T.C. SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM465 - KRİPTOLOJİYE GİRİŞ ÖDEVİ

Random Number Generators

Hazırlayan

Ferdi Sönmez

B211210375

İçindekiler

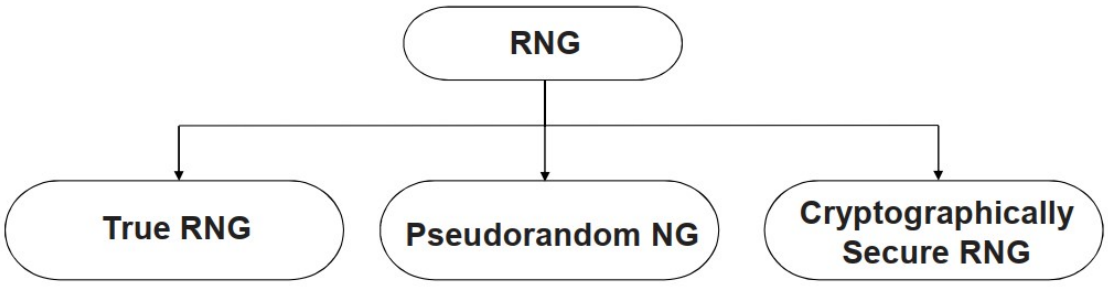
Random Number Generator Nedir?

Rastgele sayı üretici herhangi bir örüntü barındırmayan bir sayı ya da simgeler dizisi üreten berimsel ya da fiziksel aygıttır. Rastgele sayı üretiminde sıkça kullanılan donanım tabanlı sistemler genellikle beklentilerin altında kalmaktadırlar. Ne var ki, bu sistemlerin tahmin edilmesi oldukça güç sayı dizileri ortaya koydukları da açıktır. Rastgele sayı üretim yöntemleri eskiden bu yana ilgi konusu olmuştur.

Rastgele sayılar binlerce yıldır kullanılıyor. İster yazı-tura atın, ister zar kullanın, temelde amaç sonucu saf şansa bırakmaktır. Rastgele sayı üreteçleri, zarlar, karıştırılmış kartlar, bozuk para çevirme ve hatta pipet çekme gibi eski zamanlardan beri var olan rastgelelik cihazlarının sadece modern uygulamalarıdır.

Bilgisayardaki rastgele sayı üreteçleri de aynıdır, amaç tahmin edilemeyen, rastgele bir sonuca ulaşmaktır. Rasgele sayıların kullanım alanları sandığımızdan çok daha fazladır. En belirgin olan şans ve video oyunlarındaki uygulamalarıdır. Bunun yanı sıra şifreleme bilimi için de oldukça önemlidir. Şifreleme biliminde (kriptografi) olası bir saldırı durumunda saldırganın tahmin edemeyeceği bir sayı kullanmanız gerekir. Bu sebeple aynı sayıyı defalarca kullanamazsınız. Dolayısıyla bu sayıları saldırganın tahmin etmesinin güç olduğu bir şekilde üretmelisiniz. İster kendi dosyalarınızı şifreleyin, ister HTTPS protokolü kullanan bir internet sitesi kullanın, bu rastgele sayılara fazlasıyla ihtiyacınız var. Rastgele sayı üreteçleri üç kısma ayrılmaktadır.

1)True-Random Number Generator(Gerçek Rastgele Sayi Üreteçleri)
2)Pseudorandom-Random Number Generator()
3)Cryptographically Secure Random Number Generator



True Random Number Generators (TRNGs) Nedir?

True Random Number Generator üreteçleri “hakiki“ yapan şey, rassallığın kaynağının fiziki dünyadan gelen dışsal bir veri olması nedeniyle aynı sayı zincirinin tekrar üretilemeyecek olmasıdır.Tekrar aynı olasılıkta olaylaron üretilmesi mümkün değildir. Çeşitli standartlar ve sertifika dernekleri, TRNG'lerin gerçekten rastgele çözümlerin tasarımı ve sertifikasyonu için yönergeleri tanımlaması için spesifikasyonları ve doğrulama yöntemlerini yönlendiriyor. Bu dernek ve standartlar TRNG lerin öngörülemez, tek tip, bağımsız ve keşfedilemez olması gerektiğini vurguluyor.Bu özelliklerinden dolayı kontrol edilmeleri çok zordur.

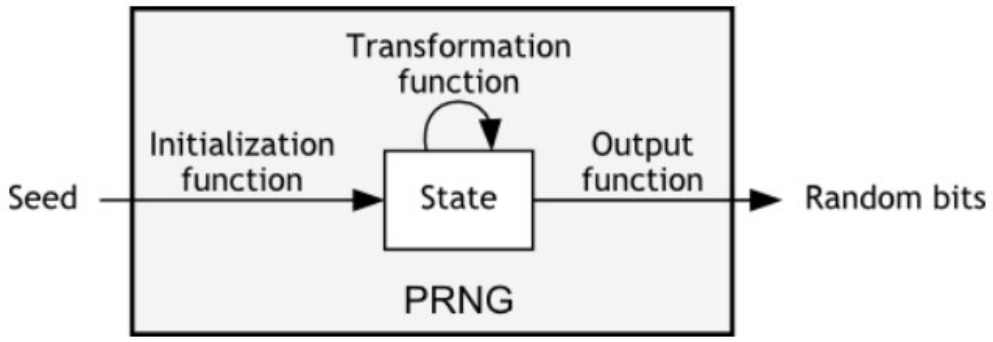
Yazı Tura: Yanlı olmayan bir para havaya atılır ve hangi yüzü (yazı mı tura mı) geldiğine bakılır. İki tane yüzü olduğu için her bir para havaya atılmasında iki alternatif sonuç beklenir ve bu iki alternatif mümkün sonuçtan biri ortaya çıkacaktır. Onun için yazı olasılığı Pr(yazı) = 1/2 = 0,5 ve tura olasılığı Pr(tura) = 1/2 = 0,5 olur.
Zar denemeleri: Bir yansız zarın üzerine benek ile işaret edilmiş altı yüzü bulunmaktadır. Tek bir zar bir defa atılınca her bir yüzün (yani beneğin) aynı olasılığı bulunur. Yani i = yüzün benek sayısı ise Pr(i) = 1/6 eğer i=1, 2, ..., 6 ise olur.

Pseudorandom Number Generator Nedir?

Sözde rassal sayı üreteçleri bir ilk değer verilerek başlatılır. Daha sonra üreteçten rassal sayı istendikçe, içerisinde bir algoritma çalışarak sıradaki değeri üretir.

$$X_{n+1} = (aX_n + b) \bmod m$$

Basit bit PRNG üreteç, bir önceki sayıyı a ile çarpıp b ile toplayıp sonucun modunu alarak sıradaki "sözde" rassal sayıyı üretir. Kullanılan üretece göre farklı algoritmalar sözkonusu olabilir. Örneğin büyük bir sayı üretilip onun n. basamağından k. basamağına kadar olan sayıyı almak da belirli bir rassallık sağlar.
Burada oluşacak olan rassal sayı zinciri sadece verilecek olan ilk değere bağlıdır. Bu ilk değere çekirdek değer (seed) adı verilir. Aynı çekirdek verildiği sürece aynı rassal sayı zinciri üretileceği için, bu tip üreteçlere "sözde(pseudo)" rassal denir. PRNG üreteçlerin, gerçek hayattaki tesadüfiliğe yakın olmasını sağlamak için, çekirdek değeri olarak genelde sistem zamanı kullanılır. .NET Framework, Java, ve meşhur birçok platformun içerisinde hazır olarak bulunan "Random" sınıfları bu tip üreteçlerdir ve çekirdek değerlerini tipik olarak belirli bir tarih-zaman üzerinden geçen milisaniye olarak alırlar. Örneğin .NET Random sınıfı rassallık zincirinin çekirdek değerini, sistemin başlangıç zamanından çağrıldığı zamana kadar geçen milisaniye sayısı olarak alır.
PRNG üreteçlerin ürettikleri sayıların, istatistiki bakış açısıyla ne kadar "rastgele" olduklarını ölçmek için birtakım testler mevcuttur. Bu testlerin temel mantığı, üretecin bir sonra üreteceği sayının ne kadar tahmin edilebilir olduğunu hesaplamak üzerine kuruludur. Programlama dillerinin standart kütüphanelerinin rastsallık testlerinde iyi sonuçlar elde edemediklerini görüyoruz. Fakat çoğu zaman rassalık ihtiyacımız yüksek hassasiyet gerektirmediği için bu kütüphanelerin kullanımı pratik ve yaygındır.

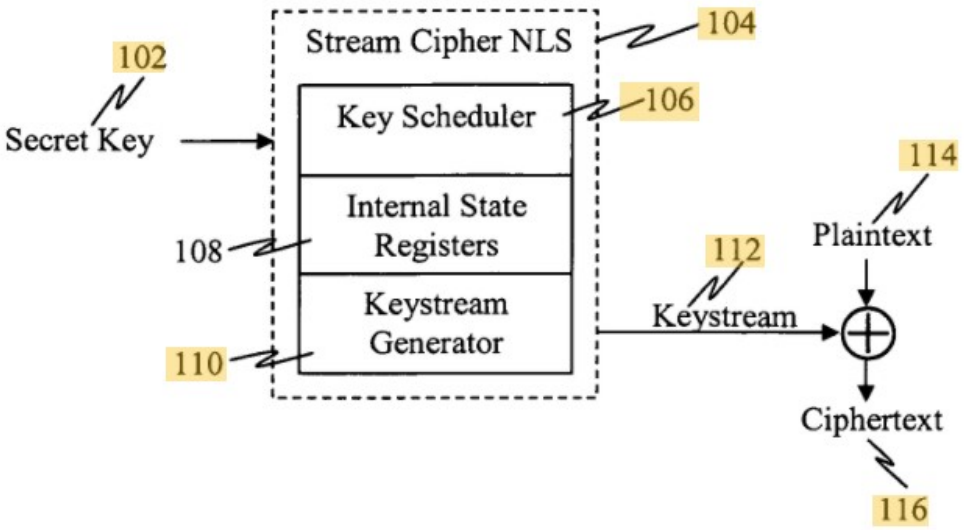


Schematic diagram of a pseudo-random number generator

Cryptographically Secure Pseudorandom Number Generators (CSPRNG) Nedir?

Kriptografik olarak güvenli bir rastgele sayı üretir, kendisini kriptografide kullanıma uygun kılan özelliklere sahip bir sözde rasgele sayı üretecidir. Çoğu kriptografik uygulama rastgele sayılar gerektirir.Bu sebeple bu rastgele sayı üretecinin kullanılması çok yaygındır.

Örneğin verilen n çıkış bitinin anahtar akışı si,si+1,...,si+n−1, burada n bir tam sayıdır, sonraki si+n,si+n+1,.... bitlerini hesaplamak, hesaplama açısından mümkün değildir.
Anahtar akışının ardışık n biti verildiğinde, polinom zaman algoritması yoktur, %50'den daha iyi başarı şansı ile bir sonraki sn+1 bitini tahmin edebilir.
CSPRNG'nin bir diğer özelliği, yukarıdaki sıra verildiğinde, hesaplamalı olması gerektiğidir. önceki si−1,si−2,.. bitlerini hesaplamak mümkün değil.CSPRNG'lerin öngörülemezliği ihtiyacının kriptografiye özgüdür. İstatiksel yaklaşımlar ile tahmin edilmesi zorlaştırılmıştır. Pseudorandom number generatordeki eksiklikler kapatılmaya çalışılmıştır.Algoritmanın çalışma zamanı polinomial bir hale getirilip kısa zamanlarda çözümlenmesinin önüne geçilmiştir.
Kriptografide, özellikle akış şifreleri için gereklidir.



Kaynakça

1) https://www.emo.org.tr/ekler/3e6f423ffcbf723_ek.pdf
2) https://dergipark.org.tr/tr/download/article-file/399021
3) Lagarias J. C., Pseudorandom Number Generators in Cryptography and Number Theory. Proc. Symp. Appl. Math., 42: 1990, pp. 115–143
4) James, F. 1990. A review of pseudorandom number generators. Computer Physics Communications. 60: 329-344. North-Holland
5) Ritter, T. 1991. The Efficient Generation of Cryptographic Confusion Sequences. Cryptologia. 15(2): 81-13
6) Paar C., Pelzl J., Understanding Cryptography A Textbook for Student and Practitioners, Springer. (2010).
7) http://docplayer.biz.tr/42512149-Kriptolojik-rasgele-sayi-uretecleri-cryptographic-random-number-generators.html
8) https://en.wikipedia.org/wiki/Cryptographically-secure_pseudorandom_number_generator
9) https://www.veracode.com/blog/research/cryptographically-secure-pseudo-random-number-generator-csprng
10) https://www.youtube.com/watch?v=gA3ua_QM1X0