



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Națională de Știință și Tehnologie Politehnica București
1.2 Facultatea	Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Telecomunicații
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclu de studii	Licență
1.6 Specializarea	Tehnologii și Sisteme de Telecomunicații

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)	Securitatea rețelelor și serviciilor Network and Services Security						
2.2 Titularul activităților de curs	Conf. Dr. Octavian Catrina						
2.3 Titularul activităților de seminar / laborator	Conf. Dr. Octavian Catrina						
2.4 Anul de studiu	3	2.5 Semestrul	II	2.6 Tipul de evaluare	V	2.7 Regimul disciplinei	Op
2.8 Tipul disciplinei	S	2.9 Codul disciplinei	04.S.06.A.227	2.10 Tipul de notare	Nota		

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2.00	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	42.00	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					
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					5
Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					
Tutorat					0
Examinări					3
Alte activități (dacă există):					0
3.7 Total ore studiu individual	8.00				
3.8 Total ore pe semestru	50				
3.9 Numărul de credite	2				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Parcurgerea și/sau promovarea următoarelor discipline: Algebră, Matematici speciale, Structuri de date și algoritmi, Programare orientată pe obiecte.
4.2 de rezultate ale învățării	Cunoștințe de programare, în special algoritmi și programare orientată pe obiecte (pentru laborator).

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)

5.1 Curs	Sală de curs dotată cu videoproiector.
----------	--



5.2 Seminar/ Laborator/Proiect	Laborator dotat cu calculatoare și videoproiector. Software-ul folosit la laborator, JDK și Eclipse, este gratuit și poate fi executat atât pe Windows, cât și pe Linux.
-----------------------------------	--

6. Obiectiv general *(Se referă la intențiile profesorilor pentru studenți, la ceea ce studenții vor fi învățați în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului științific abordat, precum și la rolul pe care acesta îl are în cadrul specializării studiate. Vor fi descrise de o manieră generală tematicile abordate, justificarea includerii cursului în planul de învățământ al specializării studiate etc.)*

Această disciplină oferă studenților cunoștințe și abilități specifice domeniului securității informatice, necesare pentru identificarea, înțelegerea și rezolvarea unor probleme de securitate esențiale pentru proiectarea și operarea rețelelor și serviciilor de comunicații. Materialul prezentat se concentrează asupra algoritmilor criptografici și a protocoalelor criptografice necesare realizării unor canale de comunicație sigure, cu autentificarea participanților și garantarea autenticității și confidențialității datelor:

- Algoritmi criptografici pentru asigurarea confidențialității și autenticității datelor, cu cheie secretă și cu cheie publică (modele de securitate, atacuri, proprietăți, exemple).

- Protocoale de securitate care utilizează acești algoritmi criptografici pentru a realiza canale de comunicație sigure, prin autentificarea participanților, distribuirea cheilor criptografice și protejarea criptografică a datelor transmise (modele de securitate, atacuri, proprietăți, exemple).

Timpul limitat disponibil pentru prelegeri și laborator permite doar introducerea conceptelor de bază și prezentarea unor exemple reprezentative de algoritmi și protocoale. Materialul este însă selectat și prezentat astfel încât să ofere studenților cunoștințele necesare pentru a înțelege cerințele sau proprietățile de securitate și funcționarea sistemelor existente, pentru a utiliza în practică algoritmi studiați și pentru a examina și înțelege alți algoritmi de același tip. În acest scop, materialul prezentat se concentrează asupra formulării precise a cerințelor și proprietăților de securitate ale componentele fundamentale și tipurilor de algoritmi criptografici studiați, folosind modele matematice riguroase, consacrate, dar relativ simple, evitând astfel detalii specifice care nu pot fi prezentate în timpul disponibil (de exemplu, un cifru bloc se comportă ca o permutare pseudoaleatoare, iar operațiile interne nu sunt relevante pentru analiza securității algoritmilor de criptare sau autentificare bazați pe cifru bloc). Similar, sunt prezentate tipuri reprezentative de construcții pentru protocoale de securitate, care reprezintă nucleul criptografic al protocoalelor folosite în practică și sunt relativ ușor de analizat. Cunoscând aceste construcții, studenții pot să înțeleagă relativ ușor funcționarea și proprietățile de securitate ale protocoalelor folosite în practică.

7. Competențe *(Capacitatea dovedită de a utiliza cunoștințe, aptitudini și abilități personale, sociale și/sau metodologice în situații de muncă sau de studiu și pentru dezvoltarea profesională și personală. Reflectă cerințele angajatorilor.)*



Specifice	<p>Această disciplină completează categoriile de competențe listate mai jos, adăugând competențe specifice îndeplinirii cerințelor de securitate a comunicațiilor:</p> <ul style="list-style-type: none">- Aplicarea cunoștințelor, conceptelor și metodelor elementare privitoare la arhitectura sistemelor de calcul, microcontrolere, limbaje și tehnici de programare. Studenții studiază funcții de securitate, algoritmi criptografici și protocoale de securitate și aplică aceste cunoștințe în lucrările de laborator pentru a implementa funcțiile de securitate necesare unei aplicații generice de comunicație prin mesaje.- O viziune globală asupra serviciilor de date, voce, video, multimedia, bazată pe înțelegerea și utilizarea conceptelor fundamentale din domeniul comunicațiilor și transmisiunii informației. Studenții studiază noțiuni și tehnici fundamentale necesare sistemelor actuale de telecomunicații, care permit protecția criptografică a comunicațiilor (autentificarea participanților și garantarea autenticității și confidențialității datelor).- Selectarea, instalarea și exploatarea echipamentelor de telecomunicații fixe sau mobile și conceperea asigurării unui amplasament cu rețele uzuale de telecomunicații. Disciplina oferă studenților cunoștințe de bază și abilități specifice securității comunicațiilor, necesare pentru a identifica, înțelege și rezolva problemele de securitate care intervin în funcționarea, configurarea și operarea rețelelor și serviciilor de telecomunicații.
Transversale (generale)	<ul style="list-style-type: none">- Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale.- Capacitatea de a se adapta la noile tehnologii și de a se documenta (în limba română și limba engleză), pentru dezvoltarea profesională și personală, prin formare continuă.- Abilitatea de a gândi în termeni științifici, de a căuta și analiza date în mod independent, precum și de a desprinde și prezenta concluzii / identifica soluții.- Capacitate de analiză și sinteză: prezintă în mod sintetic cunoștințele dobândite, ca urmare a unui proces de analiză sistematică.

8. Rezultatele învățării (Sunt enunțuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învățării reflectă realizările studentului și mai puțin intențiile profesorului. Rezultatele învățării informează studenții despre ceea ce se așteaptă de la ei din punct de vedere al performanței, pentru a obține notele și creditele dorite. Sunt definite în termeni concreți, folosind verbe similare exemplurilor de mai jos și indică ceea ce se va urmări prin evaluare. Rezultatele învățării vor fi astfel redactate încât să fie evidențiată clar relația față de competențele definite la punctul 7.)

Cunoștințe	<p>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.</p> <ul style="list-style-type: none">- Cunoaște definițiile riguroase ale noțiunilor specifice domeniului: cerințe de securitate, funcții de securitate, tipuri de algoritmi criptografici, tipuri de protocoale de securitate.- Cunoaște exemple reprezentative de algoritmi criptografici utilizați pentru criptarea și autentificarea datelor, folosind criptografie simetrică și asimetrică.- Cunoaște proprietățile de securitate ale acestor algoritmi și modul în care sunt utilizați pentru a realiza funcțiile de securitate, astfel încât cerințele de securitate să fie îndeplinite în mod demonstrabil.- Cunoaște construcții reprezentative de protocoale de securitate pentru autentificarea participanților și stabilirea cheilor secrete necesare protejării criptografice a datelor.
-------------------	--



Aptitudini	<p><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></p> <ul style="list-style-type: none">- Identifică și formulează cerințele de securitate de bază ale unui sistem de telecomunicații privind autentificarea participanților și autenticitatea și confidențialitatea datelor.- Analizează, descrie și explică funcționarea și proprietățile de securitate ale componentelor unui sistem care asigură securitatea comunicațiilor, folosind terminologie specifică.- Elaborează soluții elementare de implementare sau soluții de configurare pentru funcțiile de securitate menționate mai sus, asigurând îndeplinirea cerințelor de securitate (proprietăților de securitate).
Responsabilitate și autonomie	<p><i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.</i></p> <ul style="list-style-type: none">- Selectează surse bibliografice potrivite și le analizează.- Respectă principiile de etică academică (de exemplu, citând corect sursele bibliografice utilizate).- Demonstrează receptivitate pentru contexte noi de învățare.- Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice- Demonstrează autonomie în organizarea situației de învățare sau în situația problemelor de rezolvat.- Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile și sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială).- Analizează și valorifică oportunități de afaceri/de dezvoltare antreprenorială în domeniul de specialitate.- Demonstrează abilități de management al situațiilor din viața reală.

9. Metode de predare (Se vor avea în vedere metode care să asigure predarea centrată pe student. Se va descrie modul în care se asigură participarea studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămăneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)

Procesul de predare utilizează atât metode de predare expozitive (prelegerea, expunerea), cât și conservative-interactive, bazate pe modele de învățare prin descoperire facilitate de explorarea directă și indirectă a realității (experimentul, demonstrația, modelarea), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme.

Activitatea de predare va utiliza prelegeri bazate pe prezentări PowerPoint ilustrate prin imagini și scheme (scenarii, algoritmi, protocoale și atacuri), astfel încât informațiile să fie ușor de înțeles și de asimilat (prezentările PowerPoint sunt completate uneori cu exemple construite interactiv pe tablă). Prezentările introductive ale cursurilor și lucrărilor de laborator scot în evidență legătura cu noțiunile prezentate anterior.

La laborator, studenții realizează o aplicație simplă de comunicație prin mesaje, pornind de la o aplicație inițială care nu oferă nici un serviciu de securitate și adăugând succesiv, la fiecare lucrare, funcții de securitate suplimentare, pe măsură ce acestea sunt prezentate la curs. Aplicația este implementată în limbajul Java, folosind biblioteca standard de clase criptografice oferită de Java Cryptography Architecture (JCA), care este documentată detaliat și este ușor de utilizat. Studenții folosesc un mediu integrat de programare evoluat, Eclipse, care facilitează substanțial realizarea și testarea programelor (<https://www.eclipse.org/>). Atât mediul integrat de programare Eclipse, cât și bibliotecile criptografice utilizate sunt disponibile gratuit și studenții le pot instala cu ușurință pe propriul calculator.

Procesul de predare ține seama de diferențele cruciale dintre securitatea informației și comunicațiilor și celelalte discipline din domeniul ingineriei electronice și telecomunicațiilor. Ne confruntăm cu adversari care doresc să compromită funcționarea sistemului și dispun de cunoștințele, competențele și resursele necesare pentru a înțelege și eventual depăși măsurile de protecție, nu doar cu fenomene fizice al căror comportament este predictibil pe baza unor modele matematice. Mai mult, îndeplinirea proprietăților de



securitate este dificil sau imposibil de testat (experimental) deci trebuie să ne bazăm pe analize de securitate teoretice riguroase. Exemplele de atacuri joacă un rol important în înțelegerea vulnerabilităților, a cerințelor și proprietăților de securitate ale algoritmilor criptografici și protocoalelor criptografice.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Introducere in securitatea comunicațiilor. Vulnerabilități, amenințări, funcții de securitate.	4
2	Confidențialitatea datelor (I): Definiții. Modele de securitate pentru confidențialitatea datelor (tipuri de atacuri, cerințe de securitate).	2
3	Confidențialitatea datelor (II): Introducere în criptarea cu cheie secretă. Cifru bloc (definiții, proprietăți de securitate, AES). Scheme de criptare cu cheie secretă bazate pe cifru bloc.	3
4	Confidențialitatea datelor (III): Introducere în criptarea cu cheie publică. Funcții cu sens unic și trapă secretă. Schema de criptare cu cheie publică RSA.	3
5	Autentificarea datelor (I): Definiții. Modele de securitate pentru autentificarea datelor (tipuri de atacuri, cerințe de securitate). Funcții hash criptografice (proprietăți de securitate și exemple de algoritmi).	3
6	Autentificarea datelor (II): Introducere în autentificarea datelor cu cheie secretă. Exemple de construcții bazate pe cifru bloc și pe funcții hash. Criptare autentificată. Exemple de aplicații în comunicații.	3
7	Autentificarea datelor (III): Introducere în autentificarea datelor cu cheie publică. Schema de semnătura digitală RSA.	2
8	Protocoale de securitate (I): Concepte de bază privind canalele de comunicație sigure (secure channels). Certificate pentru chei publice. Infrastructura pentru chei publice.	3
9	Protocoale de securitate (II): Protocoale de autentificare: construcții elementare și atacuri.	2
10	Protocoale de securitate (III): Protocoale de stabilire a cheilor secrete cu autentificare: construcții elementare și atacuri; exemple de protocoale folosite în practică.	3
	Total:	28

Bibliografie:

1. Catrina Octavian, Networks and Services Security, electronic course support (Moodle platform): <https://curs.upb.ro/2021/course/view.php?id=9688>
2. Catrina Octavian. Cryptographic Algorithms and Protocols. MATRIX ROM, Bucharest, 2016. ISBN 978-606-25-0249-2.
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996, 2001. Available online: <http://cacr.uwaterloo.ca/hac/>
4. The specifications of the cryptographic algorithms studied in the course are available online in the NIST publications (National Institute of Standards and Technology, USA): <https://www.nist.gov/>

LABORATOR

Nr. crt.	Conținutul	Nr. ore
----------	------------	---------



1	Comunicații protejate prin criptare cu cheie secretă (aplicația SeCom1): Studentii extind o aplicație care nu oferă servicii de securitate, numită SeCom0, astfel încât să protejeze confidențialitatea datelor transmise folosind criptare cu cheie secretă. Aplicația va folosi în acest scop chei secrete prestabilite.	2
2	Transportul cheilor secrete folosind criptarea RSA (aplicația SeCom2): Studentii modifică SeCom1 astfel încât fiecare sesiune de comunicație să folosească o cheie secretă diferită în locul unei chei prestabilite. La începutul comunicației, un participant generează o nouă cheie secretă și o transmite celuilalt, protejându-i confidențialitatea prin criptare cu cheie publică RSA. Cheia publică RSA este distribuită în prealabil.	2
3	Autentificarea mesajelor folosind criptografie cu cheie secretă (aplicația SeCom3): Studentii extind SeCom0 pentru a proteja autenticitatea datelor transmise folosind criptografie cu cheie secretă (cod de autentificare a mesajelor). Varianta SeCom3A va asigura doar autenticitatea datelor. Varianta SeCom3AE va proteja atât autenticitatea datelor, cât și confidențialitatea lor, prin criptare autenticată.	2
4	Autentificarea mesajelor folosind criptografie cu cheie publică (aplicația SeCom4): Studentii extind SeCom0 pentru a proteja autenticitatea datelor transmise folosind criptografie cu cheie publică (semnătură digitală). Pentru distribuirea cheilor publice se vor folosi certificate digitale. În acest scop, studentii vor mai realiza și o infrastructură minimală pentru chei publice (o autoritate de certificare care emite certificatele necesare utilizatorilor).	2
5	Protocoale de stabilire a cheilor și autentificare bazate pe criptografie cu cheie secretă (aplicația SeCom5): Studentii vor extinde SeCom3AE astfel încât să permită stabilirea cheilor de sesiune folosind un protocol bazat pe criptografie cu cheie secretă (chei secrete prestabilite, cod de autentificare).	2
6	Protocoale de stabilire a cheilor și autentificare bazate pe criptografie cu cheie publică (aplicația SeCom6): Studentii vor extinde SeCom3AE astfel încât să permită stabilirea cheilor de sesiune folosind un protocol bazat pe criptografie cu cheie publică (Diffie-Hellmann cu autentificare mutuală prin semnătură și certificate).	2
7	Colocviu final de laborator.	2
Total:		14

Bibliografie:

- Catrina Octavian, Securitatea Rețelelor și Serviciilor, Îndrumar de laborator în format electronic și proiecte Java inițiale (platforma Moodle): <https://curs.upb.ro/2021/course/view.php?id=9688>
- Documentația bibliotecilor software folosite, disponibilă online, gratuit: Java Cryptography Architecture Reference Guide, documentația claselor Java standard care implementează algoritmi folosiți.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	Cunoașterea conceptelor, metodelor, algoritmilor criptografici și protocoalelor de securitate studiate.	Lucrări de verificare scrise în timpul semestrului.	30%
	Aplicarea acestor cunoștințe pentru a înțelege și a rezolva probleme elementare de securitate a comunicațiilor întâlnite în practică.	Lucrări de verificare scrise în timpul semestrului.	30%



11.5 Seminar/laborator/proiect	Analiza, proiectarea, implementarea și testarea unor aplicații elementare de securitate a comunicațiilor, pe baza exemplurilor realizate pe parcursul lucrărilor de laborator.	Colocviu practic, oral. Analiza și implementarea aplicațiilor realizate la laborator.	40%
11.6 Condiții de promovare			
Studentii trebuie să obțină minimum 50/100 la lucrările scrise și minimum 50/100 la colocviul de laborator.			

12. Coroborarea conținutului disciplinei cu așteptările reprezentanților angajatorilor și asociațiilor profesionale reprezentative din domeniul aferent programului, precum și cu stadiul actual al cunoașterii în domeniul științific abordat și practicile în instituții de învățământ superior din Spațiul European al Învățământului Superior (SEİS)

Infrastructura globală de comunicații bazată pe Internet și rețele fără fir se află într-o evoluție continuă și trebuie să facă față unor probleme noi și complexe de securitate. Succesul unor noi categorii de aplicații, din domenii aflate în ascensiune rapidă, de exemplu Internet-ul obiectelor (Internet of Things) și sistemelor informatice imbarcate în autovehicule, depinde în mod crucial de îndeplinirea unor cerințe stricte și complexe de securitate. Tehnologiile și protocoalele de securitate prezentate de această disciplină au un rol esențial în soluționarea acestor probleme și au devenit componente universal prezente în sistemele informatice și de comunicații actuale.

Industria IT solicită ingineri cu calificare multidisciplinară, capabili să rezolve problemele de securitate ale sistemelor, rețelelor și aplicațiilor distribuite, cu cunoștințe solide de electronică, tehnologii de comunicație și securitatea informației. Cursul răspunde cerințelor actuale și de perspectivă ale economiei globale în domeniile Electronică și Telecomunicații. El oferă absolvenților cunoștințe teoretice și practice de bază privind securitatea informației și rețelelor, care le îmbunătățesc competitivitatea și le permit angajarea rapidă după absolvire, fiind perfect încadrat în politica UPB, atât din punct de vedere al conținutului și structurii, cât și din punctul de vedere al aptitudinilor și deschiderii internaționale oferite studenților.

Data completării

Titular de curs

Titular(i) de aplicații

10.10.2024

Conf. Dr. Octavian Catrina

Conf. Dr. Octavian Catrina

Data avizării în departament

Director de departament

22.10.2024

Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultății Decan



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



01.11.2024

Prof. Dr. Mihnea Udrea