MINISTRY OF NATIONAL EDUCATION

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

SYLLABUS

1. Study Program

1.1	Higher Education Institute	Technical University of Cluj-Napoca
1.2	Faculty	Electronics, Telecommunications and Information Technology
1.3	Department	Communications
1.4	Study domain	Electronics and Telecommunications Engineering
1.5	Study level	Master
1.6	Study program/ Qualification	Telecommunications/ Master
1.7	Type of education	IF (Full-time learning)
1.8	Discipline code	TC-E17.40

2. Discipline

2.1	Discipline name					Information Secrecy Techniques					
2.2	Subject area					Electronics and Telecommunications Engineering					
2.3	Responsible					Professor Monica Borda, Ph.D. Monica.Borda@com.utcluj.ro					
2.4	Titular					Professor Monica Borda, Ph.D.					
2.5	Year of study	II	2.6	Semester	3	2.7	Evaluation	Exam	2.8	Type of discipline	DS/DO

3. Total estimated time

Year/ Sem	Discipline name	No. of weeks	Course [hours/week]				Applications [hours/week]				Course	Applications	Indiv. study	TOTAL	ECTS
			C	S	L	P		S	L	P					
II/3	Information Security Techniques	14	2	0	1	0	28	0	14	0	58	100	4		

3.1	Number of hours per week	4	3.2	course	2	3.3	applications	1
3.4	Total hours per curriculum	56	3.5	course	28	3.6	applications	14

Individual study	Hours
Study based on manuals, course materials, references and notes	24
Supplementary documentation in libraries, electronic platforms and on field	20
Preparation of seminars/laboratories, homeworks, essays, portfolios	20
Tutorial work	7
Assessments	3
Other activities	14

3.7	Total hours of individual study	58
3.8	Total hours per semester	100
3.9	ECTS	4

4. Prerequisites (if necessary)

4.1	Curriculum	-
4.2	Competences	Mathematics, information theory, signal processing, analog and digital circuits, programming

5. Requisites (if necessary)

5.1	Course	Video-projector, screen, whiteboard
5.2	Applications	PCs with Internet access

6 Specific competences acquired

Professional competences	Theoretical knowledge (What do the student should know)	The students will know: - the role of an cryptosystem - principles of symmetrical cryptography (classical and modern), and public key cryptography - the most important cryptographical algorithm, the way of using and selecting them - the main protocols for secure communication - the main cryptographic technologies - the main attacks and security models in information systems - the principles of authentication and digital signatures - the principles of digital watermarking - the principles of DNA cryptography - the principles of Cloud Computing
	Acquired skills (What the student is able to do)	The students will be able to: - design security information systems - implement in software or hardware cryptographical application as: e-commerce, digital watermarking, fingerprinting, image encryption - implement cryptographical algorithms - implement steganographic methods and DNA cryptography - design and implement application of cloud computing
	Acquired abilities (what equipment/ instruments/ software the student is able to handle)	The students will be able to use: - software tools (Matlab, C/C++, Java) for security purposes - hardware tools in order to design security schemes
Transversal competences		CT3 Adapting to new technologies, professional and personal development through continuing education using electronic documentation and printed sources, in Romanian and in at least one international language (English). Competencies for analysis and synthesis and optimization systems thinking. Flexibility in thinking and ability to work with interdisciplinary concepts and tools.

7 Discipline objectives (based on the grid of specific competences acquired)

7.1	General objective	Development of competences in cryptography, security systems, digital watermarking and steganography, security for cloud computing
7.2	Specific objectives	1. Acquire theoretical and practical knowledge concerning the design of security information systems 2. Acquire theoretical and practical knowledge concerning digital watermarking and image encryption 3. Acquire competences for development of algorithms and applications using software tools 4. Acquire theoretical and practical knowledge concerning DNA cryptography 5. Acquire theoretical and practical concerning security in cloud computing

8. Contents

8.1. Course (titles)		Teaching methods	Observations
1	Objectives of the course. Necessity of information security. Course structure. Bibliography 1. Introduction 1.1 Terminology 1.2. Short history 1.3 Cryptosystems 1.4 Attacks and security models	Presentation, discussions	Video projector
2	2. Basic concepts in number theory and finite fields		
3	3. Conventional (symmetrical) cryptography 3.1 Classical cryptography (Caesar, Polybius, Trithemius, Playfair, Vigenere)		
4	3.2 Modern symmetrical cryptography 3.2.1 Block chipers (DES, AES, IDEA etc, block chipers operation modes) 3.2.2 Stream chipers		
5	3.3 Confidentiality with symmetrical cryptography 3.3.1 Communication channels encryption 3.3.2 Storage encryption 3.3.3 Key management in symmetrical cryptography 3.3.4 Basic protocols for symmetrical cryptography		
6	4. Public Key Cryptography - PKC (asymmetrical cryptography) 4.1 Principles and aims 4.2 PKC algorithms (RSA, Diffie Hellman, elliptic curves cryptography)		
7	4.3 Authentication		
8	4.4 Digital signature 4.5 Protocols for digital signatures 4.6 Key management in PKC		
9	5. Digital watermarking		
10	6. DNA Cryptography		
11	7. Cloud computing security		
12	8. Security policies		
13	9. Other security applications (KERBEROS, PEM, PGP, etc)		
14	Review for exam		
8.2. Applications (laboratory work)		Teaching methods	Observations
1	Introduction. Presentation of the laboratory works and choice of mini-projects	Simulations, experiments	PC, simulator
2	Classical cryptography		
3	Encryption algorithms		
4	Public Key cryptography		
5	Watermarking		
6	Image encryption		
7	DNA cryptography. Digital certificates.		

References:

1. M. Borda, *Fundamentals in Information Theory and Coding* – Springer 2011
2. Bruce Schneier - *Applied Cryptography – Protocols, Algorithms and Source Code in C*. Second Edition- John Willey & Sons, 1996
3. William Stallings – *Cryptography and network security. Principles and practice*- Prentice-Hall, 6th edition, 2014
4. Alfred J. Menezes, Paul von Oorschot, Scott A. Vanstone- *Handbook of Applied Cryptography* - CRC Press, 1997
5. Cox, J. Bloom, M. Miller-*Digital Watermarking: Principles & Practice* - Morgan Kaufmann Publishers, 2001
6. N. Koblitz, *Algebraic aspects of cryptography,* Springer, 1999
7. G. Schmied, *High Quality messing and electronic commerce,* Spinger, 1999
8. Deitel, Deitel and Nieto, *e-Business and e-Commerce,* Prantice Hall 2001
9. J. Keyes, *Securities Technologies Handbook,* CRC Press 1998
10. H. van Tilborg, *Fundamentals of cryptology,* Kluwer Academic Publishers, 1999

9. Discipline content corroborated with the expectations of the epistemic community representatives, associations, professional and related program employers

Acquired skills will be needed in the following possible COR occupations: electronics engineer, telecommunications engineer, system and computer design engineer, or new occupations proposed to be included in COR (sales support engineer, developer of multimedia applications, network operating engineer, test engineer, project manager, traffic engineer, communications system consultant.

10. Assessment

Type of activity	10.1	Evaluation criteria	10.2	Evaluation method	10.3	The weight of the final grade
Course		Written test with 9 questions (T = 1...10) Scientific papers (S = 1…10)		Written test (T=50%) + activity during the semester (S=50%) E = T + S		E = 50%
Applications		Project developed during the semester in the laboratory (P = 0 ... 10)		Project defended at the end of semester		P = 50%
10.4 Minimum performance standard						
The final grade (N) is calculated as average of marks obtained in the evaluation of ongoing activities and application type: N = (E + P) / 2. The condition for obtaining the ECTS credits is that both components of the final grade to be higher than or equal to 5 (five).						

Date
07.02.2020

Titular
Professor
Monica BORDA, Ph.D.

Responsible
Professor
Monica BORDA, Ph.D.

Date of approval
01.10.2020

Head of Department
Professor Virgil DOBROTA, Ph.D.