KRİPTOGRAFİK İŞLEMCİ

Hayatımızın önemli parçası haline gelen ögelerden biri güvenliktir. Güvenli ortamlarda bulunmak, her zaman insanları rahatlatır. Günümüzde gelişen teknolojiyle birlikte, elektronik ortamın güvenliliği de bir sorun haline gelmiştir. Elektronik ortamda istenilen bilgiye ulaşmak gerçek yaşamdan daha kolay hale gelebiliyor. Bilgiyi gizleme, doğru bilgiye ulaşma isteği üzerine elektronik damgalama teknikleri ve güvenliği sağlamak amaçlı çeşitli algoritmalar geliştirilmeye başlandı. Her geliştirilen ürün beraberinde güvenliliğinin sürekli araştırılması ve ispatlanması gerekliliğini getirmiş. Verinin güvenliği için geliştirilen algoritmalarla birlikte kolaylıkla çalışmasını sağlayan özel şifreleme cihazları yani kriptografik sistemler de hayatımızda yer edindi. Bu kriptografik sistemlerin kullanıldığı sim kartlar, cep telefonları, uzaktan kumandalar, online bankacılık, online alışveriş ve uydu alıcıları uygulama alanlarından bazılarıdır

Kriptografik işlemciler, sistemlerde sıklıkla karşılaştığımız işlemleri veya içerisinde bulundurduğu kriptografi algoritmasının gerçeklemesini yapar. Bir kripto cihazı içinde işlenen gizli önemli verinin üçüncü kişiler tarafından kullanılmasını ya da değiştirilmesini engeller. Bahsetmiş olduğum Kriptografi, matematiğe dayalı şifre bilimidir. Kriptografik algoritmalar, veriyi anlaşılamayacak hale getiren bir anahtarla çalışır. Kriptografik işlemciler için gizli tutulması gereken algoritmalar değil anahtarlardır. Anahtar genellikle kişiye özgüdür, paylaşılması kişinin güvenliği için doğru bir hareket değildir. Bu sayede bilgi güvenliğinin temel amaçları olan: gizlilik, bütünlük, kimlik denetimi ve inkar edememe sağlanmış olur.

Anahtar temelli algoritmalar simetrik ve asimetrik olarak ikiye ayrılır. Simetrik algoritmalarda anahtar, hem şifrelemede hem de şifre çözmede kullanılır. Asimetrik algoritmalarda ise şifreleme ve çözme için farklı anahtar kullanılır. Simetrik algoritmalar, asimetrik algoritmalara göre bilgisayarlarda daha hızlı çalışır. Asimetrik algoritmaların en çok bilinen ve kullanılan örneği RSA ‘dır. Simetrik algoritmalarda ise en çok kullanılan DES ve Des ‘in tahtını almaya hedef gösterilen ve geliştirilmiş yeni bir sisteme sahip olan AES’tir.