ASAL FAKTÖRLER

Farklı şifreleme modelleri

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Klasik gizli-anahtarlı (secret-key) şifreleme modelinde Gönderici (G) ve Alıcı) bir gizli anahtar (K) üzerinde anlaşır; G bu K anahtarını kullanarak dokümanı şifreler ve A ise yine aynı K anahtarıyla şifreyi kaldırıp dokümanı elde eder. Bu model, askeri ve diplomatik haberleşme, kablosuz Internet, SSL dahil bir çok konuda mahremiyet (privacy) problemini çözebilecek kuvvete sahip. Doğal olarak anahtar dağıtım problemi var: K anahtarını G'den A'ya ulaştırmamız gerekiyor. Hem gizli anahtar dağıtım problemini çözen ve ayrıca Gönderici sayısının birden fazla olduğu durumlarda da kullanılabilen (G1, G2, ..) klasik açık-anahtarlı (public-key) şifreleme modeli var. Bu model de, herhangi bir Gi göndericisi dokumanı A'nın açık anahtarı (Kpub ile şifreler; A ise Kpriv anahtarıyla şifreyi kaldırıp dokümanı elde eder. Doğal olarak, gizli-anahtarlı ve açık-anahtarlı sistemlerin birlikte kullanıldığı modeller de söz konusu. Ancak, tamamıyla sayısallaşan ve iyice karmaşıklaşan bir dünyada, şifrelemenin başka modellerine ihtiyacımız belirmeye başladı. Örneğin, sadece kavramsal olarak şunu düşünelim. Açık-anahtarlı sistemde olduğu gibi birden fazla Gönderici (G1, G2, ..) ve bir tek Alıcının (A) olduğunu değil de, bir Gönderici (G) ve birden fazla Alıcının (A1, A2, ..) olduğunu hayal edelim. Ne gizli ne de açık anahtarlı model, burada karşımıza çıkan problemi doğru ve güzel bir şekilde çözemiyor. G farklı anahtarlar kullanabilir, diyebilirsiniz, ancak, aynı dokümanın birden fazla şifrelenmiş halinin varlığı doğru değil. Çünkü sadece "haberleşme" durumunda geçerli bir çözüm değil, genel bir çözüm arıyoruz.

Örneğin, tıbbi dokümanları düşünelim (doktor raporları, reçete, X-ray, MRI, CAT-scan). Burada herhangi bir dokümana birden fazla doktorun ulaşması gerekebiliyor, ancak her doktorun (doktor olan herkesin) ulaşması doğru değil. Sadece, hastane tarafından bu hastaya atanan (ve hastanın da onaylamış) olduğu doktorlar ulaşsın isteriz. Aynı şekilde, bir hemşirenin görmesi gereken dokümanlar (örneğin, reçete) varlar, görmemesinin daha uygun olduğu dokümanlar var (MRI, CAT-scan).

Dolayısıyla, çok daha karmaşık bir durum söz konusu. Bu problemleri nasıl çözeceğiz? Bize farklı şifreleme modelleri gerekli.