Simetrik ve Asimetrik Şifreleme

Öncelikle bizim bilgilerimizi veya dosyamızı, bir iletişim halinde başka bir kişiye gönderirken bu dosyanın veya bilginin gizli olması ve başka birimler tarafından bu bilgilere erişilmemesi önemlidir. Bu dosyaya erişebilse bile bu dosyanın içerisindeki bilgileri şifreli olmalı , böylece başka taraflar tarafından dosya alınsa bile okuyamamalıdır bunun için karmaşık ve zor hale getirmemizi sağlayan simetrik ve asimetrik şifrelemeler bulunmaktadır.

Simetrik Şifrelemede ortak bir anahtar bulunur bu anahtar sayesinde metinleri şifreler ve aynı anahtarla şifrelenmiş metinleri açık metine çevirir. Fakat bu anahtar başka birinin eline geçer ise bu anahtar sayesinde bizim okuduğumuz gibi başkaları da bu metini okuyabilir. Sadece bir anahtar kullanıcağımız için bu şifreleme hızlı bir şifrelemedir , uzun bir anahtarı yoktur, kolay ve anlaşılır bir yapısı vardır. Öte yandan kötü yanları ise; Kimlik doğrulaması yoktur böylece anahtarı olan herkes metini çözebilecektir.

Asimetrik Şifrelemede ise Simetrik Şifrelemede anahtarların dağıtılması gibi sorunlardan başa çıkılması nedeniyle çıkmıştır. Burada ise kişilerin kendi özel anahtarları(“Private”) ve ortak olarak dağıttığı bir anahtar (“Public”) bulunmakta. Burda şifreleme yapılırken karşısındaki kişi ile belirlenen ortal bir anahtar ile metini şifreler ve bunu açan tek şifre karşıdaki kişinin gizli anahtarı olacaktır. Böylece sadece 2 anahtar yani public ve private key kullanılarak başka insanların buna erişimi engellenmiş olacaktır. Private key sayesinde bu sifrelemede kimlik doğrulamada olacaktır sistemde anahtar kalabalığı olmıyacaktır ve daha güvenlidir fakat kötü yanı ise simetriğe göre daha yavaş olacatır süreçleri daha fazla olduğundan ve performans acısından simetriğe göre daha çok zorlama olacaktır. Örneğin:

Let be p = 3 and q = 11.

1. Compute **n = p * q = 3 * 11 = 33**
2. Compute **φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20**
3. Choose, e.g., the encryption key **e = 7** that satisfies the following two conditions:
   - 1 < e = 7 < φ(n) = 20 and
   - e = 7 and φ (n) = 20 are coprime.
4. Compute a value for the decryption key **d** that satisfies the following condition:
   - (d * e) % φ(n) = 1.
   - One solution is **d = 3** because (3 * 7) % 20 = 1
5. Public key is **(e, n) => (7, 33)**
6. Private key is **(d, n) => (3, 33)**

Let, e.g., m = 2 be the clear text to be encrypted with the public key **(e, n) => (7, 33)**.

7. *For encryption,* compute $c = m^e \% n$ => $\mathbf{c = 2^7 \% 33 = 29}$
8. *For decryption*, compute $m = c^d \% n$ => $\mathbf{m = 29^3 \% 33 = 2}$

-Ruhat Özgün Özcan