FIŞA DISCIPLINEI

Criptografie cuantică

Anul universitar 2025-2026

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	E	2.7. Regimul disciplinei	Opțional

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/proiect	**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 specifice acumulate[1]

[1] Se poate opta pentru competențe sau pentru rezultatele învățării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va șterge tabelul aferent celeilalte opțiuni, iar opțiunea păstrată va fi numerotată cu 6.

Competențe profesionale /esențiale	• Cunoașterea tuturor aspectelor de securitate care pot impacta procesele și infrastructura IT&C a unei organizații; • Utilizarea nuanțată și pertinentă a criteriilor și metodelor de verificare, validare și evaluare a soluțiilor software pentru a asigura securitatea acestora; • Capacitate avansată de analiză, proiectare și construcție securizată a sistemelor informatice, folosind o gamă variată de platforme hardware și software, limbaje și medii de programare și instrumente de modelare, verificare și validare;
Competențe transversale	• Abilități de comunicare profesională: descrierea clară, concisă, verbală și în scris a rezultatelor profesionale; • Comportarea onorabilă, etică, respectarea deontologiei profesionale;

6.2. Rezultatele învățării

Cunoștințe	• Studentul/absolventul cunoaște cele mai bune mecanisme de securitate care pot fi implementate în Internet • Studentul/absolventul cunoaște algoritmii matematici cei mai des folosiți în criptografie precum şi cele mai importante protocoalele din cadrul stivei TCP/IP ce implementează aceşti algoritmi • Studentul/absolventul cunoaște principalele aspecte ale criptografiei aplicate în Internet, în special ale criptografiei cu cheie publică și privată
Aptitudini	• Studentul/absolventul este capabil să dezvolte sisteme software securizate • Studentul/absolventul este capabil să identifice posibilele probleme de securitate în sistemele software • Studentul/absolventul este capabil să înțeleagă tehnicile clasice de analiză statică utilizate pentru analiza și verificarea securității programelor
Responsabilități și autonomie	• Studentul/absolventul are capacitatea de a evalua caracteristicile de securitate ale unei aplicații software la nivelul codului sursă • Studentul/absolventul dobândește deprinderile fundamentale minimale necesare pentru a scrie cod sursă fără vulnerabilități • Studentul/absolventul cunoaște mecanismele de bază ce definesc securitatea sistemului și a mediului software în care se execută o aplicație, cum ar fi: permisiunile de acces, politicile de securitate, interacțiunea cu mediul exterior

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	· Prezentarea tehnicilor matematice utilizate în comunicare și criptografie dintr-o perspectivă cuantică. · Familiarizarea studenților cu sisteme de comunicații cuantice de ultimă generație. · Familiarizarea studenților cu tehnici criptografice inovatoare, rezistente la atacurile cuantice.
7.2 Obiectivele specifice	· Dobândirea unei înțelegeri solide a principiilor cheie ale mecanicii cuantice relevante pentru criptografie. · Explorarea teoriei și a implementării practice a protocoalelor de distribuție a cheilor cuantice. · Studierea și analizarea diverselor protocoale criptografice cuantice. · Investigarea algoritmilor criptografici clasici concepuți pentru a rezista atacurilor din partea computerelor cuantice. · Explorarea potențialelor atacuri cuantice asupra sistemelor criptografice clasice. · Dobândirea de experiență practică în implementarea protocoalelor criptografice cuantice folosind simulatoare și/sau cadre de calcul cuantic (de exemplu, Qiskit sau Quipper). · Investigarea aplicațiilor din lumea reală ale criptografiei cuantice. · Analizarea limitelor, provocărilor și a întrebărilor de cercetare deschise în criptografia cuantică.

8. Conținuturi

<table>
<tr><td>8.1 Curs</td><td>Metode de predare</td><td>Observații</td></tr>
<tr><td>1. Informaţii preliminare de matematică și fizică</td><td rowspan="13">Prezentarea;

Dialogul;

Discuția.</td><td rowspan="13"></td></tr>
<tr><td>2. Comunicare clasică și criptografie</td></tr>
<tr><td>3. Comunicații cuantice - avantaje, infrastructură și protocoale</td></tr>
<tr><td>4. Distribuţia cheilor cuantice</td></tr>
<tr><td>5. Introducere în calculul cuantic</td></tr>
<tr><td>6. Reprezentări geometrice ale Qubitilor și Porților cuantice</td></tr>
<tr><td>7. Algoritmi cuantici</td></tr>
<tr><td>8. Factoriyarea - Algoritmul lui Shor</td></tr>
<tr><td>9. Efectele algoritmului Shor asupra criptografiei clasice</td></tr>
<tr><td>10. Algoritmul lui Grover și efectele sale</td></tr>
<tr><td>11.Criptografie post-cuantică</td></tr>
<tr><td>12. Probleme etice în era comunicării cuantice și a calculului cuantic.</td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td>8.2 Seminar / laborator</td><td>Metode de predare</td><td>Observații</td></tr>
<tr><td>1.Matrici unitare și hermitiene. Transformări cuantice și reprezentările lor</td><td rowspan="8">Prezentarea,
Rezolvarea problemelor,
Gândire critică</td><td rowspan="8"></td></tr>
<tr><td>2. Simularea protocolului BB84 folosind simulatoare de comunicare cuantică</td></tr>
<tr><td>3.Experimentarea cu tehnici de corecție a erorilor cuantice pentru detectarea și atenuarea erorilor de transmisie.</td></tr>
<tr><td>4. Implementarea de algoritmi cuantici simpli</td></tr>
<tr><td>5. Implementarea algoritmului cuantic de estimarea de fază</td></tr>
<tr><td>6. Implementarea algoritmului lui Shor</td></tr>
<tr><td>7. Analiza algoritmilor post-cuantici și condițiile în care aceștia sunt rezistenți la atacuri cuantice</td></tr>
<tr><td colspan="3">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.</td></tr>
</table>

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

- Conținutul este orientat spre aplicații practice în comunicațiile clasice și criptografie și către tranziția către comunicațiile cuantice. Subiectul este prezent în programele de studiu de informatică ale universităților importante.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Utilizarea conceptelor de bază în programe și exemple	Examen scris	60%
10.5 Seminar/laborator	Implementarea conceptelor și a algoritmilor prezentaţi la curs și laboratori	Evaluarea proiectelor studenților	40%
10.6 Standard minim de performanță			
● Cel puțin nota 5 (pe o scală de la 1 la 10) pentru ambele tipuri de evaluare.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)[2]

Nu se aplică.

Data completării:
...

Semnătura titularului de curs

Lector Univ. Dr. Mihoc Tudor Dan

Semnătura titularului de seminar

Lector Univ. Dr. Mihoc Tudor Dan

Data avizării în departament:
...

Semnătura directorului de departament

Conf. Dr. Adrian STERCA

[2] Păstrați doar etichetele care, în conformitate cu *Procedura de aplicare a etichetelor ODD în procesul academic*, se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "*Nu se aplică.*".