SAYISAL SİSTEMLERDE VERİ GÜVENLİĞİ - I
KLASİK KRİPTOGRAFİ – TEMEL KRİPTOSİSTEMLER

Özgür SAVAŞ*

Kadromuzun geleceğe dönük en iddialı ve devrimci açılımlarından biri olan "sayısal devlet" konusunda bize yöneltilen en yaygın soru sistemin güvenliği üzerinedir. Günümüz teknolojileri bu ihtiyacımıza cevap verecek durumdadır. Veri güvenliği en basit anlamda iki şekilde sağlanır (bu yöntemler ayrık değil bütünleşiktir yani bir arada kullanılır). Bunlar dolaylı-dışsal koruma ve doğrudan koruma olarak ayrılabilir. Dolaylı dışsal koruma veriye erişim yolunun engellenmesi üzerine kurulmuştur. Sayısal güdümlü piyasa sisteminde verinin aynı zamanda sayısal ortamda para anlamına geldiğini ya da sayısal bilgi sisteminde bir bireyin kişisel bilgileri olduğunu düşünürsek veriye erişimin kritik olduğu açıkça görülebilir. Dışsal korumaya örnek olarak ağ güvenliği kriterleri, donanımsal ve yazılımsal güvenlik duvarı (firewall), erişim ve saldırı tespit sistemleri veya ana ağ geçit yönlendiricileri üzerinde tanımlı çeşitli erişim kontrol filtreleri verilebilir (ileriki sayılarımızda bu yöntemler incelenecektir). Doğrudan koruma olarak sınıflandırabileceğimiz sistem ise verinin kendisi üzerinde yapılan değişikliklerle en kötü durum senaryosu halinde aktarım sırasında verinin ele geçirildiği durumda dahi kullanılabilir olmaması üzerinedir, yani şifreleme-kriptolama yöntemiyle verinin orijinal halinden farklı olarak aktarılması ve alıcı tarafta tekrar eski haline döndürülmesi. Bu yöntemler daha çok haberleşme sistemleri için geliştirilmiş olmakla beraber günümüzde her tür veri güvenliği amacı ile kullanılabilmektedir. Bu sistemler üzerine ayrıntılı bir teknik inceleme mesleki uygulama ve araştırma kapsamına gireceği için bu yazı dizimiz boyunca yalnızca okuyucularımıza basit anlamda veri ve iletişim güvenliği hakkında genel olarak bilgilendirme amacını güdeceğiz. Yazılarımızın ilkinde kriptografi üzerine fikir vermek amacıyla günümüzde kullanılan 3-DES, AES, DES gibi karmaşık kriptosistemlerin temelini oluşturan temel kriptosistemler üzerine bir inceleme yapacağız.

Klasik kriptografinin geçmişine baktığımız zaman binlerce yıl öncesinde Mısır'a, Babil'e, Asur'a kadar ulaşmak mümkün. Buradaki örnekler pek şifreleme çalışmaları olarak düşünülemese de M.Ö 2000 yıllarında hiyeroglifler ile yazılı iletişimin semboller üzerinde

* *Bilgisayar Mühendisi*

sağlanmış olması tarihçiler tarafından Mısır hiyerogliflerinin ilk protokriptogtafik pratikler olarak kabul edilmesine neden olmuştur. Kronolojik bir inceleme yaparsak ilk şifre kelimesine aslında Arap tarihinde rastlanmaktadır. Öyle ki zaten şifre kelimesi arapça 'hiçbir şey' anlamına gelen 'sifr' kelimesinden türetilmiş ve batı terminolojisine de 'cipher' olarak girmiştir. Kripto kelimesi ise 'şifrelenen, gizli, saklı şey' anlamına gelen Yunanca 'kryptos' kelimesinden türetilmiştir. Araplar'ın matematik ve bilimde en üst seviyede olduğu 5-6. yüzyıllarda ortaya çıkan bu kavram 7. yüzyılda batıya gelmiş, buradaki çalışmalarla temel bir sistematiğe oturmuştur. Kriptolojinin yaygınlaşmasını sağlayan etken olan 'şifreli haberleşme' konusunda bulunan ilk örnek ise Spartalılar tarafından yapılan 'skytale' adı verilen cihazdır. Bu cihaz odun üzerine sembollerin işlenip çeşitli şekillerde yerleştirilerek farklı anlamların çıkarılabilmesi esasına göre çalışmaktadır. Bu örnekler bize hemen hemen aynı dönemlerde çeşitli uygarlıklarda bu tip etkinliklerin var olduğunu göstermektedir. Daha sonraki yıllarda kriptoloji Yunan ve Perslerin çalışmalarıyla ilerlemiş, Rönesans dönemi kilise etkinlik çevrelerinde yaygınlaşmıştır. 17. yüzyıla geldiğimiz zaman batıda bugün kullanılan bir çok temel kriptosistemin oluştuğunu, sanayi çağı ve Birinci Dünya Savaşı ile bir çok ilerleme kaydedildiğini söylemek mümkündür. Kriptoloji konusunda dünya tarihinin dönüm noktası ise İkinci Dünya Savaşı olmuş Hitler'in bilim adamlarınca geliştirilen nitelikli kodların İngilizler tarafından çözülmesiyle savaşın rengi değişmiştir [1]. Günümüzdeki kripto kodları geçmişten izler taşısa da daha çok matematiksel çözüm zorluğu olan büyük sayıların faktorizasyonu ve ayrık logaritma gibi problemler üzerine oturtulmuştur. Başta da söylediğimiz gibi bu yazımızda tüm okuyucularımızın rahatlıkla anlayabileceği yüzyıllardır kullanılan en basit alfanümerik veri haberleşmesini şifreleyen kriptosistemlerden bahsedeğiz. Kriptosistemlerin seçilmesinde [2] numaralı kaynak kullanılmıştır.

EK BİLGİ: Kriptosistemlerin incelenmesine geçmeden önce ek bir bilgi olarak sayısal bir sistemde rakamların yanı sıra harflerin de nasıl barındırıldığı üzerine bir bilgi vermemiz uygun olacaktır: Sayısal sistemlerde (bilgisayarlar, sayısal haberleşme hatları vs.) her sembole karşılık bir bit dizisi karşılık düşürülür, her bir bit ise bir elektriksel işaret ya da seviye olarak barındırılır. 1 değerini temsil etmek için bir kondansatörün plakaları arasındaki potansiyel yük, elektriksel voltajın belli bir değeri ya da ışığın 'var' durumu kullanılabilirken, 0 değeri için tam tersi durum kullanılmaktadır. Bir sembolün sistemde temsil edilebilmesi için ona karşılık atanan 8 bitlik dizinin elemanlarının değerleri kullanılır. Bilgisayar sistemlerinde bitlerin reel karşılığının temsili için ikilik sayı düzeni (gerçekte sadece 0 ve 1'ler vardır) kullanılırken bilimsel kolay temsili için 16'lık sayı düzeni kullanılır. Buna göre 'A' harfinin karşılığı 16'lık sistemde '65' iken buna karşılık düşen 10'luk sistem değeri '101', ikilik dizi ise '01100101' olmakta ve sistemde 'A' karakteri bu şekilde saklanmakta ve iletilmektedir.

Öteleme Şifresi

Bu şifreleme yönteminde her bir karaktere karşılık düşen değere belli bir değer eklenerek farklı bir sayı ile temsil kullanılmaktadır. Hesaplarımızı kolaylaştırması açısından her bir harfimizi alfabetik düzendeki yerleri ile temsil edelim yani A=1 olsun. Öteleme şifresinde bu 1 değerine herhangi bir değer eklenerek A'ya karşılık yeni bir değer düşürülür ve o harf A'nın yerine kullanılır (alfabede 29 harfimiz olduğuna göre toplama işlemi modüler olarak yapılacaktır yani toplam 30 olursa anlamı 30-29=1, 35 olursa 6 olacaktır). A= 1, öteleme miktarı= 14, yeni değer= 15, buna karşılık düşen harf= L ise elimizdeki metinde A geçen yerlerde onun yerine L kullanılacaktır. Burada L bizim enkript edilmiş verimiz olmaktadır.

Bu sistemin uygulaması da çözümü (kriptanalizi) de oldukça kolaydır. En basit yöntem deneme yanılma yöntemidir. Buna göre 1'den 29'a kadar olan tüm kayıklık (öteleme) değerleri için elimizdeki metni çözeriz, anlamlı bir metin elde ettiğimiz zaman çözüme ulaştığımız anlamına gelir.

Yerine Koyma Şifresi

Bu şifreleme yöntemi gazetelerin bulmaca eklerinde her zaman rastladığımız ve kolaylıkla çözdüğümüz her harfe karşılık bir sayının verildiği sistemle aynıdır. Burada her harfin yerine başka bir harf karşılık düşürülmekte ve metin bu şekilde karmaşıklaştırılmaktadır. Örneğin A harfinin yerine M, G harfinin yerine C gelecek şekilde tüm harfler başka bir harfle temsil edilmektedir.

Bu sistemin kriptanalizi de kullanılan dile göre oldukça kolay olmaktadır. Örneğin Türkçe'de en çok kullanılan harf 'A' harfidir, yani bir metin içerisinde en sık karşılaşılan periyodu en düşük (frekansı en yüksek) harf 'A'dır. O halde eğer iletilmek istenen metin Türkçe ise içerisinde en çok geçen harf onun yerine kullanılan M olacaktır, böylece en sık kullanılan harfler rahatlıkla bulunabilecektir. (Türkçe'deki harflerin frekansları konusunda bilimsel çalışmalar mevcuttur ancak bu yazıyı hazırlarken bu kaynaklara erişemedik). Diğer harfler ise bulunan harflerin yerine konulmasıyla anlamlı sözcük takibi ya da sık tekrarlanan grupların incelenmesiyle bulunabilecektir. Örneğin İngilizce'de (maalesef Türkçesi elimizde yok) en sık tekrarlanan harf grupları 'and' 'the' ve 'ed' dir. O halde bu harflerden bir ya da birkaçının bulunmasıyla gruplar bulunacak ve kriptometin büyük oranda çözülebilecektir.

Vigenére Şifresi

Bu şifreleme yönteminde gönderici tarafından bir anahtar kelime belirlenmekte ve tüm metin sıra ile bu şifrede denk düşen harf ile toplanarak yerlerine yeni bir değer elde edilmektedir. Örneğin, metnimiz NEMUTLUTÜRKÜM ve anahtar kelimemiz de KEMAL olsun. Metnimizdeki ve anahtarımızdaki harflerin sayısal değerlerini yerlerine koyalım ve taraf tarafa toplayalım (mod 29) ve şifrelenmiş metni elde edelim;

N=17, E=06, M=16, U=27, T=24, L=15, U=27, T= 24, Ü= 26, R=21, K=14, Ü=26, M=12

K=14, E=06, M=16, A=01, L=15, K=14, E=06, M=16, A=01, L=15, K=14, E=06, M=16

+----------

B=02, İ=12, C=03, Y=28, B=02, Z=29, G=04, Ğ=09, U=27, F=07, Y=28, D=05, Y=28

Bu durumda kriptometnimiz BİCYBZGĞUFYDY olmaktadır. Vigenére şifresinin kriptanalizi önceki sistemler kadar kolay değildir, bunun için hem sezgisel yöntemler hem de matematiksel işlemler gerekir. Burada yerine koyma şifresinde olduğu gibi gruplar incelenmektedir. Bunun için kriptometne bakılır. Burada birkaç yerde rastlanan harf grupları incelenir. Örneğin 4 yerde aynı 3'lü harf grubununun tekrar ettiği gözlensin. Eğer bu gruplar arası mesafe bir tamsayının katları ise bu gruplar o dilde sık tekrar eden gruplara karşılık seçilen anahtarın aynı harflerinin tesadüf ettiği gruplar demektir. Öyleyse seçilen anahtar sözcüğün uzunluğu bu gruplar arası mesafelerin ortak katlarının en büyüğüdür. KEMAL örneğinde bu değer 5'tir. Bu değeri bulmak için Kasisti testi denen çok etkili bir matematiksel yöntem de kullanılabilir. Anahtarın uzunluğun bulunmasından sonra ise harflere ait karşılaşma indeksi değerleri bulunur, olasılık dağılım fonksiyonlarının hesaplanması ve bunların ideal frekans değerleri ile karşılaştırılması ile metin çözülebilir.

Şimdiye kadar açıkladığımız üç kriptosistem basit aritmetik ile gerçeklenmekte ve ancak kriptanaliz esnasında fonksiyon işlemlerine ihtiyaç duyulmaktadır. Sıradaki üç

yöntemimiz ise basit polinom ve permutasyon fonksiyonları ile gerçeklenmektedir, fikir verme açısından kısaca bu üç temel yöntemi de açıklayacağız.

Affine Şifresi

Affine şifresi de mantık olarak önceki şifrelere benzemektedir. Yani her bir harfin yerine bir diğer harfin koyulmasıyla metnin şifrelenmesi amaçlanmaktadır. Bu işlem gerçekleştirilirken doğrudan bir karşı sayı belirlemek yerine bir fonksiyon kullanılmaktadır. Alıcı taraf ise bu fonksiyonun tersini hesaplayarak gerçek değeri rahatlıkla bulabilmektedir. Örneğin gönderici A harfine karşı düşen değeri belirlemek üzere *f(x)= 7x+3* fonksiyonunu kullansın, yani A yerine *7*1+3=10* değerine sahip H harfini göndersin. Gönderici karşıya A'ya karşılık düşen değer olan H polinom katsayıları olan *(7,3)* çiftini göndermektedir. Alıcı ise bu fonksiyonun tersinde 10 değerini yerine koyarak gerçek değer olan A'ya karşılık düşen 1 değerini bulabilecektir. Bu yöntemin kriptanalizi oldukça kolaydır. Metinde en çok geçen iki harf alınarak iki bilinmeyenli iki denklem çözümünden kolayca ana fonksiyon elde edilebilir.

Permutasyon Şifresi

Permutasyon şifresinde izlenen yöntem öncekilerden farklı olarak yerine koyma değil yer değiştirmedir. Buna göre belirlenen bir permutasyonun değerleri kullanılarak metin alt bölümler halinde yer değiştirilecektir. Örneğin, metnimiz BAŞKENTANKARA ve permutasyonumuz: *P(1)= 3, P(2)= 5, P(3)= 1, P(4)= 6, P(5)= 4, P(6)= 2* şeklinde olsun. Bu durumda ilk 6 harf kendi içinde yer değiştirecektir yani 1. harfin yerine 3., 2. harfin yerine 5. vb. Öyleyse şifrelenmiş metnimiz şu şekilde olmaktadır: ŞEBNKANATRKAA. Permutasyonun tersten uygulanması ile şifre kolaylıkla çözülebilmektedir.

Hill Şifresi

Hill şifresinde de permutasyon şifresinde kullanılana benzer bir yol izlenmektedir ancak farklı olarak harfler kendi aralarında yer değiştirmek yerine metin alt gruplara bölünerek önceden belirlenmiş anahtar matrisler ile işleme tutularak yerlerine yeni değerler elde edilmekte böylece her bir alt gruba karşılık yeni bir alt grup elde edilmektedir. Bu yöntemin kriptanalizinde de farklı alt karakter grupları için değişik polinom boyutlarının denenmesi ile anahtar matrislerin tespiti kullanılmaktadır. Anahtar matris tespit edildikten sonra bu matrisin tersi ile her bir alt grubu işleme tabi tutma sonucu gerçek gruplar elde edilecektir.

Sonuç olarak; sayısal bir sistemin sayısal para, sayısal kimlik gibi tüm hatlarıyla kullanılabilmesi için veri güvenliği Kemalistlerin önünde duran en önemli meselelerden biridir. Günümüz teknolojisi büyük anlamda ihtiyaçları karşılamakta ancak gelecekte gerçeklenebilecek yeni sistemler de Kemalistlerin ilgisi dahilinde bulunmaktadır. Bu yazımızda yüzyıllardır kullanılan en basit şifreleme yöntemlerine örnekler vererek şifrelemenin mantığı ve veri güvenliği konusunda okuyucuyu fikir sahibi yaptığımızı umuyoruz. Günümüz gerçek kriptosistemlerinde bu yöntemler her ne kadar artık kullanılmıyor olsa da mümkün olduğunca yazı dizimizin ileriki sayılarında yer vermeyi düşündüğümüz gelişmiş kriptografi yöntemlerinde ve veri güvenliği uygulamalarının anlaşılmasında bu yöntemler yardımcı olacaktır.

KAYNAKLAR

1-Wrixon, F. B.; "Codes Ciphers & Other Crytic and Clandestine Communication"Könemann Pub.; New York; 1998.

2- Stinson, D. R.; "Cryptography Theory and Practice"; Chapman-Hall/CRC Press. New York; 2002.