BİLGİSAYAR AĞLARINDA GÜVENLİK

Dr. Meltem KURT PEHLİVANOĞLU

KAYNAK

- Cryptography and Network Security, William Stallings
- Network Security Essentials, William Stallings
- Network Security Monitoring: Basics for Beginners, Robert Collins
- Defensive Security Handbook, Amanda Berlin and Lee Brotherston
- Applied Network Security Monitoring, Chris Sanders and Jason Smith
- Understanding Cryptography: A Textbook for Students and Practitioner, Christof Paar - Jan Pelzl (http://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf)

DERS İÇERİKLERİ

- Şifreleme ve Güvenlik: Sayılar Teorisi ve Sonlu Cisimler için Temel Kavramlar
- Klasik ve Modern Şifreleme Teknikleri
- Blok Şifreler için Önemli Kavramlar ve Veri Şifreleme Standardı
- İleri Şifreleme Standardı
- Şifreleme Modları
- Açık Anahtar Kriptosistemler
- Veri Bütünlüğü Algoritmaları
- Veri Bütünlüğü Algoritmaları
- Yetkilendirme ve Kriptolama
- Ağ ve İletişim Sistemleri
- Saldırı Tespit Sistemleri
- Güvenlik Duvarı
- Proje Sunumları
- Proje Sunumları
- Final

DERS DEĞERLENDİRME ÖLÇÜTLERİ

- %50 PROJE
- %50 FİNAL

PROJE GRUP LİSTESİ

- https://docs.google.com/spreadsheets/d/121MIxY6dgc0o_2JJDu-lhlhXdd9oWwMwEt_siJQYknk/edit?usp=sharing