syllabus

1. Information regarding the programme

1.1 Higher education institution	**Babeş Bolyai University**
1.2 Faculty	**Faculty of Mathematics and Computer Science**
1.3 Department	**Department of Computer Science**
1.4 Field of study	**Computer Science**
1.5 Study cycle	**Master**
1.6 Study programme / Qualification	**Cyber Security** **(in english)**

2. Information regarding the discipline

2.1 Name of the discipline (en) (ro)			**Quantum Cryptography** **Criptografie cuantică**				
2.2 Course coordinator			Univ. Lector. Dr. Mihoc Tudor Dan				
2.3 Seminar coordinator			Univ. Lector. Dr. Mihoc Tudor Dan				
2.4. Year of study	1	2.5 Semester	2	2.6. Type of evaluation	C	2.7 Type of discipline	Opt.
2.8 Code of the discipline		MME8207					

3. Total estimated time (hours/semester of didactic activities)

3.1 Hours per week	3	Of which: 3.2 course	2	3.3 seminar/laboratory	1
3.4 Total hours in the curriculum	42	Of which: 3.5 course	28	3.6 seminar/laboratory	14

Time allotment:	hours
Learning using manual, course support, bibliography, course notes	28
Additional documentation (in libraries, on electronic platforms, field documentation)	28
Preparation for seminars/labs, homework, papers, portfolios and essays	28
Tutorship	17
Evaluations	28
Other activities:	0

3.7 Total individual study hours	133
3.8 Total hours per semester	175
3.9 Number of ECTS credits	7

4. Prerequisites (if necessary)

4.1. curriculum	· Basic knowledge of calculus and linear algebra
4.2. competencies	· Basic programming skills in C++

5. Conditions (if necessary)

5.1. for the course	Projector, blackboard
5.2. for the seminar /lab activities	· Computers that have installed Python with the mandatory package Qiskit

6. Specific competencies acquired

Professional competencies	**Understanding and use of basic algorithms and mathematical concepts related to quantum cryptography** **Ability to understand and approach problems and projects of information security from the perspective of quantum computing**
Transversal competencies	**Efficient fulfillment of organized activities in an interdisciplinary group and development of empathic abilities of interpersonal communication, relationships, and collaboration with various groups.**

7. Objectives of the discipline (outcome of the acquired competencies)

7.1 General objective of the discipline	· To present mathematical techniques employed in communication and cryptography from a quantum standpoint. · To acquaint the students with cutting-edge quantum communication systems · To familiarize the students with novel cryptographic techniques that are resilient to quantum assaults.
7.2 Specific objective of the discipline	· Gain a solid understanding of the key principles of quantum mechanics relevant to cryptography · Explore the theory and practical implementation of Quantum Key Distribution protocols. · Study and analyze various quantum cryptographic protocols. · Investigate classical cryptographic algorithms designed to resist attacks from quantum computers · Explore potential quantum attacks on classical cryptographic systems. · Gain hands-on experience in implementing quantum cryptographic protocols using simulators and/or quantum computing frameworks (e.g., Qiskit or Quipper). · Investigate real-world applications of quantum cryptography. · Analyze the limitations, challenges, and open research questions in quantum cryptography.

8. Content

8.1 Course	Teaching methods	Remarks
1. Mathematics and physics prerequisites	Exposition, dialog, discussion	
2. Classic Communication and Cryptography		
3. Quantum communications - advantages, infrastructure, and protocols		
4. Quantum Key distribution		
5. Introduction to quantum computing		

6. Geometrical representations of Qubits and Gates		
7. Quantum Algorithms (random number generators, Quantum Phase Estimation, Deutsch-Jozsa Algorithm, Quantum Fourier Transform)		
8. Factorization - Shor's Algorithm		
9. Effects of Shor's Algorithm to classical criptography		
10. Grover's algorithm and its effects		
11. Post-quantum cryptography 1: Lattice-Based Cryptography, Code-Based Cryptography, Hash-Based Cryptography		
12. Post-quantum cryptography 2: Multivariate Polynomial Cryptography, Isogeny-Based Cryptography, Ring-Learning with Errors, Symmetric Key Cryptography		
13. Post-quantum cryptography 3: Elliptic Curve Isogeny, Zero-Knowledge Proofs, Dilithium and Falcon		
14. Ethical issues in the quantum communication and computing era.		

Bibliography

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 / laboratory	Teaching methods	Remarks
1. Unitary and Hermitian matrices. Quantum transformations and their representations	Exposition, problem solving, critical thinking	A seminar/lab of 2 hours each 2 weaks.
2. Simulation of the BB84 protocol using quantum communication simulators or software like Qiskit or QuTech's Quantum Network Explorer.		
3. Experimenting with quantum error correction techniques to detect and mitigate transmission errors.		
4. Implement some simple quantum algorithms		
5. Implement the quantum estimation of phase algorithm		
6. Implement and use Shor's algorithm to break an encryption.		
7. Analyse prost quantum algorithms and the conditions on which they are quantum resistent		

Bibliography

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.

9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

The contents are directed towards practical applications in classic communications and cryptography and to the transition towards quantum communications. The topic is present in the computer science study programs of the major universities.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Share in the grade (%)
10.4 Course	Use of basic concepts in programs and examples	Written examination	50 %
10.5 Seminar/lab activities	Implement course concepts and algorithms	Project	50 %
10.6 Minimum performance standards			
Grade 5.			

Date	Signature of course coordinator	Signature of seminar coordinator
20/09/2024.	Lect. Dr. Mihoc Tudor Dan	Lect. Dr. Mihoc Tudor Dan

Date of approval ..... Signature of the head of department .....