ASAL SAYILAR-II

ASALLAR VE ŞİFRELEME

İnsanoğlu sayıları keşfeti, 4 işlemi buldu ve asal sayıyı tanımladı. O günden beri de kaygısızca asal sayıların peşinden koştu çünkü ortada cevaplanması gereken birçok soru vardı. Sorulardan kiminin cevabını hemen buldu, kiminin cevaplanamayacağını ispatladı, bazılarıysa hala yanıtsız. İşte bu nedenle insanoğlu hala asal sayıların peşinde. Üstelik en temel sorulardan biri olan "verilen bir sayı asal mı, değil mi? Değilse asal çarpanları nelerdir ve nasıl bulunur? " sorusuna hala cevap arıyor. Ama gerçek şu ki bu soruya istenildiği türden bir cevap bulunduğu zaman güvenliğimiz tehlikeye düşebilir.

Asal Olmak ya da Olmamak

Her geçen gün bir sayının asal olup olmadığını anlamak için ya da asal olmayan bir sayının asal çarpanlarını bulmak için yeni yeni algoritmalar geliştiriliyor. Bir sayının asal çarpanlarının mümkün olduğunca çabuk bulunmasını hedefleyen bu yöntemler elbetteki bilgisayarlarla yapılıyor. Fakat bu iş biraz zaman alıyor. Burada geçen "biraz" gibi belirsiz bir zaman ifadesinin tam olarak neyi kastettiğini açıklamadan önce başından beri akıllarda soru işareti bırakan konuya bir dönelim. Sayıların asal çarpanlarını bulmak yetmiyormuş gibi bir de bunu kısa sürede yapmaya çalışmak neden bu kadar önemli? Sadece asal sayıların popülaritesi mi konuyu bu noktaya taşıdı dersiniz. Ne de olsa anlaşılması kolay sorular toplumda çok çabuk yayılıp popüler oluyor. Fermat'ın son teoreminin Riemann hipotezi ya da Poincaré Sanısı'ndan daha çok biliniyor olması bu görüşü destekleyen bir fikir olabilir. Asal sayıların da çekiciliği anlaşılması oldukça basit tanımından ve yüzyılları peşinden sürükleyen ifadesi basit ama çözülmek bilmez inatçı sorularıdan geliyor olabilir. Ama doğrusunu isterseniz işin içinde (artık) meraktan daha fazlası var. Çünkü asallar 1977'den beri şifrelemenin bel kemiği, şifrelemeyse banka hesaplarımızdan tutun da ulusal güvenliğimize kadar gizlilik içeren her türlü konunun güvenliğinin temeli.

İmparator Sezar'ın Şifresi

Aslına bakarsanız kimi bilgileri saklama gereği de insanlık tarihi kadar eski. Platonik aşkınıza yollayacağınız ama yanlış bir kişinin eline geçmesinden çekindiğiniz için şifre ile yazdığınız mektup, ya da kimsenin okumasını istemediğiniz günlüğünüzü sadece sizin bildiğiniz bir şifre ile yazmanız bu konuyu örneklendirebilir. Bilinen ilk şifreleme örneğine M.Ö. 1900'lerde Mısırlıların hiyeroglif yazısında rastlanır. Daha sonra M.Ö. 100 civarlarında meşhur Roma imparatoru Sezar'ın şifresi ile karşılaşıyoruz. Sezar'ın generalleri ile güvenli bir iletişim kurmak için kullandığı şifrede savaş meydanındaki generallerine gönderdiği mesajlar yine harflerden oluşuyordu. Ama her harf aslında başka bir harfi simgeliyordu ve bunu ancak generaller biliyordu. Örneğin alfabenin harflerin bir harf geri kaydırın. Z, A yı temsil etsin, A'da B'yi. ABC demek istediğinizde ZAB yazın. Bu şifreyi kırmak sadece generallere mahsus değildir. Sıkça tekrarlayan harfler ya da kelimeler şifreyi ele verebilir. Yine de o zamanın ihtiyacını karşılamayı başarmış olduğunu söyleyebiliriz.

Herşeyin Başı Güvenlik

Siz bir komutan olsanız nasıl bir şifreleme tercih ederdiniz? İmparator Sezar zamanından günümüze kadar geçen 2000 yılda değişen çok şey oldu elbette. Bunlardan biri de iletişim sistemleri. Bugün düz metinlerimizi (mektuplarımızı) ulakla göndermek yerine elektronlarla gönderiyoruz, ne de olsa birkaç 1000 zaman hızlı oluyor. Ama mektubunuz ne yolla giderse gitsin, ulusunuz için hayati önem taşıyan bilgiler içeren bu metinlerin yanlış kişilerin eline geçmeden, ulaşması gereken yere güvenli bir biçimde ulaşmasını sağlamak yine general olarak sizin sorumluluğunuz. Fakat gelin görün ki gözle görülmeyen bu elektronları korumalar tutup korumak, tutsak olmalarını engellemek gibi somut önlemlerden bahsetmek olanağına sahip değiliz. İşte bu noktada kullandığımız aletin yani bilgisayarın doğasına dönüp onun yapısına uygun bir koruma sistemi geliştirmek gerektiğini farketmek gerekir ki bu da artık güvenliği sağlayan ve insanı güçlü kılan öğenin aslında bilgi olduğunun farkına varma zamanının geldiğinin habercisidir.

Simetrik Şifreler

Diyelim ki karşı tarafa bir mesaj yollayacaksınız. Ama kimsenin eline geçmemesi gerekiyor. Bir yolu şu olabilir. Sezar şifresi örneğinde olduğu gibi, karşı tarafla mesajlaşmaya başlamadan önce bir toplantı yaparsınız ve kullanacağınız şifreye karar verirsiniz. Böyle iki tarafın da şifreyi bilmesi simetrik şifreleme örneğidir.

Örneğin alfabenin her harfini bir sayı ile eşletirirsiniz.

A:12,B:13;C:14;D:15;E:16;F:17...

Bu durumda FEDA kelimesini göndermek istediğinizde 17161512 sayısını yollamanız güvenlidir çünkü bu sayı karşı taraftan başka hiç kimseye anlamlı gelmeyecektir ki istenen de budur. Fakat şifreniz bir şekilde yanlış kişilerin eline geçerse her şey biter! Kaldı ki her zaman şifre konusunda ortak bir karara varmak için toplantı yapmak mümkün olmayabilir. Üstelik konu iki kişi değil de daha çok insan arasında iletişim olunca şifreyi bilen bir o kadar da insan olması gerekir ki durum gittikçe tehlikeli olmaya başlar.

Asimetrik Şifreler

1960'lara kadar simetrik şifrelerle idare edilmeye çalışılmış olsa da daha güvenli bir şifreleme sistemine şiddetli bir şekilde ihtiyaç duyulmaktaydı. Peki bunun yolu ne olabilirdi? Aslında burada durup biraz düşünürseniz akılcı bir yol bulabilirsiniz. Nasıl uygulamaya koyacağınız kaygısı gütmeden hayal gücünüzün sınırlarını aşın. Zaten bilim adamları da öyle yapmış. İlk bakışta ütopik gibi de görünse de oldukça güvenli olduğu hissedilen şöyle bir yol düşünmüşler.

"Öyle bir şifre olsun ki onu çözecek anahtar sadece benim elimde olsun. Mesajları bana, benim istediğim gibi şifreleyip yollasınlar. Ama ne mesajı

gönderen, ne de onu gören kişi şifreyi kırabilecek yetiye sahip olsun. Ben kendime ihanet etmediğim sürece de kimse şifreyi öğrenemesin"

Dedik ya hayal gücü sınırsız. Ama bilim adamlarının aklına bir fikir düşmeyegörsün. Onu gerçekleştirmek için gece gündüz çalışır yine de başarırlar.

Ve Asal Sayılar Sahneye Çıkar...

Belki de bilimin olağanüstü yanlarından biri de cevabı bulunmamış soruları bile ziyan etmeyip onlardan faydalanabilmesidir. Yazımızın başında bahsettiğimiz "bir sayının asal çarpanlarını en çabuk nasıl bulunuruz" sorusunun istenildiği gibi cevaplanmadığını hatırlayın. Yani en azından 70'lerde bu böyleydi. Ve yine o yılları göz önüne alırsak çarpanlara ayırma işlemi bin yıllarla hesaplanan sürelere varabiliyordu. Elinize çok büyük -örneğin her biri 100'er basamaklı- 2 asal sayı alın. Bu iki sayının bugün bile asal olduğunun anlaşılması günler alabilir ama ikisini birbiri ile çarparsanız oluşacak yaklaşık 200 basamaklı sayının çarpanlarının bulunması aylar ya da yıllar alacaktır. Kullanılan algoritma ve harcanan para bu süreyi biraz değiştirse de sonuç yine istendiği kadar hızlı olmayacaktır.

Elde var 2 asal

1977'de Rivest, Shamir, Adleman adlı bilim adamları başkalarının kolay kolay çarpanlarına ayıramayacağı sayıyı ilan edip çarpanları yalnızca mesajı alacak kişinin bildiğini temel alan güvenli bir algoritma yazmayı başardılar. Böylece "*Öyle bir şifre olsun ki onu çözecek anahtar sadece benim elimde olsun"* hayali gerçek olmuştu çünkü artık sadece sayının asal çarpanlarını bilen kişi metni okumaya hak kazanıyordu. Fikir temel olarak bu olsa da konu hala biraz soyut görünmekte. Bu problemi çözmek için de en iyi yol basit bir örnek görmekten geçiyor. Örnek basit olsun diye elimize küçük 2 asal sayı alalım. Sizler hangi 2 asalı seçeceğinizi düşünürken bilgisayar hakkında ufak birkaç bilgi hatırlayalım.

ASCII:Her Harf Bir Sayı

Simetrik şifreleri hatırlayın; her harfe bir sayı atamış harfleri yanyana dizmek yerine sayıları dizmiş ve FEDA kelimesini uzun bir sayı dizisi haline dönüştürmüştük. Bilgisayarda da her harf, her simge, hatta boşluk bile bir sayı ile eşleştirilir. ASCII kodu olarak bilinen bu kodlar her bilgisayarda aynıdır ve 000 dan 255'e kadar her simgenin 3 basamaklı bir karşılığı vardır. Bilgisayar bünyesindeki bir metni önce bu kodları kullanarak uzun bir sayı dizisine çevirir. Örneğin FEDA'nın karşılığı:

070069068065

ASCII

+	0	1	2	3	4	5	6	7	8	9
30				!	"	#	$	%	&	'
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

Şifreden Deşifreye

Kısa olması için A:1;D:2;E:3;F:4 şeklinde bir kodlama kullanalım. FEDA:4321 sayısına dönüştü. Seçtiğimiz 2 asal da p=2 ve q=5 olsun ki çarpımları pq=10. Algoritma kurallarımız şöyle diyor:

Önce **A**=(p-1)(q-1) çarpanını hesaplayın:

A =(2-1)(5-1)=4

A ile ortak böleni olmayan ve 10'dan küçük bir sayı seçin:

örneğin **e**=7

Sonra **e** x **d** = 1(mod **A**) denkliğini sağlayan d sayısını bulun:

d=3 [7 x 3=1(mod4)]

Metni bize gönderecek kişiye ve herkese ilan ettiğimiz bilgi 2 asalın çarpımı(10) ve aklımızdan seçtiğimiz e(7) sayısı. İstediğimiz şifre ise metnin karşılık geldiği sayının e dereceden kuvvetinin mod pq sayısında eşiti. Yani 4321 için:

4^7= 4(mod10)

3^7= 7(mod10)

2^7= 8(mod10)

1^7= 1(mod10)

İlan ettiğimiz 7 ve 10 sayısı ile bize FEDA metni içi gönderilecek olan şifre 4781. Geriye, gönderilen bu şifreyi deşifre etmesi kaldı. RSA Algoritmanın bu son kısmı da şireyi çözme kodumuzu açıklar: gönderilen şifrenin d dereceden kuvvetinin mod pq sayısında eşiti

4^3= 4(mod10)

7^3= 3(mod10)

8^3= 2(mod10)

1^3= 1(mod10)

Sonuç olarak elimize 4321 kalır ki bunu yukarıdaki kodlarımızı kullanarak FEDA şeklinde çevirmekle deşifreyi tamamlamış oluruz (unutmayın gerçekte herkesin kullandığı standard kod ASCII kodlarıdır).

Özetle iki asal sayımızın çarpımını ve seçtiğimiz e sayısını herkese duyurduk. Sadece asallarımızı ayrı ayrı bilerek hesapladığımız d sayısıyla da şifreyi çözdük. İşte bu nedenle bu çözümü asalları bilmeyenler yapamayacaklardır. Asalların hesaplanma süresi kısalmadıkça da RSA güvenli bir metod olmaya devam edecektir.

RSA Algoritmasının Kaynağı

Bu algoritmanın çalışmasının temelinde Euler ve Fermat'ın henüz bilgisayarın b'sinin ortada olmadığı yıllarda ürettikleri teoremler yatar. Euler-Fermat Teoremi şöyledir:

p asal ve $n \neq 0$ olmak üzere $n^{p-1}=1(\text{mod } p)$

Bu teorem ile RSA algoritmasının çalışması arasındaki ilişkiyi kurmak da okurumuza kalsın...

Çarpanlara Ayırmada son Gelişmeler

Büyük bir sayıyı çarpanlarına ayırma işleminde bütün işi bilgisayar yapıyormuş gibi gözüksede gerçekte durum öyle değildir. Asıl işi yapan, süreyi uzatıp kısaltan algoritmadır. Örneğin 100 basamak için tutup da sayının kendinden küçük her sayıyı bölüp bölmediğini kontrol etmeye kalkarsanız torunlarınızın torunları bile sonucu öğrenemeyebilir. Uzun süredir üzerinde çalışılan bu alanda 2002 yılında 3 Hintli bilim adamı Agrawal (ve doktora öğrencileri) Kayal ve Saxena kısa zamanlı bir algoritma üretmeyi başardılar. RSA metod yine de hala güvenli. Çalışmalar ilerleyip çarpanlara ayırma süresi beklenen ölçüde kısalırsa yeni metodlar da üretileceğinden şüpheniz olmasın. Belkide bilim adamları şu sıralar şifresini kimsenin hatta kullanıcının bile bilemeyeceği bir güvenlik programı peşinde koşuyorlardır, ne dersiniz?

Nilüfer Karadağ
karadagnilufer@yahoo.com