KRİPTOLOJİYE GİRİŞ

Bir şifre bilimi olarak en basit haliyle tarif edebileceğimiz kriptoloji; iletilerin, mesajların belirli bir şifreleme algoritması kullanarak şifrelenmesi ile bilgi güvenliğini garantiye almayı amaçlayan sistemlerin ilgili olduğu bilim dalıdır. Aslında gizliliğini korumaya çalıştığımız pek çok bilgiyi şifrelemelerle kilit altına alırız. Bu kilit sistemi için de kriptolojiyi günümüzde yaygın olarak kullanırız çünkü kriptoloji içinde pek çok şifreleme algoritması bulunduran bir bilim dalıdır. Burada seçeceğimiz algoritmalar belirli özelliklerine göre seçilip kullanılır.

Kriptografinin ise direkt olarak şifreleme kelimesine karşılık geleceğini söyleyebiliriz. Veri gizliliğinin günümüzdeki öneminin yanı sıra bu güvenliği sağlayan şifreleme teknikleri de o kadar önemlidir. Verilerin gizliliği, bütünlüğü, kaynak doğrulama gibi konuların sağlanabilmesi için şifreleme kilit noktadır. Kriptografik pek çok methotta amaç verinin gizli iletimini sağlayarak aktif ve pasif saldırıları önlemek ve verinin sadece hedefteki alıcıyla paylaşılmasını sağlamaktır.

Bu noktada şifrelemeyle gizli ve okunamaz şekilde yollanan her veri alıcının mesajı algılayabilmesi açısından çözümlenmesi de gereken bir bilgi parçasıdır. Bu bilgiyi çözümlemek için anahtar bilgiye sahip olmak ya da farklı metotlarda şifreyi kırıp bilgiye ulaşmak gerekir. Bu saklı veriye çözücü bir şifre olmadan erişmeyi amaçlayan her yol aslında kriptoanaliz süreçlerine dahildir. Kriptoanaliz kısaca daha farklı çözüm teknikleriyle bilinmeyen anahtarlar bulmayı amaçlar. Kriptografide veriyi gizli tutma, bütünlüğünü koruma, kimlik doğrulama ve inkar edilemezlik ilkelerinin korunmasının tersine kriptoanalizde tek ve bilinen anahtarlardan çok daha fazlasını keşfetmek ve böylece sistem güvenliğini test etmek ve onları kırmak amaçlanır. Yani aslında birbirinin tersine çalışan iki mantıktan söz ediyoruz. Birlikte kullanıldığı zaman üst düzey bir koruma ve güvenlik sağlayabilirler fakat farklı taraflarda da bir saldırma savunma taraflarını da yaratmaktadır. Savunma tarafında iyi bir koruma sağlayabilmek için kriptografi ve kriptoanalizin birlikte çalışabilmesi oldukça önemlidir.

**Kriptolojinin Tarihçesi**

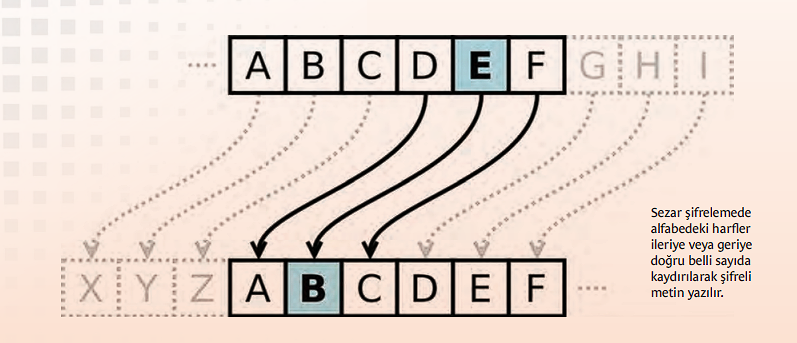
Günümüze kadar veri güvenliği, gizliliği, bütünlüğü, gibi temel ilkeler her zaman hayatımızda vardı. Bunun için hem bilgiyi karşı tarafa ulaştırma hem de diğer insanlardan gizleme iç güdüsü ile insanlar pek çok şifreleme yöntemi geliştirmiştir. Bu şifrelemelerden en eskileri Milattan öncesine kadar dayanır. M.Ö. 1900’lü yıllarda mısır yazıtlarında bazı hiyorogliflerin bilerek değiştirildiği ve şifreli mesajlar olarak kullanıldığını görebiliriz.



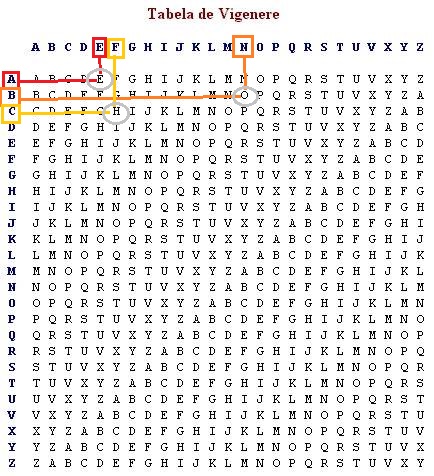
* *Skaytale Çubuğu:* M.Ö. 5. Yüzyıllarına gelindiğinde Spartalı askerler tarafından geliştirilen silindirik bir cihaz ile şifrelenen metinler sadece aynı çapta sarılı olan çubuk ile okunabiliyordu



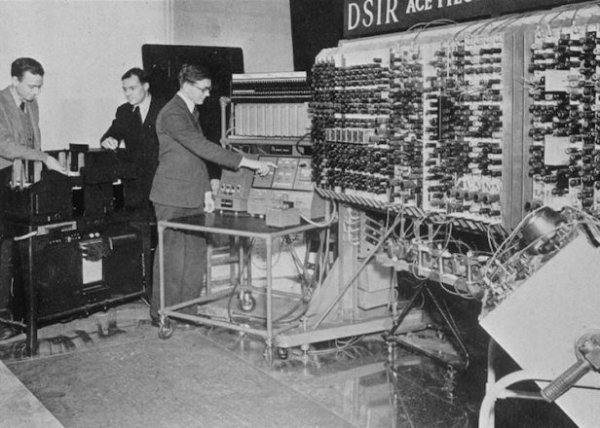
* *Sezar Şifresi (M.Ö. 1900 – M.S. 500*)*:* Roma imparatoru Jül Sezar gönderdiği mektupların ele geçirilmesi ile okunmasını önlemek için harfleri kaydırarak bir şifreleme metodu tasarlamıştır.



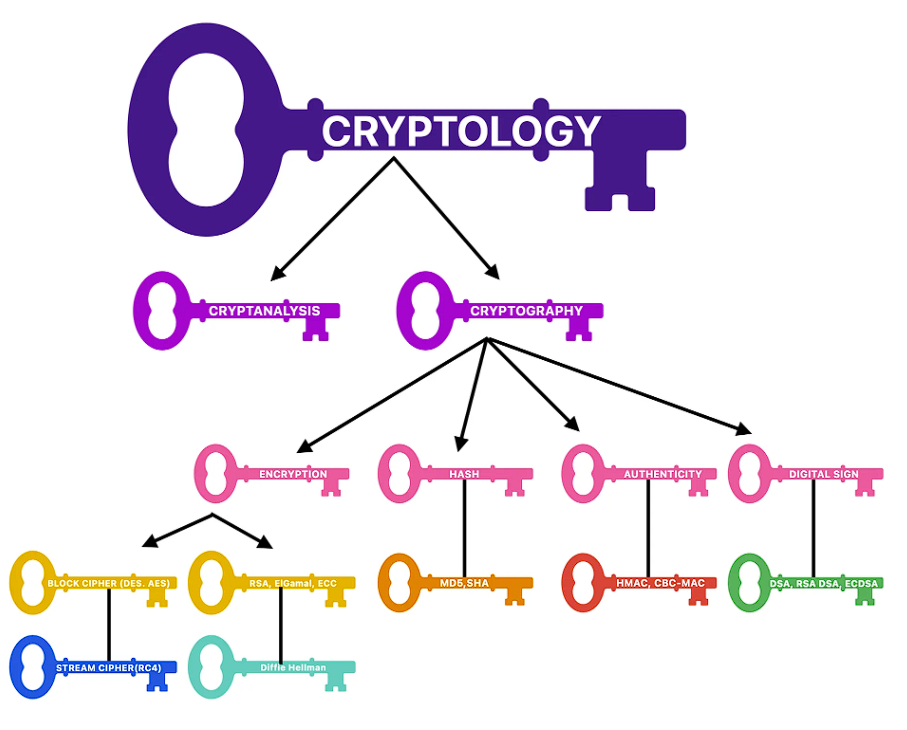
* *Orta Çağ - Frekans Analizi (500-1500):* Ortaçağlara geldiğimiz zaman artık daha gelişmiş şifreleme metodları kullanılıyordu. El-kindi ilk defa sistemli olarak yaptığı kriptoanaliz çalışmalarıyla “Frekans Analizi” yöntemini geliştirmiştir. Bu yöntem Arap harflerinin kullanım sıklığını analiz ederek şifrenin çözülmesini sağlayan bir algoritmadır. Bu sayede klasik şifreleme yöntemlerini de geride bırakıp yeni bir bakış getirmiştir.
* *Rönesans ve Erken Modern Dönem - Polyalfabetik Şifreler (1500 – 1800):* İtalyan bilim insanı Leon Batissa Alberti’nin geliştirdiği Alberti diski ile birlikte polyalfabetik şifreleme sistemi oluşturulmuştur. Bu sistem ile birlikte uzun bir süre çok fazla kullanılacak olan Viegenere şifrelemesine de ışık tutmuştur. 16. Yüzyılda Blaise de Vigenère tarafından geliştirilen Viegenere şifresinin 1800’lere kadar kırılamayacağı düşünülüyordu ve bu yüzden kullanıldığı dönemde diplomatik yazışmalar, anlaşmalar gibi önemli bilgilerin korunması gibi önemli bir roldeydi.



* *Modern Dönem ve Savaşlar (1900-1950):* Kriptoloji özellikle savaş zamanlarında çok fazla önemli hale gelmiştir çünkü savaşta iletişim kurmaya çalışan taraflar ve bu iletişimi deşifre etmeye çalışarak savaşı kendi lehine döndürmeye çalışan taraflar olması sebebiyle şifreleme ile bilgiyi gizli tutmak çok kritik hale gelmiştir. Öyle ki Enigma makinesinin deşifresi ile bir savaşın ne kadar değişebildiği görülebilmektedir. Almanların geliştirdiği Enigma makinesi çok güçlü bir şifreleme yöntemi kullanıyordu. Alan Turing ve ekibinin bu makineyi çözmesi savaşı tamamen değiştirmiş ve karşı tarafı yenilgiye uğratmıştır. Bununla birlikte de elektromanyetik şifreleme makineleri yaygınlaşmıştır.



* Dijital Kriptoloji (1950 – Günümüz): Teknolojinin günümüze kadar ilerleyişi hem kriptografiyi hem de kriptoanalizi geliştirmiştir bu yüzden dijital şifrelemeler kriptoloji ile farklı bir boyut kazanmıştır. Sayıların çokça kullanıldığı ve çok büyük hesaplamaların yapıldığı makineler ve donanımlarla güçlü şifreleme sistemleri oluşturulmaya başlanmıştır. Açık anahtarlı şifreleme, RSA algoritması ile asimetrik şifrelemenin başlaması, DES (Data Encription Standart) kabul edilmesi gibi pek çok gelişme sadece birkaç yılda olmuştur. 2000 sonrası ise DES’in yerini AES ( Advenced Encription Standard) almış ve kuantum kriptografi, Blockchain, ellipptik eğri kriptografisi gibi ileri teknolojiler hayatımıza girmiştir. Halen de pek çok teknolojinin gelişmesine katkı sağlamaya devam etmektedir.



**Kriptolojinin Kullanım Alanları**

Kriptoloji genel olarak bilgi güvenliğinin kritik olduğu her yerde kullanılan bir bilimdir. Günümüzde pek çok yerde kişisel veriler kullanılarak işlemler yapılmaktadır. Bu yüzden özellikle kişisel veri kavramının kullanıldığı her yerde kriptolojiyi görebiliriz.

1. Bankacılık ve Finans İşlemleri: Online banka işlemleri için veri gizliliği oldukça önemlidir. Şifreler, kart bilgileri, kişisel veriler, dijital imzalar vs. bu bankacılık işlemleri için kullanılırken bu verilerin şifreli olarak tutulması büyük önem taşır.
2. İnternet ve Web Güvenliği: Dijital dünyanın temelinde yer alan internet ve web her gün milyonlarca veri akışının bulunduğu bir yer olması sebebiyle bazı kritik verilerin şifrelenmesi oldukça önemlidir. Bunun için HTTPS gibi protokoller, SSL/TLS gibi şifreleme protokolleri, VPN ile veri trafiğinin gizlenmesi, online alışverişlerde kullanılan kritik veriler gibi pek çok bilgi kriptolojiye ihtiyaç duymaktadır.
3. Mesajlaşma ve Uygulamalar: Her gün insanlar birbirleriyle iletişim içerisindeyken birbirine veri aktarmaktadır. Bu verilerin hiçbiri, başkaları tarafından ele geçirilmemelidir. Sadece paylaşımın yapılacağı kişiler arasında uçtan uca şifrelemeler ile bu verilerin güvenliği sağlanmak zorundadır. Bunun için kimlik doğrulamalar, uçtan uca şifrelemeler ile paylaşılan bu verilerin korunmasında yine kriptoloji kullanılır.
4. Askeri ve Siyasi Alanlar: Devletler için bilginin sızdırılmadan korunmasını sağlamak oldukça kritik ve hayati değerler taşır bu yüzden üst düzey şifreleme yöntemlerinin sorunsuz şekilde çalışması ve veri ilkelerinin sağlanması için kriptolojiye ihtiyaç duyulur. Özellikle gizli askeri yazışmalar, diplomatik bilgi alışverişleri, üst düzey teknoloji geliştirme raporları gibi bir devlet için kritik olabilecek her türlü veri yetki alanı dışında kalan herkese kapalı olacak şekilde şifrelenmelidir.
5. Dijital kimlik ve hukuk: Dijital delillerin değiştirilmesi ve yok edilmesini önlemek amacıyla, gizli tutulması ve korunaklı ortamlarda saklanması gereklidir. Bu yüzden muhafaza etmek için şifreli ortamlar kullanılır. Bunun yanında dijital imzalar ve kimlik verileri pek çok işlemi gerçekleştirebilen yetkiler taşıması sebebiyle bu veriler için üst düzey koruma sağlamak önemlidir.
6. Veri Depolama: Bu gün birçok veri bulut sistemlerinde depolanmaktadır. İnsanlar da bu buluttaki verilere kendine ait özel şifreler ve bilgilerle girebilmelidir ki depoladıkları verilerin sızdırılması önlensin. Bu yüzden depolanan veriler için de şifreleme ve kriptolojinin önemi artmaktadır.
7. Blokzincir ve Kripto Dünyası: Günümüzde Bitcoin, Ethereum gibi pek çok dijital para kriptolojik algoritmaların bir ürünüdür. Blokzincir mimarisini oluşturan her bir blok içindeki veriler belirli fonksiyonlar ile birleşerek Blockchain yapısını oluşturur. Bu şekilde şifreleme yapılarak verilerin değiştirilemez ve bütün kalması pek çok insanı Blokzincir çözümlemeleri kullanmaya yaklaştırmıştır.
8. Sağlık verileri, kurumsal şirket verileri, e-posta verileri gibi daha pek çok gizlilik esaslı veri kriptolojinin içinde yer alan şifreleme algoritmalarını kullanarak korunmaktadır. Bu noktada dijitalden güvenli şekilde yararlanabilmek adına dijitali korumak yani verinin gizliliği, bütünlüğü, doğrulanabilmesi ve kişiye özel olabilmesi ilkelerinin arandığı her yerde kriptoloji kullanılır.

**Bilgi Güvenliği Temelleri**

Bilgi güvenliği için dış dünyaya erişimin kapalı olması gereken her türlü verinin korunabilmesi adına bilgi güvenliği ilkelerinin sağlanması çok önemlidir. Bütün bu ilkelerin sağlanabilmesi için ortaya çıkmış algoritmalar ile birlikte kriptoloji bilimi bu ilkelerin sağlanması için en önemli disiplindir diyebiliriz.

Bu ilkeler başlık olarak 3 e ayrılabilir:

-Gizlilik, Bütünlük, Erişilebilirlik.

**Gizlilik (Confidentiality):** Bilgiye ulaşan kişinin sadece yetkili kişiler olması önemlidir. Yetki sahibi olmayan insanların sisteme girmesi gizlilik ilkesinin bozulmasına neden olur. Bunun için bazı önlemler alırız. Örneğin: şifreleme, yetkilendirme ve kimlik doğrulama, erişim kontrol sistemleri, güvenli iletişim protokolleri gibi. Fakat bu önlemlerin de yeterli olmayabileceğini ve bir zaafiyetin her zaman çıkabileceğini unutmamak gerekir. Bu yüzden MFA, Captcha gibi ek önlemler ve bilginin kritiklik seviyesine göre daha fazlası her zaman düşünülmelidir.

**Bütünlük (Integrity):** Bilginin orijinalliğinin korunması, yetkisiz değiştirilmeye kapalı olması, tamlığının bozulmaması şeklinde açıklanabilir. Bilgi kolayca manipüle edilebilmesi sebebiyle yetkilendirmenin doğru yapılması ve bu yetkilere dışardan herhangi birinin erişebilmesini önlemek önemlidir. Bu noktada verilerin orijinal kalmasını kontrol altında tutmak önemlidir. Bunun için hash fonksiyonları, dijital imzalar, versiyon kontrolleri, dosyanın bütünlüğünün denetimi gibi pek çok kontrolün özellikle şüpheli durumlarda yapılması gerekir. Hash fonksiyonu en çok kullanılan yöntemler arasındadır çünkü her dosyanın veya uygulamanın kendine ait bir hash değeri bulunmaktadır. Yapılan en ufaklık değişiklikte bile bu hash değeri değişeceğinden dosyada bir değişiklik yapıldığını anlayabiliriz.

**Erişilebilirlik (Availability):** Bilgiye ve hizmete istendiği zaman kesintisiz ulaşılabilmesi. Günümüzde pek çok sunucu tarafından kesintisiz hizmet alabilirken bazı durumlarda bu hizmetin kesintiye uğraması sağlayıcıyı ve hizmet alan kişiyi mağdur edebilir. Bu, sunucuda yaşanan teknik problemlerden veya ağa yapılan servis dışı bırakma ataklarından kaynaklanabiliyor olabilir. Bu yüzden kesintisiz hizmet sağlanabilmesi için sunucunun ve ağın yedeklenmesi, DoS ve DDoS saldırılarına karşı önlem alma, sistemin belirli aralıklarla bakımdan geçmesi ve olası kriz anlarında kurtarma planları hazırlanması oldukça önemlidir.

EK OLARAK: Modern bilgi güvenliği ilkelerinde bu temel ilkeler üstüne ekleyebileceğimiz ilkelere örnek olarak da şunlardan bahsedilebilir:

* *Kimlik Doğrulama:* Kullanıcının gerçekten o kişi olup olmadığının sorgulanması için yapılan doğrulamalardır. Kullanıcı adı, şifre, çok faktörlü doğrulama örnek olabilir.
* *İnkar Edilemezlik:* İşlemi yapan kişinin (eğer gerçekten o kişiyse) bunu yalanlayamaması ve inkar edememesidir. Eğer her şey hukuka uygun şekilde yürüyorsa yaptığı işlemlerinin sorumluluğu yine kendinde olacaktır.