## İTÜ Bilişim Enstitüsü

**Bilişim Uygulamaları Anabilim Dalı**

**Bilgi Güvenliği Mühendisliği ve Kriptografi Doktora Programı**

**Doktora Yeterlik Yazılı Sınavları Kapsam Belirleme Formu**

2019-2020 eğitim-öğretim yılı Güz/Bahar döneminde yapılacak doktora yeterlik birinci ve ikinci yazılı sınavları için konu tercihleri aşağıda yer alan tablolarda işaretlenmelidir.

**Öğrencinin :**

Adı-Soyadı : Tarih:

Öğrenci No : İmza:

**Danışmanın :**

Adı-Soyadı : Tarih:

 İmza:

Tablo 1: İlk yazılı sınav için aşağıda sıralanan konulardan 3 tanesi işaretlenmelidir. Bu tercihlerden en az ikisi ilk üç konu başlığında yer alan matematik konularından olmalıdır. Sınav süresi en az üç saat olacaktır.

|  |  |
| --- | --- |
| **Tercih**  | **Konu Başlığı** |
|  | Eliptik Eğriler Kriptografisi (Cryptography with Elliptic Curves) |
|  | Ayrık Matematik (Discrete Mathematics) |
|  | Sayılar Teorisi (Number Theory) |
|  | Bilgi ve Bilgisayar Güvenliği (Information and Computer Security) |
|  | Bilgi Güvenliği ve Yönetimi (Information Security and Management) |
|  | Saldırı Saptama ve Önleme (Intrusion Detection and Prevention) |
|  | Programla İlintili Alınmış Matematik veya Bilgisayar Bilimleri Temelli Seçmeli Ders (Program Related Mathematical or Computer Science Based Taken Elective Course) |

Tablo 2: İkinci yazılı sınavda Ağ Güvenliği ve Kriptografi konuları herkes için zorunlu olup aşağıda sıralanan konulardan 2 tanesi de seçmeli olarak işaretlenmelidir. Sınav süresi en az üç saat olacaktır.

|  |  |
| --- | --- |
| **Tercih**  | **Konu Başlığı** |
|  | Ağ Güvenliği (Network Security) |
|  | Kriptografi (Cryptography) |
|  | Bilgi Sistemleri Güvenliği Mühendisliği  |
|  | E-Ticarette Güvenlik (E-commerce Security) |
|  | Bilgi Güvencesi ve Güvenli Yazılım Geliştirme (Information Security and Secure Programming) |
|  | Bilgi Güvenliği Yasa ve Politikaları |
|  | Bilgi Güvenliğinde Makine Öğrenmesi (Machine Learning Methods in Security) |
|  | Programlama Dilleri Güvenliği (Secure Programming) |
|  | Açıklık Tarama ve Önleme (Vulnerability Test and Prevention) |
|  | Şifreleme İşlemcisi Tasarımı (Cryptographic Microprocessor Design) |
|  | Bilgi Güvenliği Alanında Veri Madenciliği Yöntemleri (Data Mining Methods in Security) |
|  | Bulut Bilişim Güvenliği (Security for Cloud Computing) |
|  | Dizi Şifreleme (Stream Cipher) |
|  | Bilgi Güvenliği Denetimi ve Güvencesi (Information Security Audit and Assurance) |
|  | Bilişim Uzayındaki Savaşlar (Cyber Warefare, Cybersecurity and Defense) |
|  | Kriptografi Mühendisliği (Cryptographic Engineering) |
|  | Programla İlintili Herhangi Bir Seçmeli Ders (A Program Related Elective Course) |