İnsanoğlunun şifre merakı

ÇETİN KAYA KOÇ

Arap, Fars ve Roma tarihi, şifreleme metodlarının askeri uygulama hikayeleriyle dolu.

"Da Vinci Şifresi" kitabına ve şimdi de filmine olan ilgi, insanoğlunun şifrelemeye olan merakını en azından anektotsal olarak sergiliyor. İnsanlar şu veya bu nedenle açıkça söylemeyedikleri şeyleri şifreli bir şekilde şiirlerin veya yazıların içine gömmüşler ve zaman ve mekan içinde başka noktalarda başka insanların bu şifreleri çözmek için uykularını kaçıracaklarını herhalde hiç hesaba katmamışlardır. Bu merakın ve merakla birlikte gelen altkültür ve tarihin (her ne kadar yanlış bilgilerle, hurafe ve mitlerle dolu olsa bile) çok ilginç olduğuna hiç şüphe yok. Ancak buradan ayrıca iki tane insanlık için çok önemli sonuç ortaya çıkmıştır: birincisi şifrelemenin askeri amaçlarla kullanımı, ikincisi ise, özellikle 1975 yılında açık anahtarlı şifreleme metodunun icadı ile birlikte, şifrelemenin kişisel, finansal, kamusal ve ticari amaçlarla kullanımı.

İlk şifreciler, birinci uygulamanın, yani askeri kullanımın, çok iyi farkında idiler. Arap, Fars ve Roma tarihi şifreleme metodlarının askeri uygulama hikayeleriyle dolu zaten. Ama en uzak görüşlü eski çağ şifrecisi bile, herhalde bugün sıradan bir vatandaşın bir kitap satın almak için Internet üzerinden şifre kullanacağını hayal bile edemezdi.

Eski çağ şifrecileri genellikle anahtarsız şifreler, yani kodlar, kullanma yolunu seçtiler; eğer anahtarlı şifre kullandıysalar, bu anahtarı saklama probleminin hemen farkına vardılar.

Bu evrim bizi 1975 yılına getirdi. Şifrelemenin merakla yakın tarihini, özellikle askeri uygulamalarını, okumayı arzu eden okuyucularıma, David Kahn'ın "Codebreakers" isimli kitabını tavsiye ederim (yalnız kitabın 1169 sayfa olduğunu söylemem gerekli).

Anahtarlı şifreleme metodları, modern terimle "gizli anahtarlı kriptosistemler", 1975'den çok önce bazı hassas finans uygulamalarında kullanılmaya başlamıştı bile. Ancak anahtarı karşı tarafa ulaştırma problemi mühendisleri rahatsız etmeye devam etti. IBM'de 1950'lerde bu konuda yapılan çalışmalar master anahtarların kullanılmasını ve uygulamasını getirdi. Kriptografinin bilinen 3 bin yıllık tarihinde önemli bir adımdır, master anahtarlar. Onları kullanıp diğer bütün anahtarları şifreleriz. Bu ikinci grup anahtarlar ise veriyi şifreler. Buradan açık anahtarlı kriptografiye geçiş sanki bekleniyor gibiydi. Bugün hala açık anahtarlı şifrelemeyi 1975'den çok önce düşündüğünü söyleyen bilim adamları var. Belki de doğru söylüyorlar.

koc@cryptocode.net