RSA algoritmasına alternatifler

ÇETİN KAYA KOÇ

Daha fazla güvenlik için daha uzun anahtarlar kullanmamız gerekiyor mu?

Daha önceki yazılarımızı kısaca özetlersek, kısa ve orta dönemde, yani 2010 ve 2025 yıllarına kadar 1228 ve 2432 bitlik RSA bize gerekli ve yeterli güvenliği sağlıyor. Daha fazla güvenlik için daha uzun anahtarlar kullanmamız gerekecek. Hatta bazı paranoyak kurum ve kişilerin 16384 bitlik anahtarlar da kullandığını biliyoruz. Ancak uzun anahtar kullanmak, bir anlamda kötü mühendislik seçimi yapmak demek. Depreme dayanıklı olsun diye nasıl 4 metre genişliğinde betonarme duvar yapmıyorsak, 16384 bitlik RSA anahtarları da kullanmamıza gerek yok.

İyi mühendislik aslında daha kısa bit uzunluğu ile aynı güvenliği sağlamak. Çünkü bunları üretmek, saklamak ve bunları kullanarak işlem (şifreleme veya imzalama) yaparken daha az zaman, yonga veya kod alanı, ve daha az enerji kullanmak demek. Özellikle enerji, mobil cihazlar için (cep telefonu, PDA) çok önemli. Bu uygulamalar için bize RSA algoritmasından daha iyi algoritmalar gerekli.

Peki alternatif algoritma var mı gerçekten? Evet var. 1985 yılında iki matematikçi bilim adamının (Neil Koblitz ve Victor Miller) birbirinden bağımsız bir şekilde önerdiği elliptik eğri kriptografik algoritmaları tam istediğimiz profile uyuyor: 1024 bitlik RSA güvenliğine eşit elliptik eğri kriptografik algoritması sadece 160 bit kadar anahtar uzunluğu istiyor. Bu yüzden daha az yonga alanı, zaman ve enerjiye ihtiyaç duyuluyor ve mobil cihazlar için çok daha iyi çözümler üretiyor. Ben şahsen 10 yıldan daha uzun bir süredir öğrencilerimle birlikte bu konuda çalışıyorum. En son çalıştığımız projede, Bluetooth kulaklık ve cep telefonunun birbirleri ile elliptik eğri Diffie-Helmann algoritması yardımı ile güvenli haberleşmesi için gereken gömülü (embedded) sistemi tasarladık. Mükemmel bir elliptik eğri kriptografi uygulaması örneği yani.

Elliptik eğri kriptografik algoritmaları genellikle anahtar değiş-tokuşu, şifreleme ve rastgele sayı üretmede kullanılıyor. Elliptik eğri sayısal imza algoritması da var, adı ECDSA (Elliptic Curve Digital Signature Algorithm) ve hem ABD ulusal (FIPS 186-2) ve uluslarası bankacılık (X9.62) standardı. Ancak ECDSA kendinden beklenen yaygın kullanıma kavuşamadı ne yazık ki. Bunun en önemli nedeni RSA algoritmasının yaygın kullanımı. ECDSA, mahalleye yeni taşınan çocuk örneğinde olduğu gibi, bir türlü kendini kabul ettiremedi, çünkü mahallenin eski kabadayıları onu kabullenmek istemiyorlar!

koc@cryptocode.net