Kriptografi ve Şifreleme Temelleri Nedir?

Çalışma Kağıdı

Kriptografi, bilgiyi gizli tutmak, bütünlüğünü doğrulamak ve kimlik doğrulaması sağlamak için matematiksel teknikler kullanan bir alandır. Şifreleme ise bu tekniklerden biridir ve düz metni (plaintext) şifreli metne (ciphertext) dönüştürme işlemidir.

Sorular

1. Aşağıdakilerden hangisi kriptografinin temel amaçlarından biri DEĞİLDİR?
A) Gizlilik (Confidentiality)
B) Bütünlük (Integrity)
C) Erişilebilirlik (Availability)
D) Kimlik Doğrulama (Authentication)

2. Asimetrik şifrelemede kullanılan anahtar çifti nasıldır?
A) Tek bir gizli anahtar
B) Açık anahtar ve özel anahtar
C) Çoklu gizli anahtar
D) Rastgele oluşturulmuş birkaç anahtar

3. Bir mesajın iletim sırasında değiştirilmediğini garanti eden prensip hangisidir?
A) Gizlilik
B) Kimlik Doğrulama
C) Bütünlük
D) Erişilebilirlik

4. Basit bir Sezar şifrelemesi örneği nedir?

5. Simetrik ve asimetrik şifreleme arasındaki temel fark nedir?

6. Tanımla: Kriptografi

7. Tanımla: Şifreleme (Encryption)

8. Tanımla: Şifre Çözme (Decryption)

Cevap Anahtarı

1. C) Erişilebilirlik (Availability) — Erişilebilirlik (Availability), kriptografinin doğrudan bir amacı değildir; daha çok sistem güvenliği ve sürekliliği ile ilgilidir. Gizlilik, bütünlük ve kimlik doğrulama ise temel amaçlarıdır.

2. B) Açık anahtar ve özel anahtar — Asimetrik şifreleme, bir açık anahtar (herkesle paylaşılabilir) ve bir özel anahtar (gizli tutulur) çiftini kullanır. Açık anahtar ile şifrelenen veri, yalnızca karşılık gelen özel anahtar ile çözülebilir.

3. C) Bütünlük — Bütünlük (Integrity), verinin iletim veya saklama sırasında yetkisiz kişilerce değiştirilmediğini garanti eder. Bu genellikle özet fonksiyonları (hash functions) ile sağlanır.

4. 1. Orijinal metin: 'MERHABA' 2. Anahtar (kaydırma miktarı): 3 3. Her harfi alfabede 3 sıra kaydır: M->P, E->H, R->U, H->K, A->D, B->E, A->D 4. Şifreli metin: 'PHUKADE'

5. 1. Simetrik şifrelemede: Şifreleme ve şifre çözme için TEK bir gizli anahtar kullanılır. 2. Asimetrik şifrelemede: Şifreleme için BİR açık anahtar ve şifre çözme için KARŞILIKLI bir özel anahtar kullanılır.

6. Bilgiyi gizli, bütünlüklü ve doğrulanabilir tutmak için matematiksel teknikler bütünü.

7. Düz metni (plaintext) okunamaz şifreli metne (ciphertext) dönüştürme işlemi.

8. Şifreli metni (ciphertext) tekrar okunabilir düz metne (plaintext) dönüştürme işlemi.