

700. sayı veya 14. yıl

Elinizdeki BTHaber gazetesi 700 haftadır yayımlanıyor, yaklaşık olarak 14 yıl önce yayına başlamış. 14 yıl bilgi teknolojilerinin evrimi açısından birkaç bin biyolojik yıla eşdeğerdir dersem sanırım abartmış olmam. 14 yıl boyunca hayatta kalmış olmak ve gelişmiş olmak çok önemli: BTHaber başardı ama Clipper başaramadı!

Clipper, 16 Nisan 1993'de ABD hükümetinin başlattığı bir şifreleme projesinin ve bu projenin odak noktası olan yonganın adı. Bugün arşivsel olarak varlığını koruyan, FIPS 185 numaralı bu standart, ilk yayınlandığında büyük gürültülere neden olmuştu.

Konu şu: 70'li yılların sonundan itibaren, 80'li yıllarda ilerledikçe gelişen akademik ve endüstriyel bilgi birikimiyle, kriptografi artık hükümetlerin kontrolünden çıkmaya başlamış ve yazılım geliştiriminin kolaylaşmasıyla birlikte, dünyanın herhangi iki noktasında bulunan iki kişinin birbirleriyle şifreli olarak haberleşme ihtimali belirmişti. Bu teknolojinin kısa sürede yasa dışı (terörist veya uyuşturucu kaçakçısı) örgüt



**ÇETİN KAYA
KOÇ**

veya kişilerin eline geçeceği korkusu içinde olan bazı hükümet birimleri, şifrelemenin tekelleşmesi ve hükümet kontrolünde olması gerektiğini düşünmekteydiler. FIPS 185 bunu sağlamaya çalıştı. Her ha-

berleşme cihazı (özellikle o zaman önemli görülen telefon ve faks cihazları) içinde bir Clipper şifreleme yongası olacak ve Clipper kullanıcılarına gizlilik sağlarken, şifreleme algoritmasının kullandığı anahtarların birer örneğinin kanun yürütücüsünde olması nedeniyle, istenildiğinde (mahkeme kararıyla) herhangi bir haberleşme içeriğine ulaşmak mümkün olacaktı. Özet olarak FIPS 185 diyor ki, şifrelemek ancak benim algoritmamı ve anahtar sistemimi kullanırsan serbest, yoksa yasak!

Böyle yasaklar Amerikan bireyinin alışık olduğu anayasal çerçeveyi aşıyor. Clipper'i uygulamanın teknolojik zorlukları ise sanıldığından daha çetrefilli çıktı. Açıklandıktan bir yıl sonra, Matt Blaze isimli bir araştırmacı Clipper protokolunu kırdı, ve Clipper projesi sessizce ortadan kalktı.

koc@cryptocode.net