COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transylvania University of Brasov
1.2 Faculty	Faculty of Mathematics and Informatics
1.3 Department	Department of Mathematics and Informatics
1.4 Field of study[1)]	Informatics
1.5 Study level[2)]	Master
1.6 Study programme/ Qualification	MSc in Internet Technologies Informatics

2. Data about the course

2.1 Name of course			Cryptography and System Security					
2.2 Course convenor			Prof dr Sabin Tabirca					
2.3 Seminar/ laboratory/ project convenor			Prof dr Sabin Tabirca					
2.4 Study year	1	2.5 Semester	2	2.6 Evaluation type	E	2.7 Course status	Content[3)]	DAP
							Attendance type[4)]	DI

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**3**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/ 1 / 0**
3.4 Total number of hours in the curriculum	42	out of which: 3.5 lecture	28	3.6 seminar/ laboratory/ project	14/0/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	25
Additional documentation in libraries, specialized electronic platforms, and field research	25
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	25
Tutorial	25
Examinations	8
Other activities.....	

3.7 Total number of individual study hours	108
3.8 Total number per semester	150
3.9 Number of credits[5)]	6

4. Prerequisites (if applicable)

4.1 curriculum-related	• Linear algebrea; Java programming.
4.2 competences-related	• Competences in computer programming at the university level.

5. Conditions (if applicable)

5.1 for course development	Lecture room equipped with AV system and whiteboard	•
5.2 for seminar/ laboratory/ project development	Laboratory: generic lab room with internet connection, related software programs, and IDE for Android programming.	•

6. Specific competences

Professional competences	• Understanding the theoretical elements of linear codes and their applications to data transmission. • Knowledge of the main methods and fundamental algorithms for cryptography. • Acquiring the fundamentals of system security and applying them to Internet and mobile applications.	•

Transversal competences	• Usage of some efficient learning, research and development methods and techniques 1) to enhance the field knowledge, 2) to adapt to the challenges of a dynamic society and to the communication requirements in Romanian and other languages.	•

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• The main objective is to get familiar with the theoretical elements and main algorithms in coding theory, cryptography and system seecurity.
7.2 Specific objectives	• To understand the theoretical elements related with error correcting codes including Hamming and reed-Solomon codes. • To know the main methods in cryptology and their application to the Internet. • To understand the main vulnerabilities of the internet and to know the security techniques to prevent them.

8. Content

8.1 Course	Number of Hours	Teaching methods	Remarks
Coding theory – theoretical concepts (8 Hours): Shannon's Information Theory Linear codes for error correcting. Algebraic codes – Reed Solomon. Algorithms for Linear and Algebraic Codes. *Elements of Cryptography (10 Hours)* Symmetrical Key Cryptography Bock Ciphers of PRP and PRF Public Key Cryptography Large Prime Numbers and Fundamental Algorithms in Cryptology Digital Signatures *Security Techniques (10 Hours)* Types of Attacks and Defences for Internet Security Theoretical Models for Security Security of Internet Applications Security of Mobile Applications	*2* *2* *2* *2* *2* *2* *2* *2* *2* *2* *2* *4*	Lecturing Class Interaction Invited Guest Presentations	
	Bibliography • J. Katz and Y. Lindell, Introduction to Modern Cryptography (2nd edition), CRC Press, 2007. • Jacobus H. van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1999. • William Stallings and Lawrie Brown, Computer Security: Principles and Practice, pearson Press, 2014. • Course Official webpage.		
8.2 Seminar/ ~~laboratory/ project~~		Teaching-learning methods	Remarks
Discussing and Implementing Fundamental Algorithms for Coding theory : Computing Shannon's entropy *Discussing and Implementing Fundamental Algorithms in Cryptography. (6 Hours)* Algorithms with Symmetrical Key PRP and PRF Computations Algorithms for Large Prime Numbers	 2 2 2 2	 Team work Student presentation Discussions	

✍ Fundamental Algorithms in Cryptology *Security Techniques (4 Hours)* ✍ Applications for Web Security. ✍ Applications for Mobile Security.	2 2 *2*		
	Bibliography • J. Katz and Y. Lindell, Introduction to Modern Cryptography (2nd edition), CRC Press, 2007. • Jacobus H. van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1999. • William Stallings and Lawrie Brown, Computer Security: Principles and Practice, pearson Press, 2014. • Course Official webpage.		

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

na

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	• Achieving the main learning objectives for this subject • Acquiring the aforementioned competencies	Written examination at the end of the semester	40%
10.5 Seminar/ laboratory/ project		Continuous assessment through assignment and in lab tests.	60%
10.6 Minimal performance standard			
• Submission of course work components within the given deadlines • Designing mobile apps with interfaces and database driven.			

This course outline was certified in the Department Board meeting on 26/09/2024 and approved in the Faculty Board meeting on 26/09/2024.

Conf. Dr. Gabriel Stan	Conf. Dr. Nicusor Micuțe
Prof dr Sabin Tabirca	Prof dr Sabin Tabirca ....

Note:

1) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

2) Study level – choose from among: BA/MA/PhD;

[3] Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

[4] Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

[5] One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).