Dersin Adı: Şifreleme

Dr. Öğr. Üyesi Serkan GÖNEN
Mühendislik ve Mimarlık Fakültesi/Bilgisayar Mühendisliği

Ders İçeriği

Bilgi insanlar için her zaman kıymetli olmuştur. Tarih boyunca bilgi; savaşları kazanmak, para kazanmak ve özellikle tarihi şekillendirmek için bir araç olmuştur. Geçmişte, şifreleme (kriptoloji) bilgiyi yalnızca düşmandan gizlemek amacıyla kullanılmıştır. Günümüzde ise teknolojinin, eğitimden0 haberleşmeye, sağlıktan bankacılık işlemlerine kadar hayatımızın her alanına girmesiyle birlikte bilginin güvenliği çok daha önemli hale gelmiştir. Tarih boyunca insanlar birbirleriyle gizli haberleşme ihtiyacı duymuşlar ve bunun güvenilir yollarını aramışlardır. Bu ihtiyacı gerçekleştirmek amacıyla şifreleme (kriptoloji) bilimi ortaya çıkmıştır. Kriptoloji; şifreleme, gönderilen mesajların güvenliğini sağlayan, gönderici ile alıcı arasına üçüncü kişilerin girmesini engellemeye çalışan ve iletilerin güvenliğini sağlayan bilim dalıdır. Bir başka deyişle; anlamlı halde olan iletinin, şifreleme türleri ile araya girmeye çalışanlar için anlamsız hale getirilmesidir. Gönderilen mesajların güvenilirliği; devletlerarası iletişim için, özel kuruluşların güvenliği için, bankaların müşterilerine sunduğu güvenlik için ve daha birçok özel ve devlet kuruluşlarının güvenliği için önem arz etmektedir.

Ders İçeriği devamı:

Kriptoloji kendi içerisinde iki ana türden oluşur. Bu ayrım kullanılan anahtar sayısına göre yapılmıştır. Kısaca açıklamak gerekirse şifreleme ve şifre çözme işlemi aynı anahtar ile yapılırsa buna simetrik, şifreleme ve şifre çözme işlemleri farklı anahtarlar kullanılarak yapılırsa buna da asimetrik şifreleme denir. Diğer bir ifade ile şifreleme ve şifre çözme işlemi aynı anahtar ile yapılırsa buna simetrik, şifreleme ve şifre çözme işlemleri farklı anahtarlar kullanılarak yapılırsa buna da asimetrik şifreleme denir. Bu kapsamda dersimizde kısaca kriptolojinin tarihsel gelişimi belirtilerek, simetrik şifreleme konusu incelenecektir. Genel bilgilendirmenin devamında tarihin ilk kriptolojik teknikleri olarak bilinen Sezar ve Vernam şifreleme teknikleri ile ilgili uygulamalar yapılacaktır.

Öğrenme Çıktıları

Kriptoloji
Kriptolojinin Tarihi
Enigma
Çalışma Prensibi
Enigma Şifresinin Kırılması
Kriptolojinin Kullanım Alanları
Kullanım Amaçları
Bilgisayar Sistemlerinde Güvenlik
Şifreleme Algoritmaları ve Protokolleri
Kriptoloji Türleri
Simetrik Şifreleme
Simetrik Şifreleme Sisteminin Kurulması
Şifreleme
Şifrenin Açılması
Sezar Şifreleme
Vernam Şifreleme

Türkiye'nin en fazla

Uluslararası Akredite

edilmiş programına sahip

Üniversitesi

63 Uluslararası Akredite Program

Gelişime Açık Olun...

İSTANBUL GELİŞİM ÜNİVERSİTESİ

www.gelisim.edu.tr