, moduri de operare (ECB, CBC, OFB, CFB, etc.)	2		
Criptografia asimetrică (cu chei publice), principii, fundamente matematice	2		
Criptografia asimetrică (cu chei publice), cifrul RSA	2		
Semnaturi digitale, Funcții de hashing criptografice	2		
MAC – Coduri de autentificare a mesajelor	2		
Gestiunea cheilor, Certificate digitale	2		
Bibliografie 1. Understanding Cryptography: A Textbook for Students and Practitioners, (Paar, Pelzl -2010, Springer-Verlag New York Inc .) 2. Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels - 2010- Willey) 3. Cryptography and Network Security. Principles and Practice (Stallings, William – 2013 – Prentice Hall) 4. Cryptography: A Very Short Introduction (Piper, Fred – 2002 – Oxford University Press)			
8.2 Seminar / laborator / proiect	Nr. ore	Metode de predare	Observaţii
Elemente introductive și noțiuni fundamentale de criptografie	2	Expunere la tablă, prezentare cu video-proiectorul, discuții, exercitii.	
Cifruri fundamentale: transpozitie, substitutie monoalfabetica	2		
Cifruri fundamentale: substitutie polialfabetica, cifrul Vigenere	2		
Cifruri fundamentale: substitutie poligramica, cifrul Playfair si cifrul Hill	2		
One Time Pad, Generatoare de numere aleatoare (TRNG, PRNG)	2		
Cifruri de tip Stream (flux de date)	2		
Cifruri de tip bloc, cifrul DES	2		
Cifruri de tip bloc, cifrul AES	2		
Cifruri de tip bloc, moduri de operare (ECB, CBC, OFB, CFB, etc.)	2		
Criptografia asimetrică (cu chei publice), principii, fundamente matematice	2		
Criptografia asimetrică (cu chei publice), cifrul RSA	2		
Semnaturi digitale, Funcții de hashing criptografice	2		
MAC – Coduri de autentificare a mesajelor	2		
Gestiunea cheilor, Certificate digitale	2		
Bibliografie 1. Understanding Cryptography: A Textbook for Students and Practitioners, (Paar, Pelzl -2010, Springer-Verlag New York Inc .) 2. Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels - 2010- Willey) 3. Cryptography and Network Security. Principles and Practice (Stallings, William – 2013 – Prentice Hall) 4. Cryptography: A Very Short Introduction (Piper, Fred – 2002 – Oxford University Press)			

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

Cursuri de criptografie sunt prezente în cadrul majoritatii programelor de master din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- CSci 6331 Cryptography – The George Washington University – Washington DC, USA – Master of Science in Cybersecurity
- Cryptography (252-0407-00) – ETH Zurich – Elveția – Information Security Master
- Criptografie computațională – Academia Tehnica Militară – București – Master de Securitatea Tehnologiei Informației

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Prezență și activitate la cursuri	Examen scris (E)	50%
10.5 Seminar / Laborator / Proiect	Prezență și activitate la seminarii	Teme de seminar (S)	50%
10.6 Standard minim de performanţă: E ≥ 50% ; S ≥ 50%;			

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Prof.dr.ing. Alin Suciu - asuciu@cs.utcluj.ro	
	Aplicații	Prof.dr.ing. Alin Suciu - asuciu@cs.utcluj.ro	

Data avizării în Consiliul Departamentului Calculatoare

Director Departament,
Prof. dr. ing. Rodica Potolea

Data aprobării în Consiliul Facultății de Automatică și Calculatoare

Decan,
Prof. dr. ing. Vlad Muresan