AD/SOYAD:
ÖĞRENCİ NO:

SAKARYA ÜNİVERSİTESİ-BİLGİSAYAR MÜH.
UYGULAMALI KRİPTOLOJİ 2020-2021 BAHAR FİNAL SINAV SORULARI

- *Çözüm yapacak olduğunuz kağıtlara lütfen Ad-Soyadı bilgisini yazarak imzalayınız. Cevap kağıtlarınızı süre bitimine kadar taratarak veya fotoğrafını çekerek, sıkıştırıp tek bir dosya haline getirip sisteme yüklemeniz gerekmektedir.*
- *Cevap kağıtları el yazması olarak kabul edilmekte, bilgisayar ortamında hazırlanan cevap kağıtları değerlendirilmeyecektir.*
- *Dosyanın alt kısmında kısa sınav soruları bulunmaktadır. Bu soruları aynı doküman içinde cevaplayarak gönderebilirsiniz. Bu sorular için ek süre verilmeyecektir. Puanlaması ayrı yapılacaktır.*
- ***Toplamda 7 soru sorulmuştur, istediğiniz 5 adetini cevaplandırabilirsiniz. (5*20=100)***
- *Sisteme yükleme süresini hesaplayarak cevaplamalarınızı yapınız. Sistem 17:20'den sonra yükleme kabul etmeyecektir. LÜTFEN CEVAP KÂĞITLARINIZI BANA MAİL ATMAYIN, MAİL İLE GELEN CEVAPLAR KABUL EDİLMEYECEKTİR.*
- ***Sınav başlangıç saati 16.00 Bitiş 17.20 süreniz 80 dk.***

1-) Temel anahtar transfer protokolünü hibrit yapı üzerinde çizerek kısaca açıklayınız. (Açıklamada simetrik ve asimetrik yapı birlikte gösterilmelidir.) (20 p.)

2-) Hash fonksiyonlarının taşıması gereken temel özellikleri yazınız. Özetleme fonksiyonlarından MAC algoritması üretebilmek için kullanılan iki mimariyi açıklayınız. (20 p.)

3-)Güvenlik sistemlerinde sertifika hangi maksatla kullanılır? Temel bir sertifika bilgisi içinde bulunan bilgileri yazınız. Üretim ve doğrulama aşamalarının nasıl yapıldığını açıklayınız. (20 p.)

4-)Ağ, taşıma ve uygulama katmanlarında bulunan güvenlik protokollerine birer örnek vererek. SSL/TLS mimarisini ve sağlamış olduğu güvenlik servislerini kısaca açıklayınız. (20 p.)

5-)SSH protokolü ile port yönlendirme işleminin nasıl yapıldığını kısaca açıklayınız. (20 p.)

6-) İnternet mail protokollerinin en temel seviyede çalışma mantığını açıklayınız. SMTP protokolünün temel özelliklerini yazınız. (20 p.)

7-)IPSec protokolünün çalışmasını ve hangi maksatla kullanıldığını açıklayınız? Transport ve Tunnel mod arasındaki farkları yazınız. (20 p.)

KISA SINAV SORULARI:

1-) Aşağıdaki tabloyu doldurunuz. (50 p.)

Algoritma	**Şifreleme /Çözme**	**Dijital İmza**	**Anahtar Değişimi**
RSA			
Diffie-Helman			
DSS			
Eliptic Curve			

2-) Basit Kimlik Doğrulama işlemini ve taraflar arasında hangi bilgilerin aktarıldığını açıklayınız. (Kullanıcı-kimlik doğrulama sunucusu-sunucu) 50 p.

Doç. Dr. Ünal ÇAVUŞOĞLU

Başarılar Dilerim.