

FIȘA DISCIPLINEI

Criptografie cuantică

Anul universitar 2026-2027

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai
1.2. Facultatea	Facultatea de Matematică și Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii / Calificarea	Cyber Security
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptografie cuantică	Codul disciplinei	MME8207
2.2. Titularul activităților de curs	Lector Univ. dr. Mihoc Tudor Dan		
2.3. Titularul activităților de seminar	Lector Univ. dr. Mihoc Tudor Dan		
2.4. Anul de studiu	1	2.5. Semestrul	2
		2.6. Tipul de evaluare	Examen
2.7. Regimul disciplinei	Opțional		Disciplină de specializare (DS)

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

3.1. Număr de ore pe săptămână	4	din care: 3.2. curs	2	3.3. seminar/ laborator/ proiect	1/0/1
3.4. Total ore din planul de învățământ	56	din care: 3.5. curs	28	3.6 seminar/laborator	14/0/14
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					30
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					41
Tutoriat (consiliere profesională)					12
Examinări					6
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				119	
3.8. Total ore pe semestru				175	
3.9. Numărul de credite				7	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Cunoștințe de bază de Analiză și Algebră liniară.
4.2. de competențe	Cunoștințe de bază de programare în Python.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Proiector.
5.2. de desfășurare a seminarului/ laboratorului	Laborator cu calculatoare. Software: Anaconda, Python, Qiskit.

6.1. Competențele dobândite în urma absolvirii programului de studii (se preiau din planul de învățământ)¹

Competențe profesionale	
Codul competenței	Competență
CP1	Cunoașterea și înțelegerea principalelor paradigme care țin de protecția datelor: confidențialitatea, integritatea și disponibilitatea datelor
CP6	Însușirea unei baze teoretice și practice solide în ceea ce privește problematică comunicării prin medii nesigure precum și utilizarea protocoalelor securizate în Internet.
CP7	Însușirea modului de funcționare a principalelor forme de aplicații malware și a principalelor forme de atacuri în Internet, precum și a metodelor de protecție împotriva acestora.
Competențe transversale	
Codul competenței	Competență
CT2	Comportarea onorabilă, etică, respectarea deontologiei profesionale.
CT5	Comunicare în limba engleză.

6.2. Rezultatele învățării specifice programului de studii (se preiau din planul de învățământ)²

Rezultatele învățării vizate prin disciplină		
Codul competenței	Cunoștințe și înțelegere (Knowledge and understanding)	Abilități academice specifice (Specific academic skills)
CP3	Studentul/absolventul cunoaște principalele aspecte ale criptografiei aplicate în Internet, în special ale criptografiei cu cheie publică și privată. Studentul/absolventul înțelege aspectele fundamentale de organizare, resurse umane și management în domeniul securității organizațiilor.	Studentul/absolventul este capabil să identifice posibilele probleme de securitate în sistemele software

7. Rezultatele învățării specifice disciplinei

Cunoștințe și înțelegere (Knowledge and understanding)
1. Înțelegerea principiilor cheie ale mecanicii cuantice relevante pentru criptografie.
2. Cunoașterea protocoalelor de distribuție a cheilor cuantice și a infrastructurilor de comunicații cuantice.
3. Înțelegerea efectelor algoritmilor cuantici, în special Shor și Grover, asupra criptografiei clasice.
4. Cunoașterea limitelor, provocărilor și direcțiilor de cercetare deschise în criptografia cuantică și post-cuantică.
Abilități academice specifice (Specific academic skills)
1. Implementarea și simularea unor protocoale criptografice cuantice folosind Qiskit sau alte cadre similare.
2. Analiza algoritmilor cuantici și post-cuantici din perspectiva rezistenței la atacuri cuantice.
3. Evaluarea implicațiilor tehnice și etice ale comunicațiilor cuantice și ale calculului cuantic.

¹ Se vor prelua din Planul de învățământ al programului de studii acele competențe profesionale și/sau transversale la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa disciplinei. Pentru fiecare competență se va prelua întregul enunț, inclusiv codul competenței, cu formularea care apare în planul de învățământ, fără modificări. Dacă nu se preia nici o competență din oricare din cele două categorii, se șterge linia din tabel aferentă acelei categorii.

² Se menționează rezultatele învățării specifice programului de studiu la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa. Enunțurile, preluate fără modificări din Planul de învățământ în funcție de tipul disciplinei (DF/DS/DC) se trec în dreptul competenței asociate.

8. Conținuturi

8.1 Curs	Metode de predare - învățare	Observații ³
1. Informații preliminare de matematică și fizică. 2. Comunicare clasică și criptografie. 3. Comunicații cuantice - avantaje, infrastructură și protocoale. 4. Distribuția cheilor cuantice. 5. Introducere în calculul cuantic. 6. Reprezentări geometrice ale cubiților și porților cuantice. 7. Algoritmi cuantici. Factorizarea - Algoritmul lui Shor. 8. Criptografie post-cuantică. 9. Probleme etice în era comunicării cuantice și a calculului cuantic.	Prezentarea; dialogul; discuția.	Activități desfășurate cu suport vizual, exemple aplicative și discuții ghidate.
Bibliografie		
1. Bellare, Mihir, and Shafi Goldwasser. Lecture notes on cryptography. 2008. 2. Gisin, Nicolas, et al. Quantum cryptography. Reviews of Modern Physics 74.1 (2002): 145. 3. Yan, Song Yuan. Cryptanalytic attacks on RSA. 2007. 4. Bruß, Dagmar, and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. Applicable Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399. 5. Shor, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review 41.2 (1999): 303-332. 6. Stancil, Daniel D., and Gregory T. Byrd. Principles of Superconducting Quantum Computers. John Wiley & Sons, 2022. 7. Imre, Sandor, and Ferenc Balazs. Quantum Computing and Communications: An Engineering Approach. John Wiley & Sons, 2005.		
8.2 Seminar / laborator	Metode de predare - învățare	Observații
1. Matrici unitare și hermitiene. Transformări cuantice și reprezentările lor. 2. Simularea protocolului BB84 folosind simulatoare de comunicare cuantică. 3. Experimentarea cu tehnici de corecție a erorilor cuantice pentru detectarea și atenuarea erorilor de transmisie. 4. Implementarea de algoritmi cuantici simpli. 5. Implementarea algoritmului cuantic de estimare de fază. 6. Implementarea algoritmului lui Shor. 7. Analiza algoritmilor post-cuantici și condițiile în care aceștia sunt rezistenți la atacuri cuantice.	Prezentarea; rezolvarea problemelor; gândire critică.	Lucrări practice și proiecte aplicative.
1. Bellare, Mihir, and Shafi Goldwasser. Lecture notes on cryptography. 2008. 2. Gisin, Nicolas, et al. Quantum cryptography. Reviews of Modern Physics 74.1 (2002): 145. 3. Yan, Song Yuan. Cryptanalytic attacks on RSA. 2007. 4. Bruß, Dagmar, and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. Applicable		



















³ De exemplu aspecte organizatorice, recomandări pentru studenți, aspecte specifice legate de curs/seminar cum ar fi invitarea unor practicieni în domeniu etc.

Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399.
 5. Shor, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review 41.2 (1999): 303-332.
 6. Stancil, Daniel D., and Gregory T. Byrd. Principles of Superconducting Quantum Computers. John Wiley & Sons, 2022.
 7. Imre, Sandor, and Ferenc Balazs. Quantum Computing and Communications: An Engineering Approach. John Wiley & Sons, 2005.

9. Evaluare

Tip activitate	9.1 Criterii de evaluare ⁴	9.2 Metode de evaluare ⁵	9.3 Pondere din nota finală
	Utilizarea conceptelor de bază în programe și exemple.	Examen scris	60%
	Implementarea conceptelor și a algoritmilor prezentați la curs și la laborator.	Evaluarea proiectelor studenților	40%
9.6 Standard minim de promovare			
Cel puțin nota 5 (pe o scală de la 1 la 10) pentru ambele tipuri de evaluare.			

10. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)⁶

 Eticheta generală pentru Dezvoltare durabilă								
 1 FĂRĂ SĂRĂCIE	 2 FOAMETE „ZERO”	 3 SĂNĂTATE ȘI BUNĂSTARE	 4 EDUCATE DE CALITATE	 5 EGALITATE DE GEN	 6 APĂ CURĂTĂ ȘI SANITATE	 7 ENERGIE CURĂTĂ ȘI LA PREȚURI ACCESIBILE	 8 MUNCĂ DECENTĂ ȘI CREȘTERE ECONOMICĂ	 9 INDUSTRIE, INOVAȚIE ȘI INFRASTRUCTURĂ
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
 10 INEGALITĂȚI REDUSE	 11 ORAȘE ȘI COMUNITĂȚI DURABILE	 12 CONSUM ȘI PRODUCȚIE RESPONSABILE	 13 ACȚIUNE CLIMATICĂ	 14 VIAȚA ACVATICĂ	 15 VIAȚA TERESTRĂ	 16 PACE, JUSTIȚIE ȘI INSTITUȚII EFICIENTE	 17 PARTENERIATE PENTRU REALIZAREA OBIECTIVELOR	Nu se aplică nici o etichetă
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Data completării:
20.05.2026

Semnătura titularului de curs
Lector Univ. dr. Mihoc Tudor Dan

Semnătura titularului de seminar
Lector Univ. dr. Mihoc Tudor Dan

⁴ Criteriile de evaluare trebuie să reflecte direct rezultatele învățării vizate la nivel de program de studii, respectiv la nivel de disciplină. Mai concret, se evaluează achizițiile de învățare menționate în rezultatele anticipate ale învățării.

⁵ Se recomandă stabilirea atât a metodelor de evaluare finală, cât și a strategiei de evaluare pe parcurs.

⁶ Selectați o singură etichetă, cea care, în conformitate cu [Procedura de aplicare a etichetelor ODD în procesul academic](#), se potrivește cel mai bine disciplinei. Dacă disciplina tratează tema dezvoltării durabile la modul general (de ex. prin prezentarea/introducerea cadrului general al dezvoltării durabile etc.) atunci se poate alocă eticheta generală de Dezvoltare Durabilă. Dacă niciuna dintre etichete nu descrie disciplina, selectați ultima opțiune: „Nu se aplică nici o etichetă”.

Data avizării în departament:

...

Semnătura directorului de departament

Conf. dr. Adrian STERCA