



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Națională de Știință și Tehnologie Politehnică 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 Ciclul de studii	Masterat
1.6 Specializarea	Comunicații Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro)		Protocoloale de securitate pentru comunicații wireless					
(en)		Wireless Communications Security Protocols					
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	2	2.5 Semestrul	I	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei	DS	2.9 Codul disciplinei	UPB.04.M3.O.21-22	2.10 Tipul de notare	Nota		

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

3.1 Număr de ore pe săptămână	2.5	Din care: 3.2 curs	1.5	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	35.00	Din care: 3.5 curs	21	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					55
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					
Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					
Tutorat					0
Examinări					3
Alte activități (dacă există):					0
3.7 Total ore studiu individual	65.00				
3.8 Total ore pe semestru	100				
3.9 Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Algoritmi criptografici, Rețele de calculatoare, Programarea calculatoarelor.
4.2 de rezultate ale învățării	Noțiunile de bază asociate disciplinelor listate mai sus.

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

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



5.2 Seminar/ Laborator/Proiect	Laborator dotat cu calculatoare și videoproiector. Software-ul utilizate în lucrările de laborator este gratuit (emulator de rețele GNS, Java JDK, Eclipse IDE).
-----------------------------------	--

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.*)

Obiectivul general al acestei discipline este familiarizarea studenților cu concepte, tehnologii, arhitecturi și protocoale utilizate în practică pentru a asigura securitatea comunicațiilor de date și a rețelelor de telecomunicații. Motivația studierii securității comunicațiilor derivă din faptul că utilizarea pe scară largă a tehnologiei informației, în toate domeniile de activitate, nu a adus doar avantaje importante, ci și riscuri de securitate fără precedent. Securitatea comunicațiilor de date are o importanță deosebită, deoarece acestea au rol esențial în funcționarea sistemelor informatice distribuite și, în același timp, oferă principalele căi de atac asupra acestor sisteme.

Cursul prezintă concepte și tehnologii fundamentale de securitate, precum și arhitecturi și protocoale de securitate standardizate, folosite în rețelele de telecomunicații, rețelele de întreprindere și în Internet:

- Funcții de securitate: autentificarea datelor, autentificarea participanților, confidențialitatea datelor, controlul accesului. Soluții criptografice utilizate pentru a implementa aceste funcții, împreună cu modelele lor de securitate, proprietățile standard de securitate și exemple de atacuri.
- Protocoale pentru canale de comunicație care asigură autentificarea și confidențialitatea datelor.
- Protocoale de autentificare și de distribuție a cheilor: principii de proiectare, atacuri și analiza securității.
- Protocoale de securitate pentru nivelul Rețea: IPsec, IKE; rețele private virtuale securizate folosind IPsec.
- Protocoale de securitate pentru nivelul Transport: TLS, SSH; rețele private virtuale securizate folosind TLS.

Cursul oferă cunoștințe teoretice și practice care să permită înțelegerea aspectelor fundamentale ale protocoalelor de securitate, pentru a le putea proiecta, implementa, configura și întreține. Prezentarea conceptelor teoretice este însoțită de o suită de lucrări de laborator: într-o primă lucrare, studenții se familiarizează cu exemple reprezentative de protocoale de securitate standardizate (IPsec, IKE), iar în următoarele lucrări implementează și testează o serie de protocoale de securitate, folosind construcții tipice și algoritmi criptografici standardizați.

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	<ul style="list-style-type: none">- Definirea riguroasă a cerințelor și funcțiilor de securitate a comunicațiilor, a tipurilor de algoritmi criptografici utilizați pentru implementarea lor și a proprietăților standard de securitate pe care trebuie să le îndeplinească (și pe care se bazează proiectarea și analiza securității protocoalelor).- Descrierea, analiza și explicarea soluțiilor tipice de construcție a protocoalelor de securitate (în special a proprietăților lor de securitate), a avantajelor și dezavantajelor diferitelor categorii de soluții în contextul unor aplicații practice cu cerințe diferite (de exemplu, protocoale bazate pe criptografie cu cheie secretă, protocoale bazate pe criptografie cu cheie publică și soluții mixte).- Elaborarea unor soluții de securitate a comunicațiilor care îndeplinesc cerințele de securitate, scalabilitate și performanțe ale aplicațiilor, folosind componente standard.
------------------	--



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 sau de a identifica soluții.- Capacitatea de analiză și sinteză: prezentarea în mod sintetic a cunoștințele dobândite, ca urmare a unui proces de analiză sistematică.- Abilitatea de a coopera cu specialiști din domeniu și de a lucra în echipă, comunicând eficient și coordonându-și eforturile cu ceilalți pentru soluționarea problemelor.- Respectare principiilor de etică academică, în particular, citarea corectă a surselor bibliografice utilizate în activitatea de documentare.
------------------------------------	---

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><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></p> <ul style="list-style-type: none">- Cunoaște noțiunile specifice domeniului și subiectelor tratate în curs: funcții de securitate, algoritmi criptografici și proprietățile lor de securitate, construcții tipice de protocoale, soluții standardizate pentru protocoale și componentele lor.- Cunoaște modul în care noțiunile de securitate, algoritmi criptografici și protocoalele de securitate sunt utilizate pentru în practică, pentru a înțelege și specifica riguros cerințele sau proprietățile de securitate și performanțe ale aplicațiilor și pentru a elabora soluții care îndeplinesc aceste cerințe.
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 riscurile și cerințele (de bază) de securitate a comunicațiilor.- Analizează, descrie și explică rolul și funcționarea componentelor unei soluții de asigurare a securității comunicației (funcții, algoritmi, protocoale), folosind terminologie specifică.- Identifică, implementează și testează soluții de securitate a comunicațiilor bazate pe componente standard (algoritmi și protocoale), care să îndeplinească cerințele aplicațiilor.



Responsabilitate și autonomie	<i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.</i>
	- 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 expositive (prelegerea, expunerea), cât și conversative-interactive, bazate pe modele de învățare prin descoperire facilitate de explorarea directă și indirectă a realității (experimente conceptuale sau practice), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme.

Activitatea de predare utilizează prelegeri bazate pe prezentări PowerPoint ilustrate prin imagini și scheme (arhitecturi, mesaje, diagrame pentru algoritmi și interacțiuni), astfel încât informațiile să fie mai ușor de înțeles și de asimilat. Prezentările PowerPoint sunt completate 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 explorează, implementează și testează construcții tipice de protocoale de securitate pentru canale securizate de comunicații. Exercițiile de implementare sunt esențiale pentru a înțelege corect operațiile efectuate și mesajele transmise de aceste protocoale, iar experimentele permit urmărirea pas cu pas a evoluției stării protocoalelor și a informației accesibile adversarului. 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 comunicațiilor și celelalte discipline din domeniul ingineriei electronice și telecomunicațiilor. În acest domeniu, 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 și a soluțiilor utilizate de protocoalele de securitate.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Introducere. Amenințări și atacuri asupra securității comunicațiilor. Funcții de securitate și soluții criptografice pentru realizarea lor. Exemplu: securitatea rețelelor WiFi.	3



2	Componente ale protocoalelor de securitate (I): Confidențialitatea datelor folosind algoritmi cu cheie secretă (ENCS). Proprietăți de securitate. Cifru bloc. Construcții tipice de scheme ENCS folosind cifru bloc.	3
3	Componente ale protocoalelor de securitate (II): Autentificarea datelor folosind algoritmi cu cheie secretă (MAC). Proprietăți de securitate. Funcții hash criptografice. Construcții tipice de scheme MAC folosind funcții hash sau cifru bloc.	3
4	Protocoale pentru comunicație pe canale sigure ("secure channel"). Criptarea autentificată a datelor. Proprietăți de securitate. Construcții tipice. Exemple de protocoale pentru canale sigure utilizate în practică (IPsec, TLS Record, WiFi).	3
5	Componente ale protocoalelor de securitate (III): Confidențialitatea și autentificarea datelor folosind algoritmi cu cheie publică (ENCP, SIG). Proprietăți de securitate. Construcții tipice de scheme ENCP și SIG folosind funcții cu sens unic bazate pe problema RSA și pe problema logaritmului discret.	4
6	Componente ale protocoalelor de securitate (IV): Generarea și distribuția cheilor. Generarea șirurilor pseudoaleatoare și derivarea cheilor secrete folosind algoritmi MAC. Distribuția cheilor publice. Certificate și infrastructura pentru chei publice.	3
7	Protocoale de autentificare și stabilire a cheilor secrete. Construcții tipice de protocoale pentru autentificarea participanților și pentru stabilirea cheilor secrete folosind criptografie cu cheie secretă și criptografie cu cheie publică. Proprietăți de securitate. Atacuri.	6
8	Protocoale pentru crearea canalelor de comunicație sigure. Exemple tipice de protocoale de autentificare și stabilire a cheilor secrete utilizate în practică (IKEv2, TLS Handshake).	3
Total:		28

Bibliografie:

1. Catrina Octavian, Protocoale de Securitate pentru Comunicații Wireless, suport de curs electronic (platforma Moodle): <https://curs.upb.ro/2021/course/view.php?id=9563>
2. Catrina Octavian. Cryptographic Algorithms and Protocols. Editura MATRIX ROM, București, 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. Disponibilă în format electronic (gratuit): <http://cacr.uwaterloo.ca/hac/>
4. Specificațiile algoritmilor și protocoalelor din curs sunt disponibile online (gratuit) în publicațiile NIST (National Institute of Standards and Technology, <https://www.nist.gov/>) și IETF (<https://www.ietf.org>).

LABORATOR

Nr. crt.	Conținutul	Nr. ore
1	Securitate comunicațiilor în practică: Rețele private virtuale care asigură autenticitatea și confidențialitatea datelor ("secure VPN") realizate folosind IPsec, GRE și IKEv2. Implementare, experimente și analiză folosind un emulator de rețele, analizor de protocoale și rutere Cisco.	4
2	Implementarea protocoalelor care asigură autenticitatea și confidențialitatea datelor prin criptare autentificată. Aplicație implementată în Java folosind biblioteca standard de clase criptografice (SecPro1). Experimente și analiză.	2



3	Implementarea protocoalelor de autentificare și stabilire a cheilor secrete (I): Construcții bazate pe criptografie cu cheie secretă. Aplicație realizată în Java folosind biblioteca standard de clase criptografice (SecPro2). Experimente și analiză.	4
4	Implementarea protocoalelor de autentificare și stabilire a cheilor secrete (II): Construcții bazate pe criptografie cu cheie publică și infrastructură pentru chei publice. Aplicație realizată în Java folosind biblioteca standard de clase criptografice (SecPro3). Experimente și analiză.	4
Total:		14

Bibliografie:

1. Catrina Octavian, Protocoale de Securitate pentru Comunicații Wireless, Îndrumar de laborator în format electronic și proiecte Java inițiale (platforma Moodle): <https://curs.upb.ro/2021/course/view.php?id=9563>
2. 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, tehnicilor, algoritmilor și protocoalelor de securitate studiate la curs. - Abilitatea de a descrie, analiza și explica funcționarea și proprietățile de securitate ale protocoalelor și componentelor lor în diverse situații întâlnite în practică (scenarii de comunicație, atacuri).	Examen scris	50%
11.5 Seminar/laborator/proiect	Analiza, proiectarea, implementarea și testarea unor aplicații elementare care asigură securitatea comunicațiilor, pe baza exemplelor realizate pe parcursul lucrărilor de laborator.	Colocviu final de laborator	50%
11.6 Condiții de promovare			
Studentii trebuie să obțină minimum 50/100 la examen 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 (SEIS)

Societatea modernă se bazează pe o vastă rețea de sisteme informatice utilizate în economie, finanțe și administrație, în infrastructuri și servicii esențiale, precum și în viața de zi cu zi a cetățenilor. Această informatizare masivă a adus atât avantaje importante, cât și riscuri de securitate fără precedent.

Tehnologiile de securitate au devenit, prin urmare, componente esențiale ale acestei rețele de sisteme informatice. Aceste tehnologii oferă o gamă largă de funcții și servicii de securitate: permit accesul la resurse și servicii doar utilizatorilor legitimi, protejează integritatea, autenticitatea și confidențialitatea datelor, asigură disponibilitatea sistemelor, rețelelor și serviciilor. În particular, securitatea comunicațiilor de date are o importanță deosebită, deoarece acestea au rol esențial în sistemele informatice distribuite și, în același timp, oferă principalele căi de atac asupra acestor sisteme. Industria IT solicită ingineri cu o 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.






Universitatea Națională de Știință și Tehnologie Politehnica București

**Facultatea de Electronică, Telecomunicații și
Tehnologia Informației**



Prin urmare, cursul răspunde cerințelor actuale și de perspectivă ale economiei globale în domeniile Electronică și Telecomunicații. El oferă absolvenților cunoștințe teoretice și practice esențiale privind securitatea informației, care le îmbunătățesc competitivitatea și le permit angajarea rapidă după absolvire, fiind perfect încadrat în politica Universității Politehnica din București, atât din punctul 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	
27.10.2024	Conf. Dr. Serban Georgica Obreja 	
Data aprobării în Consiliul Facultății	Decan	
25.10.2024	Prof. Dr. Mihnea Udrea 