|  |  |
| --- | --- |
| ***Kodu ve Adı:*** | **MAT6220 Sayılar Teorisi ve Kriptoloji** |
| ***Birimi:*** | Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı |
| ***Ayrıntısı:*** | **Dönemi:** | 2023-2024 Bahar | **Statüsü:** | Seçmeli | **Sınıfı:** | 1 | **Kredisi:** | 3-0-0-3 | **AKTS:** | 6 | **Dili:** | Türkçe |

|  |  |  |
| --- | --- | --- |
| **Ders Sorumlusu** |  | **Ders Yardımcısı** |
| Unvanı, Adı ve Soyadı: |  **……** |  | Unvanı, Adı ve Soyadı: | **……** |
| Telefon: | **……** | Telefon: | **……** |
| E-posta: | **.......@firat.edu.tr** | E-posta: | **……** |
| Sosyal Hesap: | **……** | Sosyal Hesap: | **……** |
| Öğrenci Günü ve Saati: | **……** | Öğrenci Günü ve Saati: | **……** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Ders Haftalık***  | ***Pazartesi*** | ***Salı*** | ***Çarşamba*** | ***Perşembe*** | ***Cuma*** | ***Cumartesi*** |
| ***Programı:*** |  |  |  |  |  |  |

|  |  |
| --- | --- |
| ***İşlenişi:*** |  **Haftalık her saat için en az 45 dakika yüz yüze yapılacaktır.** |
| ***Yeri:*** | **YY:** |  Sınıf Yazılacak  | **UE:** |  **-**  |

|  |  |
| --- | --- |
| ***Amacı:*** | Bu dersin amacı Kriptoloji ile bağlantısını vermeden önce sayılar teorisinin temel tanım ve teoremlerini vermektir. |

|  |  |
| --- | --- |
| ***Materyali:*** | 1. Elementary Number Theory, David M. Burton 2-Sayılar Teorisi ve Uygulamaları, Hüseyin Altındiş 2. Ankara Üniversitesi, Açık Ders Malzemeleri, Ders notları. |

|  |  |
| --- | --- |
| ***Öğrenci******Sorumluluğu:*** |  **Öğrencilerin derse %70 devam sorumluluğu vardır.**  |

|  |  |  |  |
| --- | --- | --- | --- |
| ***Haftalık Ders Planı*** | **Hafta** | **Konu** | **Yöntem** |
| **1** | Dersin Amacı ve Planlama: Ders gerekçesi, içeriği, planı ve işleniş biçiminin tanıtılması, Ders kaynaklarının tanıtılması, Ders çıktılarının önemi, Ders konularıyla ilgili güncel konular. | **YY** |
| **2** | Konu Başlığı: Tam Sayılar Alt konu başlıkları: İyi Sıralılık Prensibi, İndüksiyon | **YY** |
| **3** | Konu Başlığı: Finonacci Sayıları Alt konu başlıkları: Finonacci Sayıları ve özellikleri | **YY** |
| **4** | Konu Başlığı: Bölünebilme, Asal sayılar Alt konu başlıkları: Bölünebilme, Asal sayılar, Asalların Dağılımı, Asallarla ilgili konjektür | **YY** |
| **5** | Konu Başlığı: En Büyük Ortak Bölen , En Küçük Ortak Kat Alt konu başlıkları: En Büyük Ortak Bölen , En Küçük Ortak Kat ve özellikleri | **YY** |
| **6** | Konu Başlığı: Euclid Algoritması Alt konu başlıkları: Euclid Algoritması ve özellikleri | **YY** |
| **7** | Konu Başlığı: Aritmetiğin Temel Teoremi Alt konu başlıkları: Aritmetiğin Temel Teoremi ve ilgili örnekler | **YY** |
| **8** | Konu Başlığı: Fermat Çarpanlara Ayırma Yöntemi Alt konu başlıkları: Fermat Çarpanlara Ayırma Yöntemi ve özellikleri | **YY** |
| **9** | Konu Başlığı: Ara Sınav Alt konu başlıkları: Ara sınav yapılır | **YY** |
| **10** | Konu Başlığı: Açık Anahtar Kripto Sistemleri Alt konu başlıkları: Trapdoor tek yönlü fonksiyon, Anahtar Alışverişi | **YY** |
| **11** | Konu Başlığı: Dijital İmza ve Özet Fonksiyonlar Alt konu başlıkları: RSA de imza, Özet fonksiyonları | **YY** |
| **12** | Konu Başlığı: Konu Başlığı: Dijital İmza ve Özet Fonksiyonlar Alt konu başlıkları: RSA de imza, Özet fonksiyonları | **YY** |
| **13** | Konu Başlığı: Dijital İmza ve Özet Fonksiyonlar Alt konu başlıkları: Kriptografik özet fonksiyon | **YY** |
| **14** | Konu Başlığı: Eliptik Eğri Çarpanlara Ayırma Metodu Alt konu başlıkları: p-1 Algoritması, Eliptik egri çarpanlara ayırma algoritması | **YY** |
| ***Ölçme ve Değerlendirme*** |  | **Metot** | **Sayı** | **Ağırlık** |
| **Ara** **Sınav** | Sınav |  Yüz yüze | 1  |  %50  |
| Kısa Sınav |  Yapılmayacaktır. |  -  |   |
| Ödev | Ara sınav öncesi ve sonrası etkinlikler verilecektir. | 2  |   |
| Proje |  Verilmeyecektir. |  - | - |
|   |   |   |   |
| **Genel** **Sınav** |  Yüz Yüze  | 1  | %50  |
| ***Ders Kazanımları*** | **1** | Sayılar Teorisi ve Kriptoloji ilişkisini öğrenir. |
| **2** | Açık Anahtar Kripto Sistemlerinni öğrenir. |
| **3** | Dijital İmza ve Özet Fonksiyonları öğrenir. |
| **4** | Eliptik Eğri Kripto Sistemlerini öğrenir. |
| **5** | Kriptolojinin tanımını ve RSA Kripto Sistemi, ElGamal Kripto Sistemini öğrenir. |
| **Derse Özel Açıklamalar:** |
| **UE:** Uzaktan Eğitim; **YY:** Yüz Yüze Eğitim |