CSE 4057 Information System Security

Instructor: Assist. Prof. Ömer Korçak   **E-mail:** omer.korcak@marmara.edu.tr

Office: 452   **Office hours:** TBA

Course Description: This course covers basics of symmetric key and public key cryptography, confidentiality, integrity, authentication, digital signatures, availability, privacy, anonymity, network security in various layers, web application security and some topics on OS security.

Lecture hours: Monday 9:30 – 10:20 (MB 241), Tuesday 15:30 – 17:20 (MB 241)
　　　　　　　　3 hours/week, 5 ECTS

Reference Textbooks:
J.F. Kurose and K.W. Ross, Computer Networking: A Top Down Approach, 7th edition (Chapter 8).
Stallings, W., & Brown, L. (2012). Computer security. Principles and practice (2nd edition).
Stallings, W., & Tahiliani, M. P. (2014). Cryptography and network security: principles and practice.

Grading (tentative):
Midterm: 30%
Programming Assignment(s): 25%
Homework and/or Quizzes: 5%
Final: 40%

Academic Integrity: Any kind of cheating and plagiarism will be severely penalized. Write everything in your own words and sentences (your own English, even if it is broken!).

Course Outline (tentative):
1. Introduction to Computer Security.
2. Cryptography: Classical cryptographic algorithms.
3. Cryptography: Stream Ciphers, Block Ciphers, CBC, DES, AES.
4. Cryptography: Public Key Cryptography, RSA, Diffie Helman, Elliptic Curve.
5. Cryptography: Data Integrity and Authentication, digital signatures, Hash functions, Message Authentication codes.
6. Network Security: E-mail security, Transport Layer Security, SSL.
7. Network Security: Network Layer Security, IPSec, VPNs.
8. Network Security: WLAN Security
9. Network Security: Organizational Security, Firewalls and Intrusion Detection Systems
10. Network Security: Case studies.
11. Web Application Security: SQL Injection, Cross Site Scripting
12. Web Application Security: Cross Site Request Forgery (CSRF), other vulnerabilities and countermeasures.
13. Operating System Security: Buffer overflow, control hijacking
14. Privacy, Anonymity and cencorship resistance