



Ministerul Educației și Cercetării
Universitatea Valahia din Târgoviște
Facultatea de Inginerie Electrică, Electronică și Tehnologia Informației
Departamentul de Electronică, Telecomunicații și Inginerie Energetică

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Valahia din Târgoviște
1.2 Facultatea/Departamentul	Facultatea de inginerie Electrică, Electronică și Tehnologia Informației
1.3 Departamentul	Electronică, Telecomunicații și Inginerie energetică
1.4 Domeniul de studii	Inginerie Electronică și Telecomunicații
1.5 Ciclu de studii	Master
1.6 Programul de studii/Calificarea	Sisteme Avansate de Telecomunicații, Prelucrarea și Transmisia Informației

2. Date despre disciplină

2.1 Denumirea disciplinei	Prelucrarea și codarea informației în rețelele de comunicații						
2.2 Titularul activităților de curs	Conf. univ. dr. ing. Dan Constantin PUCHIANU						
2.3 Titularul activităților de seminar/laborator	Conf. univ. dr. ing. Dan Constantin PUCHIANU						
2.4 Anul de studiu	II	2.5 Semestrul	I	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	B F

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	3	din care: 3.2 curs	2	3.3 seminar/laborator	1L
3.4 Total ore din planul de învățământ	42	din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp					Ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat					13
Examinări					10
Alte activități					-
3.7 Total ore studiu individual					83
3.8 Total ore pe semestru					125
3.9 Numărul de credite					5

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Teoria transmisiunii informației
4.2 de competențe	-

5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului	Videoproiector, tablă inteligentă, whiteboard, laptop, Moodle, Microsoft Teams.
-------------------------------	---

5.2 de desfășurare a seminarului/laboratorului	Laboratorul se va desfășura într-o sală dotată cu tablă inteligentă, calculatoare, videoproiector și mediul de dezvoltare Matlab/Octave, Python.
--	--

6. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

6.1 Obiectivul general al disciplinei	Disciplina asigură însușirea cunoștințelor de bază din domeniul criptologiei moderne: însușirea conceptelor de criptologie simetrică și asimetrică, însușirea conceptelor de securitate informatică și de evaluare a nivelului de securitate. Însușirea practică a noțiunilor predate la curs, prin implementarea de programe software în limbajul Python; rezolvarea unor probleme practice concrete care includ aspecte legate de securitatea datelor și verificarea /validarea nivelului de securitate al sistemului.
6.2 Obiectivele specifice	Crearea abilităților de a aplica cunoștințe generale de matematici fundamentale și de algoritmică în analiza rezistenței sistemelor criptografice moderne. Posibilitatea de a realiza aplicații software care implementează atacuri asupra sistemelor criptografice. Dezvoltarea calităților necesare evaluării nivelului de securitate (din perspectiva criptografică) oferit de un sistem sau de o componentă a acestuia.

7. Rezultatele învățării

7.1 Cunoștințe (<i>Rezultatul asimilării de informații prin învățare. Cunoștințele reprezintă ansamblul de fapte, principii, teorii și practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice și/sau faptice</i>)
La finalizarea disciplinei, studentul: - explică fundamentele teoretice care permit înțelegerea modului de funcționare a unui criptosistem - prezintă cele mai importante metode și criptosisteme de interes practic - dezvoltă abilități de a proiecta noi sisteme de cifrare eficiente - asimilează cunoștințe teoretice și practice privind componenta criptografică a securității sistemelor care asigură protecția datelor.
7.2 Aptitudini (<i>Capacitatea de a aplica cunoștințe și de a utiliza know-how pentru a duce la îndeplinire sarcini și a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) sau practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente)</i>)
Studentul este capabil să: - argumenteze soluțiile identificate/modurile de rezolvare. - stăpânească teoria și tehnicile de protecție a informației, metodele de proiectare, realizare și evaluare a unui algoritm criptografic - estimeze nivelulul de impact al unor vulnerabilități teoretice sau practice, ce pot apărea asupra unui sistem cu componente criptografice. - utilizeze metodele criptografice în alte domenii (codarea imaginilor, algoritmi complecși) sau cu alte scopuri (evaluarea entropiei și redundanței din surse naturale, generarea de numere pseudoaleatoare, etc).
7.3 Responsabilitate și autonomie (<i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale</i>)
Studentul: - are capacitatea de a estima realist nivelul de securitate oferit de un sistem care conține componente criptografice. - respectă principiile de etică academică, citând corect sursele bibliografice utilizate. - manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice - demonstrează receptivitate pentru contexte noi de învățare - conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile/sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială).

8. Conținuturi

8.1 Curs	Metode de predare	Observații
Noțiuni de bază ale criptografiei	Prelegerea, Prelegerea-dezbateri, Explicația,	4h
Cifruri clasice	Problematizarea,	4h
Algoritm de criptare DES	Brainstorming-ul, Reflecția	4h
Algoritm de criptare AES	personală, Studiul de caz	4h
Algoritm de criptare cu cheie publică		4h

Semnături digitale	Mijloace de învățământ Slide-uri PPT, Videoproiector/Tablă inteligentă, Laptop	4h
Criptanaliza Algoritmilor RC5 și RC6		4h

Bibliografie

1. Puchianui D.C., Prelucrarea și codarea informației în rețelele de comunicații - note de curs, Moodle <https://moodle.valahia.ro/course/view.php?id=107>
2. Cryptography for Intelligent Healthcare Systems, Agbotiname Lucky Imoize, Mohammad S Obaidat, Houbing Herbert Song, Hardback, 2026
3. Joan Vicenç Gómez i Urgellés, Criptografia. Arta pastrării secretelor, Ed. Litera, 2022
4. J. K. Nguyen, "Compositional leakage analysis for embedded cryptographic modules," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp.45–59, 2021
5. K. S. Wang and Y. J. Zhang, "Cache based key extraction in cloud virtual machines," IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 113–126, 2020
6. Aurel Andrei, Marilena Stanculescu, Criptografie vs. criptanaliză, Editura Printech, Bucuresti, 2014
7. Adrian Anatanasiu, Introducere în Criptografie - Funcții Criptografice, Fundamente Matematice și Computaționale, 2012
8. R. L. Rivest, "The RC4 stream cipher," RFC 6229, Internet Engineering Task Force, 2011
9. C. S. Liu, K. L. Lee, and A. P. Huang, "High speed timing attack on RSA with CRT," IEEE Transactions on Information Forensics & Security, vol. 5, no. 2, pp.215–225, 2010

8.2 Seminar/Laborator	Metode de predare	Observații
Laborator	Problematizarea, Reflecția personală, Exercițiul, Dezbaterea, Studiul de caz	
Cifruri clasice - Cifruri de substituție; Cifrul de transpoziții		2h
Algoritm de criptare DES		2h
Algoritm de criptare AES		2h
Algoritm de criptare cu cheie publică		4h
Semnături digitale		2h
Test de laborator		2h

Bibliografie

1. Prelucrarea și codarea informației în rețelele de comunicații - laborator, Moodle, <https://moodle.valahia.ro/course/view.php?id=107>
2. Cryptography for Intelligent Healthcare Systems, Agbotiname Lucky Imoize, Mohammad S Obaidat, Houbing Herbert Song, Hardback, 2026
3. Joan Vicenç Gómez i Urgellés, Criptografia. Arta pastrării secretelor, Ed. Litera, 2022
4. J. K. Nguyen, "Compositional leakage analysis for embedded cryptographic modules," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp.45–59, 2021
5. K. S. Wang and Y. J. Zhang, "Cache based key extraction in cloud virtual machines," IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 113–126, 2020
6. Aurel Andrei, Marilena Stanculescu, Criptografie vs. criptanaliză, Editura Printech, Bucuresti, 2014
7. Adrian Anatanasiu, Introducere în Criptografie - Funcții Criptografice, Fundamente Matematice și Computaționale, 2012
8. R. L. Rivest, "The RC4 stream cipher," RFC 6229, Internet Engineering Task Force, 2011
9. C. S. Liu, K. L. Lee, and A. P. Huang, "High speed timing attack on RSA with CRT," IEEE Transactions on Information Forensics & Security, vol. 5, no. 2, pp.215–225, 2010

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

Criptografia a fost și este un domeniu interdisciplinar, de mare interes și foarte actual, urmărind asigurarea confidențialității și a protecției informației. Indirect, dar în același timp foarte important pentru cercetarea științifică în lume, aceste preocupări creează un spațiu, o platformă extinsă de lucru, conectând domenii și tehnici de lucru foarte diverse și relevând aspecte noi în beneficiul științei în general. Înțelegerea principiilor de bază ale sistemelor criptografice moderne are un aport semnificativ în pregătirea viitorilor programatori din domeniul securității datelor, a specialiștilor din domeniul cyber-security, a administratorilor de sisteme informatice și a multor altor tipuri de specialiști în domenii conexe

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Examen scris	Test scris cu subiecte de sinteză; cursuri la vedere; timp de lucru 120 min.	60%

10.5 Seminar/laborator	Referate de laborator / Test	Evaluarea activității în clasă funcție de modul de lucru, implicarea studentului și rezultatele așteptate	40%
10.6 Standard minim de performanță			
Pentru promovarea disciplinei, studentul trebuie să îndeplinească cumulativ următoarele condiții: - obține minimum 50% din punctajul total cumulat și minimum 50% din punctajul aferent probei scrise. - demonstrează înțelegerea conceptelor de criptare și securitate a informației. - analizează corect un scenariu de citare și securitatea informației - utilizează corect instrumentele software de laborator (Python, Matlab) pentru implementarea și evaluarea unor aplicații specifice pentru prelucrarea și codarea informației în rețelele de comunicații. - demonstrează rigoare în realizarea activităților de laborator și în interpretarea rezultatelor experimentale sau simulate. Standardul minim de performanță validează atingerea rezultatelor învățării definite la pct. 7.			

Fișa disciplinei corespunde planului de învățământ care se aplică pentru anul I începând cu anul universitar 2025-2026.

Data completării
10.09.2026

Titularul de curs
Conf. univ. dr. ing. Dan Constantin
PUCHIANU

Titularul de laborator
Conf. univ. dr. ing. Dan Constantin
PUCHIANU

Data avizării în
departament
23.09.2026

Director de departament
Conf. univ. dr. ing. Dan Constantin PUCHIANU

Data avizării în
Consiliul Facultății
24.09.2026

Decan
Conf. univ. dr. ing. Nicoleta ANGELESCU