1024-Bit RSA anahtarlarının güvenliği hakkında

ÇETİN KAYA KOÇ

Bugüne kadar çarpanlarına ayrılabilen en uzun RSA modulus sayısı 663 bit.

Önceki yazımızda başladığımız bu konu hakkında bilgi ve görüşlerimizi anlatmaya devam ediyoruz. RSA algoritmasının güvenliği RSA modulus sayısı n'in çarpanlarına ayrılmasının zorluğuna dayalı. Bugüne kadar çarpanlarına ayrılabilen en uzun RSA modulus sayısı 663 bit. Bu zahmetli çalışma, dünya yüzeyine dağılmış matematikçiler ve bilgisayar mühendislerinden oluşan bir ekibin 1.5 yıllık bir çabası sonucu elde edildi. Aynı uzunlukta başka bir modulus için gereken çaba, yine buna yakın olacak. Çünkü bir modulus sayısını çarpanlarına ayırırken elde edilen ara sonuçlar ile başka bir modulus için elde edilen ara sonuçlar arasında pek bir örtüşme yok. Yani herşeyi sil-baştan hesaplamak zorundayız. Ayrıca elimizde devamlı kullanabileceğimiz bir cihazımız da yok. Aynı ekibi ikna edip, çalışmalarının organizasyonunu sağlamamız gerekecek.

Buradan yola çıkıp, 1024 bitlik sayıların çarpanlarına ayrılmasının çok zor olduğunu söyleyebilir miyiz? Hayır, diyemeyiz. Çarpanlarına ayırabildiğimiz en uzun RSA modulus, 1999 yılında 465 bit, 2003 yılında 576 bit, 2005 yılında ise 663 bitdi. Yani 6 yılda yüzde 42 bir ilerleme. Peki çarpanlarına ayırma yetkinliğimiz lineer olarak mı artıyor? Eğer bu doğruysa, 2011 yılında 941 bit bir sayıyı çarpanlarına ayırabilmeliyiz. Hayır, bu da pek doğru değil. Yapmamız gereken, elimizdeki en iyi algoritmaları kullanarak, tasarlayıp gerçekleme ihtimalimiz olan en iyi "çarpanlara ayıran bilgisayar" sistemlerinin maliyetlerini, böyle sistemler üzerinde çarpanlara ayırma işlemlerinin ne kadar süreceğini ve çarpanlarına ayırabileceğimiz en büyük RSA modulus sayısının uzunluğunu tahmin etmek.

Burada önemli iki faktör var: Bu sistemin maliyeti ve bunun üzerinde herhangi bir 1024-bit RSA modulus sayısının çarpanlarına ayırmanın ne kadar zaman alacağı. Ayrıca bu cihazı başka modulusslar için de kullanabilmeliyiz. Böyle bir çalışma Weizman Bilim Enstitüsü araştırmacıları Adi Shamir ve Eran Tromer tarafından 2003 yılında yapıldı: Twirl adı verilen hipotetik bir çarpanlarına ayırma cihazının 1024-bitlik RSA modulus sayısını 1 yılda çarpanlarına ayıracak şekilde tasarlanıp, ilk örneğinin yapılması maliyetini 10 milyon dolar olarak belirlediler. Çok uzak olmayan bir gelecekte, masaüstü Twirl makinelerinin yapılacağını ve 10 bin dolara satılacağını da kolaylıkla hayal edebiliriz. Olmaz derseniz, size bilgisayar teknolojisinin son 25 yıllık tarihçesini hatırlatmak isterim.

koc@cryptocode.net