Açık Anahtar Kriptografi ve RSA Nedir?

Çalışma Kağıdı

Açık anahtar kriptografi, her kullanıcı için birbiriyle ilişkili iki anahtar (biri açık, diğeri özel) kullanarak iletişimin gizliliğini ve bütünlüğünü sağlar. RSA algoritması, bu anahtar çiftlerini üretmek için büyük asal sayıların çarpımının çarpanlarına ayrılmasının zorluğuna dayanır.

$$E(m) = m^e \pmod{n} \quad D(c) = c^d \pmod{n}$$

m = Mesaj (plaintext)
E = Şifreleme fonksiyonu
c = Şifreli mesaj (ciphertext)
D = Şifre çözme fonksiyonu
e = Açık anahtar (public exponent)
d = Özel anahtar (private exponent)

Sorular

1. RSA algoritmasında, şifreleme için hangi anahtar kullanılır?
A) Özel Anahtar
B) Açık Anahtar
C) Her İki Anahtar
D) Hiçbiri

2. Aşağıdakilerden hangisi açık anahtar kriptografisinin bir avantajı DEĞİLDİR?
A) Gizlilik
B) Bütünlük
C) Hız
D) Kimlik Doğrulama

3. RSA'da n değeri nasıl hesaplanır?
A) İki büyük asal sayının toplamı
B) İki büyük asal sayının çarpımı
C) Bir asal sayının karesi
D) İki sayının EBOB'u

4. RSA ile basit bir şifreleme ve şifre çözme örneği yapalım.

5. Açık anahtar kriptografisinin temel avantajları nelerdir?

6. Tanımla: Açık Anahtar Kriptografisi Nedir?

7. Tanımla: RSA Algoritmasının Temeli Nedir?

8. Tanımla: RSA'da Açık Anahtar Nedir?

Cevap Anahtarı

1. B) Açık Anahtar — RSA'da şifreleme işlemi, alıcının açık anahtarı (e, n) kullanılarak yapılır.

2. C) Hız — Açık anahtar kriptografisi, simetrik kriptografiye göre genellikle daha yavaştır.

3. B) İki büyük asal sayının çarpımı — RSA'da modülüs n, p ve q gibi iki büyük asal sayının çarpımı olarak elde edilir.

4. 1. Alice, iki büyük asal sayı seçer: p=61, q=53. Modülüs n = p*q = 61 * 53 = 3233.,2. Euler'in totient fonksiyonu hesaplanır: φ(n) = (p-1)*(q-1) = 60 * 52 = 3120.,3. Açık anahtar 'e' seçilir. e, 1 < e < φ(n) ve e ile φ(n) aralarında asal olmalı. Örneğin, e=17.,4. Özel anahtar 'd' hesaplanır. d, e*d ≡ 1 (mod φ(n)) olmalı. 17*d ≡ 1 (mod 3120). Genişletilmiş Öklid algoritması ile d=2753 bulunur.,5. Alice'in açık anahtarı (e=17, n=3233), özel anahtarı (d=2753, n=3233).,6. Bob, Alice'e 'Merhaba' mesajını göndermek istiyor. Mesajı sayıya çevirir (örneğin, 'H' = 8).,7. Bob, mesajı Alice'in açık anahtarıyla şifreler: c = 8^17 mod 3233 = 2790.,8. Alice, şifreli mesajı kendi özel anahtarıyla çözer: m = 2790^2753 mod 3233 = 8. Orijinal mesaj 'H' elde edilir.

5. 1. Gizlilik: Sadece özel anahtara sahip olan kişi mesajı okuyabilir.,2. Bütünlük: Mesajın gönderildikten sonra değiştirilmediğinden emin olunur.,3. Kimlik Doğrulama: Gönderenin kimliği doğrulanabilir (dijital imza ile).,4. Anahtar Değişimi: Güvenli bir kanal olmadan bile anahtar değişimi yapılabilir.

6. Her kullanıcı için bir açık ve bir özel anahtar çifti kullanan şifreleme yöntemidir.

7. Büyük asal sayıların çarpımının çarpanlarına ayrılmasının zorluğudur.

8. Şifreleme için kullanılır ve herkesle paylaşılabilir (e, n).