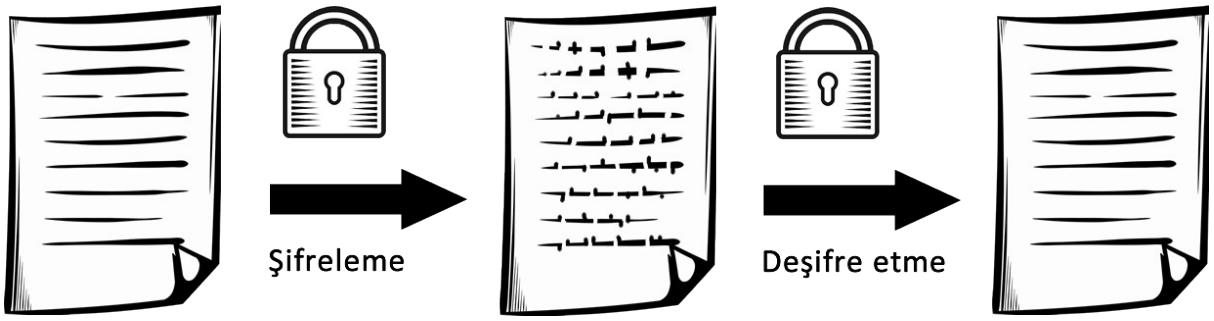
Şifreciliğe Giriş

Terminoloji ve genel bilgiler

Giriş

Tarihi bir perspektiften bakıldığında bilgi güvenliğinin insanlığın var olduğu zamandan beri uygulanagelen ilk örneği şifrelemedir. Şifreleme sadece eski zamanlarda kullanılan bir yöntem değildir. Günümüzde de bilgi güvenliği açısından önemini artan şekilde korumaktadır. Veri ve bilgilerin saklanması ve istenilmeyen kişilerin anlamasını zorlaştırma üzerine yapılan tüm çalışmalar şifreleme bilimi (kriptoloji) olarak adlandırılmaktadır. Kriptoloji kelimesinin, Yunanca “kryptoslogos” yani "gizli kelime" den geldiği literatürde belirtilmiş olsa da dilimize Fransızca “cryptologie” kelimesinden girmiştir. Kriptoloji, Türk Dil Kurumu Sözlüğün’de “gizli yazılar, şifreli belgeler bilimi veya incelenmesi” olarak tanımlanmaktadır. Matematiksel tabana dayanan uygulamalar ve teknikleri üzerinde çalışılan bilim dalıdır.



Şifreleme bir mesajın belirli bir mantıkla anlaşılmaz hale getirilmesi, deşifre etme ise şifrelenmiş mesajın çözülerek anlaşılır hale geritilmesidir. Kullanılan mantık hem gönderici, hem de alıcı tarafından bilinen bir metodu ifade eder. Anahtar ise bu metodu kullanırken deşifreci tarafından ihtiyaç duyulan bilgi olarak tanımlanır.