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	
1.5 Study cycle	
1.6 Study programme / Qualification	Quantum Computing and Communication (în limba engleză)

2. Information regarding the discipline

2.1 Name of the discipline (en) (ro)			Classical and quantum communications Comunicare clasică și comunicare cuantică				
2.2 Course coordinator			Mihoc Tudor Dan				
2.3 Seminar coordinator			Mihoc Tudor Dan				
2.4. Year of study	1	2.5 Semester	1	2.6. Type of evaluation	E	2.7 Type of discipline	DF
2.8 Code of the discipline		PQE0003					

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	1
3.4 Total hours in the curriculum	20	Of which: 3.5 course	20	3.6 seminar/laboratory	10
Time allotment:					hours
Learning using manual, course support, bibliography, course notes					15
Additional documentation (in libraries, on electronic platforms, field documentation)					15
Preparation for seminars/labs, homework, papers, portfolios and essays					10
Tutorship					5
Evaluations					2
Other activities:					

3.7 Total individual study hours	45
3.8 Total hours per semester	75
3.9 Number of ECTS credits	3

4. Prerequisites (if necessary)

4.1. curriculum	·
4.2. competencies	·

5. Conditions (if necessary)

5.1. for the course	· Basic knowledge of calculus and linear algebra

5.2. for the seminar /lab activities	· Basic programming skills in C++

6. Specific competencies acquired

Professional competencies	**C1.5 Development of program units and corresponding documentation** **C3.3 Use of computer science and mathematical models and tools for solving specific problems in the application field**
Transversal competencies	**CT2 Efficient fulfillment of organized activities in an interdisciplinary group and development of empathic abilities of interpersonal communication, relationship 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 algorithms used in communication and cryptography from a classic and quantum perspective.
7.2 Specific objective of the discipline	· Number-theoretic and algebra algorithms will be studied and implemented in projects

8. Content

8.1 Course	Teaching methods	Remarks
1. Introduction in classical cryptography	Exposition, dialog, discussion	
2. Complexity theory and number theory background	Presentation, dialog, exemplification	
3. Pseudo-random number generators. Block ciphers. Pseudo-random functions.	Exemplification, exposition	
4. Private-key and public-key encryption	Interactive exposure, explanation, didactical demonstration	
5. Key distribution in classical cryptography	Presentation, dialog	
6. Schor's algorithm	Exemplification, exposition	
7. Post quantum cryptography. Quantum Computing Attacks on RSA	Presentation, dialog	
8. Quantum key distribution (QKD)	Presentation, dialog, , exemplification	

9. Noise in QKD (eye dropper)	Presentation, dialog, exemplification	
10. Overview of QKD networks	Presentation, dialog, exemplification	

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.

8.2 Seminar / laboratory	Teaching methods	Remarks
1. RSA (Rivest–Shamir–Adleman) algorithm	Problematization, example, algorithms implementation	
2. Caesar Cypher.	Problematization, example, algorithms implementation	
3. Electronic codebook mode	Problematization, example, algorithms implementation	
4. Factoring Algorithms (Pollard’s p-1 method, Lentra’s elliptic curve factoring algorithm)	Problematization, example, algorithms implementation	
5. Probability primality tests	Problematization, example, algorithms implementation	
6. Quantum FFT	Problematization, example, algorithms implementation	
7. Quantum Order Finding Attack	Problematization, example, algorithms implementation	
8. Quantum Algorithm for Integer Factorization	Problematization, example, algorithms implementation	
9. Quantum algorithm for discrete logarithms	Problematization, example, algorithms implementation	

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.

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 programme 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 examples	Written examination	50
10.5 Seminar/lab activities	Implement course concepts and algorithms	Practical examination	50
10.6 Minimum performance standards			
Grade 5			

Date	Signature of course coordinator	Signature of seminar coordinator
.....	Univ. Lect. Dr. Mihoc Tudor Dan	Univ. Lect. Dr. Mihoc Tudor Dan

Date of approval

Signature of the head of department

....