CRYPTOGRAPHY

1	Course Title:	CRYPTOGRAPHY	
2	Course Code:	BM5114	
3	Type of Course:	Optional	
4	Level of Course:	Second Cycle	
5	Year of Study:	1	
6	Semester:	2	
7	ECTS Credits Allocated:	6.00	
8	Theoretical (hour/week):	3.00	
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:	Dr. Ögr. Üyesi CENGİZ TOĞAY	
15	Course Lecturers:	-	
16	Contact information of the Course Coordinator:	Tel: 02242942796 ctogay@uludag.edu.tr	
17	Website:		
18	Objective of the Course:	Classical cryptography: some simple crypto systems, analysis of simple crypto systems. Shannon theory: probability theory, properties of entropy, product cryptosystems. Block encryption algorithms: change-permutation networks, linear cryptanalysis, differential cryptanalysis, data encryption standard (DES), advanced encryption standard (AES), encryption modes. Cryptographic summary functions: summary functions and data integrity, security of summary functions, iterative summary functions, message verification codes. RSA cryptosystem: open-key Introduction to cryptosystems, number theory. Open keyed based on discrete logarithm problem cryptosystems: ElGamal cryptosystem, finite fields, elliptic curve cryptosystem. Digital signature: security requirements of digital signature systems, ElGamal digital signature system, DSA, ECDSA.	
19	Contribution of the Course to Professional Development:	It will be provided to have knowledge about secure communication techniques.	
20	Learning Outcomes:		
		1	77/5000 They learn how to develop classical cryptography systems.
		2	They can carry out data encryption standard (DES) and advanced encryption standard (AES).
		3	They can implement the RSA cryptosystem.
		4	Examine and implement ElGamal and elliptic curve cryptosystems.
		5	Learn ElGamal digital signature system, DSA and ECDSA.
		6	
		7	
		8	

	9	
	10	

21	Course Content:

Course Content:

Week	Theoretical	Practice
1	Classical cryptography: some simple crypto systems, analysis of simple crypto systems.	
2	Classical cryptography: some simple crypto systems, analysis of simple crypto systems.	
3	Shannon theory: probability theory, properties of entropy, product cryptosystems.	
4	Block encryption algorithms: change-permutation networks, linear cryptanalysis, differential cryptanalysis, data encryption standard (DES), advanced encryption standard (AES), encryption modes.	
5	Block encryption algorithms: change-permutation networks, linear cryptanalysis, differential cryptanalysis, data encryption standard (DES), advanced encryption standard (AES), encryption modes.	
7	Cryptographic data integrity, security of summary functions, iterative summary functions, message verification codes.	
8	Cryptographic summary functions: summary functions and iterative summary functions, message verification codes.	
11	Open keyed based on discrete logarithm problem cryptosystems: ElGamal cryptosystem, finite fields, elliptic curve cryptosystem.	
12	Open keyed based on discrete logarithm problem cryptosystems: ElGamal cryptosystem, finite fields, elliptic curve cryptosystem.	
13	Digital signature: security requirements of digital signature systems, ElGamal digital signature system, DSA, ECDSA.	
14	Digital signature: security requirements of digital signature systems, ElGamal digital signature system, DSA, ECDSA.	

Activites	Number	Duration (hour)	Total Work Load (hour)
Theoretical	14	3.00	42.00
Practicals/Labs	0	0.00	0.00
Self study and preperation	0	0.00	0.00
Homeworks	0	0.00	0.00
Projects	0	0.00	0.00
Field Studies	0	0.00	0.00
Midterm exams	1	60.00	60.00
Others	0	0.00	0.00
Final Exams	1	80.00	80.00
Total Work Load			242.00
Total work load / 30 h			6.07
ECTS Credit of the Course			6.00

22	Textbooks, References and/or Other Materials:	1) Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition by Bruce Schneier (Oct 18, 1996) Wiley; 2nd edition (October 18, 1996) 2) Christof Paar, Understanding Cryptography: A Textbook for Students and Practitioners", Springer; 1st Edition.2nd Printing edition (July 8, 2010). 3) Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, "Cryptography Engineering: Design Principles and Practical Applications" Wiley; 1 edition (March 15, 2010)
23	Assesment	

TERM LEARNING ACTIVITIES	**NUMBER**	**WEIGHT**
Midterm Exam	1	40.00
Quiz	0	0.00
Home work-project	0	0.00
Final Exam	1	60.00
Total	2	100.00
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		Written Exam

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	4	3	5	3	0	0	0	0	0	0	0	0	0	0
ÖK2	3	4	4	5	3	5	0	0	0	0	0	0	0	0	0	0
ÖK3	3	4	1	3	3	4	0	0	0	0	0	0	0	0	0	0
ÖK4	3	4	2	3	3	1	0	0	0	0	0	0	0	0	0	0
ÖK5	3	4	1	5	4	4	0	0	0	0	0	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**