1024-Bit RSA ne kadar güvenli?

ÇETİN KAYA KOÇ

RSA algoritması Avrupa ve ABD'de önemli olduğu kadar Türkiye'de de çok önemli.

Daha önceki yazılarımızda SHA-1 fonksiyonun güvenlik derecesi hakkında bilimsel tartışmaları aktarmış ve görüşlerimi belirtmiştim. Bu günden itibaren birkaç yazı da ise RSA algoritması hakkında size bilgi ve görüşlerimi aktarmak istiyorum. RSA algoritması Avrupa ve ABD'de önemli olduğu kadar Türkiye'de de önemli çünkü e-imza altyapımız RSA algoritmasına dayanıyor.

RSA algoritmasının güvenliği RSA modulus sayısı n'nin çarpanlarına ayrılmasının zorluğuna dayalı. Eğer n sayısını çarpanlarına ayırabilirsek, kullanıcının gizli anahtarını açık anahtarından hesaplayabiliriz. Saldırgan bir kere bunu becerdikten sonra işi kolay: Kullanıcıya gelen her şifreli mesajı açıp okuyabilir ve daha da kötüsü onun adına elektronik imza icra edebilir, kısacası saldırgan tam manası ile kullanıcı yerine geçer.

RSA algoritmasını bulan üç bilim adamının adıyla (Rivest, Shamir, Adleman) kurulmuş olan RSA Security şirketi, kendini biraz da RSA algoritmasının güvenlik derecesini belirleyip kamuoyunu bilgilendirmek konusunda sorumlu hissediyor. Bu amaçla sürekli bir yarışma düzenlenmiş ve herkes farklı uzunluklarda bir dizi modulus sayısını çarpanlarına ayırmaya davet edilmiş: http://www.rsasecurity.com/rsalabs/node.asp?id=2092

Dünyada değişik bölge ve ülkelere dağılmış, matematikçi ve bilgisayar mühendisi çalışma grupları ise bu yarışmaya gönüllü olarak katılıp, bu sayılardan bazılarını çarpanlarına ayırmaya çalışıyorlar.

Peki şimdiye kadar çarpanlarına ayrılan en uzun RSA modulus sayısı kaç bit? Daha önceki çalışmaların detaylı bir kayıdı tutulmadığı için 1999'dan başlayalım: 185 kadar PC ve işistasyonu 1 ay kadar çalışıp 465 bitlik bir RSA modulusu çarpanlarına ayırdı. 2003 yılı sonunda ise 576 bitlik bir sayı çarpanlarına ayrıldı. 2004 yılı başlarından itibaren çalışmaya başlayan başka bir ekip ise aşağı yukarı 1.5 senelik bir çalışma sonucunda 663 bitlik bir RSA modulus sayısını çarpanlarına ayırmayı başardı. 663 bitlik bu sayı insanoğlunun şimdiye kadar çarpanlarına ayırdığı en büyük sayı olmaya devam ediyor. Onlar çalışmalarını bitirdikçe, başarı öykülerini duyacağız. Fakat yapılması gereken bir iş daha var: Elimizde olan 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.

koc@cryptocode.net