# Kriptografi ve Şifreleme Algoritmaları Nedir?

Çalışma Kağıdı

Kriptografi, bilgiyi gizlemek ve güvenli bir şekilde iletmek için kullanılan matematiksel teknikler bütünüdür. Şifreleme algoritmaları ise bu teknikleri uygulayan yöntemlerdir.

## Sorular

1. Hangi şifreleme türünde gönderici ve alıcının aynı anahtarı kullanması gerekir?
A) Asimetrik Şifreleme
B) Simetrik Şifreleme
C) Hibrit Şifreleme
D) İstasyonel Şifreleme

2. Bir mesajın değiştirilmediğini garanti eden kriptografik özellik nedir?
A) Gizlilik
B) Kimlik Doğrulama
C) Bütünlük
D) Erişilebilirlik

3. Aşağıdakilerden hangisi yaygın bir şifreleme algoritmasıdır?
A) HTTP
B) AES
C) HTML
D) SQL

4. Basit bir Sezar şifrelemesi nasıl çalışır?

5. Simetrik ve asimetrik şifreleme arasındaki temel fark nedir?

6. Tanımla: Kriptografi

7. Tanımla: Şifreleme (Encryption)

8. Tanımla: Şifre Çözme (Decryption)

# Cevap Anahtarı

1. B) Simetrik Şifreleme — Simetrik şifrelemede, veriyi şifrelemek ve şifreyi çözmek için aynı gizli anahtar kullanılır.

2. C) Bütünlük — Bütünlük, verinin iletim sırasında veya saklanırken yetkisiz kişilerce değiştirilmediğini garanti eder.

3. B) AES — AES (Advanced Encryption Standard), günümüzde yaygın olarak kullanılan güçlü bir simetrik şifreleme algoritmasıdır.

4. Her harf, alfabede belirli bir sayıda (örneğin 3) kaydırılarak şifrelenir. 'A' harfi 'D' olur, 'B' harfi 'E' olur vb. Çözmek için ters yönde kaydırma yapılır.

5. Simetrik şifrelemede aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. Asimetrik şifrelemede ise biri gizli (özel) diğeri açık (genel) olmak üzere iki farklı anahtar kullanılır.

6. Bilginin gizliliğini, bütünlüğünü ve kimlik doğruluğunu sağlama bilimi.

7. Okunabilir veriyi (açık metin) okunamaz hale getirme (şifreli metin) süreci.

8. Şifreli metni tekrar okunabilir açık metne dönüştürme süreci.