AYRIK MATEMATIK FINAL SORULARI (A GRUBU)

***Cevap:***

***Soru 1.* RSA E-İmza Algoritması**

**Step 1. Anahtar Üretimi:** A şahsı anahtar üretmek için aşağıdaki işlemleri yapar ve kendi açık anahtarını B şahsına iletir;

1. İki asal sayı seçiniz ( ve )

2. hesaplayınız.

3. hesaplayınız.

4. Bir e sayısı seçiniz öyle ki dir. ()

5. Bir sayısı bulunuz öyle ki dir.

6. Açık anahtar:

7. Gizli anahtar:

**Step 2. İmzalama:** A şahsı bir doğrulama sayısı seçer ve

değerini hesaplar ve B Şahsına kapalı metnini gönderir.

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

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

Yukarıdaki RSA e-imza algoritmasını kullanarak,

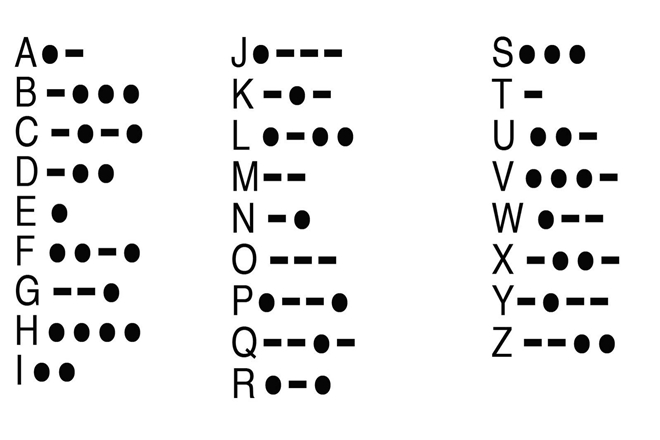
yi önce şifreleyip daha sonra deşifre ediniz.

**İpucu 1:** İşlem kolaylığı için, ve yü küçük seçiniz.

**İpucu 2:** Mod alma işleminde, aşağıdaki örnekteki gibi bir yol izleyebilirsiniz;

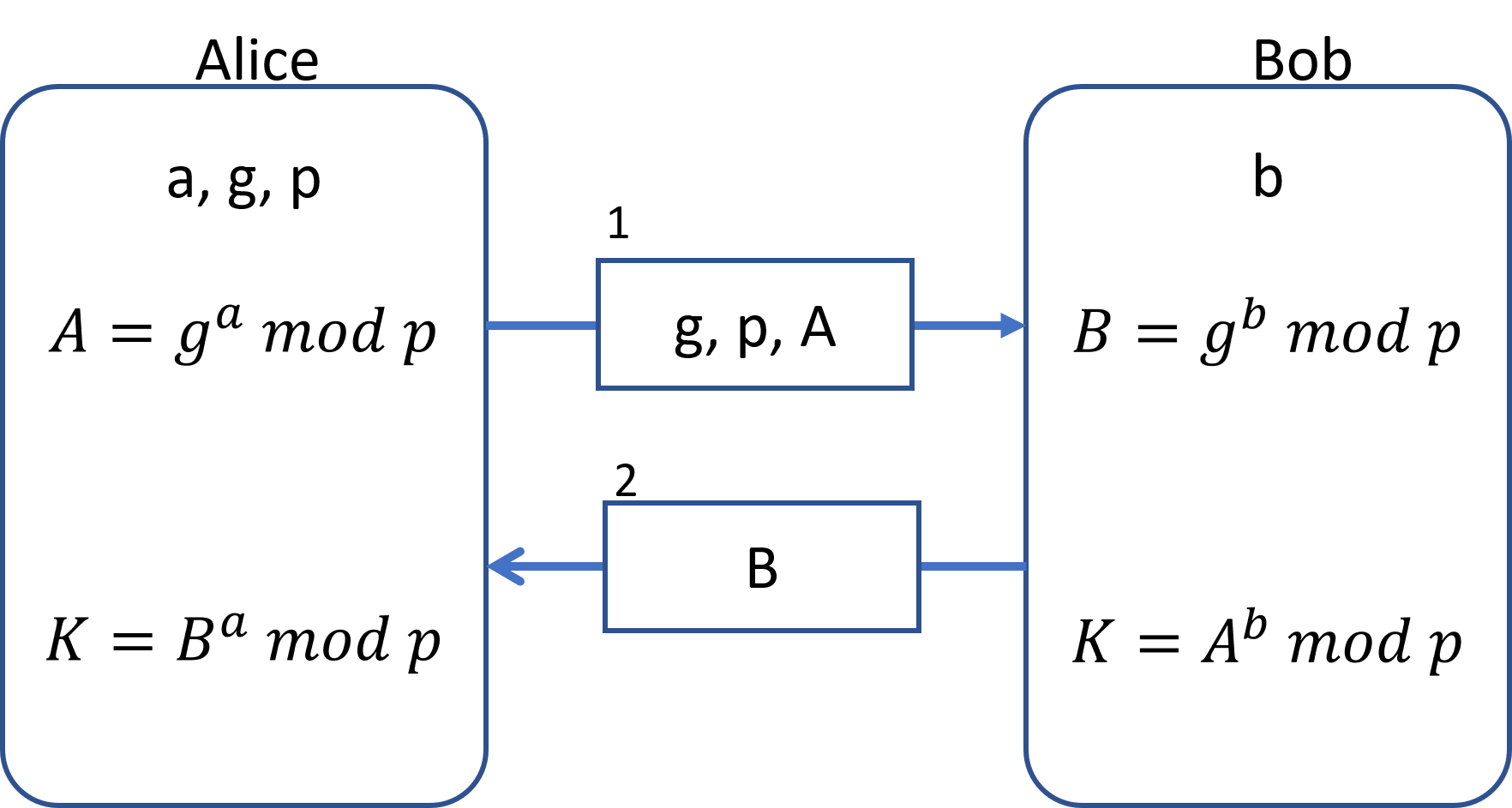
***Cevap:***

***Soru 2.***



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

**…. . .-.. .-.. --- .-- --- .-. .-.. -..**

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.

***Soru3.***

***Cevap:***

***Cevap:***

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

|  |  |  |  |
| --- | --- | --- | --- |
| ⊕ | X | Y | Z |
| X | X | X | Y |
| Y | Z | Y | X |
| Z | Y | Z | Z |

**mesaj ⊕ 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).

***Soru 4.***

***Cevap:***

**Soru 5.**

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