Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti

Facultatea de Electronică, Telecomunicaţii şi

Tehnologia Informaţiei

FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**
1.2 Facultatea	**Electronică, Telecomunicaţii şi Tehnologia Informaţiei**
1.3 Departamentul	**Telecomunicaţii**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Licenţă
1.6 Specializarea	Tehnologii şi Sisteme de Telecomunicaţii

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Securitatea reţelelor şi serviciilor Network and Services Security			
2.2 Titularul activităţilor de curs				Conf. Dr. Octavian Catrina			
2.3 Titularul activităţilor 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 activităţilor 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 învăţământ	42.00	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii şi eseuri					5
Tutorat					0
Examinări					3
Alte activităţi (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. Precondiţii (acolo unde este cazul)

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

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor 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 algoritmii 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	Această disciplină completează categoriile de competenţe listate mai jos, adăugând competenţe specifice îndeplinirii cerinţelor de securitate a comunicaţiilor: - Aplicarea cunoştinţelor, conceptelor şi metodelor elementare privitoare la arhitectura sistemelor de calcul, microcontrolere, limbaje şi tehnici de programare. Studenţii studiază funcţii de securitate, algoritmi criptografici şi protocoale de securitate şi aplică aceste cunoştinţe în lucrările de laborator pentru a implementa funcţiile de securitate necesare unei aplicaţii generice de comunicaţie prin mesaje. - O viziune globală asupra serviciilor de date, voce, video, multimedia, bazată pe înţelegerea şi utilizarea conceptelor fundamentale din domeniul comunicaţiilor şi transmisiunii informaţiei. Studenţii studiază noţiuni şi tehnici fundamentale necesare sistemelor actuale de telecomunicaţii, care permit protecţia criptografică a comunicaţiilor (autentificarea participanţilor şi garantarea autenticităţii şi confidenţialităţii datelor). - Selectarea, instalarea şi exploatarea echipamentelor de telecomunicaţii fixe sau mobile şi conceperea asigurării unui amplasament cu reţele uzuale de telecomunicaţii. Disciplina oferă studenţilor cunoştinţe de bază şi abilităţi specifice securităţii comunicaţiilor, necesare pentru a identifica, înţelege şi rezolva problemele de securitate care intervin în funcţionarea, configurarea şi operarea reţelelor şi serviciilor de telecomunicaţii.
Transversale (generale)	- Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluţii consacrate, asigurând astfel îndeplinirea sarcinilor profesionale. - Capacitatea de a se adapta la noile tehnologii şi de a se documenta (în limba română şi limba engleză), pentru dezvoltarea profesională şi personală, prin formare continuă. - Abilitatea de a gândi în termeni ştiinţifici, de a căuta şi analiza date în mod independent, precum şi de a desprinde şi prezenta concluzii / identifica soluţii. - Capacitate de analiză şi sinteză: prezintă în mod sintetic cunoştinţele dobândite, ca urmare a unui proces de analiză sistematică.

8. Rezultatele învăţării *(Sunt enunţuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învăţării reflectă realizările studentului şi mai puţin intenţiile profesorului. Rezultatele învăţării informează studenţii despre ceea ce se aşteaptă de la ei din punct de vedere al performanţei, pentru a obţine notele şi creditele dorite. Sunt definite în termeni concreţi, folosind verbe similare exemplelor de mai jos şi indică ceea ce se va urmări prin evaluare. Rezultatele învăţării vor fi astfel redactate încât să fie evidenţiată clar relaţia faţă de competenţele definite la punctul 7.)*

Cunoştinţe	*Rezultatul asimilării de informaţii prin învăţare. Cunoştinţele reprezintă ansamblul de fapte, principii, teorii şi practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice şi/sau faptice.* - Cunoaşte definiţiile riguroase ale noţiunilor specifice domeniului: cerinţe de securitate, funcţii de securitate, tipuri de algoritmi criptografici, tipuri de protocoale de securitate. - Cunoaşte exemple reprezentative de algoritmi criptografici utilizaţi pentru criptarea şi autentificarea datelor, folosind criptografie simetrică şi asimetrică. - Cunoaşte proprietăţile de securitate ale acestor algoritmi şi modul în care sunt utilizaţi pentru a realiza funcţiile de securitate, astfel încât cerinţele de securitate să fie îndeplinite în mod demonstrabil. - Cunoaşte construcţii reprezentative de protocoale de securitate pentru autentificarea participanţilor şi stabilirea cheilor secrete necesare protejării criptografice a datelor.

Aptitudini	*Capacitatea de a aplica cunoştinţe şi de a utiliza know-how pentru a duce la îndeplinire sarcini şi a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive şi creative) sau practice (implicând dexteritate manuală şi utilizarea de metode, materiale, unelte şi instrumente).* - Identifică şi formulează cerinţele de securitate de bază ale unui sistem de telecomunicaţii privind autentificarea participanţilor şi autenticitatea şi confidenţialitatea datelor. - Analizează, descrie şi explică funcţionarea şi proprietăţile de securitate ale componentelor unui sistem care asigură securitatea comunicaţiilor, folosind terminologie specifică. - Elaborează soluţii elementare de implementare sau soluţii de configurare pentru funcţiile de securitate menţionate mai sus, asigurând îndeplinirea cerinţelor de securitate (proprietăţilor de securitate).
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* - Selectează surse bibliografice potrivite şi le analizează. - Respectă principiile de etică academică (de exemplu, citând corect sursele bibliografice utilizate). - Demonstrează receptivitate pentru contexte noi de învăţare. - Manifestă colaborare cu ceilalţi colegi şi cadre didactice în desfăşurarea activităţilor didactice - Demonstrează autonomie în organizarea şituaţiei de învăţare sau în situaţia problemelor de rezolvat. - Conştientizează valoarea contribuţiei sale în domeniul ingineriei la identificarea de soluţii viabile şi sustenabile care să rezolve probleme din viaţa socială şi economică (responsabilitate socială). - Analizează şi valorifică oportunităţi de afaceri/de dezvoltare antreprenorială în domeniul de specialitate. - Demonstrează abilităţi de management al situaţiilor din viaţa 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 studenţilor la stabilirea propriului parcurs de învăţare, cum se identifică eventualele rămâneri în urmă şi ce măsuri remediale se adoptă în astfel de cazuri.)*

Procesul de predare utilizeaază atât metode de predare expozitive (prelegerea, expunerea), cât şi conversative-interactive, bazate pe modele de învăţare prin descoperire facilitate de explorarea directa şi indirectă a realităţii (experimentul, demonstraţia, modelarea), dar şi pe metode bazate pe acţiune, precum exerciţiul, activităţile practice şi rezolvarea de probleme.
Activitatea de predare va utiliza prelegeri bazate pe prezentări PowerPoint ilustrate prin imagini şi scheme (scenarii, algoritmi, protocoale şi atacuri), astfel încât informaţiile să fie uşor de înţeles şi de asimilat (prezentările PowerPoint sunt completate uneori cu exemple construite interactiv pe tablă). Prezentările introductive ale cursurilor şi lucrărilor de laborator scot în evidenţă legătura cu noţiunile prezentate anterior.
La laborator, studenţii realizează o aplicaţie simplă de comunicaţie prin mesaje, pornind de la o aplicaţie iniţială care nu oferă nici un serviciu de securitate şi adăugând succesiv, la fiecare lucrare, funcţii de securitate suplimentare, pe măsură ce acestea sunt prezentate la curs. Aplicaţia este implementată în limbajul Java, folosind biblioteca standard de clase criptografice oferită de Java Cryptography Architecture (JCA), care este documentată detaliat şi este uşor de utilizat. Studenţii folosesc un mediu integrat de programare evoluat, Eclipse, care facilitează substanţial realizarea şi testarea programelor (https://www.eclipse.org/). Atât mediul integrat de programare Eclipse, cât şi bibliotecile criptografice utilizate sunt disponibile gratuit şi studenţii le pot instala cu uşurinţă pe propriul calculator.
Procesul de predare ţine seama de diferenţele cruciale dintre securitatea informaţiei şi comunicaţiilor şi celelalte discipline din domeniul ingineriei electronice şi telecomunicaţiilor. Ne confruntăm cu adversari care doresc să compromită funcţionarea sistemului şi dispun de cunoştinţele, competenţele şi resursele necesare pentru a înţelege şi eventual depăşi măsurile de protecţie, nu doar cu fenomene fizice al căror comportament este predictibil pe baza unor modele matematice. Mai mult, îndeplinirea proprietăţilor 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 chiei 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	Comunicaţii protejate prin criptare cu cheie secretă (aplicaţia SeCom1): Studenţii extind o aplicaţie care nu oferă servicii de securitate, numită SeCom0, astfel încât să protejeze confidenţialitatea datelor transmise folosind criptare cu cheie secretă. Aplicaţia va folosi în acest scop chei secrete prestabilite.	2
2	Transportul cheilor secrete folosind criptarea RSA (aplicaţia SeCom2): Studenţii modifică SeCom1 astfel încât fiecare sesiune de comunicaţie să folosească o cheie secretă diferită în locul unei chei prestabilite. La începutul comunicaţiei, un participant generează o nouă cheie secretă şi o transmite celuilalt, protejându-i confidenţialitatea prin criptare cu cheie publică RSA. Cheia publică RSA este distribuită în prealabil.	2
3	Autentificarea mesajelor folosind criptografie cu cheie secretă (aplicaţia SeCom3): Studenţii 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 şi confidenţialitatea lor, prin criptare autentificată.	2
4	Autentificarea mesajelor folosind criptografie cu cheie publică (aplicaţia SeCom4): Studenţii 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, studenţii vor mai realiza şi o infrastructură minimală pentru chei publice (o autoritate de certificare care emite certificatele necesare utilizatorilor).	2
5	Protocoale de stabilire a cheilor şi autentificare bazate pe criptografie cu cheie secretă (aplicaţia SeCom5): Studenţii 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 şi autentificare bazate pe criptografie cu cheie publică (aplicaţia SeCom6): Studenţii 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 şi certificate).	2
7	Colocviu final de laborator.	2
	Total:	14

Bibliografie:

1. Catrina Octavian, Securitatea Reţelelor şi Serviciilor, Îndrumar de laborator în format electronic şi proiecte Java iniţiale (platforma Moodle): https://curs.upb.ro/2021/course/view.php?id=9688
2. Documentaţia bibliotecilor software folosite, disponibilă online, gratuit: Java Cryptography Architecture Reference Guide, documentaţia claselor Java standard care implementează algoritmii folosiţi.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	Cunoaşterea conceptelor, metodelor, algoritmilor criptografici şi protocoalelor de securitate studiate.	Lucrări de verificare scrise în timpul semestrului.	30%
	Aplicarea acestor cunoştinţe pentru a înţelege şi a rezolva probleme elementare de securitate a comunicaţiilor întâlnite în practică.	Lucrări de verificare scrise în timpul semestrului.	40%

11.5 Seminar/laborator/proiect	Analiza, proiectarea, implementarea și testarea unor aplicații elementare de securitate a comunicațiilor, pe baza exemplelor realizate pe parcursul lucrărilor de laborator.	Colocviu practic, oral. Analiza și implementarea aplicațiilor realizate la laborator.	30%
11.6 Condiții de promovare			
Studenții trebuie să obțină minimum 50/100 din punctajul total și minimum 50/100 la colocviul de laborator și lucrările de verificare.			

12. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor angajatorilor şi asociaţiilor profesionale reprezentative din domeniul aferent programului, precum şi cu stadiul actual al cunoaşterii în domeniul ştiinţific abordat şi practicile în instituţii de învăţământ superior din Spaţiul European al Învăţământului Superior (SEÎS)

Infrastructura globală de comunicaţii bazată pe Internet şi reţele fără fir se află într-o evoluţie continuă şi trebuie să facă faţă unor probleme noi şi complexe de securitate. Succesul unor noi categorii de aplicaţii, din domenii aflate în ascensiune rapidă, de exemplu Internet-ul obiectelor (Internet of Things) şi sistemelor informatice îmbarcate în autovehicule, depinde în mod crucial de îndeplinirea unor cerinţe stricte şi complexe de securitate. Tehnologiile şi protocoalele de securitate prezentate de această disciplină au un rol esenţial în soluţionarea acestor probleme şi au devenit componente universal prezente în sistemele informatice şi de comunicaţii actuale.
Industria IT solicită ingineri cu calificare multidisciplinară, capabili să rezolve problemele de securitate ale sistemelor, reţelelor şi aplicaţiilor distribuite, cu cunoştinţe solide de electronică, tehnologii de comunicaţie şi securitatea informaţiei. Cursul răspunde cerinţelor actuale şi de perspectiva ale economiei globale în domeniile Electronică şi Telecomunicaţii. El oferă absolvenţilor cunoştinţe teoretice şi practice de bază privind securitatea informaţiei şi reţelelor, care le îmbunătăţesc competitivitatea şi le permit angajarea rapidă după absolvire, fiind perfect încadrat în politica UPB, atât din punct de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor.

Data completării	Titular de curs	Titular(i) de aplicaţii
10.10.2024	Conf. Dr. Octavian Catrina	Conf. Dr. Octavian Catrina
Data avizării în departament	Director de departament	
	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

Prof. Dr. Mihnea Udrea