Kriptografik Algoritmalar Nedir?

Çalışma Kağıdı

Kriptografik algoritmalar, veriyi şifreleyerek (gizleyerek) ve şifreyi çözerek (orijinal haline getirerek) dijital iletişimin ve depolamanın güvenliğini sağlayan matematiksel işlemler bütünüdür.

Sorular

1. Aşağıdakilerden hangisi kriptografik algoritmaların temel amacıdır?

A) Veri sıkıştırma
B) Veri gizliliğini ve bütünlüğünü sağlama
C) Veri formatını değiştirme
D) Veri yedekleme

2. Simetrik şifrelemede kaç anahtar kullanılır?

A) Bir açık anahtar
B) Bir gizli anahtar
C) Bir çift anahtar
D) Tek bir anahtar

3. RSA algoritması hangi şifreleme türüne örnektir?

A) Simetrik Şifreleme
B) Asimetrik Şifreleme
C) Özet Fonksiyonu
D) İkili Şifreleme

4. Simetrik Şifreleme (AES) Örneği

5. Asimetrik Şifreleme (RSA) Örneği

6. Özet Fonksiyonu (SHA-256) Örneği

7. Tanımla: Simetrik Şifreleme

8. Tanımla: Asimetrik Şifreleme

9. Tanımla: Özet Fonksiyonu (Hash)

Cevap Anahtarı

1. B) Veri gizliliğini ve bütünlüğünü sağlama — Kriptografik algoritmalar, veriyi yetkisiz erişime karşı koruyarak gizliliğini ve değiştirilmediğini garanti eder.

2. D) Tek bir anahtar — Simetrik şifrelemede, hem şifreleme hem de şifre çözme için aynı tek anahtar kullanılır. Bu bazen bir çift anahtar gibi algılanabilir ancak özünde tek bir gizli anahtar söz konusudur.

3. B) Asimetrik Şifreleme — RSA, açık anahtar ve gizli anahtar olmak üzere iki farklı anahtar kullandığı için asimetrik şifreleme türüne örnektir.

4. 1. Gönderici, veriyi şifrelemek için gizli bir anahtar kullanır. 2. Şifrelenmiş veri ağ üzerinden gönderilir. 3. Alıcı, aynı gizli anahtarı kullanarak veriyi çözer.

5. 1. Gönderici, alıcının açık anahtarını kullanarak veriyi şifreler. 2. Şifrelenmiş veri gönderilir. 3. Alıcı, kendi gizli anahtarını kullanarak veriyi çözer.

6. 1. Herhangi bir boyuttaki veri, sabit uzunlukta benzersiz bir özet (hash) değere dönüştürülür. 2. Bu özet, verinin bütünlüğünü kontrol etmek için kullanılır.

7. Aynı anahtar hem şifreleme hem de şifre çözme için kullanılır (örn: AES).

8. Farklı anahtarlar (açık ve gizli) kullanılır (örn: RSA).

9. Verinin bütünlüğünü kontrol etmek için kullanılır, geri döndürülemez (örn: SHA-256).