SYLLABUS

Quantum Cryptography

University year 2025-2026

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
1.7. Form of education	Full time

2. Information regarding the discipline

2.1. Name of the discipline	**Quantum Cryptography**					Discipline code	**MME8207**
2.2. Course coordinator				Lector Univ. dr. Mihoc Tudor Dan			
2.3. Seminar coordinator				Lector Univ. dr. Mihoc Tudor Dan			
2.4. Year of study	1	2.5. Semester	2	2.6. Type of evaluation	E	2.7. Discipline regime	Optional

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

3.1. Hours per week	**4**	of which: 3.2 course	**2**	3.3 seminar/ laboratory/project	**1/0/1**
3.4. Total hours in the curriculum	56	of which: 3.5 course	28	3.6 seminar/ laboratory/project	**14/0/14**
Time allotment for individual study (ID) and self-study activities (SA)					**hours**
Learning using manual, course support, bibliography, course notes (SA)					30
Additional documentation (in libraries, on electronic platforms, field documentation)					30
Preparation for seminars/labs, homework, papers, portfolios and essays					41
Tutorship					12
Evaluations					6
Other activities:					0
3.7. Total individual study hours	**119**				
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 Python.

5. Conditions (if necessary)

5.1. for the course	Projector.
5.2. for the seminar /lab activities	Laboratory with computers. Software: Anaconda, Python, Qiskit.

6.1. Specific competencies acquired [1]

[1] One can choose either competences or learning outcomes, or both. If only one option is chosen, the row related to the other option will be deleted, and the kept one will be numbered 6.

Professional/ essential competencies	• Knowledge of all security aspects that can impact the processes and IT&C assets of an organization; • Proficient use of verification, validation, and evaluation criteria and methods in order to ensure software security; • Demonstrate advanced skills to analysis, design, and construction of secure software systems, using a wide range of hardware / software platforms, programming languages and environments, and modeling, verification and validation tools;
Transversal competencies	• Professional communication skills; concise and precise description, both oral and written, of professional results; • Ethic and fair behaviour, commitment to professional deontology;

6.2. Learning outcomes

Knowledge	• The student / graduate knows which are the best security mechanisms that can be implemented on the Internet • The student / graduate knows the most commonly used mathematical cryptographic algorithms as well as the most important protocols in the TCP / IP stack that implement these algorithms • The student / graduate has knowledge about Internet applied cryptography, especially knowledge related to the public and private key cryptography
Skills	• The student / graduate is able to develop secure software systems • The student / graduate is able to identify possible security issues in software systems • The student / graduate is able to understand the classical static analysis techniques used to analyze and verify the security of programs
Responsibility and autonomy:	• The student / graduate has the ability to evaluate the security features of software applications at the source code level • The student / graduate acquires the minimum basic skills needed to write a clean source code without vulnerabilities • The student / graduate knows the basic mechanisms that define the security of the system and the software environment in which an application runs, such as: access permissions, security policies, interaction with the external environment

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; Dialogue; 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		
8. Factorization - Shor's Algorithm		
9. Effects of Shor's Algorithm to classical cryptography		
10. Grover's algorithm and its effects		
11. Post-quantum cryptography		
12. Ethical issues in the quantum communication and quantum 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	
2. Simulation of the BB84 protocol using quantum communication simulators		
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 Shor's algorithm		
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

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of final grade
10.4 Course	Use of basic concepts in programs and examples	Written Exam	60%
10.5 Seminar/laboratory	Implement course concepts and algorithms	Evaluation of students' projects	40%
10.6 Minimum standard of performance			
● At least grade 5 (from a scale of 1 to 10) for both evaluation types.			

11. Labels ODD (Sustainable Development Goals)[2]

Not applicable.

Date:
...

Signature of course coordinator

Lecturer PhD. Tudor Dan Mihoc

Signature of seminar coordinator

Lecturer PhD. Tudor Dan Mihoc

Date of approval:
...

Signature of the head of department

Assoc. Prof. PhD. Adrian STERCA

[2] Keep only the labels that, according to the *Procedure for applying ODD labels in the academic process*, suit the discipline and delete the others, including the general one for *Sustainable Development* – if not applicable. If no label describes the discipline, delete them all and write „*Not applicable.*”.