Modern kriptografinin 60. yılı

ÇETİN KAYA KOÇ

Birçok yazar, Claude Shannon'un Ekim 1949 tarihli makalesini modern (ve akademik) kriptografinin doğum tarihi olarak kabul eder. Bu durumda, kriptografi 60 yaşında ve hala genç (!) bir bilim dalı. Kriptografi, Shannon'un teorisini kurduğu temeller üzerinde son 60 yıldır çok önemli atılımlarda bulundu. Biz 4 mihenk taşından bahsedelim.

1976 yılında ABD ulusal standart olarak yayınlanan DES algoritması, bundan sonraki 20 yıl boyunca bankamatik makinelerinden uluslararası bankalar arasında veri alışverişine kadar güvenlik amacıyla kullanıldı ve 3DES denilen sürümü hala kullanılmaya devam ediyor. Tüm anahtarları deneme metodu hariç, DES algoritmasını kırmak için etkin matematiksel bir kısayol hala bulunmuş değil.

1977 yaz aylarında ikisi teorik bilgisayar bilimcisi (Rivest ve Shamir) ve üçüncüsü matematikçi (Adleman) olan üç MIT'li genç profesör, sonradan isimleriyle anılacak (RSA) denilen bir algoritmayı ortaya atarak, etkileri bugünde devam eden ve daha da yıllarca devam edecek olan (belki, Vestel şirketi Quantum ev bilgisayarları yapıp satmaya başlayıncaya kadar!) bir kriptografi devrimini başlattı. Elektronik imzadan güvenli internet alışveriş protokollerine kadar birçok konuda uygulanan RSA algoritması 1978 yılında yayınlandı.

1983 yılında iki matematikçi (Miller ve Koblitz), elliptik eğri kriptografiyi birbirinden bağımsız bir şekilde icat ederek, özellikle mobil cihazlar için çok önemli olan ve büyük bir ihtimalle RSA algoritması ömrünü tamamladıktan sonra bile varlığını sürdürecek olan bir kriptografik sistemi ortaya atmış oldular.

Dördüncü önemli adım ise 2001 yılında, DES'in yerine geçerek ulusal standart haline gelen AES algoritması. Orijinal adı Rijndael olan bu algoritmanın tasarımcıları iki Belçikalı genç kriptografi uzmanı (Rijmen ve Daemen). AES algoritmasına biçilen ömür yaklaşık 20 yıl. Büyük bir ihtimalle 2021'den çok önce, yeni bir algoritmayı tasarlayıp standart olarak yayınlamak gerekecek.

koc@cryptocode.net