CENG-686
Selected Topics in Computer Engineering II (Data and Network Security)
Credits: (3:0)3

Instructor : Atila BOSTAN
Office : Faculty of Engineering –Eng.Bld Block-l, Room # L-206
E-Mail : atilabostan@cankaya.edu.tr

Course Description: This course aims to teach the theoretical aspects and fundamentals of data and network security.

Content : Encryption techniques and algorithms. Block Cypher Operations. Public-key encryption. Hash functions. Message Authentication Codes. Digital signatures. Key Management and Distribution. User Authentication. Web, E-mail, Wireless Network, IP security.

Prerequisite(s) : None (Background knowledge in computer networks and cryptology will be helpful)

Text Book :

Cryptography and Network Security: Principles and Practice
W. Stallings, Prentice-Hall, (>=5th Edition).

References :

- Computer Security, by Dieter Gollmann, ISBN 978-0-470-74115-3December ©
- Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. R.Nichols, D. Ryan, and J. Ryan. McGraw-Hill.
- Network Security: A Beginner's Guide. Eric Maiwald. McGraw Hill.
- VPNs: A Beginner's Guide, J. Mairs. McGraw Hill/Osborne.
- Introduction to Cryptography with Coding Theory, 2/E, Wade Trappe, Lawrence Washington, Pearson International Edition.
- http://www.ieee-security.org/index.html
- http://csrc.nist.gov/
- http://sans.org/
- http://www.rsasecurity.com/rsalabs/
- http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html

Attendance Policy:

You will not fail due to insufficient attendance. Attending the class sessions is entirely your choice. However, in case of not attending, you'll take the risk of missing the quizzes!!!. Attention quizzes will be pop-up (not informed).

Grading : (Tentative)

Final : % 45
Midterm(s) : % 35
Homework/Quizzes : % 20

WEEKLY SCHEDULE AND PRE-STUDY PAGES		
Week	Topics	Pre-study Pages
1	Introduction and History of Computer Security and overview of the coverage	Chapter 1 (main text)
2	Classical Encryption Techniques	Chapter 2

3	Block Cyphers and Data Encryption Standard (DES)	Chapter 3
4	Advanced Encryption Standard (AES)	Chapter 5
5	Block Cypher Operations	Chapter 6
6	Public Key Cryptography	Chapter 9
7	Diffie-Hellman Key Excghange, ElGamal Cryptpgraphy, Eliptic Curve	Chapter 10
8	Cryptographic Hash Functions	Chapter 11
9	Message Authentication Codes	Chapter 12
10	Digital Signatures	Chapter 13
11	Key Management and Distribution	Chapter 14
12	User Authentication	Chapter 15
13	Selected Topics (Web, E-Mail, Wireless Network, IP security)	Chapters 16,7,18,19,20
14	Selected Topics (Web, E-Mail, Wireless Network, IP security)	Chapters 16,7,18,19,20