RSA Algorithm in Cryptography

Kriptografide RSA Algoritması

Asimetrik kriptografiye bir örnek:

1. Bir istemci (örneğin tarayıcı) genel anahtarını sunucuya gönderir ve bazı veriler ister.
2. Sunucu, istemcinin genel anahtarını kullanarak verileri şifreler ve şifrelenmiş verileri gönderir.
3. İstemci bu verileri alır ve şifresini çözer.

Kriptografide RSA Algoritması

Fikir! RSA fikri, büyük bir tam sayıyı çarpanlara ayırmanın zor olduğu gerçeğine dayanmaktadır. Genel anahtar, bir sayının iki büyük asal sayının çarpımı olduğu iki sayıdan oluşur. Özel anahtar da aynı iki asal sayıdan türetilir. Yani birisi büyük sayıyı çarpanlara ayırabilirse özel anahtar tehlikeye girer. RSA anahtarları genellikle 1024, 2048 veya 4096 bit uzunluğunda olabilir. Dolayısıyla şifreleme gücü tamamen anahtar boyutuna bağlıdır ve anahtar boyutunu iki veya üç katına çıkarırsak şifrelemenin gücü katlanarak artar.

RSA algoritmasının arkasındaki mekanizmayı öğrenelim : >> Genel Anahtar Oluşturma:

İki asal sayı seçin. **P = 53 ve Q = 59** olduğunu varsayalım

. Şimdi Genel anahtarın ilk kısmı: n = P*Q = 3127.

Ayrıca e diye küçük bir üsse de ihtiyacımız var : **Ama e Bir tamsayı olmalı .**

1 < e < Φ(n) Şimdi bunun 3'e eşit olduğunu düşünelim.

Açık Anahtarımız n ve e'den yapılmıştır

>> Özel Anahtar Oluşturma:

Φ(n) : Öyle ki **Φ(n) = (P-1)(Q-1)** hesaplamamız gerekir
, yani Φ(n) = 3016
Şimdi Özel Anahtarı hesaplayalım, **d :**
d = (k*Φ(n) + 1) / e bazı k tamsayıları için
k = 2 için d'nin değeri 2011'dir.

Şifreleme adımı

Artık – Genel Anahtarımız (n = 3127 ve e = 3) ve Özel Anahtarımız (d = 2011) ile hazırız.

Şimdi “HI” yı şifreleyeceğiz :

Harfleri sayılara çeviririz : H = 8 ve I = 9

Böylece **Şifrelenmiş Veri** $\mathbf{c = (89^{e}\ )mod\ n}$

Böylece Şifrelenmiş Verimiz 1394 olur.

Şifre Çözme adımı

Şimdi şifresini çözeceğiz **1394** : Şifresi **Çözülmüş Veri = (c^d) mod n**

Böylece Şifrelenmiş Verimiz Veriler 89 -> 8 = H ve I = 9 yani "HI" olarak çıkıyor