RSA güvenliği hakkında son sözler

ÇETİNKAYA KOÇ

1977'de duyurulduğunda "kırılmasının milyonlarca yıl gerektirdiği" iddia edilen RSA, 27 Nisan 1994'te, yani yaklaşık 17 yıl sonra kırılmış oldu.

RSA algoritmasının güvenliği hakkında söylenen ilk sözlerin bir yanılgı olduğu 17 senelik bir zaman süresi içinde belli oldu. Bu yüzden benim de bu algoritmanın güvenliği hakkında "son sözleri" söylemek gibi bir iddiam olamaz, tabi. Ancak bu 3 yazılık dizinin son yazısında, birkaç tane son söz söylemekte yarar var.

İki gizli asal sayının çarpımı olan bir sayının, çarpanlarına ayırmanın zorluğuna dayanan bu algoritma, 1977 yılının ilkbaharında bulundu. Araştırmacılar MIT adına 14 Aralık 1977'de ABD patent enstitüsüne başvurdular ve sonunda 4,405,829 numaralı patenti edindiler.

Scientific American dergisindeki "Mathematical Games" köşesinde Martin Gardner meraklı matematik problemleri ve bunların çözümlerinden bahsediyordu. Burada ilk defa RSA algoritmayı kamuoyuna sundu ve 129 rakamlı (425 bit) bir RSA modulus sayısını faktör etmeleri için okurlarına çağrı yaptı. Yazının başlığı "A new kind of cipher that would take millions of years to break-Kırılması milyonlarca yıl gerektiren yeni bir tür şifre" idi. Ancak 27 Nisan 1994'te, yani yaklaşık 17 yıl sonra bu "milyonlarca yıl gerektiren" sayı çarpanlarına ayrıldı, yani şifre kırılmış oldu. Bugün elimizdeki en iyi algoritmalar ve akademinin ulaşabileceği bilgisayar sistemleri ile bu büyüklükte bir sayıyı çarpanlarına ayırmak sadece birkaç haftalık bir çalışma gerektiriyor.

RSA güvenliği için sizi bir web sayfasına davet etmek isterim: http://keylength.com. Lenstra-Verhaul denilen bir modele göre (bence bu model oldukça tutucu ve üstelik sürpriz gelişmeleri de dikkate almıyor) hesap yapan araştırmacılar size şunu öneriyor; Genel ve kısa amaçlı kullanım (2010 yılına kadar) için RSA-1228. Orta dönemli güvenlik (2025 yılına kadar) için RSA-2432. Uzun dönemli güvenlik (2035 yılına kadar) için RSA-3248. Çok uzun dönemli güvenlik için RSA-15424.

Tabi bu sayılar sadece RSA algoritmasının güvenliği için verilmiş. Bir yandan RSA-4096 kullanırken (bkz. Tübitak kök sertifikası) diğer taraftan SHA-1 özet algoritmasını kullanırsanız, bu sertifikaların güvenliğini artık 4096 bitlik RSA değil, 160 bitlik SHA-1 özet algoritması belirler. SHA-1 güvenliğinin sadece 63 bit olduğunu daha önce yazmıştık.

koc@cryptocode.net