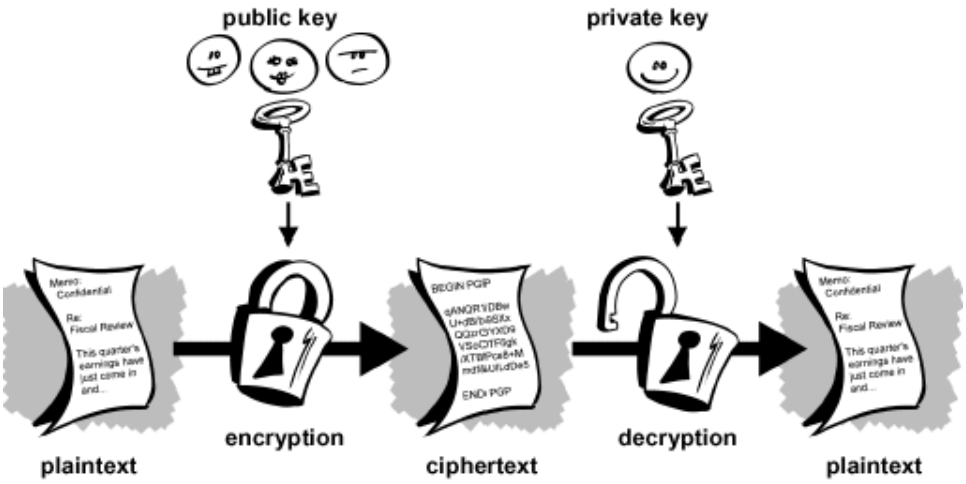
Asimetrik Şifreleme veya Açık Anahtar Şifreleme(Asymmetric encryption(Public Key Encryption):

Bu yazımda sizlere, Kriptografinin bel kemiği olan, Asimetrik şifrelemeyi anlatacağım. Asimetrik şifrelemeyi anlatmadan önce Simetrik şifreleme nasıl çalışıyor bilmemiz gerekiyor çünkü Asimetrik şifreleme ve Simetrik şifreleme, birbirleri ile ilişkili çalışıyor. Bunla ilgili yazımıda web sitemde bulabilirsiniz. 1970 yılında temelleri atılan Asimetrik şifreleme, Simetrik şifrelemenin getirmiş olduğu güvenlik zafiyeti için geliştirildi. Simetrik şifrelemenin çalışma prensibini çok kısa özet geçmek gerekirse, Hem şifreleme hem de şifre çözme için bir anahtarın kullanılmasını içerir. İşte bu noktada Simetrik şifrelemenin zafiyeti doğuruyor. Şifrelemeyi yapacak olan Secret Key'in(gizli anahtarın) alıcıdada bulunması gerekiyor. internet gibi güvensiz bir dünyada bu anahtarın doğrudan ulaşması bizim için bir zafiyet. ve bunun üzerine Asimetrik şifreleme veya diğer adı Açık anahtar şifrelemesi hayatımıza giriyor, Asimetrik şifrelemede 2 tür anahtarımız var, Public Key(Açık anahtar) ve Private Key(Gizli Anahtar).

***Public Key**: Güvenli veya Güvensiz, Bütün her yerde özgürce paylaşabileceğiniz anahtar. Bir kişi bize veri yollamak istediği zaman bu anahtarı kullanır.*

***Private Key**: İlgili kişi hariç kimseyle paylaşılmaması gereken Anahtar, Public Key anahtarımız ile bize yollanan veriyi, Bu anahtarı kullanarak çözümleyebiliyoruz.*

Çalışma prensibini anlatmak gerekirse, Bir kişi bize veri yollamak istediği zaman, Herkese açık olan Public Key anahtarımıza veriyi şifreler ve bize yollar. Biz ise Private Key anahtarımızı kullanarak, Public key anahtarının şifresini çözebiliriz. Eğer biz bir kişiye veri yollamak istersek aynı işlemi bizde tekrarlarız. Anlattığım bu çalışma prensibini, aşağıdaki görsel ile birleştirirseniz, olaya daha vakıf olacağınıza inanıyorum.

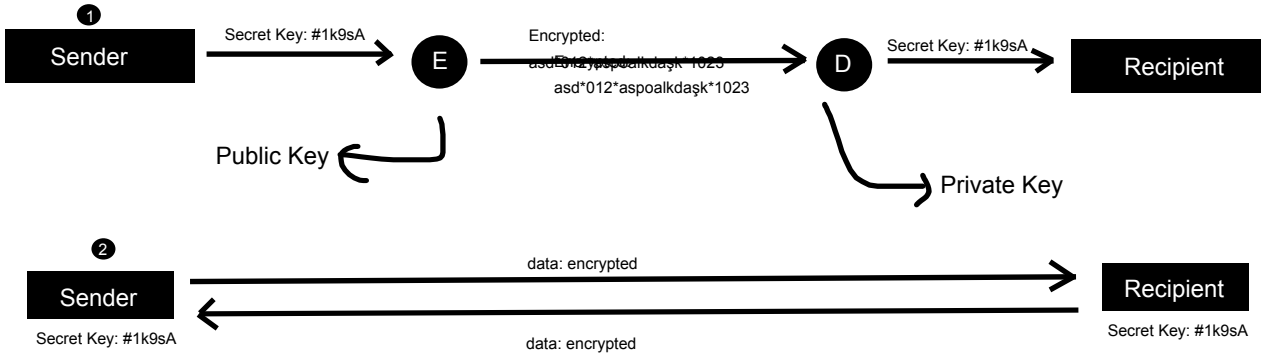


Bu yazıdan önce Asimetrik şifrelemenin çalışma prensibi ile ilgili bir yazı okuduysanız, şöyle bir yazı görmüşsünüzdür diye düşünüyorum.

"Bir veri yollamak istediğimiz zaman, Private key anahtarımıza ile veriyi şifreler ve hedefe yollarız, hedef ise Public Key anahtarımız ile Şifreyi çözer."

evet bu çalışma prensibi doğru. Nedeni ise, Private Key ile Public Key anahtarlarının, birbirlerini çözümleyebilmesi. fakat Public key anahtarının herkeste olması nedeniyle, bu bir güvenlik problemi oluşturur. Stack overflow veya Quora gibi forumları okuduğumuz zaman, bu durumu tartışan insan sayısı çok fazla. Bunuda bilmekte faydalı olacağını düşünüyorum çünkü mülakatlarda, Asimetrik nedir ve nasıl çalışır sorusunun üzerine, bazı hocalarımız bu durumuda izah etmenizi isteyebilir. ama genelde bu sorunun cevabı, yukarıda anlattığım çalışma prensibi diyebilirim.

Asimetrik Şifrelemenin en büyük sorunu ise, Hız konusu. Bunu her yazımda beyan ediyorum. Bilgisiyar dünyasında hız çok önemlidir. Bir düşünün, bir veri yollamak istediğimiz zaman durmadan Public key ile şifreliyip karşı tarafa mı yollayacağız, Tabi ki de hayır, işte bu noktada Asimetrik şifreleme ile Simetrik şifreleminin, birbirleri ile ilişkili çalıştığı durum doğuyor. Simetrik Şifrelemede, şifrelemeyi yapan anahtar ile şifreyi çözecek anahtarın aynı olması gerektiğini biliyoruz. peki alıcı taraf, bu gizli anahtara(secret key) güvenlik bir şekilde nasıl sahip olacak?. işte bu sorunun cevabını, Asimetrik şifreleme ile çözüyoruz. Karşı tarafa ulaştırmak istediğimiz gizli anahtarı(secret key), Karşı tarafın Public key'ini kullanarak, ulaştırıyoruz. bu anlatılan durumu, aşağıdaki örnek üzerinden daha vakıf olacağınıza inanıyorum.



Asimetrik şifrelemenin en basit anlatımı bu olduğuna inanıyorum. Bir çok insanın yanlış düştüğü algı, Veri transferinin Asimetrik şifreleme ile yapıldığı yönünde, bu algıyı yukarıda anlattığım diyagram üzerinden bitirdiğime inanıyorum. Asimetrik şifreleme dediğimiz zaman, aklınıza HTTPS ve SSH protokolleri gelebilir. çok kısa şunu söyleyebilirimki Asimetrik şifrelemenin HTTPS ve SSH protokollerinde çalışma prensibi birbirlerinden farklı, bunun için Sertifaka otoritelerine ve SSH-Key çalışma prensibini bilmemiz gerekiyor. bunlarda web sitemde mevcut, okumanızı tavsiye ederim.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/