FIȘA 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 si Tehnologia Informatiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiilor si 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 aplicata***	
2.2 Titularii de curs				Prof.dr.ing. Alin SUCIU (asuciu@cs.utcluj.ro)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Prof.dr.ing. Alin SUCIU (asuciu@cs.utcluj.ro)	
2.4 Anul de studiu	II	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DOp

3. Timpul total estimat

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

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	69
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Securitatea informațiilor
4.2 de competenţe	Programare C, Arhitectura sistemelor de operare, Cunoștințe de bază de rețele de calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la seminar obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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 de criptografie, cum ar fi SHA256, AES128/256, RSA2048. Se urmărește dobândirea de către studenți a capacității de folosire a diverselor metode și tehnici de criptografie și de apreciere a valorii și implicațiilor acestora din punctul de vedere al securității informației, a capacității de a face corelări cu domeniul criptografiei pentru a putea căuta informații și analize mai detaliate referitoare la activitățile de dezvoltare a aplicațiilor și de analiză a incidentelor de securitate.
7.2 Obiectivele specifice	1. Înțelegerea primitivelor și metodelor criptografice existente (elementele lor de bază, funcționarea lor, rolul lor, interacțiunea dintre ele), 2. Înțelegerea metricilor și a metodelor de comparare și evaluare a 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	Observații
Elemente introductive și noțiuni fundamentale de criptografie	2	Expunere la tablă, prezentare cu video-proiectorul, discuții. Platforme online	
Aplicațiile criptografiei în lumea reală. Generatoare de numere aleatoare	2		
Criptografia simetrică. Cifruri de tip stream. OTP, eSTREAM	2		
Criptografia simetrică. Cifruri de tip block	2		
DES, AES128/196/256, alte cifruri de tip bloc	2		
Criptografia asimetrică (cu chei publice)	2		
RSA, alte cifruri asimetrice	2		
Funcții hash criptografice. SHA-1, SHA-2, SHA-3	2		
Semnături digitale și infrastructurile PKI. Sisteme de criptare hibride	2		
Gestiunea cheilor criptografice	2		
Noțiuni introductive de criptografie cuantică și criptografie probabilistică, exemple	2		
Noțiuni introductive de steganografie, exemple	2		
Noțiuni introductive de criptanaliză, studii de caz	2		
Prezentarea unor atacuri de implementare (tip side-channel)	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

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)
5. Microsoft MSDN, Cryptography API: Next Generation (disponibil online)
6. Diferite articole

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Algoritmi criptografici clasici – aplicații, partea 1	2	Expunere la tablă, discuții si platforme online	
Algoritmi criptografici clasici – aplicații, partea 2	2		
Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 1	2		
Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 2	2		
Implementarea unor cifruri de tip stream în C	2		
Implementarea unor cifruri de tip bloc în C	2		
Implementarea unor funcții hash în C	2		
Folosirea bibliotecilor Windows CNG și OpenSSL	2		
Primitive de criptografie în hardware: TPM-ul	2		
Primitive de criptografie în hardware: instrucțiuni Intel AES	2		
Alte metode de criptografie hardware	2		
Prezentarea unor cazuri recente de atacuri criptografice 1. Discuții	2		
Prezentarea unor cazuri recente de atacuri criptografice 2. Discuții	2		
Topic-uri și metode noi de criptografie	2		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

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)
5. Microsoft MSDN, Cryptography API: Next Generation (disponibil online)

6. Diferite articole

** Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Cursuri de criptografie sunt prezente în cadrul multor alte masterate 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	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Examen scris si/sau oral sau Examen online scris si/sau oral folosind platforme online (E)	50%
Seminar	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar	Prezentarea/rezolvarea unei teme de seminar/cercetare din domeniul cursului și/sau rezolvarea și prezentarea soluției unor probleme similare cu cele discutate în timpul orelor de seminar (fizic sau folosind platforme online) (S)	50%
Laborator			
Proiect			
Standard minim de performanţă: E ≥ 50% ; S ≥ 50% Nota finala disciplina: N = 0.5*S + 0.5*E			

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Prof.dr.ing. Alin SUCIU	
	Aplicații	Prof.dr.ing. Alin SUCIU	

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. Liviu Miclea