TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Eylül Ayının Ödüllü Soru ve Cevapları

Soru 1:

Açık Yazı	*Gizli Yazı*
TÜRKİYE	13 7 23 53 61 3 89
?	43 109 53 89 97 37 41 3 109

Cevap 1:

MAKEDONYA

Açık yazılardan gizli yazılar oluşturulurken:

(i) Her bir açık yazı harfi koduna (0-28 arasında) eklenince, bu kodu 29' a tamamlayan sayı (S) bulunmuş,

(ii) S. asal sayı gizli harf olarak yazılmıştır

Yani:

TÜRKİYE → T' nin kodu = 23 → S = 6 → 6. asal sayı = 13
Ü' nün kodu = 25 → S = 4 → 4. asal sayı = 7
R' nin kodu = 20 → S = 9 → 9. asal sayı = 23
K' nin kodu = 13 → S = 16 → 16. asal sayı = 53
İ' nin kodu = 11 → S = 18 → 18. asal sayı = 61
Y' nin kodu = 27 → S = 2 → 2. asal sayı = 3
E' nin kodu = 5 → S = 24 → 24. asal sayı = 89

olmaktadır.

Aynı kural, verilen gizli yazı için kullanılırsa, yukarıda verilen MAKEDONYA cevabına erişilir.

Soru 2:

Asal S sayısının rakamlarla yazılışı $abcd$ olsun. Eğer,

$$a + b + c + d = 20$$

$$a \cdot d = 72$$

ise, olası S sayılarını bulunuz.

Cevap 2:

8039, 8219

$a \cdot d = 72$ olduğundan, a ve d nin rakam olabilmesi için, a = 8, d = 9 olarak bulunur (tersi durum, yani d = 8, a = 9 mümkün değildir, bu durumda 9XX8 sayısı çift olacağından asal olamaz).

$a + b + c + d = 20$ olduğundan, a = 8, d = 9 kullanılarak,

$$b + c = 20 - 8 - 9 = 3$$

bulunur.

b ve c rakamları için tüm olasılıkları yazalım:

b	**c**
0	3
1	2
2	1
3	0

Kontrol edeceğimiz sayılar kümesi:

8039 → asal
8129 → asal değil
8219 → asal
8309 → asal değil

olarak yukarıda verilen cevaba erişilir.

Soru 3:

1. AES şifreleme sistemi, en az 100 bit anahtar gerektirir.

   D Y

2. Kriptolojide, DES, “Digital Electronic Signal” in kısaltmasıdır.

   D Y

3. 3. asal sayı 7 den küçüktür.

   D Y

4. Pi sayısının virgülden sonraki 4. basamağı, 5’tir.

   D Y

5. TÜBİTAK BİLGEM web sayfasındaki “Ödüllü Kriptoloji Soruları” köşesi, Haziran 2010’da yayına başlamıştır.

   D Y

6. 256 bit anahtarlı AES şifreleme sistemi, Feistel yapısındadır.

   D Y

7. Üç harf ötelemeli Sezar şifreleme sistemi ile, BRÜTÜS açık yazısı, DTZVZÜ ye dönüşür.

   D Y

8. 11 sayısı, bir uzun asaldır.

   D Y

9. Açık yazı harfleri x, gizli yazı harfleri y, ve $y = 7x \pmod{29}$ şeklinde tanımlanan çarpımsal şifreleme ile, KALEM açık yazısı, DAİFÖ gizli yazısına dönüşür.

   D Y

10. Bletchley Park, Amerika Birleşik Devletleri’nin Maryland eyaletinde, II. Dünya Savaşı sırasında kullanılmış olan, Alman şifrelerini kırma merkezinin adıdır.

    D Y

Cevap 3:

1. Y 2. Y 3. D 4. D 5. D

6. Y 7. Y 8. Y 9. D 10. Y