Araştırma Ödevi Yönergesi

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ ALGORİTMALARI

Öğrenci Adı:	.....	**Sınıf / Şube:**	.....
Okul No:	.....	**Teslim Tarihi:**	.... / .... / 2026

ÖDEV ADIMLARI VE GÖREV TANIMI

Aşağıda verilen adımları sırasıyla gerçekleştirerek araştırma ödevinizi zamanında ve eksiksiz olarak tamamlayınız.

1 **Temel Şifreleme Algoritmaları:** Kişisel bilgilerin ve verilerin korunmasında kritik rol oynayan temel şifreleme algoritmalarını (**AES, DES, RSA** gibi) detaylıca araştırınız.

2 **Çalışma Mantığı ve Veri Güvenliği:** Bu algoritmaların teknik olarak nasıl çalıştığını (simetrik/asimetrik yapılarını) ve dijital ortamlarda ne tür bir veri güvenliği (gizlilik, bütünlük, kimlik doğrulama) sağladığını inceleyiniz.

Veri Şifreleme (AES / DES / RSA)

Asal Sayı Dışı Matematik (Eliptik Eğri Kriptografisi)

Geleceğin Teknolojisi (Kuantum Kriptoloji)

3 **Asal Sayı Kullanmayan Yöntemler:** RSA mimarisinin aksine, güvenliğini asal sayı çarpanlarına ayırma zorluğundan almayan alternatif şifreleme yöntemlerini (**Eliptik Eğri Kriptografisi - ECC** gibi) araştırınız.

4 **Kuantum Bilgisayarlar ve Gelecek:** Gelecekte hayatımıza girecek olan kuantum bilgisayarların, mevcut kriptoloji yöntemleri üzerindeki tehditlerini ve bu alana getirebileceği yenilikleri (Kuantum Sonrası Kriptografi) analiz ediniz.