## ÖN ŞARTLAR

Eğitime katılacak olanların temel seviyede programlama ve matematik bilgisine sahip, ve terimlere hakim olabilecek seviyede İngilizce bilgisine sahip olması beklenmektedir

## AMAÇ

Kriptografi, günümüzde hem bireysel hem de kurumsal anlamda bilginin korunmasına yönelik çözümlerin temelini oluşturmaktadır. Yapılan uygulamalarda kriptografinin hatalı kullanımı en ciddi güvenlik zafiyetlerinden birisi olarak görülmektedir. Bu eğitim, katılımcıların, hem kriptografi alanında farkındalığını arttırmayı hem de günlük yaşamda kullanıcı ve geliştirici bakış açısıyla kriptografi'nin etkin ve doğru bir şekilde kullanımını sağlamalarını amaçlamaktadır.

Eğitim sonrası katılımcıların;

- Kriptografi ve kriptografiye ait kavramlar hakkında işleyişi kavramış olması,
- Kendi sistemlerinde (uygulamalarda vb. yerlerde) kullanmak üzere kriptografik algoritma lara ve yöntemlere karar verebilecek seviyede olması,
- Güvenlik ayarları konfigürasyonun yapılması gereken durumlarda parametre seçimlerine hakim olması,
- TLS yapılandırma ayarlarını yapabilecek seviyede olması beklenmektedir.

Kriptografinin Temelleri ve Uygulamaları

1- Kriptoloji'ye Giriş

- Sayılar, taban aritmetiği ve mantıksal operatörler
- Kriptoloji Tarihi
- Modern Kriptografi
- Simetrik Kriptografi
- Asimetrik Kriptografi
- Özet Fonksiyonlar
- Mesaj Doğrulama Kodları
- Rasgele Sayı Üreteçleri
- Kriptoanaliz Kavramı

2- Protokoller
- Kriptografik Protokol Kavramı
- Melez Şifreleme
- Elektronik İmza
- Veri Saklama Yöntemleri
- Kablosuz Ağ Güvenliği
- Tek Kullanımlık Parolalar
- Uydu Yayınları Güvenliği
- GSM Altyapısı Güvenliği

3- TLS
- TLS nedir?
- Public-key Pinning
- HSTS
- TLS Kütüphaneleri ve Web sunucularda yapılandırılması (OpenSSL ve Apache Örneği)

4- Günlük Yaşamda Kriptografi Kullanımı
- PGP, Truecrypt, CryptoCat, KeePass vb.
- Yazılımlarda Kriptografi kullanımı