



## Şubat Ayının Ödüllü Soruları

### Soru 1:

Aşağıdaki sayıları küçükten büyüğe (örnek:  $b < c < a$ ) sıralayınız.

- a: 256 bitle gösterilebilecek tüm AES anahtarlarının sayısı
- b: 512 ve daha az bit ile gösterilebilecek asal sayıların sayısı (asal sayılar teoremine göre)
- c: Dünyadaki tüm atomların sayısı

## Cevap 1:

$$c < a < b$$

Sözü edilen sayıların yaklaşık büyüklüklerini şöyle bulalım:

**a:**

AES -Advanced Encryption Standard- 3 farklı uzunluktaki (128, 192, ya da 256 bit) anahtarları kullanabilen bir simetrik şifreleme algoritmasıdır. 256 bit ile gösterilebilecek AES anahtarlarının sayısı yaklaşık olarak,

$$a = 2^{256} \approx 1,2 \cdot 10^{77}$$

bulunur.

**b:**

Asal sayılar teoremi (prime number theorem), basit bir anlatımla,  $x$  sayısından küçük ya da  $x$ 'e eşit asal sayıların sayısının, çok büyük  $x$  değerleri için,  $\frac{x}{\ln(x)}$

değerine yakınsadığını söyler. Bu durumda,

$$b \approx \frac{2^{512}}{\ln(2^{512})} \approx 3,8 \cdot 10^{151}$$

bulunur.

**c:**

Dünyadaki tüm atomların sayısını, dünyanın yaklaşık kütlesi, dünyayı oluşturan moleküllerin dağılımı, bu moleküllerdeki atomların kütleleri ve Avogadro sabiti (yaklaşık  $6,02 \cdot 10^{23}$ ) olarak adlandırılan fiziksel sabiti kullanarak bulmamız mümkündür.

Bilim adamları her ne kadar dünyanın merkezinin moleküler yapısını tam olarak bilemeseler de (gözlenebilen dünya yüzeyinin moleküler yapısı hayli kesin olarak bilinmektedir), bununla ilgili bazı kestirimlerde bulunabilmektedirler.

Bu kestirimlerle, dünyadaki tüm atomların sayısı, yaklaşık olarak

$$c \approx 1,3 \cdot 10^{50}$$

bulunur (kaynak: Jefferson Laboratuvarı, ABD).

Bu durumda, elimizdeki 3 sayıyı küçükten büyüğe doğru sıralarsak,

$$c < a < b$$

eşitsizliğine erişiriz.

**Soru 2:**

$$f(170) = \text{CEO}$$

$$f(180) = \text{CCÇÇE}$$

$$f(175) = ?$$

## Cevap 2:

### EEG

f() fonksiyonu, arguman olarak aldığı sayının asal çarpanlara ayrılmış halini oluşturmakta:

$$f(170) \rightarrow 170 = 2 \times 5 \times 17 ,$$

ve buradaki her bir asal sayının, aşağıdaki şekilde harflere dönüşmüş halini, çıktı dizisine yazmaktadır:

C: sıra no: 2,  
Ç: sıra no: 3,  
E: sıra no: 5,  
G: sıra no: 7,  
İ: sıra no: 11,  
K: sıra no: 13,  
O: sıra no: 17,  
P: sıra no: 19,  
T: sıra no: 23

Yani,  $170 = 2 \times 5 \times 17 = \text{CEO}$  gizli yazısı oluşmaktadır.

Bu durumda, sorulan arguman için çıktı:

$$f(175) \rightarrow 175 = 5 \times 5 \times 7 = \text{EEG} \text{ olarak bulunmaktadır.}$$

**Soru 3:**

<i>Açık Yazı</i>	<i>Gizli Yazı</i>
MAKALE	254535OEOEOI
?	15452131UEUEAİEİ

## Cevap 3:

### TARAYICI

Açık yazıdan gizli yazı oluşturulurken:

- (i) Açık yazıdaki her bir harfin kendisinden sonra gelen ilk sesli harfe ne kadar uzakta olduğu ve bu sesli harf kodlanmıştır:

MAKALE →

M → 2O

A → 5E

K → 4O

A → 5E

L → 3O

E → 5I

- (ii) Bu kodlar toplamının, öncelikle rakamları, sonra da harfleri sırasıyla yazılarak gizli yazı oluşturulmuştur:

MAKALE → 254535OEOEOI

Bu kural ışığında verilen gizli yazıyı incelersek:

15452131UEUEAİEİ → 1. kod: 1U → açık harf: **T**  
→ 2. kod: 5E → açık harf: **A**  
→ 3. kod: 4U → açık harf: **R**

...

yukarıda verilen TARAYICI cevabına erişiriz.