ASAL FAKTÖRLER

WikiLeaks & AES 256

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Bu konuda bir yazı da ben yazmış olayım! Biliyorsunuz, Julian Assange, ABD ve başka birkaç ülke hükümetine hitaben, "eğer beni tutuklar veya Wikileaks operasyonunu engellemeye çalışırsanız, insurance.aes256 isimli dosyanın şifreleme anahtarını bıraktığım arkadaşlarım bu anahtarı yayınlayacaklar ve sizi çok daha fazla mutsuz edecek birtakım dosyalar ortaya çıkacak", diye bir bildiri yayınlamıştı. Bir anlamda bu WikiLeaks'in devamlılık sigortası anlamında isimlendirilmiş olan bu şifreli dosya şimdi birçok sunucuda duruyor. Dosya, Julian Assange'nin dediği gibi, şifreyle kapatılmış bir dosya. İçeriğini öğrenmek için, anahtar yardımıyla şifreyi açmak (decrypt) etmek gerekiyor. Anahtarı bilince, açmak için saniyeler yeterli. Veya, becerebiliyorsanız, anahtarı siz bulmaya çalışırsınız! Yani, şifreyi kırarsınız. Olayın siyasi, sosyal, veya kültürel yanlarını bir kenara bırakıp, kriptolojik yanından bahsedeyim. Dosyanın ismi, şifreleme algoritmasının AES 256 olduğunu ima ediyor. WikiLeaks'ın bu algoritmayı kullandığını bilemiyoruz. Elimizde olan, sadece 1.4 GB büyüklüğünde şifreli bir doküman. Başka bir algoritma da kullanılmış olabilir. AES 256 algoritmasının kullanıldığını varsayalım.

AES algoritması bir uluslararası standart. 2000 yılında iki Belçikalı kriptolog (Vincent Rijmen & Joan Daemen) tarafından tasarlandı ve ABD standartlar enstitüsünün (NIST) açtığı bir dizi uluslararası konferans sonucunda, kriptoloji konusundan çalışan bilim adamları tarafından sunulanların en iyisi olarak seçilerek Mayıs 2002'de standart olarak yayınlandı. AES algoritması anahtar uzunluğu 128, 192 veya 256 bit olabiliyor. Eğer Julian Assange, 256-bit anahtar kullanmışsa, mümkün olan anahtarların sayısı 2^256, yani 10^77. Hiç de küçümsenecek bir sayı değil, 1'in önünde 77 tane sıfır var, yani yüz quadrillion (10^15) quintillon (10^30) quintillon (10^30). Eğer anahtarı biliyorsanız, dosyayı beyaz MacBook'unuzda açmak için gereken zaman yaklaşık 9 saniye. Eğer anahtarı bilmiyorsanız, 10^77 anahtar arasından aramanız gerekiyor. Bunun için bir trillion (10^12) MacBook'un 10^50 yıl (yüz bin quadrillion quintillion yıl) hiç durmadan çalışması gerekiyor. Bu çok uzun bir süre. Bildiğimiz kainatın yaşı 10^14 yıl (yüz trillion yıl). Yani, Julian Assange'den korkan hükümetler kendilerini şimdilik "garanti"de hissedebilirler. Bir hackerin dosyayı açma ihtimali yok. Ancak unutulmaması gereken bir konu, kriptoloji biliminin (veya sanatının) sürprizlerle dolu bir tarihçeye sahip olduğu! 1977 yılında Scientific American'da yayınlanan bir şifreyi kırmak için öngörülen zaman 40 quadrillion yıl iken bu şifre 1993-1994 yıllarında 600 kadar bilgisayar mühendisinin 1600 kadar bilgisayarı yaklaşık 6 ay çalıştırması sonucunda kırıldı! Bu başarının arkasında hem gelişen bilgisayar teknolojisi (daha hızlı bilgisayarlar) ve hem de insan yaratıcılığı (daha iyi algoritmalar) var.