Content

Course Code	Course Name	Semester	Theory	Practice	Lab	Credit	ECTS
INF 524	Cryptography With Public Key	2	3	0	0	3	6

Prerequisites	
Admission Requirements	

Language of Instruction	English
Course Type	Elective
Course Level	Masters Degree
Objective	This course introduces modern cryptography (asymmetric encryption ie public key encryption) techniques, their cryptanalysis and their use. Computer programs of these encryption techniques are written through homework and important articles within the scope of the course are examined.
Content	Week 1: Introduction to number theory. Week 2: Divisibility properties and related theorems. Week 3: Theorems of number theory. Week 4: Theorems of number theory. Week 5: Theorems of number theory. Week 6: Theorems of number theory. Week 7: Diffie-Helman's article (1976). Week 8: RSA's article (1978). Week 9: Theorems of RSA algorithm. Week 10: Application of RSA algorithm. Week 11: Application of RSA algorithm. Week 12: Articles on faster RSA algorithms. Week 13: PGP (Pretty Good Privacy) Week 14: Applications on public key cryptography (SSL).
References	1. Ders kapsamındaki orijinal makaleler. 2. Singh, S., “Kod Kitabı”, Klan Yayınları, 2004.

Theory Topics

Week	Weekly Contents
1	Introduction to number theory
2	Divisibility properties and related theorems
3	Theorems of number theory I
4	Theorems of number theory II
5	Theorems of number theory III
6	Theorems of number theory IV
7	Diffie-Helman's article (1976)
8	RSA's article (1978)
9	Theorems of RSA algorithm
10	Application of RSA algorithm I
11	Application of RSA algorithm II
12	Articles on faster RSA algorithms
13	PGP (Pretty Good Privacy)
14	Applications on public key cryptography (SSL)