Content

Course Code	Course Name	Semester	Theory	Practice	Lab	Credit	ECTS
INF441	Fundamentals of Cryptology	5	3	0	0	3	5

Prerequisites	
Admission Requirements	

Language of Instruction	Turkish
Course Type	Elective
Course Level	Bachelor Degree
Objective	Although cryptography is a very old science, it has recently undergone a real revolution. Techniques from arithmetic helped to construct so-called unidirectional properties. For example, while it is very easy to encrypt for anyone who knows the public key, it has become impossible to decrypt for those who do not know the private key. Modern encryption is used to secure access to computers, e-commerce systems, banking transactions, even to authenticate a digital document or for electronic voting. In this context, the objectives of this course can be listed as follows: - Teaching the main algorithms used in public key cryptosystems: "greedy" algorithms, Euclid algorithm and fast computation algorithms in modulo n strength - Proof of major arithmetic theorems used in public key systems - Application of theorems to Merkle-Hellman, RSA and El Gamal cryptosystems - Explaining the security-based features of the systems - Demonstration of how encryption systems are also used in authentication systems - Introducing the old (Ceaser, Vigenère, ...) and Modern (one-time password, Hill encryption) secret key encryption systems to the student - Presenting different block cipher systems.
Content	Week 1 Glouton algorithm, applications in cryptography Week 2 Euclide's algorithm and mod n application Week 3 Lagrange and Fermat theorems, fast and modular computation applications Week 4 RSA encryption system Week 5 Block RSA encryption Week 6 Discrete logarithm problem Week 7 Diffie-Hellman key exchange method Week 8 Midterm Exam Week 9 El Gamal encryption system Week 10 Electronic signature, signature and hash functions Week 11 César, Vigénère, etc. classical encryption methods such as Week 12 Hill encryption Week 13 Principles and working mechanisms of block ciphers Week 14 Feistel chart
References	1.Ders Notları: http://uni.gsu.edu.tr/moodle/course/view.php?id=53 2. Cours de cryptographie, Gilles Zémor, Cassini. ISBN 2-84225-020-6

Theory Topics

Week	Weekly Contents
1	Glouton algorithm, applications in cryptography
2	Euclide's algorithm and mod n application
3	Lagrange and Fermat theorems, fast and modular computation applications
4	RSA encryption system
5	Block RSA encryption
6	Discrete logarithm problem
7	Diffie-Hellman key exchange method
8	Midterm Exam

Week	Weekly Contents
9	El Gamal encryption system
10	Electronic signature, signature and hash functions
11	César, Vigénère, etc. classical encryption methods such as
12	Hill encryption
13	Principles and working mechanisms of block ciphers
14	Feistel chart