TAMAMEN RASTGELE

İki matematik delisi, bir lav lambası ve bir Web kamerasıyla İnternet'e nasıl kaos salacak?

İşte rasgele bir düşünce: "Bilgisayar çağında gizlilik ve güvenliği sağlamak için yaptığımız herşey, rasgele sayılara bağlıdır."

Şifreleme uzmanı ve "İnternet güvenlik duvarları kurmak" kitabının yazarı olan Simon Cooper böyle söylüyor. Rasgele sayı serileri, 4000 yıldır çevremizde olmalarına karşın, bunlara asla şimdiki kadar talep olmamıştı. Nedeni, şifrebilimin temel taşları olmaları. Örneğin E*Trade'e bir SSL (Secure Server Link: Güvenli Sunucu Bağlantısı) kurduğunuzda, perde arkasında çalışan bir rakamlar dizisi var. 368 ikil (bit) kadar rasgele veri bağlantısının yaratılmasında, 128 bitlik bir şifreleme anahtarının yapılmasında, doğrulama kodları ve yanıt hücumlarının engellenmesinde, kredi kartı bilgilerinin bir e-ticaret sitesinin "güvenli sunucusuna" gönderilmesinde ya da tıbbi kayıtların İnternet üzerinden sigorta şirketine gönderilmesinde, bu gerekli. Orta Doğu'daki komutanlar arasında uçuşan mesajların gizliliği bile, rasgele sayılara bağlı.

Bir seri, içerisinde hiçbir örüntü bulunmuyorsa rasgele kabul ediliyor. Seri ne kadar uzunsa, şifreleme o kadar güçlü oluyor. Bu kombinasyonları üretmek, özenli bir çalışma gerektiriyor. Landon Noll'a sorun. 42 yaşında bir matematikçi olan ve bilgisayar güvenliği firması System Experts için şifrebilimcilik yapan Noll yaklaşık 10 yıldır kaosa düzen getirme çabası içinde, rasgele sayı üreticileriyle çalışıyor. "Kaosta olağanüstü güzellik var" diyor. "Eğer Büyük Kanyon düzgün bir hendek olsaydı, bu kadar popüler olmazdı. Zor olan, kaosu kontrol edip yöneterek, onu işe yarar hale getirmek."

1996'da Noll ve Silicon Graphics'deki iki meslektaşı, rasgele sayı üretmek için lav lambalarını kullanan patentli bir sistem olan Lavarand'ı yarattılar. Web sitesi, milyonlarca ziyaretçiyi kendine çekti. Bazıları lav lambalarının kabarcıklı görüntülerini tüm akışkanlığıyla görmek için; diğerleriyse, fizik ve matematiğin, rasgele sayı tohumları yaratmak için kullanılmasına göz atmak için geliyordu.

Noll, şimdi Cooper ile birlikte, LavaRnd adı verilen geliştirilmiş bir rasgele sayı üreticisi üzerinde çalışıyor. Yeni süreç lav lambalarını, daha Zen-vari bir entropi kaynağıyla değiştiriyor: lens kapağı kapalı bir web kamerası. Web kamerasının yaydığı kaotik ısı "gürültüsü" sayısallaştırılıp, rakam grubunu karıştıran bir arapsaçı (hash) algoritmasından geçiriliyor ve bu rakam grubunun istenmeyen tahmin edilebilir bölümleri yok oluyor. Sonuç, gerçek dünyada kullanıma hazır ve şifrebilimsel olarak güçlü bir rakam serisi. Yeni servis açık-kod, patentsiz ve lisanssız olduğu için, herhangi biri düşük bir maliyetle bir LavaRnd sunucusu kurup, ücret ödemeden kullanabilecek.

Noll, her zaman sayılardan büyülenmiş. Birkaç asal ve mükemmel sayı keşfetmiş, ve bir dönem, tek başına ya da başkalarıyla birlikte asal sayıyla ilgili 9 dünya rekoru sahibi olmuş. Sırasıyla 221701-1 ve 223209-1 olan, 25. ve 26. Marsenne asallarını keşfedenlerden olan Noll, LavaRnd ile başkalarının da matematiksel eğlenceye katılmasını sağlıyor. "İnsanlara kendi rasgele sayılarını üretme olanağını vermeye çalışıyoruz" diyor. "Web kamerası ucuz, kolay bulunan ve tahmin edilemeyen bir uyarıcı. İyi gelişigüzel sayılar üretmek zor. Kolay olduğunu söyleyenler, sıklıkla bu işi yanlış yapıyorlar."

İnsanlar, günlük yaşamda rasgele sözcüğünü, hiç de rasgele olmayan şeyler için sıklıkla kullanıyorlar. Örneğin CD çalardaki "rasgele" (random) tuşu, adından üzüntü verici derecede azını sağlıyor. Bastığımızda aynı şarkıyı asla iki, üç ya da on kere arka arkaya dinleyemiyoruz. Bazı CD çalarlarda bu özellik, daha doğru bir şekilde, "karışık" (shuffle) olarak adlandırılıyor. Bilgisayardaki rasgele ulaşım hafızası (RAM), aslında rasgele değil. Rasgele ulaşım hafızası, verilerin belirli alanlarda verimli olarak saklanıp geri alınmasını sağlıyor. Daha iyi bir isim "sırasal olmayan hafıza" olabilirdi.

Gerçek rasgelelik, katı bir angaryacı. Rasgele sayıların içerisinde eğilimler ve desenler olmamalı. Verilen bir zamanda üretilen bir sayı, önceki değerlerle hiçbir şekilde ilişkili olmamalı. Gerçek bir rasgele sayı dizisinde, bir sonraki

sayıyı bulmaya çalışan bir hacker (saldırgan), bunu hesapsal olarak olanaksız bulmalı.

İlk rasgele sayı üreticileri, Eski Sümer ve Mısır zamanından beri, şans oyunlarındaki anahtar elemanlar olan zarlar. Zarlar bu konuda, oldukça verimli. Hileli olmadıkları ve atıldıkları ortama belirli bir sonuca ulaşacak şekilde müdahale edilmediği sürece, zar atmak güvenilir bir rasgele sayı akışı sağlıyor. Sorun, düşük üretim. Yalnızca atabildiğiniz hızda sayı üretebiliyorsunuz ve bu, örneğin bir barbut oyununu, büyük seriler üretmek için pratik olmayan bir yöntem haline getiriyor.

20 yüzyılda, rasgele sayılara olan talep patladı. Seriler, anketörlerin toplumu temsil eden örnek grupları seçebilmelerinde; bilim adamlarının kaotik molekül hareketlerini modellemelerinde; fizikçilerinse, nükleer patlama simülasyonlarında kullanılıyor. Rasgele sayılar, piyangolar ve kumarda da yaşamsal rol oynuyor.

100 yıl kadar önce bilimsel çalışmalar için rasgele sayılara ihtiyacı olan insanlar, hâlâ yazı tura atıyor, zar kullanıyor, kağıt dağıtıyor, şapkalardan rakam çekiyor ya da nüfus sayımı kayıtlarını rasgele rakamlar için tarıyorlardı. 1927'de, istatistikçi L.H.C. Tippett, İngiliz kiliselerinin alan ölçümlerinin orta rakamlarını alarak oluşturduğu, 41.600 rasgele sayılık bir tablo yayımladı. 1955'te Rand Şirketi, rasgele sayı tablolarıyla dolu büyük bir kitap olan "100.000 Normal Sapma ile 1 Milyon Rasgele Sayı"yı yayımladı. Test sırasında keşfedilen ufak eğilimleri ortadan kaldırmak için, 1 milyon rakam, tüm çiftler eklenip son hane alınarak, iyice rasgelele hale getiriliyordu. Rand'ın kitabı, bugün bile, anket yapılacak alanın belirlenmesi gibi düşük düzeyli uygulamalarda kullanılan, standart bir referans haline geldi.

Ancak e-ticaret siteleri, bilgiyi şifrelemek için günde milyonlarca rasgele rakamı tüketmeye başlayınca, kitap sayfalarını karıştırmak yeterli olmuyor. Gereken, düzensizlik ve gerçek rasgelelik üretebilen yüksek çıkışlı bir üreteç; ki bu, yeryüzündeki herhangi bir bilgisayarın becerisi dışında bir görev.

Bilgisayarlar, rasgele sayı üreticisi olarak "berbat" kabul ediliyorlar. Dijital bir alet, bir sayının ikillerini, daha önce üretilen sayılarla ilişkisiz gibi gözükecek bir sonuç üretecek şekilde karıştırmaya programlanabiliyor. Ancak, bilgisayarlar yalnızca; sadece kurallar ve prosedürleri takip ediyorlar. Aynı süreci aynı noktadan başlatırsanız, bir örüntü ortaya çıkıyor. Böyle sistemler, sıklıkla yalancı-rasgele sayı üreticiler olarak adlandırılıyorlar.

Rasgele sayı üreticileri, bu kusurlarını, tahmin edilemez görünen kaynaklardan tohumlar üreterek kapatmaya çalışıyorlar. Ancak bu tohum kaynaklarının sıklıkla rasgele olmaması, sistemin saldırıya rasgele bir kaynaktan daha açık olması demek. 1990'ların sonunda, güvenlik uzmanları, Netscape'in rasgele sayı üreticisinin sadece 3 kaynaktan türetildiğini keşfettiler: gün içindeki zaman, süreç numarası (process ID) ve ana süreç numarası (parent process ID). Bir saldırgan, bu rakamları tahmin edebiliyor ve sıradan bir algoritma uygulayarak, kullanılan tohumu hesaplayabiliyor. Daha iyi bir yaklaşım, Intel'in 800 serisi yongalarda yaptığı gibi, tümüyle tahmin edilemez bir entropi kaynağını, donanımın içine katmak. Yongaların parçası olan bir rasgele sayı üretici, dirençlerin yaydığı ısı gürültüsünü algılıyor. Kuantum fiziği yasalarına göre, radyoaktif elementler, bozulma hızları tümüyle tahmin edilemez olduğu için, çok iyi entropi kaynakları.

Autodesk'in kurucusu John Walker tarafından yürütülen HotBits (www.fourmilab.ch/hotbits) adındaki bir rasgele sayı servisi, kripton-85 kapsülüne doğrultulmuş bir Geiger sayacı kullanıyor. Ziyaretçiler, sitede rasgele sayılar bile ısmarlayabiliyorlar. Random.org adında başka bir servis de, değişik frekanslara ayarlanmış iki tane ikinci el radyonun atmosferik gürültüsünü entropi kaynağı olarak kullanıyor. Dublin Trinity College'de bilgisayar bilimi eğitmeni olan Mads Haahr, günde yaklaşık 111 milyon rasgele ikil üreten bir sistem tasarlamış. Sürekli müşterileri arasında, bu sistemi İnternet üzerinden tavla hizmetinde kullanan Danimarka TV2, eşi olmayan albüm kapakları yapmakta kullanan Amerikalı rock grubu Technician, ve açıklanmayan bir amaç için kullanan açıklanmayan bir askeri laboratuvar var.

Landon Noll

Rasgele sayılar, CD'de de mevcut. 1996'da, Florida State Üniversitesi'nde bilgisayar bilimcisi olan George Marsaglia, 60 adet 10 Megabaytlık dosya halinde, beş milyar rasgele ikilden oluşan bir disk üretti. Marsaglia, bu ikilleri üretirken, 3 adet elektronik beyaz gürültü kaynağını, bir rasgele sayı üreticisinin çıkışıyla birlikte kullandı.

Landon Noll'un yeni LavaRnd süreci, en iyi rasgele sayı üreticileri arasında. Saniyede 165.000 ikil rasgele veri üretebiliyor; ki bu Intel'in rasgele sayı üreticisinin iki katından daha hızlı ve çoğu talebi karşılayabiliyor. LavaRnd, C ve Perl'de kodlandığı için, ucuza da mal oluyor. Buna, "toplum için rasgelelik" diyebiliriz. Ayrıca lav lambası almanıza bile gerek yok. Noll "Lav lambalarını artık kullanmıyor olmamız çok kötü. Onlara bakmak çok hoştu" diyor. "Ancak ampul değiştirmek gerçek bir problem olmuştu."

Noll ve Simon, tüm görkemli düzensizlikleriyle lav lambalarının resimlerini, eski zamanların hatırına, hâlâ sitelerinde tutuyorlar. Bu resimler bize, modern dünyada koyu ve yapışkan rasgeleliğe farkında olmadan ne kadar bağımlı olduğumuzu hatırlatmaya yarıyor.

"Totally Random" Wired, 2003. 08:088-089.

Çeviri: Ekin Dino