**UTI513 Bilgi, Güvenlik ve Mahremiyet**

**ARASINAV**

**20 Kasım 2014**

**Bir A4 yardım kağıdı. Süre 120 dakika.**

**Dilediğiniz 5 soruyu yanıtlayınız. Yanıtlamadığınız soruyu açıkça işaretleyiniz.**

**1. a)** (5 p) Bilgisayar güvenliğini tanımlayınız.

1. (5 p) En çok kullanılan güvenlik teknolojilerinden beşinin adlarını yazınız.
2. (5 p) En temel üç güvenlik servisini listeleyiniz ve kısaca tanımlayınız.
3. (5 p) *Data Origin Authentication*, *Data Integrity*, *Non-repudiation* servislerinin her biri için Şifreleme, Sayısal imza, Erişim kontrolü, Data Integrity mekanizmalarından hangilerinin kullanımına gerek olduğunu bir tablo üzerinde işaretleyiniz.

**2.**

1. (10 p) Belli başlı dört açık anahtarlı sistemini (ing. *public-key systems*) listeleyiniz. Bu sistemlerin her birinin Anahtar dağıtımı, kısa anahtar şifreleme ve sayısal imza uygulamalarından hangilerinde kullanıldığını bir tablo üzerinde işaretleyiniz.
2. (5 p) Simetrik şifrelemenin güvenli kullanımı için gerekli iki temel gereksinim nelerdir?
3. (5 p) Açık anahtar sertifikası nedir? Açıklayınız.

**3.**

1. (5 p) Kullanıcıların kimlik doğrulaması için kullanılan dört temel yaklaşım nelerdir? Birer cümle ile açıklayınız.
2. (5 p) Aşağıdaki Şekil 3.5’deki grafiği birkaç cümle ile yorumlayınız.



1. (10 p) Bir parola (ing. *password*) üreteci altı harfli parolaları üçer harflik iki parça olarak üretmektedir. Her bir parça (Sessiz,Sesli,Sessiz) harf desenine sahiptir. Türkçede 8 sesli ve 21 sessiz harf olduğuna göre;
2. Bu üretecin toplam parola uzayı büyüklüğü nedir?
3. Bir saldırganın bir parolayı doğru tahmin etme olasılığı nedir?

**4.** a)(5 p) Erişim denetimi bağlamında DAC ve MAC arasındaki farkı kısaca açıklayınız.

b) (5 p) Erişim denetim listesi ve yetenek bileti (ing. *capability list*) arasındaki farkı kısaca açıklayınız.

c) (5 p) Bir erişim denetim sistemindeki üç temel özne (ing. *subject*) sınıfını tanımlayınız.

1. (5 p) Üç temel rol hiyerarşi kısıt (ing. *constraint*) türünü açıklayınız.
2. **a)** (10 p) N görevin olduğu bir sistem olsun. Görev *i* için Ui o görev ünvanına sahip çalışanların sayısı ve Pi ise o görevin gerektirdiği erişim izinlerinin sayısı olsun.
3. Klasik DAC yaklaşımında kullanıcılar ile erişim izinleri arasında tanımlanan ilişki sayısı nedir?
4. RBAC yaklaşımında kullanıcılar ile erişim izinleri arasında tanımlanan ilişki sayısı nedir?
5. N=5, Ui = i, Pi = 4 için DAC ve RBAC yaklaşımlarında tanımlanan ilişki sayılarını bulunuz.
6. (5 p) Veritabanı şifrelemenin avantajlarını ve dezavantajlarını yazınız.
7. (5 p) Aşağıdaki şekilde bir tablo üzerindeki erişim hakları için verilen “Grant” işlemleri dizisi görülmektedir. T=70’de B’nin verdiği hakları C’den geri almış olsun. Bu geri alma işlemi sonucu oluşacak yeni diyagramı çiziniz.



1. **a)** (5 p)Habis yazılımların en yaygın üç yayılma mekanizması nelerdir?

**b)** (5 p)Bir virüs yada solucan’ın tipik operasyon aşamaları nelerdir?

**c)** (5 p)Anti-virüs yazılımlarının dört kuşağını kısaca anlatınız.

**d)** (5 p) Bir kimlik doğrulama programında yer alan aşağıdaki kod parçası ne tür bir habis (zararlı) yazılım içermektedir?

