DERS BİLGİ FORMU

DERSİN ADI	**SİSTEM VE AĞ TEMELLERİ**	
DERSİN SINIFI	**9. Sınıf**	
DERSİN SÜRESİ	**Haftalık 5 Ders Saati**	
DERSİN AMACI	Bu derste öğrenciye; iş sağlığı ve güvenliği tedbirlerini alarak sistem, ağ temelleri, siber güvenlik temelleri ve kriptoloji ile ilgili bilgi ve becerilerin kazandırılması amaçlanmaktadır.	
DERSE AİT ALAN BECERİSİ	**Sistem ve ağ uygulamalarını yapma**	
EĞİLİMLER	E1.1. Merak E1.4. Kendine İnanma (Öz Yeterlilik) E2.2. Sorumluluk E3.2. Odaklanma E3.7. Sistematiklik	
PROGRAMLAR ARASI BİLEŞENLER	**Sosyal-Duygusal Öğrenme Becerileri**	SDB1.1. Kendini Tanıma (Öz Farkındalık) SDB1.2. Kendini Düzenleme (Öz Düzenleme) SDB2.1. İletişim SDB2.2. İş Birliği SDB3.3. Sorumlu Karar Verme
	Değerler	D3. Çalışkanlık D8. Mahremiyet D11. Özgürlük D16. Sorumluluk D17.Tasarruf
	Okuryazarlık Beceriler	OB1. Bilgi Okuryazarlığı OB2. Dijital Okuryazarlık OB8. Sürdürülebilirlik Okuryazarlığı
DİSİPLİNLER ARASI İLİŞKİLER	Matematik, Mesleki Yabancı Dil	
BECERİLER ARASI İLİŞKİLER	KB2.3. Özetleme KB2.4. Çözümleme KB2.7. Karşılaştırma KB2.10. Çıkarım Yapma KB2.13. Yapılandırma KB2.16. Muhakeme (Akıl Yürütme) KB2.19. Mantıksal Denetleme KB3.1. Karar Verme KB3.2. Problem Çözme BTYAB1. Bilişim Teknolojilerini Kullanma BTYAB2. Bilgi İşlemsel Düşünme BTYAB6. Dijital Güvenlik Önlemleri Alma MAB2. Matematiksel Problem Çözme	
ÖĞRENME ÇIKTILARI	Donanım birimlerinin montajını yapabilme Ağ iletişim modellerini kullanabilme İşletim sistemlerini kullanabilme Sanallaştırma ve bulut bilişim teknolojilerini kullanabilme Siber güvenliğe giriş uygulamaları yapabilme Kriptografi kullanabilme	

<table>
<tr><td>ÖĞRENME KANITLARI
(Ölçme ve Değerlendirme)</td><td colspan="3">Bu derste öğrenci performansını belirlemeye yönelik çalışmalar değerlendirilirken gözlem formu, derecelendirme ölçeği, dereceli puanlama anahtarı gibi ölçme araçlarından uygun olanlar seçilerek kullanılabilir. Örneğin iç donanım birimlerinin montajı, kablo sonlandırma, ağ protokolü yapılandırma, işletim sistemi kurma ile ilgili performans görevi verilebilir. İç ve dış donanım birimleri ile ilgili kavram haritası, T tablosu, karşılaştırma tablosu veya zihin haritası ölçme araçları kullanılabilir. Bunun yanında öz değerlendirme ve akran değerlendirme formları kullanılarak öğrencilerin öğretim sürecine aktif katılımları sağlanabilir. Ayrıca ağ referans modelleri ile ilgili ölçme aracı olarak e-portfolyo kullanılabilir. Bu ölçme yöntemleri, sürecin her aşamasında geri bildirim sağlamak ve öğrencilerin gelişimlerini sistematik bir şekilde izlemek için kullanılabilir.</td></tr>
<tr><td rowspan="2">ÖĞRENME-ÖĞRETME YAŞANTILARI</td><td>Temel Kabuller

Öğrencilerin sistem ve ağ temelleri dersinde yer alan temel bilgisayar kullanım becerileri, yazılım ve donanım arasındaki fark, dosya yönetimi ve temel ofis yazılımlarını kullanma hakkında bilgi sahibi olduğu kabul edilmektedir.</td><td>Ön Değerlendirme

Öğrencilerin siber sistem güvenliği dersindeki mevcut bilgi ve becerilerini ortaya çıkarmak amacıyla giriş-çıkış kartları kullanılabilir. Ayrıca yazılım ve donanım arasındaki fark, dosya yönetimi veya temel bilgisayar kullanımı ve güvenliğine yönelik örnek olaylar verilerek öğrencilerin bu olayları yorumlamaları istenebilir.</td><td>Köprü Kurma

Öğrencilerin bilgisayar sistemleri ve ağ teknolojileri konusundaki bilgi ve deneyimlerini ortaya çıkarmak amacıyla sanallaştırma ve bulut bilişim gibi güncel teknolojiler bağlamında sınıf içi tartışmalar yapılır. Günümüzde sık karşılaşılan güvenlik ihlalleri ve bu ihlallerin yol açtığı sonuçlar üzerine öğrencilerin görüşlerini paylaşmaları sağlanır. Sanallaştırma ve bulut teknolojilerinin günlük yaşam ve meslek alanlarındaki etkileri, önemi ve işlevine yönelik farkındalık oluşturmak amacıyla sunumlar izlettirilir ve öğrencilerden bu teknolojilerin günlük hayatta kullanım alanlarını örneklerle ifade etmeleri sağlanabilir.</td></tr>
<tr><td colspan="3">Öğrenme Öğretme Uygulamaları

Donanım Birimleri: Donanım birimleri hakkında temel bilgiler verilir. Öğrencilerin dikkatini çekmek için kavramlar, senaryo hâlinde sunulur ve örneklerle açıklanır. Öğrencilerden donanım birimleri hakkında araştırma yaparak kavram haritası oluşturmaları ve sınıfta sunmaları beklenir (OB1, KB2.3). Bu süreç, çalışma yaprağı aracılığıyla değerlendirilebilir. Kuantum bilgisayarlar hakkında güncel bilgiler, kısa videolar ve görsellerle açıklanır. Öğrencilerden kuantum bilgisayarlar konusunda güncel bir makaleyi okuyarak özet çıkarması ve dijital bir video sunum hazırlayarak sınıfta paylaşması beklenir (OB2, KB2.3, E1.1.). Hazırlanan özetler ve sunumlar, dereceli puanlama anahtarı ile değerlendirilebilir. Bilgisayarın iç donanım birimlerinin montajı uygulamasını öğretmen adım adım gösterir. Öğrenciler gruplara ayrılarak bir bilgisayarın iç donanım birimlerinin montajını yapar. Bu süreçte öğrencilerin iş bölümü ve işbirliği yaparak iletişim sergilemesi sağlanır (BTYAB1.2, SDB1.1). Montaj uygulamaları, gözlem formu ile takip edilerek öğrencilerin uygulama becerileri değerlendirilebilir. Bilgisayarın dış donanım birimlerinin bağlantıları uygulamalı olarak gösterilir ve bağlantı süreci sınıfta açıklanır. Öğrencilerden bilgisayarın dış donanım birimlerinin bağlantılarını yapmaları ve bu bağlantıları gösteren kısa bir dijital içerik (video/afiş) oluşturmaları beklenir (OB2, BTYAB1.2). Hazırlanan dijital içerikler dereceli puanlama anahtarı kullanılarak değerlendirilebilir. Öğrencilerden kendi öğrenme süreçlerini değerlendirerek donanım birimlerini nasıl öğrendiklerini paylaşması beklenir (SDB1.1, KB2.3).Öz değerlendirme formu ile öğrencilerin öğrenme süreçleri izlenebilir ve değerlendirilebilir. Donanım birimlerinin fiyat, performans, enerji tüketimi ve kullanım alanları karşılaştırmaları, örnek tablolar ile açıklanır. Öğrencilerden gruplar oluşturması ve donanım birimlerini fiyat, performans,</td></tr>
</table>

	enerji tüketimi ve kullanım alanları bakımından karşılaştırma tabloları hazırlayıp sınıfta tartışması beklenir **(OB1, KB2.3)**. Hazırlanan karşılaştırma tabloları dereceli puanlama anahtarı ile değerlendirilebilir. Öğrencilerden bir ofis ortamı için enerji verimli donanım envanter listesi hazırlaması beklenir **(KB2.7, KB2.13, OB2)**. Öğrenciler merak ettiği donanım bileşenleri hakkında kısa sorular hazırlayarak sınıf arkadaşlarına yöneltebilir. Böylece tartışma ortamı oluşturulması beklenir **(E1.1)**. Hazırlanan soru ve tartışmalar, gözlem formu ve akran değerlendirme formları ile değerlendirilebilir. **Ağ İletişimi:** Sayı sistemleri uygulamaları hakkında temel bilgiler sunulur ve örnek çözüm tabloları senaryo hâlinde gösterilir. Öğrencilerden sayı sistemleri uygulamaları yaparak örnek çözüm tabloları oluşturması ve sunması beklenir **(MAB2.1, E1.4)**. Hazırlanan çözüm tabloları, çalışma yaprağı veya dereceli puanlama anahtarı ile değerlendirilebilir. IPv4 alt ağlara bölme ve VLSM uygulamaları görsellerle adım adım açıklanır ve örnek hesaplamalar sınıfta yapılır. IPv4 alt ağlara bölme ve VLSM uygulamalarıyla ağ adresleri hesaplanması ve en verimli olanların karşılaştırma tabloları ile incelenmesi beklenir **(MAB2.1, KB2.7)**. Hazırlanan karşılaştırma tabloları dereceli puanlama anahtarı ile değerlendirilebilir. IPv4, IPv6 adresleri ile yönlendirici ve istemcilerin yapılandırılması adım adım gösterilir. Bağlantı testleri senaryo hâlinde sunulur. Öğrencilerin, IPv4 ve IPv6 adresleriyle yönlendirici ve istemcileri gruplar hâlinde yapılandırmaları ve bağlantı sonuçlarını birlikte test etmeleri beklenir. **(SDB2.2, D3.4, D16.3)**.Uygulama sonuçları gözlem formu ile izlenebilir ve değerlendirilebilir.568A ve T568B standartlarına uygun RJ45 kablo sonlandırma işlemleri uygulamalı olarak gösterilir ve bunların sınıfta karşılaştırmaları yapılır. Öğrencilerden T568A ve T568B standartlarına uygun RJ45 kablo sonlandırma işlemleri gerçekleştirilerek uygulama sonuçlarını sınıfta karşılaştırması beklenir **(KB2.7, SDB2.2)**. Kablo sonlandırma uygulamaları, gözlem formu ile değerlendirilebilir. Kablo test cihazı ile sağlamlık testleri adım adım gösterilir. Öğrencilerden kablo test cihazı ile sağlamlık testlerini uygulaması ve test sonuçlarını dijital rapor hâlinde paylaşması beklenir **(OB, OB2)**.Hazırlanan dijital raporlar dereceli puanlama anahtarı ile değerlendirilebilir. DHCPv4 ve DHCPv6 uygulamaları sayesinde ağda otomatik IP dağıtımı süreci görseller ve örneklerle açıklanır. Öğrencilerin, DHCPv4 ve DHCPv6 uygulamalarıyla ağdaki otomatik IP dağıtımını gözlemlemeleri ve sonuçlarını sınıfta sunmaları beklenir. **(OB8, E1.4)**.IP dağıtım uygulamaları gözlem formu ile takip edilerek değerlendirilebilir. ARP, DNS, ICMP, TFTP, Telnet, SSH, SMTP, POP3, HTTP/HTTPS ve FTP protokollerinin çalışma süreçleri tablo ve sunum örnekleri ile açıklanır. Öğrencilerin bunları defterlerine not almaları sağlanır. Öğrencilerden ARP, DNS, ICMP, TFTP, Telnet, SSH, SMTP, POP3, HTTP/HTTPS ve FTP protokollerinin çalışma sürecini izleyerek elde ettiği verileri tablo veya sunum hâlinde paylaşması beklenir**(KB2.7, OB8, E1.4)**. Hazırlanan tablolar ve sunumlar dereceli puanlama anahtarı ile değerlendirilebilir. Temrinler boyunca öğrenme sürecinin değerlendirilmesi ve ekip içi tartışma çalışmaları yapılması sayesinde öğrencilerden ekip çalışmasına katılması ve özverili davranışlar sergilenmesi beklenir **(SDB2.2, D3.4)**.Ekip içi tartışmalar, gözlem formu ve akran değerlendirme formları ile değerlendirilebilir. **İşletim Sistemleri:** Linux işletim sistemi kurulumu yaparak sistemin temel işleyişi açıklanır. Öğrencilerden kurulum adımlarını sunum hâline getirmesi ve sunması beklenir**(E2.2, E3.7)**.Kurulum adımları dereceli puanlama anahtarı ile değerlendirilebilir. Yardımcı yazılımların Linux üzerinde kurulumu sınıfta adım adım uygulanır ve işleyiş süreci görsellerle açıklanır. Öğrencilerden yardımcı yazılımları Linux üzerinde kurması, sistem işlevselliğini artırması ve süreci sınıfta adım adım paylaşılması beklenir**(OB1, KB3.2)**. Kurulum süreçleri ve paylaşımlar, gözlem formu ile değerlendirilebilir. Terminal komutları uygulamaları örneklerle açıklanır ve senaryo hâlinde uygulanır. Öğrencilerin bunları defterlerine not alması sağlanır. Öğrencilerden terminal komutlarının uygulamalarını yaparak algoritmik düşünme ve problem çözme becerilerini geliştirmesi beklenir**(BTYAB2.1, KB3.2)**. Uygulanan komutlar ve sonuçları çalışma yaprağı veya gözlem formu ile değerlendirilebilir. Linux işletim sistemi editörlerini kullanarak kısa betik dosyaları oluşturma süreci görseller ve örneklerle açıklanır. Öğrencilerden Linux işletim sistemi editörlerini kullanarak kısa betik dosyaları oluşturması ve dijital içerik olarak paylaşması beklenir**(OB2,**

	OB1).Hazırlanan betik dosyaları ve dijital içerikler, dereceli puanlama anahtarı ile değerlendirilebilir. Windows işletim sistemi kurulumu ve temel DOS komutları sınıfta adım adım gösterilir ve sistem yapılandırması senaryolaştırılır. Öğrencilerden Windows işletim sistemi kurulumu ve temel DOS komutları uygulamaları ile sistem yapılandırması yapması beklenir**(E2.2)**. Kurulum ve DOS komutları uygulamaları, gözlem formu ile değerlendirilebilir. PowerShell komutları ve betik dosyaları oluşturma süreci görsellerle açıklanır. PowerShell komutları ve betik dosyaları oluşturma ile öğrencilerin problem çözme ve algoritmik düşünme becerilerini geliştirmesi beklenir**(BTYAB2.1, KB3.2)**.Hazırlanan betikler dereceli puanlama anahtarı ile değerlendirilebilir. Windows yönetim araçları kullanılarak sistem yönetimi süreci, sınıfta örneklerle açıklanır ve raporlama süreci gösterilir. Öğrencilerden Windows yönetim araçlarını kullanarak sistem yönetimi süreçlerini izlemesi ve raporlaması beklenir**(OB1, E3.7)**. Hazırlanan raporlar dereceli puanlama anahtarı ile değerlendirilebilir. Sunucu işletim sistemi kurulumu ve servis yapılandırması senaryo ile adım adım sınıfta gösterilir. Öğrencilerden sunucu işletim sistemi kurulumu ve servis yapılandırması yapması(ekip çalışması yapması ve sistematik yaklaşım sergilenmesi) beklenir**(SDB2.1, E3.7)**.Kurulum ve yapılandırma süreci gözlem formu ile değerlendirilebilir. Ekip çalışması, akran değerlendirme formları ile izlenebilir. Sunucuda veri güvenliği adımları görseller ve örneklerle açıklanır. Öğrencilerin, sunucuda veri güvenliği adımlarını uygulamaları, e-güvenlik önlemlerini almaları ve olası riskleri tespit etmeleri beklenir**(OB2, KB3.2)**.Uygulanan güvenlik adımları, gözlem formu ile değerlendirilebilir. Sunucu güvenlik testleri sınıfta adım adım uygulanır. Öğrencilerden sunucu güvenlik testlerini yaparak problem çözme ve girişimcilik becerilerini geliştirmesi beklenir**(D16.3, KB3.2)**. Yapılan testler, dereceli puanlama anahtarı ile değerlendirilebilir. **Sanallaştırma ve Bulut Bilişim:** Tip 1 sanallaştırma uygulaması, sınıfta adım adım uygulanır ve sanallaştırmanın temel kavramları, senaryo ve görsellerle açıklanır. Öğrencilerin bunları defterlerine not almaları sağlanır. Öğrencilerden tip 1 sanallaştırma uygulaması yaparak sanallaştırmanın temel kavramlarını deneyimlemesi ve yapılandırma adımlarını sunu hâline getirmesi beklenir **(E3.2, KB2.13)**.Hazırlanan sunum ve yapılandırma adımları, dereceli puanlama anahtarı ile değerlendirilebilir. Tip 2 sanallaştırma uygulaması sınıfta örneklerle gösterilir ve farklı sanallaştırma türleri açıklanır. Avantaj ve dezavantajlar tablo ve görsellerle açıklanır. Öğrencilerden tip 2 sanallaştırma uygulaması gerçekleştirmesi, farklı sanallaştırma türlerini karşılaştırması ve avantaj-dezavantaj tabloları oluşturması beklenir**(KB3.1, D11.2)**.Hazırlanan tablolar dereceli puanlama anahtarı ile değerlendirilebilir. Konteyner mimarisi uygulaması sınıfta yapılır, sistem kaynaklarının etkin kullanımı senaryo ve görsellerle açıklanır. Öğrencilerden konteyner mimarisi uygulaması ile sistem kaynaklarının etkin kullanımını gözlemlemesi ve bu süreçte problemleri tanımlayıp çözmesi beklenir**(SDB3.3, E3.2)**. Uygulama ve gözlemler, gözlem formu ile değerlendirilebilir. Hipervizör (Tip 1) ve konteyner sanallaştırma teknolojileri sınıfta bir arada uygulanır. Elde edilen çözüm önerileri örneklerle açıklanır ve senaryo hâlinde paylaşılır. Öğrencilerden, geliştirdikleri çözüm önerilerini sürdürülebilirlik açısından eyleme dönüştürmeleri ve sunum hâlinde paylaşmaları beklenir**(OB8, KB2.13)**.Hazırlanan çözüm önerileri ve sunumlar dereceli puanlama anahtarı ile değerlendirilebilir. Temrinler sırasında dinlemeye ve izlemeye hazırlık yapılarak sınıf içi tartışmalarda aktif katılım sağlanması beklenir**(SDB3.3)**.Sınıf içi tartışmalar, gözlem formu ve akran değerlendirme formları ile değerlendirilebilir. **Siber Güvenliğe Giriş:** Bu öğrenme birimi işlenirken, etik, gizlilik ve bilgi güvenliği ilkeleri tanımlanır. Telif hakları, Kişisel Verilerin Korunması Kanunu (KVKK), Fikir ve Sanat Eserleri Kanunu (FSEK) gibi yasal çerçeveler, güncel örneklerle açıklanır. Siber güvenlik uzmanlarının mesleki sorumlulukları, etik ikilemler ve yasal yükümlülükler vaka analizleri üzerinden gösterilir. Verilen bir siber güvenlik olayı (örn. bir veri sızıntısı, izinsiz yazılım kullanımı veya siber zorbalık vakası) senaryosu üzerinde etik ilkeler ve ilgili yasal sorumluluklar açısından analiz yapılır. Bu analize dayanarak, siber güvenlik uzmanı olarak atılması gereken adımlar ve alınması gereken önlemler belirlenir. Belirlenen adımlar, etik ve yasal çerçeveye uygun olacak şekilde raporlanır veya simüle edilmiş bir ortamda uygulanır **(E1.1, OB1, D8.2, KB2.4, KB2.16, SDB3.3, BTYAB6.3).** Öğrencinin verilen siber güvenlik senaryosu üzerinde etik ilkeler ve yasal sorumluluklar açısından

	yaptığı analizlerin doğruluğu ve derinliği vaka analiz raporu ile değerlendirilebilir. Siber güvenlik ve bilgi güvenliği kavramları, gizlilik, bütünlük, erişilebilirlik ilkeleri örneklerle açıklanır. Bilgi güvenliği ile siber güvenlik arasındaki farklar vurgulanır. Güvenli dijital vatandaşlık, siber zorbalık, etik ilkeler ve yasal sorumluluklar (KVKK, GDPR, FSEK vb.) vaka analizleri üzerinden gösterilir. Hacker türleri (siyah, beyaz, gri şapkalı), siber saldırı yaşam döngüsü (cyber kill chain) ve başlıca siber saldırı türleri (zararlı yazılımlar, arka kapı, kimlik avı vb.) gerçek dünya örnekleriyle açıklanır. Zafiyet testi, sızma testi (pentest), kırmızı, mavi ve mor takımların görev ve farkları üzerinde durulur. Kırmızı takım hizmeti ile sızma testi farkı açıklanır. Fiziksel güvenliğin önemi, temel önlemleri ve dijital arşivleme süreçleri açıklanır. Bilgi güvenliği standartları (ISO/IEC 27001, 27002, 27032) ve başlıca siber güvenlik sertifika programları tanıtılır. Sosyal mühendislik ve phishing saldırı yöntemleri açıklanır. Varlık, tehdit, zafiyet, risk kavramları ve risk değerlendirme süreçleri açıklanır. Öğrencinin verilen bir senaryo (örn. bir kurumun veya bireyin dijital varlıklarının korunması) için kapsamlı bir siber güvenlik değerlendirme projesi hazırlaması beklenir. Bu projede; öğrencinin dijital ortamda sorumlu davranışlar sergilemesi beklenir (**E1.1, OB1, OB2, KB2.4, KB2.16, SDB2.2, SDB3.3, D16.3).** Değerlendirme için sınıf içi tartışma yapılabilir. Öğrencinin güvenli dijital vatandaşlık, etik ve yasal sorumluluklar konularındaki tartışmalara aktif katılımı, eleştirel düşünme ve sorumlu davranışlar sergileme becerileri gözlemlenebilir. Fiziksel güvenliğin bilişim sistemleri ve hassas veriler için önemi detaylı bir şekilde açıklanır. Başlıca fiziksel güvenlik tehditleri (yetkisiz erişim, hırsızlık, sabotaj, doğal afetler) ve bu tehditlere karşı alınabilecek önlemler (erişim kontrol sistemleri, kamera sistemleri, alarm sistemleri, çevre güvenliği, yangın söndürme sistemleri, iklimlendirme vb.) örneklerle gösterilir. Gerçek dünya vakaları üzerinden fiziksel güvenlik ihlallerinin sonuçları incelenir. Öğrenciden verilen bir senaryo (örn. bir bilişim laboratuvarı, küçük bir veri merkezi veya bir ofis ortamı) için fiziksel güvenlik tehditleri belirlemesi beklenir. Bu tehditlere karşı alınması gereken fiziksel güvenlik önlemleri listelemesi ve her bir önlemin gerekçesi açıklaması beklenir. Hazırlanan önlemler bir "Fiziksel Güvenlik Kontrol Listesi" veya "Güvenlik Planı Taslağı" biçiminde sunması beklenir **(E1.1, OB1, OB2, KB2.10, SDB3.3, D3.1, D3.2).** Değerlendirme için vaka analiz raporu ve sınıf içi tartışma yapılabilir. Kişisel Verilerin Korunması Kanunu (KVKK) temel hükümleri, veri sorumlusu ve veri işleyenin yükümlülükleri açıklanır. Bilgi Güvenliği Yönetim Sistemi (ISO/IEC 27001) standardının amacı, temel maddeleri ve belgelendirme süreci açıklanır. ISO/IEC 27002'nin bilgi güvenliği kontrolleri (örn. erişim kontrolü, şifreleme, olay yönetimi) ve bunların nasıl uygulanabileceği gösterilir. Siber güvenlik ve İnternet güvenliği yönergeleri (ISO/IEC 27032) tanıtılır. Gerçek dünya vaka çalışmaları ve örnek uygulamalar üzerinden bu standartların siber güvenlik bağlamındaki önemi ve işlevleri analiz edilir. Öğrenciden verilen bir senaryo (örn. bir e-ticaret sitesi, bir sağlık kurumu veya bir eğitim kurumu) için bilgi güvenliği standartları ve KVKK uygulama analiz etmesi beklenir **(E1.1, OB1, OB2, KB2.4, SDB3.3, D8.2, D16.3).** Değerlendirme için performans değerlendirmesi kullanılabilir. Fiziksel ve dijital arşivleme kavramları, her birinin avantajları ve dezavantajları örneklerle açıklanır. Dijital arşivlemenin önemi, sürdürülebilirliği ve erişilebilirlik sağlama yeteneği vurgulanır. Dijital arşivleme adımları (belge tarama, meta veri ekleme/indeksleme, dosya formatı seçimi, depolama çözümleri, yedekleme stratejileri, erişim kontrol mekanizmaları ve güvenlik önlemleri) detaylı bir şekilde açıklanır. Öğrenciden verilen bir senaryoya uygun olarak dijital arşivleme adımlarını planlayabilmesi beklenir **(OB1, KB2.19, SDB1.2, D17.2).** Öğrencinin hazırladığı dijital arşivleme planının mantıksal tutarlılığı, kapsamı, senaryoya uygunluğu ve güvenlik önlemleri, değerlendirme rubriği ve gözlem formu kullanılarak değerlendirilebilir. Siber güvenlik sektöründeki farklı kariyer yolları (örn. sızma test uzmanı, güvenlik analisti, adli bilişim uzmanı) tanıtılır. Bilgisayar Ağ Temelleri (CCNA), Siber Güvenlik Temelleri (CyberOps), Beyaz Şapkalı Hacker (CEH), Siber Olaylara Müdahale Ekibi (CIRT), Ofansif Güvenlik (OSCP) ve Adli Bilişim sertifika programları detaylı bir şekilde açıklanır. Her bir programın odak alanı, kazanımları, hedef kitlesi ve kariyerdeki karşılığı örneklerle gösterilir. Öğrenciden temel siber güvenlik sertifika programlarını kariyer hedefleri doğrultusunda değerlendirmesi için "Kariyer Yolu ve Sertifika Planı" hazırlaması beklenir **(E1.1, KB2.10, SDB1.2, D3.3).** Rubrik kullanılarak değerlendirilebilir. **Kriptografi:** Bu öğrenme birimi işlenirken, kriptografi ve kriptanaliz kavramları, amaçları ve tarihteki örnekleriyle (el-Kindî, İbn Adlan, Osmanlı Şifre Kalemi) açıklanır. Şifreleme

	kavramları (encrypt, decrypt, key, plain text, cipher text) detaylı bir şekilde tanımlanır. Encoding (kodlama) kavramının şifrelemeden farkı ve veri temsili (örn. Base64) örneklerle gösterilir. El-Kindî'nin frekans analizi yöntemi ile basit şifre çözme uygulaması gerçekleştirilir. Öğrenciden, düz bir metni kriptoloji temel kavramları ve şifreleme prensipleri doğrultusunda analiz ederek uygun bir şifreleme yöntemiyle şifrelemesi beklenir **(E1.1, OB1, KB2.4, SDB3.3, D3.3, D16.3).** Rubrik ile değerlendirme yapılabilir. Klasik kriptografi sistemlerinin (Sezar, Vigenere, Yerine Koyma, Vernam Cipher) temel prensipleri, çalışma mantıkları ve tarihsel bağlamları açıklanır. Her bir şifreleme algoritmasının anahtar, düz metin ve şifreli metin ilişkisi detaylı olarak gösterilir. Bu algoritmaların avantajları, dezavantajları ve kırılabilirlik noktaları analiz edilir. Online şifreleme/şifre çözme araçlarının kullanımı canlı olarak gösterilir ve uygulama adımları açıklanır. Öğrenciden verilen bir düz metnin, çevrimiçi araçlar veya kâğıt-kalem yöntemiyle klasik kriptografi uygulamalarını gerçekleştirmesi beklenir **(E1.1, OB2, KB2.19, SDB1.2, D16.3).** Rubrik ile değerlendirme yapılabilir. MD5 ve SHA hash algoritmalarının (SHA-1, SHA-256, SHA-512) çalışma prensipleri, çıktı uzunlukları ve kullanım alanları açıklanır. MD5'in çakışma zafiyetleri ve bu nedenle SHA'ya geçişin nedenleri vurgulanır. Salting kavramı, parola güvenliğindeki önemi ve nasıl uygulandığı detaylı bir şekilde açıklanır. Online ve offline araçlar (örn. Hash Calculator, certutil, Get-FileHash, md5sum, sha256sum, sha512sum) kullanılarak farklı dosyalar ve metinler üzerinde hash (MD5, SHA) hesaplama uygulamaları canlı olarak gösterilir. Simüle edilmiş bir ortamda parola hashing ve salting uygulaması gerçekleştirilir. Öğrenciden, özet (Hash) fonksiyonlarının (MD5, SHA, Bycrpt) prensiplerini ve salting kavramını temel alarak, online ve offline araçlarla hash hesaplama ve salting uygulamalarını yapması beklenir **(E1.1, OB2, KB2.4, SDB1.2, D16.3).** Değerlendirme için rubrik veya performans görevi değerlendirme formu kullanılabilir. Simetrik kriptografi kavramı, önemi, temel prensipleri (tek anahtar kullanımı) ve avantaj/dezavantajları açıklanır. DES, 3DES, AES ve RC4 kripto algoritmalarının çalışma mantıkları, anahtar uzunlukları, güvenlik seviyeleri ve kullanım alanları karşılaştırılarak açıklanır. Scytale gibi eski şifreleme yöntemlerinden günümüzdeki modern simetrik algoritmalarına geçişin nedenleri ve faydaları vurgulanır. Online ve offline simetrik şifreleme/şifre çözme araçlarının kullanımı canlı olarak gösterilir ve uygulama adımları açıklanır. Öğrenciden, çevrimiçi araçlarla simetrik şifreleme uygulamalarını gerçekleştirmesi beklenir **(E1.1, OB2, SDB1.2).** Değerlendirme için performans görevi formu ve rubrik kullanılabilir. Asimetrik kriptografi kavramı, önemi, temel prensipleri (açık/gizli anahtar çifti kullanımı) ve simetrik kriptografiye göre avantaj/dezavantajları açıklanır. RSA Algoritmasının çalışma mantığı (anahtar üretimi, şifreleme, şifre çözme adımları, güvenlik seviyesi ve kullanım alanları detaylı olarak gösterilir. Diffie-Hellman algoritmasının anahtar değişimi prensibi, ortak gizli anahtar oluşturma süreci ve güvenliği açıklanır. Online ve offline asimetrik şifreleme/şifre çözme ve anahtar değişimi araçlarının kullanımı gösterilir ve uygulama adımları açıklanır. Öğrenciden, online ve offline araçlarla asimetrik şifreleme ve anahtar değişimi uygulamalarını gerçekleştirmesi beklenir **(E1.1, OB2, SDB3.3).** Değerlendirme için performans görevi formu ve rubrik kullanılabilir. Dijital imza (e-imza) kavramı, kimlik doğrulama, veri bütünlüğü ve inkar edilemezlik özelliklerini nasıl sağladığı detaylı olarak açıklanır. 5070 sayılı Elektronik İmza Kanunu'nun temel hükümleri ve dijital imzanın hukuki geçerliliği vurgulanır. Dijital imzalama sürecinin (hash değeri oluşturma, gizli anahtarla şifreleme, açık anahtarla doğrulama) adımları ve asimetrik kriptografi ile ilişkisi analiz edilir. Dijital imza oluşturma ve doğrulama adımları openssl aracı ile uygulamalı gösterilir. Öğrenciden openssl aracı ile dijital imza oluşturma ve doğrulama adımlarını uygulaması beklenir. Dijital sertifikaların (SSL/TLS) yapısı, sertifika yetkilileri (CA), güven zinciri ve web sitelerinin kimlik doğrulamasındaki işlevi açıklanır. Öğrenciden, dijital imza ve sertifikaların kimlik doğrulama ve veri bütünlüğü süreçlerindeki prensiplerini ve işleyişini analiz etmesi beklenir **(E1.1, OB2, KB2.4, KB2.16, SDB3.3).** Değerlendirme için performans görevi formu ve rubrik kullanılabilir. Veri gizleme (Steganografi) tekniği, kriptografiden farkı, kullanım alanları ve temel prensipleri açıklanır. Çevrimiçi ve çevrimdışı steganografi araçlarının (örn. Steghide, Steganography online tools) çalışma mantıkları, avantajları ve dezavantajları karşılaştırılarak gösterilir. Resim içinde metin gizleme ve resim içinde resim gizleme uygulamalarının adımları, kullanılan dosya formatları ve gizleme kapasiteleri detaylı olarak açıklanır. Steghide aracı ile komut satırı üzerinden veri gizleme ve çıkarma uygulaması gösterilir. Çevrimiçi steganografi hizmeti veren web sayfası örneği üzerinden uygulama adımları takip edilir. Öğrenciden, veri

	gizleme (Steganografi) araçlarıyla veri gizleme uygulamalarını gerçekleştirmesi beklenir **(E1.1, OB2, KB2.4, SDB1.2).** Değerlendirme için performans görevi formu ve rubrik kullanılabilir.	
ĞRENME ÖĞRETME ORTAM VE DONANIMI	**Ortam:** Siber Güvenlik Laboratuvarı **Donanım:** Etkileşimli tahta / projeksiyon, bilgisayar, yazıcı / tarayıcı, bilgisayar programı, yazılım vb. araç gereçler **Güvenlik ve Altyapı:** Laboratuvarda acil stop düğmeleri ve enerjisiz çalışma alanları bulunmalıdır. Kişisel koruyucu donanım setleri (örneğin anti-statik bileklikler, göz koruyucular) her öğrenci için sağlanmalıdır. Uyarı levhaları, yangın söndürücü ve kablo düzenleyiciler **Ağ Cihazları:** Grup başına bir bilgisayar ve ağ cihazları (switch, router) sağlanmalıdır. Sunucu (server) erişimi ve sanal makineler için uygun altyapı olmalıdır. RJ-45 kablolar, fiber konnektörler ve çift bükümlü kablolar **Ölçüm ve Test Cihazları:** RJ-45 test cihazı, kablo soyucu ve RJ-45 pense Ağ bağlantılarını ve donanım testlerini yapmak için gerekli yazılım araçları **Temel Donanım Birimleri:** İç donanım birimleri: anakart, bellek, işlemci vb.Sunucu ve istemci bilgisayarlar, yönlendirici (router) ve anahtar (switch) cihazları.Temel ağ cihazları ve bağlantı elemanları **Bağlantı İletkenleri:** RJ-45 kablolar, fiber kablolar, kelepçeler ve kablo pabuçları **El Aletleri:** Kablo soyucu, RJ-45 pense, vida ve montaj aletleri, gerektiğinde multimetre veya ağ performans ölçüm cihazları (opsiyonel) **Sunum, Kayıt ve Düzen:** Bilgisayar, yazıcı, akıllı tahta ve projeksiyon cihazı	
ÖĞRENME BİRİMİ / MODÜL VE SÜRE TABLOSU	**ÖĞRENME BİRİMİ/MODÜL**	**ÖĞRENME BİRİMİ/MODÜL SÜRESİ**
	Donanım Birimleri	40/25
	Ağ İletişimi	40/35
	İşletim Sistemleri	40/35
	Sanallaştırma ve Bulut Bilişim	40/30
	Siber Güvenliğe Giriş	40/30
	Kriptografi	40/25
TOPLAM		**240/180**

ÖĞRENME BİRİMİ / MODÜL	**ÖĞRENME ÇIKTISI GRUBU VE AÇIKLAMALARI**		**İÇERİK ÇERÇEVESİ**
Donanım Birimleri	**Donanım birimlerinin montajını yapabilme**	**İç donanım birimlerinin montajını yapar.** Anakart ve bileşenleri açıklanır. İşlemci ve yapısı açıklanır. İşlemcinin iletişim hatları açıklanır. İşlemcinin çalışma mekanizması açıklanır. RISC ve CISC işlemci mimarileri açıklanır.	

		İşlemci soğutma yöntemleri açıklanır. Bellek ve yapısı açıklanır. Bellek türleri açıklanır. Disk sürücüsü ve türleri açıklanır. RAID teknolojisi açıklanır. Ekran kartı ve yapısı açıklanır. Ağ arayüz kartı ve türleri açıklanır. MAC adresi yapısı açıklanır. Bilgisayar kasası ve türleri açıklanır. Güç kaynağı açıklanır. İç donanım birimleri birleştirilerek bilgisayar kasasına montaj uygulaması yaptırılır. **Dış donanım birimlerinin bağlantısını yapar.** Giriş aygıtları açıklanır. Çıkış aygıtları açıklanır. Dış donanım birimlerinin bağlantısı yaptırılır. **Enerji verimliliğini dikkate alarak uygun donanım birimlerini seçer.** Donanım birimlerinin enerji verimlilik sınıfları açıklanır. Enerji verimliliği yüksek donanımlar belirlenir. Donanım birimleri performans ve enerji dengesine göre sıralanır. Enerji verimli donanımlar seçilerek tablo veya liste hâline getirilir.	**İç Donanım Birimleri** **Dış Donanım Birimleri** **Enerji Verimli Donanım Birimleri**
Ağ İletişimi	**Ağ iletişim modellerini kullanabilme**	**OSI referans modelini kullanarak ağ iletişimini gerçekleştirir.** Ağ ve türleri (LAN, MAN, WAN, VPN) açıklanır. Ağ topolojileri (fiziksel ve mantıksal topolojiler vb.) açıklanır. Ağ cihazları açıklanır. OSI referans modeli açıklanır. Kapsülleme (encapsulation) ve kapsül açma (de-encapsulation) kavramları açıklanır. Uygulama katmanı açıklanır. Sunum katmanı açıklanır. Oturum katmanı açıklanır. Taşıma katmanı açıklanır. TCP başlığı ve üç yollu el sıkışma süreci (Three Way Handshake) açıklanır. UDP başlığı açıklanır. TCP ve UDP farkları açıklanır. Ağ katmanı ve başlığı açıklanır. Sayı sistemleri (ikili, onlu ve on altılık) açıklanır. Sayı sistemleri uygulaması yaptırılır. IPv4 protokolü açıklanır. IPv4 adres türleri (Unicast, Multicast ve Broadcast) açıklanır. IPv4 özel adres aralıkları (Private IP address) açıklanır. IPv4 genel adresi (Public IP address) açıklanır. Alt ağ maskesi açıklanır.	**OSI Referans Modeli** **TCP/IP Protokol Kümesi** **Ağ Protokolleri**

		Alt ağ geçidi açıklanır. APIPA IP adresi açıklanır. Loopback IP adresi açıklanır. IPv4 alt ağlara bölme işlemi açıklanır. IPv4 alt ağlara bölme uygulaması yaptırılır. VLSM uygulaması yaptırılır. IPv6 protokolü açıklanır. IPv6 adres türleri (Unicast, Multicast, Anycast ve Loopback) açıklanır. IPv6 sadeleştirme açıklanır. IPv6 sadeleştirme uygulaması yaptırılır. ICMP protokolü açıklanır. Yönlendirici ve istemciler statik olarak IPv4 adresi ile yapılandırılarak bağlantı testi (ping, tracert) yaptırılır. Yönlendirici ve istemciler statik olarak IPv6 adresi ile yapılandırılarak bağlantı testi (ping, tracert) yaptırılır. ARP protokolü açıklanır. ARP protokolünün çalışma sürecini simülasyon programında izleme uygulaması yaptırılır. Veri bağı katmanı ve başlığı açıklanır. Veri bağı katmanı protokolleri (Ethernet, Wi-Fi, HDLC ve PPP) açıklanır. Fiziksel katman ve standartları (PoE, 10BASE-T vb.) açıklanır. Ağ medyaları açıklanır. Bakır kablo türleri açıklanır. Bükümlü çift yama kablo türleri (düz, çapraz ve auto mdix) açıklanır. Bükümlü çift kablo sonlandırma standartları açıklanır. Bakır kablo konnektör türleri açıklanır. T568A standardına göre RJ45 konnektör ile düz kablo sonlandırma uygulaması yaptırılır. T568B standardına göre RJ45 konnektör ile düz kablo sonlandırma uygulaması yaptırılır. T568A ve T568B standartlarına göre RJ45 konnektör ile çapraz kablo sonlandırma uygulaması yaptırılır. Kablo test cihazı ile sağlamlık testi yaptırılır. Fiber optik kablo türleri açıklanır. Fiber optik kablo konnektörleri açıklanır. **TCP/IP protokol kümesini kullanarak ağ iletişimini gerçekleştirir.** TCP/IP protokol kümesi (TCP/IP modeli) açıklanır. TCP/IP modeli ile OSI referans modeli karşılaştırılır. Aynı ağdaki iki bilgisayarı TCP/IP yapılandırması ile haberleştirme uygulaması yaptırılır. **Network protokollerini kullanarak ağ topolojisi hazırlar.**	

		DHCP protokolü açıklanır. DHCPv4 süreci (DORA) açıklanır. DHCPv4 uygulaması yaptırılır. DHCPv6 süreci (Durumsuz Auto Config Modu, Durumsuz Auto Config + DHCP Modu ve Durumlu DHCP) açıklanır. DHCPv6 uygulaması yaptırılır. DNS protokolü açıklanır. DNS protokolü uygulaması yaptırılır. HTTP ve HTTPS protokolleri açıklanır. HTTP ve HTTPS protokolü uygulaması yaptırılır. FTP protokolü açıklanır. FTP protokolü uygulaması yaptırılır. SMTP ve POP3 e-posta protokolleri açıklanır. SMTP ve POP3 e-posta protokolleri uygulaması yaptırılır. Telnet ve SSH protokolü açıklanır. Telnet ve SSH protokolleri uygulaması yaptırılır. TFTP protokolü açıklanır. TFTP protokolü ile ağ cihazı işletim sistemi ve konfigürasyon dosyasının yedeğini alma uygulaması yaptırılır.	
İşletim Sistemleri	**İşletim sistemlerini kullanabilme**	**İhtiyacı doğrultusunda farklı türde işletim sistemlerinin özelliklerini kullanır.** İstemci ve sunucu mimarisi açıklanır. Mobil işletim sistemleri ve özellikleri açıklanır. Linux işletim sistemleri ve özellikleri açıklanır. Linux işletim sistemi açılış süreci açıklanır. Linux dosya sistemi açıklanır. Linux işletim sistemi kurulumu yaptırılır. Linux işletim sisteminde yardımcı yazılımların kurulumu yaptırılır. Linux işletim sisteminin dizin yapısı açıklanır. Linux işletim sisteminde terminal komutları (yardım ve bilgi alma, dosya ve dizin yönetimi, arşivleme, dosya indirme, yetkilendirme, kullanıcı ve grup yönetimi, süreç yönetimi, ağ, zamanlanmış görev oluşturma vb.) açıklanır. Linux işletim sisteminde terminal komutları kullanılarak uygulamalar yaptırılır. Linux işletim sistemi editörleri (nano, vim) açıklanır. Linux işletim sistemi editörleri kullanılarak uygulama yaptırılır. Windows işletim sistemi ve özellikleri açıklanır. Windows işletim sistemi açılış süreci açıklanır. Windows dosya sistemi açıklanır. Windows işletim sistemi kurulumu yaptırılır.	**Masaüstü Bilgisayarlar ve Mobil İşletim Sistemleri** **Sunucu İşletim Sistemleri**

		Windows işletim sisteminde DOS komutları (yardım, dosya ve klasör yönetimi, dosya indirme, kullanıcı ve grup yönetimi, süreç yönetimi, ağ, zamanlanmış görev oluşturma vb.) açıklanır. Windows işletim sisteminde DOS komutları kullanılarak uygulama yaptırılır. Windows PowerShell komut satırı ve özellikleri açıklanır. Windows işletim sisteminde PowerShell komutları açıklanır. Windows işletim sisteminde PowerShell komutları kullanılarak uygulama yaptırılır. Windows PowerShell betik programlama yapıları açıklanır. Windows işletim sisteminde PowerShell programlama dili ile betik dosyaları oluşturma uygulamaları yaptırılır. Windows işletim sistemi yönetim araçları açıklanır. Windows işletim sistemi yönetim araçları kullanılarak uygulamalar yaptırılır. **İhtiyacı doğrultusunda sunucu işletim sistemlerini kullanır.** Sunucu işletim sistemi açıklanır. Sunucu işletim sistemi kurulumu yaptırılır. Sunucu işletim sistemi servis yapılandırması yaptırılır. Sunucuda veri güvenliği adımları açıklanarak uygulama yaptırılır. Sunucu güvenlik testi yaptırılır.	
Sanallaştırma ve Bulut Bilişim	**Sanallaştırma ve bulut bilişim teknolojilerini kullanabilme**	**Sanallaştırma teknolojisini kullanır.** Sanallaştırma kavramı açıklanır. Hipervizör türleri (tip 1 ve tip 2) açıklanır. Tip 1 ve tip 2 sanallaştırma arasındaki farklar açıklanır. Tip 1 sanallaştırma uygulaması (VMware ESXi, Proxmox VE) yaptırılır. Tip 2 sanallaştırma uygulaması yaptırılır. Konteyner mimarisi (Docker ve Kubernetes) açıklanır. Konteyner mimarisi uygulamaları yaptırılır. Hipervizör (tip 1) ve konteyner sanallaştırma teknolojileri bir arada kullanılarak uygulama (Proxmox Virtual Environment) yaptırılır. **Bulut bilişim modellerini günlük uygulamalarda kullanır.** Bulut bilişim açıklanır. Bulut bilişim dağıtım modelleri açıklanır. Bulut bilişim hizmet modelleri (IaaS, PaaS, SaaS) açıklanır. Bulut bilişim işletim sistemleri açıklanır. Dosya depolama, paylaşma, eş zamanlı çalışma vb. için bulut ortamında çalışan uygulama yaptırılır.	**Sanallaştırma Bulut Bilişim**

Siber Güvenliğe Giriş	**Siber güvenliğe giriş uygulamaları yapabilme**	**Siber güvenlik alanındaki etik ilkelere ve yasal sorumluluklara uygun hareket eder.** Etik, gizlilik ve bilgi güvenliği ilkeleri açıklanır. Telif hakları ve yasal zorunluluklar (KVKK, GDPR, FSEK, TCK 243-244-245 vb.) açıklanır. Güvenli dijital vatandaşlık ve siber zorbalık açıklanır. Siber güvenlik uzmanının mesleki sorumlulukları açıklanır. **Siber güvenlik risklerini dikkate alarak güvenlik çözümlerini uygular**. Siber güvenlik ve bilgi güvenliği kavramları, gizlilik, bütünlük, erişilebilirlik ilkeleri ve aralarındaki farklar açıklanır. Belirlenen parola standartlarına göre güçlü ve güvenli parolalar oluşturması sağlanır. Bütünlük kontrolü uygulaması yaptırılır. Hacker türleri (siyah, beyaz, gri şapkalı) açıklanır. Zararlı yazılım türleri açıklanır. Zero day saldırısı açıklanır. Tehdit aktörleri (APT grupları vb.) ve motivasyonları açıklanır. Tehdit istihbaratı ve yöntemleri (MITRE ATT&CK Framework, MITRE D3FEND vb.) açıklanır. Sosyal mühendislik saldırı türleri açıklanır. Sosyal mühendislik saldırılarından korunma yöntemleri uygulaması yaptırılır. Siber saldırı yaşam döngüsü (cyber kill chain) ve başlıca siber saldırı türleri açıklanır. Varlık, tehdit, zafiyet, risk kavramları ve risk değerlendirme süreçleri açıklanır. Risk değerlendirme diyagramı oluşturma uygulaması yaptırılır. Zafiyet testi, sızma testi (pentest) kavramları ve farkları açıklanır. Siber güvenlik takımlarının (kırmızı, mavi, mor takım) görevleri karşılaştırılır. Önleyici (Preventive), tespit edici (Detective) ve düzeltici (Corrective) güvenlik kontrolleri açıklanır. Bilgi güvenliği standartları (ISO/IEC 27001, 27002, 27032) açıklanır. Uluslararası siber güvenlik çerçeveleri açıklanır. Siber güvenlik sertifika programları kariyer hedefleri doğrultusunda açıklanır. **Fiziksel güvenliğin önemini ve alınması gereken önlemleri değerlendirir.** Fiziksel güvenliğin bilişim sistemleri ve veriler için önemi açıklanır.	**Etik ve Yasal Sorumluluklar** **Genel Güvenlik Konsepti** **Fiziksel Güvenlik** **Dijital Arşivleme**

		Fiziksel güvenlik önlemleri (erişim kontrolü, çevre güvenliği, kamera sistemleri, yangın/sel önlemleri vb.) açıklanır. **Dijital arşivleme adımlarını planlar.** Fiziksel ve dijital arşivleme kavramları, avantajları ve dezavantajları açıklanır. Dijital arşivleme adımları (tarama, indeksleme, depolama, yedekleme, erişim kontrolü, güvenlik önlemleri) açıklanır.	
Kriptografi	**Kriptografi kullanabilme**	**Kriptoloji temel kavramlarını ve şifreleme prensiplerini uygular.** Kriptografi ve kriptanaliz kavramları açıklanır. Şifreleme kavramları (encrypt, decrypt, key, plain text, cipher text) açıklanır. Encoding kavramı ve şifreleme ile farkı açıklanır. Encoding uygulaması gerçekleştirilir. Frekans analizi yöntemi ile basit şifre çözme uygulaması gerçekleştirilir. Düz metin şifreleme uygulaması gerçekleştirilir. **Klasik kriptografi uygulamalarını gerçekleştirir.** Klasik kriptografi sistemlerinin (Sezar, Vigenere, Yerine Koyma, Vernam Cipher) genel prensipleri açıklanır. Sezar algoritmasının çalışma mantığı açıklanır. Sezar şifreleme uygulaması yaptırılır. Vigenere şifrelemesinin çalışma mantığı açıklanır. Vigenere şifreleme uygulaması yaptırılır. Yerine koyma şifrelemesi (Substitution Cipher) prensipleri açıklanır. Vernam Cipher şifreleme algoritmasının temel mantığı açıklanır. **Hash ve salting uygulamalarını gerçekleştirir.** MD5 hash algoritması açıklanır. SHA hash algoritması açıklanır. Online ve offline araçlar kullanılarak hash (MD5, SHA) hesaplama uygulamaları gerçekleştirilir. Salting kavramı açıklanır. Bcrypt, scrypt, Argon2 algoritmaları açıklanır. Salting uygulaması gerçekleştirilir. **Simetrik şifreleme uygulamalarını gerçekleştirir.** Simetrik kriptografi kavramı, önemi ve temel prensipleri açıklanır.	**Kriptoloji Temelleri** **Klasik Kriptografi** **Özet Fonksiyonları** **Simetrik Kriptografi** **Asimetrik Kriptografi** **Dijital İmza ve Sertifikalar** **Veri Gizleme**

		DES, 3DES, AES ve RC4 kripto algoritmalarının çalışma mantıkları, anahtar uzunlukları ve güvenlik özellikleri açıklanır. Online araçlar ve openssl kullanılarak simetrik şifreleme uygulaması gerçekleştirilir. **Asimetrik şifreleme ve anahtar değişimi uygulamalarını gerçekleştirir.** Asimetrik kriptografi kavramı, önemi ve temel prensipleri (açık/gizli anahtar çifti) açıklanır. RSA algoritmasının çalışma mantığı (anahtar üretimi, şifreleme, şifre çözme) açıklanır. Diffie-Hellman algoritmasının anahtar değişimi prensibi açıklanır. ECC (Elliptic Curve Cryptography) algoritmasının çalışma mantığı açıklanır. Online araçlar ve openssl kullanılarak asimetrik şifreleme ve anahtar değişimi uygulaması gerçekleştirilir. **Dijital imza uygulamalarını gerçekleştirir.** Dijital imza (e-imza) kavramının; kimlik doğrulama, inkâr edilemezlik ve veri bütünlüğü ile ilişkisi açıklanır. Dijital imzanın hukuki dayanağı 5070 sayılı Elektronik İmza Kanunu çerçevesinde açıklanır. Dijital imzalama sürecinin adımları ve asimetrik kriptografi ile ilişkisi açıklanır. OpenSSL aracı kullanılarak dijital imza oluşturma ve doğrulama uygulaması gerçekleştirilir. Dijital sertifikaların (X.509) yapısı, sertifika otoritesi (CA) kavramı, güven zinciri ve SSL/TLS protokollerindeki kimlik doğrulama işlevi açıklanır. **Steganografi araçlarıyla veri gizleme uygulamalarını gerçekleştirir.** Veri gizleme (Steganografi) tekniğinin amacı, kullanım alanları ve kriptografiden farkı açıklanır. Steganografi yöntemleri (dijital görüntü, ses, video, metin tabanlı vb.) açıklanır. Çevrimiçi araçlar kullanılarak resim içinde metin gizleme uygulaması gerçekleştirilir. Çevrimiçi araçlar kullanılarak resim içinde resim gizleme uygulaması gerçekleştirilir. Steghide aracı kullanılarak veri gizleme ve gizlenen veriyi çıkarma uygulamaları gerçekleştirilir.	

UYGULAMA FAALİYETLERİ/TEMRİNLER
Uygulama faaliyeti / temrinler; ders öğrenme çıktısına uygun olarak okulun fiziki kapasitesi ve donatımı, öğrenci sayısı göz önünde bulundurularak en fazla uygulama faaliyeti / temrini yaptıracak şekilde meslek alan zümre öğretmenler kurulu tarafından seçilir. Meslek alan zümre öğretmenleri tarafından aşağıda yer alan temrinlerden farklı temrinlerin uygulanmasına karar verilebilir.

ÖĞRENME BİRİMİ / MODÜL	UYGULAMA FAALİYETLERİ / TEMRİNLER	İLİŞKİLİ BİLEŞENLER
Donanım Birimleri	Donanım birimleri ile ilgili kavram haritası oluşturmak Kuantum bilgisayarlar hakkında sunu hazırlamak İç donanım birimlerini birleştirerek bilgisayar kasasına montaj uygulaması yapmak Dış donanım birimlerinin bağlantısını yapmak Enerji verimli donanım envanteri hazırlamak	E1.1. Merak SDB1.1. Kendini Tanıma (Öz Farkındalık) OB1. Bilgi Okuryazarlığı OB2. Dijital Okuryazarlık KB2.3. Özetleme KB2.7. Karşılaştırma KB2.13. Yapılandırma BTYAB1.2. Bilişim Teknolojileri ile Çalışma
Ağ İletişimi	Sayı sistemleri uygulaması yapmak IPv4 alt ağlara bölme uygulaması yapmak VLSM uygulaması yapmak IPv6 sadeleştirme uygulaması yapmak Yönlendirici ve istemcileri statik olarak IPv4 adresi ile yapılandırarak bağlantı testi yapmak Yönlendirici ve istemcileri statik olarak IPv6 adresi ile yapılandırarak bağlantı testi yapmak T568A standardına göre RJ45 konnektör ile düz kablo sonlandırma uygulaması yapmak T568B standardına göre RJ45 konnektör ile düz kablo sonlandırma uygulaması yapmak T568A ve T568B standartlarına göre RJ45 konnektör ile çapraz kablo sonlandırma uygulaması yapmak Kablo test cihazı ile sağlamlık testi yapmak DHCPv4 uygulaması yapmak DHCPv6 uygulaması yapmak ARP protokolünün çalışma sürecini izleme uygulaması yapmak ICMP protokolü ile iletişim testi yapmak DNS protokolü uygulaması yapmak HTTP ve HTTPS protokolü uygulaması yapmak FTP protokolü uygulaması yapmak SMTP ve POP3 e-posta uygulamaları yapmak Telnet ve SSH uygulamaları yapmak TFTP protokolü ile ağ cihazı işletim sistemi ve konfigürasyon dosyasının yedeğini alma uygulaması yapmak	E1.4. Kendine İnanma (Öz Yeterlilik) SDB2.2. İş Birliği D3.4. Çalışmalarda aktif rol almak D16.3. Görev bilincine sahip olmak OB8. Sürdürülebilirlik Okuryazarlığı KB2.7. Karşılaştırma MAB2.1. Matematiksel Çözümler Geliştirme
İşletim Sistemleri	Linux işletim sistemi kurulumu yapmak	E2.2. Sorumluluk

	Linux işletim sisteminde yardımcı yazılımların kurulumunu yapmak Linux işletim sisteminde terminal komutları uygulamaları yapmak Linux işletim sistemi editörlerini kullanmak Windows işletim sistemi kurulumu yapmak Windows işletim sistemi DOS komutlarını kullanmak Windows işletim sistemi PowerShell komutlarını kullanmak Windows işletim sisteminde PowerShell programlama dili ile betik dosyaları oluşturmak Windows işletim sistemi yönetim araçlarını kullanmak Sunucu işletim sistemi kurulumu yapmak Sunucu işletim sistemi servis yapılandırması yapmak Sunucuda veri güvenliği adımlarını uygulamak Sunucu güvenlik testi yapmak	E3.7. Sistematik Olma SDB2.1. İletişim D11.1. Cesaretli ve girişimci olmak D16.3. Görev bilincine sahip olmak OB1. Bilgi Okuryazarlığı OB2. Dijital Okuryazarlık KB3.2. Problem Çözme BTYAB2.1. Algoritmik Düşünme
Sanallaştırma ve Bulut Bilişim	Tip 1 sanallaştırma uygulaması yapmak Tip 2 sanallaştırma uygulaması yapmak Konteyner mimarisi uygulaması yapmak Hipervizör (tip 1) ve konteyner sanallaştırma teknolojilerini bir arada kullanarak uygulama yapmak Bulut ortamında eş zamanlı çalışma olanağı veren uygulama yapmak	E3.2. Odaklanma SDB3.3. Sorumlu Karar Verme D11.2. Kararlı olmak OB8. Sürdürülebilirlik Okuryazarlığı KB2.13.Yapılandırma KB3.1. Karar Verme
Siber Güvenliğe Giriş	Verilen siber güvenlik senaryoları (örn. veri sızıntısı, izinsiz erişim, etik hackleme) üzerinde etik ilkeler ve ilgili yasal sorumluluklar açısından analiz raporu hazırlayıp sınıf ortamında sunmak Verilen bir siber saldırı senaryosu üzerinde saldırının yaşam döngüsü adımları belirleme ve senaryoda yer alan siber saldırı türleri analiz etmek ve kırmızı, mavi ve mor takımların bu senaryodaki olası rol ve sorumlulukları tartışmak Bir veri merkezi, bilişim laboratuvarı veya ofis ortamı için fiziksel güvenlik tehditleri ve alınması gereken önlemler listelenerek bir güvenlik raporu taslağı hazırlamak Kimlik avı saldırılarını konu alan örnek e-posta veya mesajlar oluşturarak, gerçek ve sahte içerikleri ayırt etmeye yönelik bir değerlendirme raporu taslağı hazırlamak Sosyal mühendislik ve parola güvenliği tehditlerine yönelik örnek senaryolar oluşturarak, riskleri sınıf içinde tartışmak Bir kurumun bilgi güvenliği süreçlerini iyileştirmek amacıyla KVKK ve ISO/IEC 27001 standardının temel	E1.1. Merak OB1. Bilgi Okuryazarlığı OB2. Dijital Okuryazarlık KB2.4. Çözümleme KB2.10. Çıkarım Yapma KB2.16. Muhakeme (Akıl Yürütme) KB2.19. Mantıksal Denetleme SDB1.2. Kendini düzenleme (Öz Düzenleme) SDB2.2. İş birliği SDB3.3. Sorumlu Karar Verme D3.1. Azimli Olmak D3.2. Planlı Olmak D3.3. Araştırmacı ve Sorgulayıcı Olmak

	gereklilikleri doğrultusunda yapılması gerekenler listelemek Küçük bir işletme veya kişisel kullanım için dijital arşivleme adımlarını içeren bir plan taslağı oluşturmak "5 Yıllık Siber Güvenlik Kariyer Gelişim Planı ve Sertifika Yol Haritası" hazırlayıp sunmak Verilen basit bir bilişim sistemi veya uygulama senaryosu için risk değerlendirme diyagramı oluşturmak	D8.2. Kişisel Bilgilerin Gizliliğini Korumak D16.3. Görev Bilincine Sahip Olmak D17.2. İsraftan Kaçınmak BTYAB6.3. Siber Saldırılara Karşı Savunma Stratejilerini Kullanma
Kriptografi	Frekans analizi yöntemiyle şifre çözme uygulaması yapmak Verilen bir düz metni, kriptoloji temel kavramları ve şifreleme prensipleri doğrultusunda analiz ederek uygun bir şifreleme yöntemiyle şifrelemek Sezar ve Vigenere şifreleme algoritmalarını kullanarak metin şifreleme ve deşifreleme uygulamaları yapmak Verilen bir metni Base64 ve URL Encoding yöntemleri ile kodlama uygulamaları yapmak Çevrimiçi veya çevrimdışı araçlar kullanarak verilen bir dosyanın MD5 ve SHA hash değerlerini hesaplamak ve Bcrypt algoritmasını kullanarak salting uygulaması yapmak Çevrimiçi araçlar ve openssl kullanarak AES gibi simetrik şifreleme algoritmaları ile metin veya dosya şifreleme/deşifreleme uygulamaları yapmak Çevrimiçi araçlar ve openssl kullanarak RSA gibi asimetrik şifreleme ve Diffie-Hellman gibi anahtar değişimi uygulamalarını gerçekleştirmek Dijital imza oluşturma, doğrulama süreçleri ile dijital sertifikaların işleyişini bir senaryo üzerinden analiz etmek Dijital imza oluşturma ve doğrulama işlemlerini openssl aracıyla yapmak Steganografi araçları (örn. Steghide) kullanarak bir resim dosyası içine metin gizleme ve gizli metni çıkarma uygulaması yapmak	E1.1. Merak OB1. Bilgi Okuryazarlığı OB2. Dijital Okuryazarlık KB2.4. Çözümleme KB2.16. Muhakeme (Akıl Yürütme) KB2.19. Mantıksal Denetleme SDB1.2. Kendini Düzenleme (Öz Düzenleme) SDB3.3. Sorumlu Karar Verme D3.3. Araştırmacı ve Sorgulayıcı Olmak D16.3. Görev Bilincine Sahip Olmak

DERSİN UYGULANMASINA İLİŞKİN AÇIKLAMALAR
Her öğrencinin uygulama yapması için ortam oluşturulmalıdır. Uygulama faaliyetlerinde iş sağlığı ve güvenliğine ilişkin risk ve tehlike oluşturacak her türlü duruma karşı tedbirler alınmalıdır. Bu dersin işlenişi sırasında (sorumluluk) israf etmeme, okuluna ve çevresine karşı sorumlu olma, emanete sahip çıkma, emeğe saygı duyma, birlikte iş yapabilme, paylaşma vb. değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir. Bu etkinliklerde beyin fırtınası, grup tartışması, düz anlatım, soru cevap, örnek olay incelemesi gibi yöntem ve teknikler kullanılabilir. Anlatımdan ve örnek çalışmalardan sonra, dersin öğrenme çıktılarının öğrencide pekiştirilmesi amacıyla birden fazla uygulama faaliyeti yapılmalıdır.

Ahilik kültürüne ilişkin değerler ile programlar arası bileşenler altındaki “Değerler” eşleştirilerek öğrenme ve öğretme faaliyetleri içinde öğrenciye verilmelidir.