

Adı SoyadıÖğ. Nosu:İmza:

1. (15p) a) ISO tarafından tanımlanmış ağ yönetim alanları hangileridir?

b) Ağ yönetim altyapısını oluşturan bileşenleri tanımlayınız.

c) SNMP’de *request-response* ile *trap* mesajları arasındaki fark nedir?

2.(10p)Güvenli bir haberleşmede istenen sırdaşlık (confidentiality), kimlik doğrulama (authentication), mesajın tamlığı (message integrity), kullanılrlık ve erişim kontrolü (availability and acces control) terimlerini açıklayınız.

3.(10p) N adet kişiden her biri geri kalan N-1 kişi ile haberleşmek istesin. *Simetrik* anahtar şifrelemesi için kaç adet anahtara ihtiyaç vardır? *Kamusal* anahtar şifrelemesi için kaç adet anahtara ihtiyaç vardır?

4. (5p) Bir davetsiz kullanıcın (intruder) elinde bir mesajın hem şifreli hem de şifresi çözülmüş sürümleri olsun. Bu durumda hangi saldırıyı gerçekleştirebilir?

5.(20p) Sırdaşlık, mesaj tamlığı ve kimlik doğrulama özelliklerinin bulunduğu güvenli e-mail gönderme nasıl gerçekleştirilir? Bütün detayları blok diyagram üzerinde gösteriniz.

6. (10p) Kamusal anahtar şifrelemesi, sırdaşlık, mesaj tamlığı ve kimlik doğrulama gibi alanların hepsinde başarı ile kullanılabilmesinin nedenini matematiksel olarak açıklayınız.

7.(15p) Poisson sürecine uygun şekilde bir yönlendiriciye paketler ortalama 500 paket/sn hızında gelmektedirler. Yönlendiricinin hizmet süresi üstel dağılmakta ve ortalama 1 milisaniye’dir.

a) Gelen paketin yönlendiriciyi boş bulma olasılığını bulunuz.

b) Yönlendiricideki ortalama paket sayısını bulunuz.

c) Ortalama bekleme süresini bulunuz.

d) Paketin kuyrukta geçirdiği süreyi bulunuz.

8.(15p) Bir yönlendirici M/M/1 ile modellenmekte ve paketlerin geliş hızı ortalama 10 paket/msn. Zamanın %99.9’unda yönlendiricide en çok 3 paket olması için hizmet hızı ne olmalıdır?