**BİLİŞİM TEKNOLOJİLERİ VE İNTERNET KULLANIMINDA DİKKAT EDİLMESİ GEREKEN ETİK İLKELER**

Bilişim teknolojilerinin ve İnternet’in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere bilişim etiği denir.

**1. Fikrî Mülkiyet:** Kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır. Fikrî ve kültürel eserlerden bazıları Creative Commons (CC) organizasyonuna dâhildir. Creative Commons, telif hakları konusunda esneklik sağlamayı amaçlayan, eser sahibinin haklarını koruyarak, eserlerin paylaşımını kolaylaştırıcı modeller sunan, kâr amacı gütmeyen bir organizasyondur. Bu organizasyona dâhil olan eserler, kaynağı belirtmek ön şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir.

**Koşullar:**

* **Atıf:** Eserin ilk sahibinin belirtilmesi koşulu.
* **Aynı Lisansla Paylaş:** Lisans modelinin korunması koşulu.
* **Ticari Olmayan:** Eserin ticari amaçlı kullanılmaması koşulu.
* **Türetilemez:** Eserin türevinin yaratılmaması koşulu.

**2. Erişim:** Bu başlık bilgiye erişimi anlatmaktadır. Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişim olarak düşünülebilir.

***Bu durumda karşımıza üç sorun çıkmaktadır:***

* Bilgiye erişebilecek düzeyde bilişim bilgisi,
* Bilginin yararlılığını test edecek düzeyde bilgi okuryazarlığı,
* Bilgiye erişmenin varsa maddi karşılığı olan ekonomik güç.

**3. Gizlilik:** Kişiye ait her türlü bilgiyi (ki bu bilgi sadece ad ve soyadı değil, kişinin duygu, düşünce, siyasi eğilim, dini inancı, planı, fantezi dünyası ve korku gibi bilgilerini de içerir) saklama becerisidir.

**4. Doğruluk:** Uluslararası Bilgisayar Etik Enstitüsüne göre bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi için aşağıda belirtilen 10 kurala uyulması gerekmektedir.

* Bilişim teknolojilerini başkalarına zarar vermek için kullanmamalısınız.
* Başkalarının bilişim teknolojisi aracılığı ile oluşturduğu çalışmaları karıştırmamalısınız.
* Başkasına ait olan verileri incelememelisiniz.
* Bilişim teknolojilerini hırsızlık yapmak için kullanmamalısınız.
* Bilişim teknolojilerini yalancı şahitlik yapmak için kullanmamalısınız.
* Lisanssız ya da kırılmış/kopyalanmış yazılımları kullanmamalısınız.
* Başkalarının bilişim teknolojilerini izinsiz kullanmamalısınız.
* Başkalarının bilişim teknolojileri aracılığı ile elde ettiği çalışmalarını kendinize mal etmemelisiniz.
* Yazdığınız programların ya da tasarladığınız sistemlerin sonuçlarını göz önünde bulundurmalısınız.
* Bilişim teknolojilerini her zaman saygı kuralları çerçevesinde kullanmalı ve diğer insanlara saygı duymalısınız.

***İnternet ortamındaki bilgiler kullanılmadan önce bir dizi tedbir almak önemlidir. Bu tedbirler:***

* Kullanıcıya bilgi aktaran kanal (İnternet sitesi, sosyal medya hesabı), kaynak belirtmelidir. Kaynağı belirtilmemiş bilgiye şüpheyle yaklaşılmalıdır.
* Elde edilen bilgiler üç farklı kaynaktan teyit edilmelidir.
* Bilgiyi aktaran İnternet sitesinin adresi kontrol edilmelidir.

***Alan adı uzantıları birçok İnternet sitesi için fikir verebilir. Örneğin;***

* .com ya da .net: İnternet siteleri ticari amaçlı sitelerdir.
* .gov: Devlet kurumlarının resmî sitelerinin uzantısıdır.
* .org: Ticari amacı olmayan vakıf, dernek ve organizasyonların kullandığı uzantıdır.
* .edu: Üniversite ve akademik kuruluşların siteleri için kullanılır.
* .k12: Okul öncesi, ilkokul, ortaokul ve lise gibi eğitim kurumlarına ait uzantıdır.

**5. İnternet Etiği:** İnternet kullanımı ile ilgili olarak dikkat edilmesi gereken etik ilkeler; kişilik hakları, özel yaşamın gizliliği ve veri güvenliği gibi başlıklar altında incelenebilir.

***İnternet ortamında uyulması gereken etik kurallar aşağıda verilmiştir:***

* Bize yapılmasından hoşlanmadığımız davranışları başkalarına yapmaktan kaçınmalıyız.
* Bir durum karşısında İnternet’te nasıl davranmamız gerektiği konusunda kararsız kaldığımız zaman gerçek hayatta böyle bir durum karşısında nasıl davranıyorsak öyle davranmalıyız.
* İnternet’te karşılaştığımız ancak yüzünü görmediğimiz, sesini duymadığımız kişilere saygı kuralları çerçevesinde davranmalıyız.
* İnternet’i kullanırken her kültüre ve inanca saygılı olmak, yanlış anlaşılabilecek davranışlardan kaçınmak gerektiği unutulmamalıdır.
* İnternet’i yeni kullanmaya başlayan kişilerin yapacağı yanlış davranışlara karşı onlara anlayış gösterip yardımcı olmaya çalışmak ve yol göstermek gerektiği de unutulmamalıdır.
* Özellikle sosyal medya, sohbet ve forum alanlarındaki kişiler ile ağız dalaşı yapmaktan kaçınmalı, başka insanları rahatsız etmeden yazışmaya özen göstermeliyiz. Ayrıca, sürekli olarak büyük harfler ile yazışmanın İnternet ortamında bağırmak anlamına geldiği unutulmamalıdır.
* İnsanların özel hayatına karşı saygı göstererek kişilerin sırlarının İnternet ortamında paylaşılmamasına dikkat edilmesi gerektiği unutulmamalıdır.
* İnternet’te kaba ve küfürlü bir dil kullanımından kaçınarak gerçek hayatta karşımızdaki insanlara söyleyemeyeceğimiz ya da yazamayacağımız bir dil kullanmamalıyız.
* İnternet’i başkalarına zarar vermek ya da yasa dışı amaçlar için kullanmamalı ve başkalarının da bu amaçla kullanmasına izin vermemeliyiz.
* İnternet ortamında insanların kişilik haklarına özen göstererek onların paylaştığı bilginin izinsiz kullanımından kaçınmamız gerektiği de unutulmamalıdır.

İnternet ortamında başkalarından kaynaklanan kötü davranışlara maruz kalabilirsiniz. İnternet etiğine uymayan bu davranışlara siber (dijital) zorbalık denir.

***Siber zorbalığa maruz kalmanız durumunda yapmanız gerekenler:***

* Zorbalık yapan hesaplara cevap vermeyiniz, onlarla tartışmaya girmeyiniz. İlk yapmanız gereken, zorbalık yapan hesabı engellemektir.
* Bu hesapları, bulunduğunuz sosyal medya platformundaki “Bildir/Şikâyet Et” bağlantısını kullanarak şikâyet ediniz.
* Size yönelik etik dışı davranışlar artarak ve ağırlaşarak devam ederse bunların ekran görüntülerini ve mesajları kaydediniz. Bu kanıtlarla birlikte ailenizin ya da rehber öğretmeninizin gözetiminde hukuki yollara başvurunuz.
* Siber zorbalığa maruz kalan başka kişiler de olabilir. Böyle durumlarda bu kişilere ne yapmaları gerektiği konusunda yardımcı olabilir, kötü kullanım bildirimini siz de yapabilirsiniz.

**BİLGİ GÜVENLİĞİ**

Bilgi güvenliğini oluşturan unsurlardan gizlilik, bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır.

* Gizlilik, bilginin yetkisiz kişilerce görülmesinin engellenmesidir. e-posta hesap bilgisinin bir saldırgan tarafından ele geçirilmesi buna örnek verilebilir.
* Bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunması ya da bozulmamasıdır. Bir web sayfasında yer alan bilgilerin saldırgan tarafından değiştirilmesi, bütünlük ilkesinin bozulmasına örnek verilebilir.
* Erişilebilirlik ise bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır. Bir web sitesine erişimin saldırı sonucunda engellenmesi erişilebilirlik ilkesinin ihlal edilmesine örnek olarak verilebilir.

**1. Bilgi Güvenliğine Yönelik Tehditler:** Bilgi ve bilişim teknolojileri güvenliğinde başlıca tehdit, korsan ya da saldırgan olarak adlandırılan kötü niyetli kişiler ve bu kişilerin yaptıkları saldırılardır. Bir bilişim teknolojisi sistemine sızmak, sistemi zafiyete uğratmak, sistemlerin işleyişini bozmak ve durdurmak gibi kötü niyetli davranışlar; siber saldırı veya atak olarak adlandırılmaktadır. Bu tür saldırı türlerinin tanınması, doğru şekilde analiz edilmesi ve gereken tedbirlerin alınabilmesi siber güvenlik için çok önemlidir. ***Siber güvenlik;*** siber ortamda yaşanabilecek suç, saldırı, terörizm, savaş, gibi tüm kötü niyetli hareketlere karşı alınacak tedbirler bütünüdür.

***Siber ortamda yaşanabilecek kötü niyetli hareketler aşağıda tanımlanmıştır:***

* **Siber Suç:** Bilişim teknolojileri kullanılarak gerçekleştirilen her tür yasa dışı işlemdir.
* **Siber Saldırı:** Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıdır.
* **Siber Savaş:** Farklı bir ülkenin bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.
* **Siber Terörizm:** Bilişim teknolojilerinin belirli bir politik ve sosyal amaca ulaşabilmek için hükûmetleri, toplumu, bireyleri, kurum ve kuruluşları yıldırma, baskı altında tutma ya da zarar verme amacıyla kullanılmasıdır.
* **Siber Zorbalık:** Bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür.

**2.Sayısal Dünyada Kimlik ve Parola Yönetimi:** Her gün sıkça kullandığımız şifre ve parola kavramlarını inceleyecek olursak “parola” bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir. “Şifre” ise sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır. Kullanıcı adı, her kullanıcıdan sadece bir tane olduğunu garantilemek amacıyla benzersiz bir bilgi olarak oluşturulur. Parola ise içinde büyük ya da küçük harfler, rakamlar ve özel karakterler barındıran bir karakter dizisidir.

***Parolanın kötü niyetli kişiler tarafından ele geçmesi durumunda,***

* Elde edilen bilgiler yetkisiz kişiler ile paylaşılabilir ya da şantaj amacıyla kullanabilir.
* Parolası ele geçirilen sistem başka bir bilişim sistemine saldırı amacıyla kullanılabilir.
* Parola sahibinin saygınlığının zarar görmesine yol açabilecek eylemlerde bulunulabilir.
* Ele geçirilen parola ile ekonomik kayba uğrayabilecek işlemler yapılabilir.
* Parola sahibinin yasal yaptırım ile karşı karşıya kalmasına yol açabilir.

Güçlü ve kırılması zor bir parolanın oluşturulması için olabildiğince sayı, büyük/küçük harfler ile özel karakterler içermesine dikkat edilmesi son derece önemlidir.

***Güçlü bir parolanın belirlenmesi için aşağıdaki kurallar uygulanmalıdır:***

* Parola, büyük/küçük harfler ile noktalama işaretleri ve özel karakterler içermelidir.
* Parola, -aksi belirtilmedikçe- en az sekiz karakter uzunluğunda olmalıdır.
* Parola, başkaları tarafından tahmin edilebilecek ardışık harfler ya da sayılar içermemelidir.
* Her parola için bir kullanım ömrü belirleyerek belirli aralıklar ile yeni parola oluşturulması gerekir.
* Parolanın güvenliği açısından, aşağıdaki kurallara dikkat edilmelidir:
* Parolanın başkalarıyla paylaşılmaması son derece önemlidir.
* Parolalar, basılı ya da elektronik olarak hiçbir yerde saklanmamalıdır.
* Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

***Parola oluştururken;***

* G yerine 6,
* g yerine 9,
* Ş yerine $
* a yerine @
* i, l yerine 1 gibi karakterler kullanılabilir.

**3.Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği:** Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan Virüs, Solucan, Truva Atı ya da Casus yazılım gibi kötü niyetlerle hazırlanmış yazılım veya kod parçaları zararlı programlar olarak adlandırılır.

***Bu zararlı programlar,***

* İşletim sisteminin ya da diğer programların çalışmasına engel olabilir.
* Sistemdeki dosyaları silebilir, değiştirebilir ya da yeni dosyalar ekleyebilir.
* Bilişim sisteminde bulunan verilerin ele geçirilmesine neden olabilir.
* Güvenlik açıkları oluşturabilir.
* Başka bilişim sistemlerine saldırı amacıyla kullanılabilir.
* Bilişim sisteminin, sahibinin izni dışında kullanımına neden olabilir.
* Sistem kaynaklarının izinsiz kullanımına neden olabilir.

**Virüsler;** bulaştıkları bilgisayar sisteminde çalışarak sisteme ya da programlara zarar vermek amacıyla oluşturur. Virüsler bilgisayara e-posta, bellekler, İnternet üzerinden bulaşabilir. Bilgisayarın yavaşlaması, programların çalışmaması, dosyaların silinmesi, bozulması ya da yeni dosyaların eklenmesi virüs belirtisi olabilir.

**Bilgisayar Solucanları;** kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır. Sistem için gerekli olan dosyaları bozarak bilgisayarı büyük ölçüde yavaşlatabilir ya da programların çökmesine yol açabilir.

**Truva Atları; s**isteme bulaşan bir Truva Atı ilk olarak güvenlik yazılımlarını devre dışı bırakarak saldırganların bilişim sisteminin tüm kaynaklarına, programlarına ve dosyalarına erişmesine olanak sağlar. Güvensiz sitelerden indirilen dosyalar, tanınmayan kişilerden gelen e-postalar ya da taşınabilir bellekler aracılığı ile yayılabilir.

**Casus Yazılımlar;** İnternet’ten indirilerek bilgisayara bulaşan ve gerçekte başka bir amaç ile kullanılsa bile arka planda kullanıcıya ait bilgileri de elde etmeye çalışan programlardır.

***Zararlı Programlara Karşı Alınacak Tedbirler***

* Bilgisayara antivirüs ve İnternet güvenlik programları kurularak bu programların sürekli güncel tutulmaları sağlanmalıdır.
* Tanınmayan/güvenilmeyen e-postalar ve ekleri kesinlikle açılmamalıdır.
* Ekinde şüpheli bir dosya olan e-postalar açılmamalıdır. Örneğin resim.jpg.exe isimli dosya bir resim dosyası gibi görünse de uzantısı exe olduğu için uygulama dosyasıdır.
* Zararlı içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
* Lisanssız ya da kırılmış programlar kullanılmamalıdır.
* Güvenilmeyen İnternet kaynaklarından dosya indirilmemelidir.

**PROBLEM ÇÖZME KAVRAMLARI VE YAKLAŞIMLAR**

**1.Programlama Nedir:** Problem çözme; problemleri formüle edebilme, farklı ve yaratıcı çözüm yolları önerebilme, çözümü kesin ve doğru biçimde ifade edebilme becerisidir. Bilgi işlemsel düşünme aşağıdaki özellikleri barındıran bir problem çözme sürecidir.

* Problemleri bilgisayar veya başka araçlar yardımı ile çözebilir hâle getirme
* Mantıklı bir şekilde verileri düzenleme ve çözümleme
* Model ve benzetim desteği ile verileri sunma
* Algoritmik düşünme çerçevesinde çözümleri otomatikleştirme
* Kaynakları verimli bir şekilde kullanarak uygun çözümleri tanımlama, çözümleme ve uygulama
* Bulunan çözümü farklı problemlere transfer etme ve genelleştirme

***Bir programlama sisteminin iki bileşeni vardır:***

* Bilgisayara kurulmuş olan bileşen − programlama ortamı
* Programcı tarafından oluşturulan algoritma ve program kodları

**2.Program Nedir:** Program, yapılacak bir işlemi ya da hesaplamayı gerçekleştirmek için birbirini izleyen komut ya da yönergelerden oluşan yapıdır. İşlemler matematiksel ya da mantıksak olabilir.

* **Girdi:** Klavyeden, dosyadan veya başka bir aygıttan veri almadır.
* **Çıktı:** Ekranda veriyi görüntüleme veya veriyi dosyaya veya başka bir aygıta göndermedir.
* **Matematik:** Toplama, çarpma gibi bazı temel matematiksel işlemleri gerçekleştirmedir.
* **Koşullu yürütme:** Belirli durumları sınamak ve komutları uygun bir sıraya göre çalıştırmaktır.
* **Tekrarlama:** Bazı eylemleri genellikle ufak tefek değişikliklerle yineleme işlemidir.

**3.Hata Ayıklama Nedir:** Programlama, karmaşık bir süreçtir ve programcılar programlamada hata (bug) yapabilirler. Programlama hatalarını bulma ve düzeltme işlemine hata ayıklama (debugging) denilir.

***Bir programda üç tür hata oluşabilir:***

* **Söz dizimsel hatalar:** Söz dizimi, programın yapısı ve bu yapı hakkındaki kurallar demektir.
* **Çalışma zamanı hataları: Bu** hatalar ancak program çalıştırıldıktan sonra ortaya çıkar. Hesaplanması mümkün olmayan işlemler (sıfıra bölünme) ya da hiç gerçekleşmeyecek koşulların (5<3) yürütülmesi gibi durumlarda ortaya çıkar.
* **Anlam bilimsel hatalar:** Bu durumda program, genellikle hata vermeden çalışır ancak çoğu zaman beklenen sonucu üretmez. Bu yüzden programı satır satır çalıştırarak, farklı adımlardaki çıktıları gözlemleyerek nerede mantık hatası yapıldığını bularak program doğru biçimde çalışana kadar bu hataları ayıklamak gerekir.

**4.Günlük Hayatta Problem Çözme:** Günlük hayatımızda problemlerimizi çözmek için yaşantımızı etkileyen pek çok karar veririz. Bu kararlar yalnızca yaşantımızı etkilemekle kalmaz, bazen yaşam kalitemizi ve geleceğimizi bile etkileyebilir. Örneğin karşılaştığımız problemler, televizyonda hangi kanalı seyretsem gibi basit de olabilir, hangi mesleği seçmeliyim gibi çok önemli de olabilir. Yanlış bir karar verilirse zaman ve kaynaklar boşa gidebilir, bu nedenle nasıl doğru karar verildiğini öğrenmek önemlidir.

**ETİK DEĞERLER**

Etik; bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır. Temelinde barındırdığı güzel ahlaklı, adaletli ve iyi insan olma özellikleri değişmese de zamana, bilimsel gelişmelere ve toplumun gereklerine göre etik kavramına yüklenen anlam değişebilmektedir. Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı etik değerler olarak tanımlanabilir.

**PROBLEM ÇÖZME SÜRECİ**

**1.Problem Çözme Teknikleri:** Programlama sürecinde de problemin çözümüne yönelik yol ve yaklaşımları belirlemek gerekir ama öncelikle genel kural ve teknikleri bilmek yararlıdır.

* **Her Zaman Bir Planınız Olsun:** Belirsiz bir durumu yaşamak yerine her zaman bir planınız olmalıdır.
* **Problemi Tekrar İfade Edin:** Önceki problemlerde de gördüğümüz üzere bazen problemi tekrar ifade etmek, göremediğimiz bir ayrıntıyı görmemizi ya da problemi daha kolay çözmek adına bir ipucu yakalamamızı sağlayabilir.
* **Problemi Küçük Parçalara Ayırın Problemi Küçük Parçalara Ayırın: Verilen** problemi adımlara ya da bölümlere ayırmak, çözümü kolaylaştırır.
* **Önce Bildiklerinizden Yola Çıkın:** Programlama yaparken öncelikle bildiklerimiz ile başlamalı ve sonra yeni çözümler arayışına girmeliyiz.
* **Problemi Basitleştirin:** Çözmekte zorlandığınız bir problemle karşılaşırsanız problemin kapsamını daraltmayı deneyebilirsiniz.
* **Benzerlikleri Arayın:** Burada ele aldığımız benzerlik kavramı, çözülmesi istenen problemle önceden çözülen problem arasındaki olası örtüşme ya da yeni çözüme ilham verme olarak tanımlanabilir.
* **Deneme Yapın:** Bazen bir problemi çözmenin en kolay yolu denemek ve sonuçlarını gözlemlemektir.
* **Asla Vazgeçmeyin:** Kararlılık, güven ve istek kaybolduğu zaman açık düşünemezsiniz, işlemler olması gerektiğinden uzun sürer ve gittikçe zorlaşır. Hatta öf ke ve kızgınlığa bile dönüşebilir. Böyle durumlarda en etkili çözüm ara vermektir.

**2.Problem Çözme Adımları:** Problem çözme sürecinde en iyi kararı verebilmek için izlenmesi gereken 6 adım vardır:

* **Problemi Tanımlama:** Problemi çözmeye başlamadan önce problemin açık, anlaşılır ve çok doğru bir şekilde tanımlanmış olması gerekir.
* **Problemi Anlama:** Çözüme doğru yol almadan önce problemi çok iyi anladığınızdan emin olmanız gerekir.
* **Problemin Çözümü İçin Farklı Yol ve Yöntemler Belirleme:** Problemin çözümü için olabildiğince farklı yol ve yöntem belirlemeli ve bu listenin, tüm olasılıkları içerdiğinden emin olmalısınız.
* **Farklı Çözüm Yolları Listesi İçerisinden En İyi Çözümü Seçme:** Bu adımda her bir çözümün olumlu ve olumsuz yönlerini ortaya koymalısınız.
* **Seçilen Çözüm Yolu ile Problemi Çözmek İçin Gerekli Yönergeleri Oluşturma:** Bu adımda numaralandırılmış ve adım adım yönergeler oluşturmanız gerekir.
* **Çözümü Değerlendirme:** Çözümü test etmek ya da değerlendirmek, sonucun doğruluğunu kontrol etmek anlamına gelir.

**3.Problem Türleri:** Problemlerin her zaman sıradan çözümleri olmaz. Kek yapmak ya da araba kullanmak gibi problemleri çözmek için bir dizi eylem gerekir. Adım adım yönergelere dayalı olan bu çözümlere “algoritmik çözümler” denir. En iyi yolu seçtikten sonra sonuca, ilgili adımları izleyerek ulaşılır. Bu adımlardan oluşan yapıya “algoritma” denir. En lezzetli ekmeği seçmek ya da işleri büyütmek için yatırım yapmak gibi problemlerin ise açık ve net ifade edilen yanıtları yoktur. Bu çözümler bilgi ve deneyim gerektirir, bir dizi deneme ve yanılma sürecinden oluşur. Doğrudan işlem adımları ile ulaşılamayan sonuçlara “keşfe dayalı çözümler” denir.

**4.Bilgisayarla Problem Çözme:** Bu ders kapsamında “çözüm” demek problem çözme sürecinin 5. adımında yer alan işlem adımları ya da yönergeler anlamına gelmektedir. “Sonuç” demek, çıktı ya da tamamlanmış bilgisayar destekli yanıt demektir. “Program” ise herhangi bir bilgisayar dilinde kodlanmış, çözümü oluşturan işlem adımlarının tamamını ifade etmektedir. Bilgisayarlar, zor ve zaman alıcı olabilen algoritmik çözümler ile ilgilenmek üzere tasarlanmıştır. İnsanlar, keşifsel çözümleri bulma konusunda daha iyidirler ancak bilgisayarların çözebildiği ileri düzey hesaplama ve karmaşık problemleri çözme konusunda bilgisayarların hızlarına ulaşamazlar. Keşifsel problem türleri ile ilgilenen bilgisayar dalına “yapay zekâ” adı verilmektedir. Yapay zekâ uygulamaları, bilgisayarlara mevcut bilgileri kullanarak yeni bilgiler inşa etmesini sağlamaktadır.