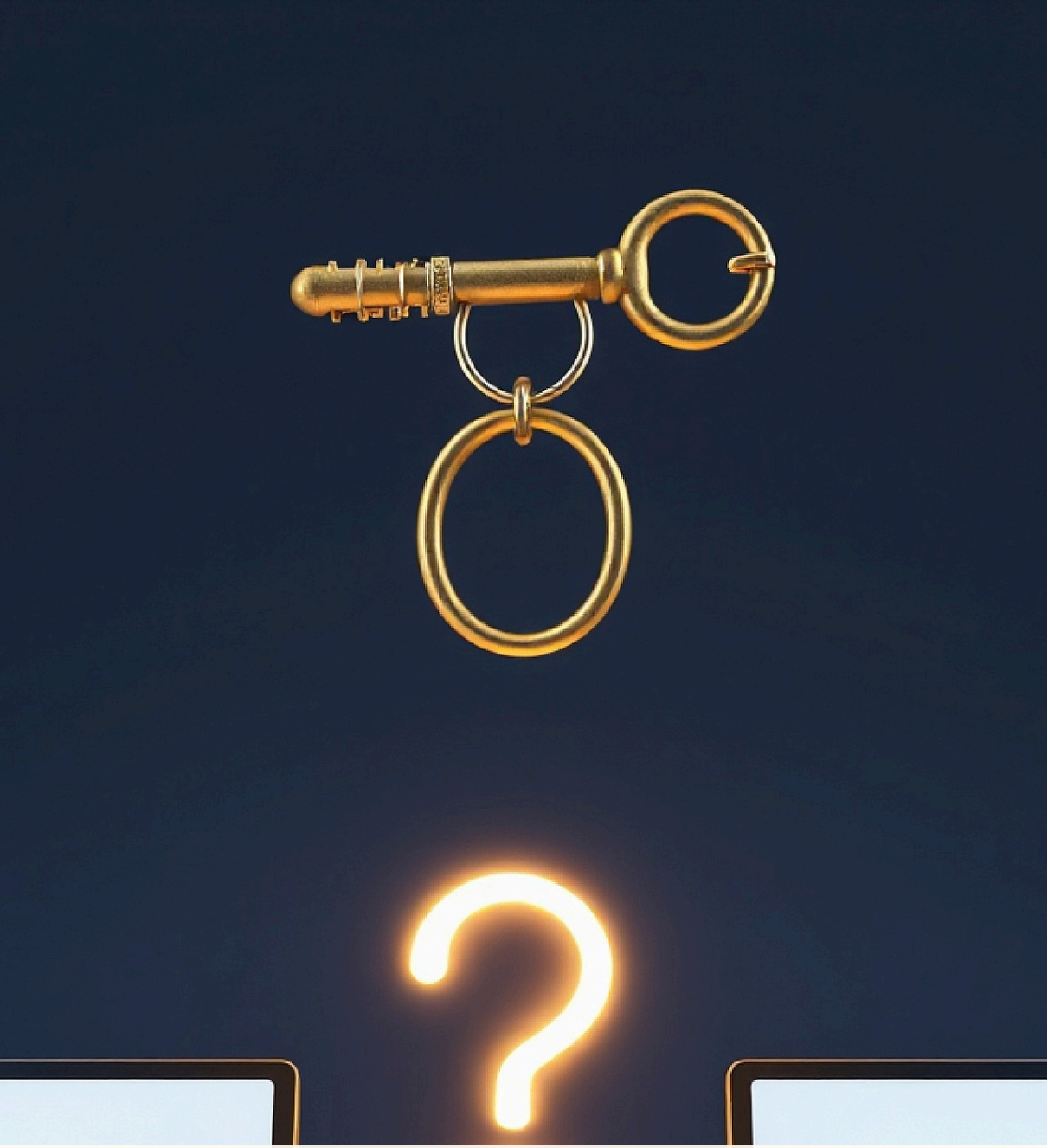
Simetrik ve asimetrik şifreleme arasındaki fark nedir?



www.yzokul.com.tr

Simetrik ve asimetrik şifreleme arasındaki fark nedir?



Soru basit: simetrik ve asimetrik şifreleme arasındaki fark nedir? Kısa yanıt, simetrik şifrelemenin veriyi hem kilitlemek hem de açmak için tek bir ortak gizli anahtar kullandığı, asimetrik şifrelemenin ise birbiriyle bağlantılı bir anahtar çifti kullandığıdır: bir açık anahtar ve bir özel anahtar. Bu kitap her parçayı adım adım açıklar; böylece nasıl farklılaştıklarını ve nasıl birlikte çalıştıklarını görürsün.



Anahtar, veriyi kilitlemek ve açmak için kullanılan bir bilgi parçasıdır. Veri bir anahtarla kilitlendiğinde karıştırılır ve okunamaz hale gelir. Yalnızca doğru anahtara sahip olan kişi kilidi açıp özgün mesajı okuyabilir. Doğru anahtar olmadan karıştırılmış veri korunmuş kalır. Anahtarlar tüm şifrelemenin kalbidir.



Şifreleme, okunabilir veriyi karıştırılmış veriye dönüştürür. Şifre çözme, bu karıştırılmış veriyi yeniden okunabilir veriye dönüştürür. Anahtarların denetlediği iki eylem bunlardır. Şifrelerken mesajı karıştırmak için bir anahtar kullanırsın. Şifreyi çözerken onu çözmek için bir anahtar kullanırsın. Anahtarlar olmadan şifreleme ve şifre çözme gerçekleşemez.



Simetrik şifrelemede aynı tek anahtar her iki işi de yapar: veriyi şifreler ve verinin şifresini çözer. İkinci bir anahtar devreye girmez. Gönderen mesajı kilitlemek için anahtarı kullanır, alıcı da kilidi açmak için aynı anahtarı kullanır. Bu, simetrik şifrelemeyi basit ve hızlı kılar, çünkü tüm süreç için yalnızca bir anahtar gerekir.



Simetrik şifrelemedeki püf noktası, her iki tarafın da aynı gizli anahtara önceden sahip olması gerektiğidir. Bu anahtarı diğer kişiye güvenli biçimde ulaştırmak zor kısımdır. Anahtar paylaşılırken biri onu ele geçirirse tüm mesajları okuyabilir. Bu yüzden ortak gizli anahtar güvenli bir kanaldan iletilmelidir; bu da her zaman kolay değildir.



Her biri aynı anahtara sahip iki kişiyi düşün. Biri kutuyu anahtarla kilitler ve gönderir. Diğeri kutunun kilidini aynı anahtarla açar. Bu tek ortak anahtar, simetrik şifrelemenin tüm fikridir. Her iki taraf da güvenli iletişim kurabilmeden önce aynı gizli anahtara sahip olmalıdır.



Asimetrik şifreleme, birbiriyle bağlantılı iki farklı anahtar kullanır. Bir anahtarın kilitlediğini diğer anahtar açar. Bu iki anahtar bir çift oluşturur: bir açık anahtar ve bir özel anahtar. Açık anahtar veriyi kilitlemek için, özel anahtar ise kilidi açmak için kullanılır. İki anahtar matematiksel olarak ilişkilidir ancak birbirinden türetilemez.



Açık anahtar herkesle açıkça paylaşılabilir. Anahtarın sahibine gönderilen veriyi kilitlemek için kullanılır. Açık anahtarını sana mesaj göndermek isteyen herkese verebilirsin. Onlar mesajı senin açık anahtarınla şifreler ve yalnızca senin özel anahtarın şifreyi çözebilir. Açık anahtarın gizli tutulması gerekmez.



Özel anahtar sahibi tarafından gizli tutulur ve asla paylaşılmaz. Açık anahtarın kilitlediği şeyin kilidini açabilecek tek anahtar odur. Özel anahtarını güvende tutarsan, açık anahtarınla şifrelenmiş mesajları başka kimse okuyamaz. Özel anahtar dikkatle korunmalıdır çünkü sırlarının anahtarı odur.



İsteyen herkese açık asma kilitler dağıtan birini düşün. Bu asma kilitler açık anahtarlar gibidir. Herkes bir kutunun üzerine asma kilidi kapatıp onu kilitleyebilir. Ancak yalnızca eşleşen anahtarı saklayan kişi asma kilidi açabilir. Özel anahtar, sahibi tarafından gizli tutulan o eşleşen anahtardır.



Asimetrik şifrelemenin büyük avantajı, iki tarafın önceden bir gizli anahtar alışverişi yapmasına gerek olmamasıdır. Açık anahtar tehlike olmadan açıkça dolaşabilir. Herkes bir mesajı şifrelemek için açık anahtarı kullanabilir, ancak yalnızca özel anahtarın sahibi şifreyi çözebilir. Bu, simetrik şifrelemenin ortak sır sorununu çözer.



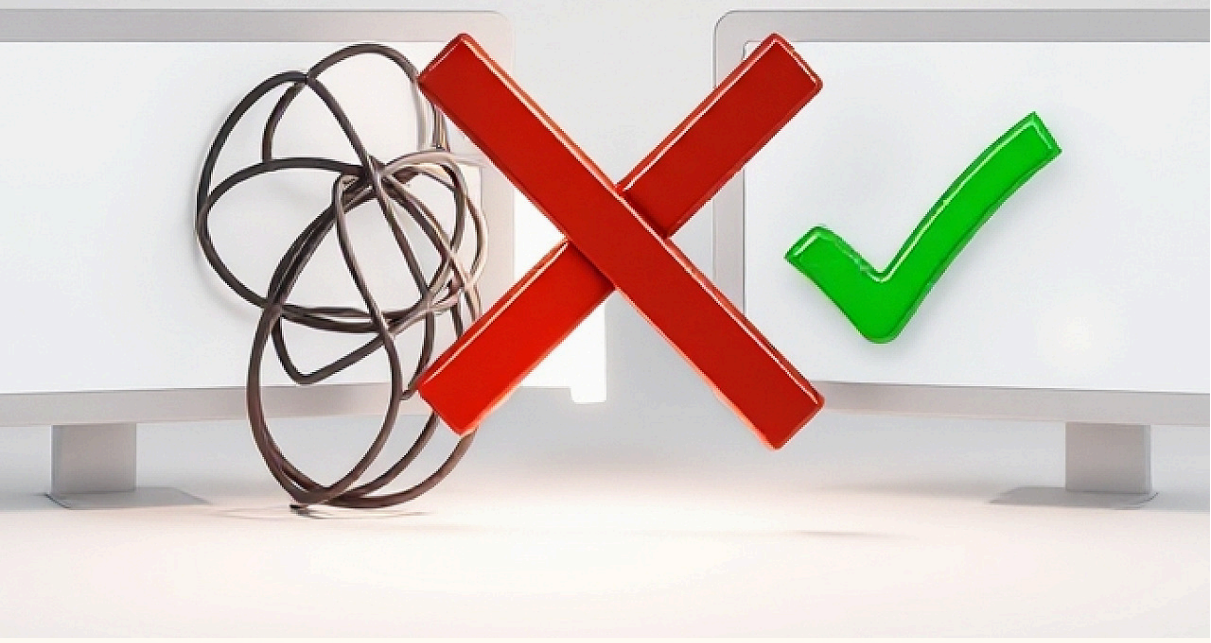
Asimetrik yöntemler simetrik olanlardan daha yavaş ve daha ağırdır. Daha fazla hesaplama gücü gerektirir ve büyük miktarda veriyi şifrelemek için ideal değildir. Bu yüzden asimetrik şifreleme genellikle gerçek veri aktarımı için kullanılmaz. Bunun yerine anahtar anlaşması ve dijital imzalar gibi daha küçük görevler için kullanılır.



İki yöntem sıklıkla birleştirilir; her biri en iyi yaptığı işi üstlenir. Asimetrik şifreleme, anahtar üzerinde anlaşma gibi zor kurulum işlerini yürütür. Simetrik şifreleme hızlı olduğu için asıl veri yükünü üstlenir. Bu birleşim sana hem güvenlik hem de hız verir. Günümüzde çoğu güvenli bağlantı iki yöntemi birlikte kullanır.



Güvenli bir bağlantı kurulurken anahtar anlaşması için asimetrik yöntemler kullanılır. Bu, her iki tarafın güvenle ortak bir gizli anahtar üzerinde anlaşmasını sağlar. Ortak gizli anahtar üzerinde anlaşıldıktan sonra gerçek veri aktarımı için simetrik şifreleme devreye girer. Asimetrik kısım anahtar alışverişini, simetrik kısım ise veriyi korur.



Tipik karışıklıkları gider: açık anahtar gizli değildir; paylaşılmak içindir. Özel anahtar asla paylaşılmaz; sahibinde kalır. Simetrik daha güvenli demek değildir; her yöntemin kendi rolü vardır. Simetrik daha hızlıdır, asimetrik anahtar alışverişi sorununu çözer. İkisini birlikte kullanmak iki dünyanın en iyisini verir.



Özetle: simetrik şifreleme, veriyi hem kilitlemek hem de açmak için tek bir ortak gizli anahtar kullanır. Asimetrik şifreleme, açık anahtarın kilitlediği ve özel anahtarın kilidini açtığı bir açık-özel anahtar çifti kullanır. Birlikte bağlantıları güvence altına alırlar; anahtar anlaşması için asimetrik, veri için hızlı simetrik şifreleme kullanılır.