GEBZE TEKNİK ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
MÜFREDAT PROGRAMI

DERSİN ADI : CRYPTOGRAPHY AND COMPUTER SECURITY
DERSİN KODU : CSE 470
DERSİN SAAT VE KREDİSİ : (3+0=3)
DERS KİTAPLARI : W. Stallings,"Network Security Essentials" P.Hall 2000 ,ISBN0-13016-093-8
W. Stallings, "Cryptography and Network Security",P.Hall 1999 ,ISBN0-0-13-869017-0.
Documents of Course
DERSİN İŞLENİŞ ŞEKLİ : Topics will be explained as face to face/online in the course. Examples will be given. Sample problem solutions related to the subject will be made.
SINAV VE DEĞERLENDİRME : The passing grade will be determined by taking 40% of the quiz (midterm exam + homework) to be given during the semester and 60% of the final exam at the end of the semester (exams will be face-to-face)

WEEK	DATE	ACTION/TOPICS
1	26-30 EYL 2022	Computer security/Cyber Security and Cryptographic applications, Term project determination,
2	03-07 EKM 2022	History, types and place of cryptography in Cyber Security,
3	10-14EKM. 2022	Number, Group theory and modular arithmetic
4	17-21 EKM. 2022	Cryptographic functions and Discrete logarithm problem
5	24 -28 EKM 2022	Fundamentals of Symmetric Encryption and the DES algorithm
6	31 EKM-04 KSM. 2022	Feistel Network Based Symmetric Encryption Algorithms
7	07-11 KSM. 2022	Cryptanalysis methods
8	14-18 KSM. 2022	AES and block cipher operating modes
9	21-25 KSM 2022	Theoretical foundations and applications of Omnipotent Functions,
10	28 KSM-02 ARA. 2022	Fundamentals of Asymmetric (Public Key) encryption Methods and RSA Diffie-Hellman key exchange and El-Gamal algorithm
11	05-09 ARA. 2022	Elliptic Curve Cryptography, (Midterm Exam)
12	12-16 ARA. 2022	Fundamentals of Quantum Cryptography
13	19-23 ARA 2022	Computer/network security attacks and applications of cryptographic protocols,
14	26-30 ARA. 2022	Ensuring Communication Security and data integrity