CRYPTOLOGY

1	Course Title:	CRYPTOLOGY	
2	Course Code:	BLPS260	
3	Type of Course:	Optional	
4	Level of Course:	Short Cycle	
5	Year of Study:	2	
6	Semester:	4	
7	ECTS Credits Allocated:	3.00	
8	Theoretical (hour/week):	2.00	
9	Practice (hour/week):	0.00	
10	Laboratory (hour/week):	0	
11	Prerequisites:	None	
12	Language:	Turkish	
13	Mode of Delivery:	Face to face	
14	Course Coordinator:	Öğr. Gör. Dr. ABDURRAHMAN DAYIOĞLU	
15	Course Lecturers:		
16	Contact information of the Course Coordinator:	dayioglu@uludag.edu.tr	
17	Website:		
18	Objective of the Course:	To gain basic concept knowledge in the field of cryptography.	
19	Contribution of the Course to Professional Development:	By providing the student with basic concept knowledge in the field of cryptography, the infrastructure will be ready in various situations that (s)he may encounter in (her)his professional life.	
20	Learning Outcomes:		
		1	Defines basic cryptography concepts.
		2	Explain the basic mathematical concepts of cryptography.
		3	Gain theoretical and practical knowledge and experience about encryption algorithms.
		4	List the basic principles of public-key cryptographic systems.
		5	Understands the role that cryptography plays in overall security.
		6	Gain the ability to use best practice encryption schemes from what they have learned for various real-world scenarios.
		7	Suggest new encryption and cryptography methods using knowledge of Mathematics and Computer science.
		8	Can apply encryption and cryptography methods in different security systems.
		9	Uses primality tests, applies factorization methods and defines basic cryptanalysis methods.
		10	
21	Course Content:		

Course Content:

Week	Theoretical	Practice
1	Presentation of the course.	
2	Basic objectives of cryptography, Introduction to classical cryptography systems.	

3	Detailed overview of classical cryptography systems.	
4	Introduction to basic number theory.	
5	Block ciphers with arithmetic operations on numbers and polynomials.	
6	Flowing ciphers with arithmetic operations on numbers and polynomials.	
7	Introduction to Public-Key Cryptosystems.	
8	Public-Key Cryptosystems.	
9	Discrete logarithm problem	
10	Diffie-Hellman Key Exchange	
11	DSA, Al-Gamal	
12	RSA	
13	Primality tests	
14	Factoring methods and cryptanalysis methods	

22	Textbooks, References and/or Other Materials:	Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005. Nigel Smart, Cryptography: An Introduction, Mcgraw-Hill Publication, 2004 William, Stallings, and William Stallings. Cryptography and Network Security, 6/E. Pearson Education India, 2014.
23	Assesment	Kriptolojiye Giris Ders Notları, Uygulamalı Matematik

Activites	Number	Duration (hour)	Total Work Load (hour)
Theoretical	14	2.00	28.00
Practicals/Labs	0	0.00	0.00
Self study and preperation	14	2.00	28.00
Homeworks	14	2.00	28.00
Projects	0	0.00	0.00
Field Studies	0	0.00	0.00
Midterm exams	1	3.00	3.00
Others	0	0.00	0.00
Final Exams	1	3.00	3.00
Total Work Load			90.00
Total work load/ 30 hr			3.00
ECTS Credit of the Course			3.00

	Contribution of Term (Year) Learning Activities to Success Grade	40.00
	Contribution of Final Exam to Success Grade	60.00
	Total	100.00
	Measurement and Evaluation Techniques Used in the Course	Relative evaluation.
24	**ECTS / WORK LOAD TABLE**	

25	**CONTRIBUTION OF LEARNING OUTCOMES TO PROGRAMME QUALIFICATIONS**															
	PQ1	**PQ2**	**PQ3**	**PQ4**	**PQ5**	**PQ6**	**PQ7**	**PQ8**	**PQ9**	**PQ10**	**PQ11**	**PQ12**	**PQ13**	**PQ14**	**PQ15**	**PQ16**
ÖK1	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK2	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0

ÖK3	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK4	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK5	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK6	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK7	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK8	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK9	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0

LO: Learning Objectives PQ: Program Qualifications

Contribution Level:	**1 very low**	**2 low**	**3 Medium**	**4 High**	**5 Very High**