TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Nisan Ayının Ödüllü Soru ve Cevapları

Soru 1:

15, 21, 33, 35, 39, 51, 55, 57, 65, 69, 77, 85, 87, 91, 93, 95, 111, 115, ?

Cevap 1:

119

Dizide, iki (farklı) tek asalın çarpımı olan (ör. 3x5, 5x7 ...) sayılar, küçükten büyüğe yazılmışlardır. RSA sisteminde kullanılan sayılar da bu dizinin çok çok ötedeki terimlerinde kendilerine yer bulacaklardır!

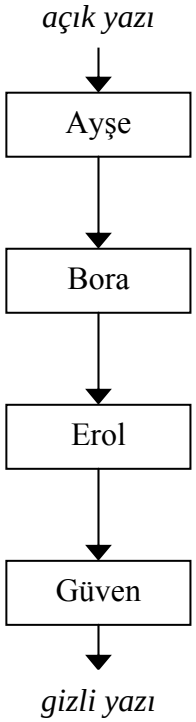
3x şeklindeki sayılar	5x şeklindeki sayılar	7x şeklindeki sayılar	11x şeklindeki sayılar	13x şeklindeki sayılar	...
15 21 33 39 51 57 69 87 93 111 123 ...	35 55 65 85 95 115 145 ...	77 91 119 133 ...	143 ...	221 ...	...

→ Sıralı dizi: 15, 21, 33, 35, 39, 51, 55, 57, 65, 69, 77, 85, 87, 91, 93, 95, 111, 115 ...

olur. Böylece, dizinin sorulan 19. terimi, 119 olarak bulunur.

Soru 2:

Ayşe, Bora, Erol ve Güven, aşağıdaki şekilde gösterilen sırayla, kendilerine verilen açık yazıyı gizli yazıya çeviriyorlar:



- Ayşe, %40 olasılıkla, x3 çarpımsal şifreleme yapıyor; %60 olasılıkla, her harfi 3 ötesindekiyle değiştiriyor.
- Bora, sadece, her harfi 2 gerisindekiyle değiştiriyor.
- Erol, %80 olasılıkla, her harfi 4 gerisindekiyle değiştiriyor; %20 olasılıkla, x7 çarpımsal şifreleme yapıyor.
- Güven, sadece, her harfi 1 ötesindekiyle değiştiriyor.

SİNYAL açık yazısı için, çıktı olabilecek tüm gizli yazıları ve bunların olasılıklarını bulunuz (A = 0, B = 1, ..., Z = 28 kodlamasını kullanınız).

Cevap 2:

AZLÖUĞ (%32)
ŞMDÇNR (%8)
PHLÜYJ (%48)
IYDTĞP (%12)

- Verilen açık yazı (SİNYAL) için Ayşe' nin çıktısı, %40 olasılıkla EDPTAK, %60 olasılıkla ise ULPBÇO olacaktır.
- Bu çıktılar için, Bora, sırasıyla, ÇCOSYİ ve ŞJOZBM çıktılarını üretecektir.
- Erol, eğer ÇCOSYİ yi girdi olarak almışsa, ZYKOTG çıktısını (%32), veya SLÇCMP çıktısını (%8) üretecektir. Erol, eğer, ŞJOZBM yi girdi olarak almışsa, ÖĞKUVİ çıktısını (%48), veya HVÇŞGÖ çıktısını (%12) üretecektir.
- Bu 4 olası çıktı için, Güven, sırasıyla, AZLÖUĞ (%32), ŞMDÇNR (%8), PHLÜYJ (%48), IYDTĞP (%12) gizli yazılarını üretecektir.

Soru 3:

FUTBOL → ĞVĞCAT

TENİS → ĞVÜFG

GÜREŞ → ?

Cevap 3:

SOUVS

Okların solundaki kelimelerin harfleri x_i olmak üzere,

$$(x_i)^2 + 1 \pmod{29}$$

şeklinde bulunan harfler, çıktıyı oluşturmuştur:

F → $(6)^2 + 1 = 37 = 8 \pmod{29}$ → Ğ
U → $(24)^2 + 1 = 577 = 26 \pmod{29}$ → V
T → $(23)^2 + 1 = 530 = 8 \pmod{29}$ → Ğ
B → $(1)^2 + 1 = 2 \pmod{29}$ → C
O → $(17)^2 + 1 = 290 = 0 \pmod{29}$ → A
L → $(14)^2 + 1 = 197 = 23 \pmod{29}$ → T

olmaktadır. Aynı kuralı, GÜREŞ e uygularsak, yukarıda verilen cevaba erişiriz.