Ad Soyad:
Numara:
Süre: 75 dakika

1Q	2Q	3Q	4Q	5Q	Toplam

AYRIK MATEMATIK FINAL SORULARI (A GRUBU)

Soru 1. **<u>RSA E-İmza Algoritması</u>**

Step 1. Anahtar Üretimi: A şahsı anahtar üretmek için aşağıdaki işlemleri yapar ve kendi açık anahtarını B şahsına iletir;
1. İki asal sayı seçiniz (p ve q)
2. $n = p \times q$ hesaplayınız.
3. $\phi(n) = (p-1) \times (q-1)$ hesaplayınız.
4. Bir e sayısı seçiniz öyle ki $obeb(e, \phi(n)) = 1$ dir. $(1 < e < \phi(n))$
5. Bir d sayısı bulunuz öyle ki $\boldsymbol{d \times e \bmod \phi(n) \equiv 1}$ dir.
6. Açık anahtar: (e, n)
7. Gizli anahtar: (d, n)

Step 2. İmzalama: A şahsı bir m $(0 \leq m < n)$ doğrulama sayısı seçer ve

$$\boldsymbol{c = m^d \bmod n}$$

değerini hesaplar ve B Şahsına (m, c) kapalı metnini gönderir.

Step 3. Doğrulama: B Şahsı mesajın A şahsından gelip-gelmediğini anlamak için

$$\boldsymbol{c^e \bmod n}$$

değerini hesaplar ve bu değer m ye eşit ise, mesajın A şahsından geldiğini anlar.

Yukarıdaki RSA e-imza algoritmasını kullanarak, $m = 7$ yi önce şifreleyip daha sonra deşifre ediniz.
İpucu 1: İşlem kolaylığı için, p ve q yü küçük seçiniz.
İpucu 2: Mod alma işleminde, aşağıdaki örnekteki gibi bir yol izleyebilirsiniz;

$$4^{10} \bmod 7 \equiv (4^2)^5 \bmod 7 \equiv (16)^5 \bmod 7$$
$$\equiv 2^5 \bmod 7 \equiv 32 \bmod 7 \equiv 4$$

Cevap:

Soru 2.

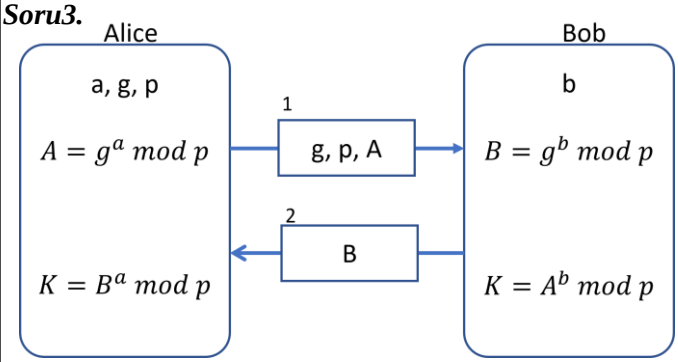
A ●−	J ●−−−	S ●●●
B −●●●	K −●−	T −
C −●−●	L ●−●●	U ●●−
D −●●	M −−	V ●●●−
E ●	N −●	W ●−−
F ●●−●	O −−−	X −●●−
G −−●	P ●−−●	Y −●−−
H ●●●●	Q −−●−	Z −−●●
I ●●	R ●−●	

Mors alfabesi yukarıda verilmiştir. Buna göre, aşağıda şifrelenmiş metni aşağıdaki gibi olan plaintexti (düz metni) bulunuz (her bir harf arasında bir boşluk bulunmaktadır).

···· · .-.. .-.. --- .-- --- .-. .-.. -..

Cevap:

Soru3.



Yukarıda Alice ve Bob'un Diffie-Helmann yöntemi ile ortak anahtar (K) üretimi verilmiştir. Alice ve Bob aralarında anlaşıp asal sayı olarak **p=5** ve taban olarak **g=3** seçerler. Alice gizli bir **a=10** sayısı seçer ve Bob'a g, p ve hesapladığı A'yı gönderir. Bob gizli bir **b=6** sayısı seçip B'yi hesaplayıp Alice'e gönderir. Buna göre ürettikleri ortak K anahtarını bulunuz.

Cevap:

Soru 4. Üç harfli alfabe {X,Y,Z} ile verilen aşağıdaki işlem tablosunu göz önünde bulundurun:

$\oplus$	X	Y	Z
X	X	X	Y
Y	Z	Y	X
Z	Y	Z	Z

mesaj $\oplus$ anahtar = şifreli metin

Şifreli metin yandaki gibi verilsin: **ZYYXXX**
Şifreli metnin yukarıda verilen tablo ve formule göre **XZYYZX** anahtarı kullanılarak şifrelendiğini de biliyorsunuz. Mesajı deşifre ediniz (bulunuz).

Cevap:

<u>Soru 5.</u>

Asimetrik kriptografi nedir? Çalışma prensibini, avantajlarını ve dezavantajlarını açıklayınız. Simetrik kriptografiden farkı nedir?

Cevap: