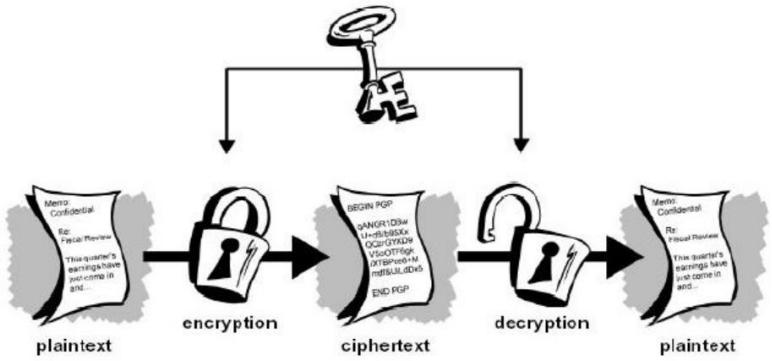
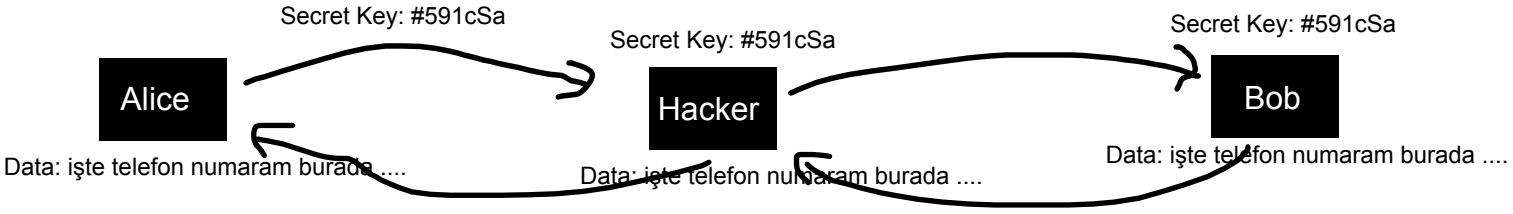
Simetrik Şifrelme:

Bu yazımda size binlerce yıl öncesine dayanan şifreleme biçimi olan Simetrik şifreleme türünü anlatacağım, en basit şekilde ve matematiksel temele inmeden size çalışma prensibini lanse etmeye çalışacağım. aslında simetrik şifreleme türü, günümüz dünyasında çok sıkça kullandığımız bir şifreleme türü, bugün evinizden çıktıktan sonra kapıyı kitlediğiniz bir durumda, sizde bulunana anahtarın kopyası başka birisinde mevcut ise(kardeş,baba...) evin kapısını açabilir. işte bu örnek üzerinden yola çıkarsak, İnternet dünyasında şifreleri bir veri yollamak istediğimiz zaman, Veriyi şifrelemede kullanılan anahtar aynı zamanda çözümleme amacıyla da kullanılır. Bunu örnek üzerinden anlatmak gerekirse.



her gün çok sıklıkla duyduğumuz simetrik şifrelemenin çalışma prensibi en basit anlatımı hali bu olduğuna inanıyorum. Simetrik şifreleme günümüz dünyasında çok sıklıkla veri transferinde kullandığımız bir şifreleme türü, bunun böyle olmasının nedeni, diğer şifreleme biçimlerinde kat ve kat daha hızlı olması. Benim ilk öğrendiğimde kendime şu soru soruyu sordum, benim şifrelediğim anahtarı karşı tarafa nasıl gidiyor, işte burada Simetrik şifreleme biçiminin zafiyeti ortaya çıkıyor. Bir veri yollamak istediğimiz zaman, karşı tarafla hangi secret key(gizli anahtar) kullanacağı konusunda anlaşma sağlamamız gerekiyor, ve işte o anlaşma sırasında ağda sniffing yapan bir kişi varsa ve belirlenmiş olan secret key(gizli anahtarı) ele geçirirse, şifreli mesajları hepsini, şifresiz hale getirir ve gizliliği ortadan kaldırır, bunu aşağıdaki örnek üzerinden olaya daha vakıf olacağınız inanıyorum.



işte bu simetrik şifrenin getirmiş olduğu en büyük sorundu, bu sorunun üzerine hayatımıza asimetrik şifreleme dahil oldu,bunu burada anlatmayacağım fakat çok kısa bilgi vermek açısından şunu söyleyebilirimki, secret key değerimizi, Asimetrik şifreleme biçimini kullanarak ulaştırıyoruz karşı tarafa.

bu konuya daha vakıf olmak için web sitemden Asimetrik şifreleme biçimine ve SSL/TLS yazısına bakmanızı öneriyorum. Tabi ki de simetrik şifreleme türlerinide konuşmak gerekiyor özellikle AES,DES ve bit kavramlarını fakat şimdilik bunu bilmeniz sizin yararınız olacaktır.

e-mail

berathanakcakaya@gmail.com

linkedin

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