Bil 443

CIA Tria
Protection of Data and Systems
Bilgi Güvenilirliğinin Ana ölçüleri → Şifreleme / Erişim kontrolü / Saldırı tespiti

Hocanın istediği cevap şekli

Şifreleme bilgilerin gizliliğinin ve bütünlüğünün sağlanması amacıyla korunmasıdır

Erişim kontrolü
Saldırı Tespiti ve Önleme Stratejileri (IDS/IPS)

non chalant

Bilgi Güvenliğinin Önemi
Bilgi Güvenliği Uygulamaları ve Sağlama Yöntemleri

Tekrar edilen kısım

Bilgi Güvenliği: Bilginin korunması için uygulamalı önlemler dizisidir.
Bilginin gizliliğini bütünlüğünü ve erişilebilirliğini sağlama sürecidir.

CIA Tria → Gizlilik / Bütünlük / Erişebilirlik

↳ Bütünlük sağlanması güvenlik olarak direnci hale getirir.

Bütünlük → Dijital imzalar
Erişebilirlik → Yedekleme Sistemleri

Doğrulama Yöntemleri (örnek)

Yetkilendirme → Banka çalışanının sadece kendi departmanına erişmesi

Sorumluluk ve İzlenebilirlik.

Risk Yönetimi → Uygun güvenlik önlemlerinin alınma sürecidir.

Veri ve sistemlerin korunması → Hem Fiziksel hem Dijital olarak korunması
Hastane Örneği

Yasal Düzenleyici Uyumluluk → KVK

2. hafta

Cesar Şifreleme , Afi → (Simetrik şifrelemeye girer)

Plaintex
Chipertest
Key
Encryption
Decryption

Simetrik şifreleme (aynı anahtar?) ikili taraf
DES blue fish two fish

Anahtar Yönetimi

Asimetrik Şifreleme

Açık anahtar
özel anahtar

Avantaj / Dezavantaj

RSA ECC ECA

Hibrit Şifreleme

Simetrik Şifreleme: Veriyi şifrelemek ve gizlemek için kullanılır
Şifreyi çözmek için

Asimetrik: Anahtarı dağıtmak ve paylaşmak için

Dezavantajı: Hesaplama maliyeti (işlemci)
Karmaşıklık

Anahtar üretimi ve Şifreleme . Şifre Çözme