

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclu de studii	Licență
1.6 Programul de studii / Calificarea	Calculatoare române / Inginer
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	54.2

2. Date despre disciplină

2.1 Denumirea disciplinei	Criptologie				
2.2 Titularii de curs	Prof. dr. ing. Suci Alin-Dumitru - Alin.Suciu@cs.utcluj.ro				
2.3 Titularul / Titularii activităților de seminar / laborator / proiect	Prof. dr. ing. Suci Alin-Dumitru - Alin.Suciu@cs.utcluj.ro				
2.4 Anul de studiu	IV	2.5 Semestrul	8	2.6 Tipul de evaluare (E – examen, C – colocviu, V – verificare)	E
2.7 Regimul disciplinei	DF – fundamentală, DD – în domeniu, DS – de specialitate, DC – complementară				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DOp

3. Timpul total estimat

3.1 Număr de ore pe săptămână	5	din care:	Curs	2	Seminar	1	Laborator	2	Proiect	-
3.2 Număr de ore pe semestru	70	din care:	Curs	28	Seminar	14	Laborator	28	Proiect	-
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										28
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										22
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										26
(d) Tutoriat										0
(e) Examinări										4
(f) Alte activități:										0
3.4 Total ore studiu individual (suma (3.3(a) ... 3.3(f)))					80					
3.5 Total ore pe semestru (3.2+3.4)					150					
3.6 Numărul de credite					6					

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Programarea Calculatoarelor, Sisteme de Operare, Programare Logica, Programare OO
4.2 de competențe	Competențele disciplinelor de mai sus

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Tabla, proiector, calculator, platforme online
5.2. de desfășurare a laboratorului	Calculatoare multicore, software specific, platforme online

6. Competențele specifice acumulate

6.1 Competențe profesionale	C3 - Soluționarea problemelor folosind instrumentele științei și ingineriei calculatoarelor C3.1 - Identificarea unor clase de probleme și metode de rezolvare caracteristice sistemelor informatice C3.2 - Utilizarea de cunoștințe interdisciplinare, a tiparelor de soluții și a uneltelor, efectuarea de experimente și interpretarea rezultatelor lor C3.3 - Aplicarea tiparelor de soluții cu ajutorul uneltelor și metodelor ingineresti C3.4 - Evaluarea comparativă, inclusiv experimentală, a alternativelor de rezolvare, pentru optimizarea performanțelor C3.5 - Dezvoltarea și implementarea de soluții informatice pentru probleme concrete C5 - Proiectarea, gestionarea ciclului de viață, integrarea și integritatea sistemelor hardware, software și de comunicații C5.1 - Precizarea criteriilor relevante privind ciclul de viață, calitatea, securitatea și interacțiunea sistemului de calcul cu mediul și cu operatorul uman C5.2 - Utilizarea unor cunoștințe interdisciplinare pentru adaptarea sistemului informatic în raport cu cerințele domeniului de aplicații C5.3 - Utilizarea unor principii și metode de bază pentru asigurarea securității, siguranței și usurinței în exploatare a sistemelor de calcul C5.4 - Utilizarea adecvată a standardelor de calitate, siguranță și securitate în prelucrarea informațiilor C5.5 - Realizarea unui proiect incluzând identificarea și analiza problemei, proiectarea, dezvoltarea și demonstrând o înțelegere a nevoii de calitate C6 - Proiectarea sistemelor inteligente C6.1 - Descrierea componentelor sistemelor inteligente C6.2 - Utilizarea de instrumente specifice domeniului pentru explicarea și înțelegerea funcționării sistemelor inteligente C6.3 - Aplicarea principiilor și metodelor de bază pentru specificarea de soluții la probleme tipice utilizând sisteme inteligente C6.4 - Alegerea criteriilor și metodelor de evaluare a calității, performanțelor și limitelor sistemelor inteligente C6.5 - Dezvoltarea și implementarea de proiecte profesionale pentru sisteme inteligente
6.2 Competențe transversale	N/A

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Să aibă capacitatea de a identifica necesitatea aplicării unor tehnici criptografice existentă într-o anumită problemă concretă și de ale implementa în mod corespunzător, ținând cont de atacurile criptanalitice posibile în acele cazuri.
7.2 Obiectivele specifice	- Să înțeleagă conceptele fundamentale de criptografie și criptanaliză - Să știe implementa algoritmi criptografici folosind diverse limbaje de programare (C, Java, C#, Prolog, etc.) - Să știe implementa algoritmi criptanalitici folosind diverse limbaje de programare (C, Java, C#, Prolog, etc.)

8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere, Noțiuni fundamentale de criptologie	2		
Algoritmi criptografici clasici; criptanaliza lor (1)	2		

Algoritmi criptografici clasici; criptanaliza lor (2)	2	Expunere la tablă, prezentare cu videoproiectorul, discuții interactive.	Nu sunt
Generatoare de numere pseudoaleatoare criptografic sigure (CSPRNG)	2		
Generatoare de numere real-aleatoare (TRNG); testare statistică	2		
One Time Pad – cifrul perfect	2		
Cifruri de tip flux de date ("stream ciphers")	2		
Cifruri de tip bloc, AES	2		
Cifruri de tip bloc – moduri de operare	2		
Criptografie cu chei publice, RSA	2		
Semnaturi digitale, studiu de caz RSA	2		
Funcții de hashing criptografice	2		
Gestiunea cheilor, certificate digitale	2		
Recapitulare, sinteză, pregatire pt examen	2		
Bibliografie (bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)			
1. C. Paar, J. Petzl, T. Güneysu, <i>Understanding Cryptography</i> , Springer, 2024.			
2. H. C.A. van Tilborg, <i>Fundamentals of Cryptology</i> , Kluwer Academic Publishers, 1999 (disponibilă online).			
8.2 Aplicații - seminar / laborator / proiect	Nr.ore	Metode de predare	Observații
Algoritmi criptografici clasici; criptanaliza lor (1)	2		
Algoritmi criptografici clasici; criptanaliza lor (2)	2		
Algoritmi criptografici clasici; criptanaliza lor (3)	2		
Generatoare de numere pseudoaleatoare criptografic sigure (CSPRNG)	2		
Generatoare de numere real-aleatoare (TRNG); testare statistică	2		
One Time Pad – cifrul perfect	2		
Cifruri de tip flux de date ("stream ciphers")	2		
Cifruri de tip bloc, AES	2		
Cifruri de tip bloc – moduri de operare	2		
Criptografie cu chei publice, RSA	2		
Semnaturi digitale, studiu de caz RSA	2		
Funcții de hashing criptografice	2		
Gestiunea cheilor, certificate digitale	2		
Colocviu de laborator	2		
Bibliografie (bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)			
1. C. Paar, J. Petzl, T. Güneysu, <i>Understanding Cryptography</i> , Springer, 2024.			
2. H. C.A. van Tilborg, <i>Fundamentals of Cryptology</i> , Kluwer Academic Publishers, 1999 (disponibilă online).			

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

Având în vedere explozia de aplicații care folosesc algoritmi criptografici pentru securizarea datelor, rezultă necesitatea de a cunoaște diverse metode, tehnici și tehnologii care țin de criptografie și criptanaliză, deci de criptologie. Conținutul cursului este aliniat la ultimele standarde internaționale din domeniu, și răspunde cerințelor profesionale și ale angajatorilor din domeniu.

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 și/sau oral (E)	70%

Seminar	Abilitatea de rezolvare a unor probleme specifice domeniului; discutare studii de caz	----- (S)	0%
Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de laborator	Verificare scrisă și/sau Teme de laborator transmise (L)	30%
Proiect	-	-	-
Standard minim de performanță: $E \geq 50\%$; $L \geq 50\%$ Nota finală disciplină: $N = 0.7 * E + 0.3 * L$			

Data completării: 26.02.2025	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. Vlad Mureșan