



Mart Ayının Ödüllü Soruları ve Cevapları

Soru 1:

Aşağıda verilen şifrebilim ile ilgili konferansların/çalıştayların isimlerini ve 2010 yılında hangi ülkede düzenlendikleri bilgisini doğru olarak eşleştiriniz.

Eurocrypt 2010	Türkiye
RFIDsec 2010	Singapur
Africacrypt 2010	ABD
CHES 2010	Monako
Asiacrypt 2010	Güney Afrika

Cevap 1:

Eurocrypt 2010	Monako
RFIDsec 2010	Türkiye
Africacrypt 2010	Güney Afrika
CHES 2010	ABD
Asiacrypt 2010	Singapur

Soru 2:

<i>Açık Yazı</i>	<i>Gizli Yazı</i>
PAROLA	EYBPFDDRC SYU
?	THFÇJRIAÜLZSGJÖVHD

Cevap 2:

PARMAKIZİ

Açık yazıdan gizli yazı oluşturulurken, her açık yazı harfi, 2 adet harfin alfabemizdeki sıra numaralarının farkı olacak şekilde düşünülmüştür.

Bu iki adet harf de, gizli yazının en sol ve en sağından başlayıp ortaya doğru gidecek şekilde sırayla yazılmışlardır (hangi harfin sol tarafa, hangisinin sağ tarafa yazılacağı rastgele seçilmiştir).

Yani:

1. açık yazı harfi: P → sıra numarası: 19
→ farkları 19 olan iki harf: E (5) ve U (24)

Gizli yazı durumu: E ... U

2. açık yazı harfi: A → sıra numarası: 0
→ farkları 0 olan iki harf: Y (27) ve Y (27)

Gizli yazı durumu: EY ... YU

3. açık yazı harfi: R → sıra numarası: 20
→ farkları 20 olan iki harf: B (1) ve S (21)

Gizli yazı durumu: EYB ... SYU

olmaktadır. Bu kurala göre, verilen diğer gizli yazı incelenirse, yukarıda verilen PARMAKIZİ cevabına erişilir.

Soru 3:

$$19 + 5 \rightarrow 157$$

$$14 + 23 \rightarrow 471$$

$$26 + 9 \rightarrow ?$$

Cevap 3:

425

Okların sol tarafındaki “toplama” işlemi yapılırken, verilen sayıların ikili gösterimleri arka arkaya eklenmiş, ve oluşan bu karma sayının ondalık tabandaki değeri sonucu oluşturmuştur.

Yani:

19: 10011

5: 101

$$19 + 5 = \text{ondalık}(10011101) = 157$$

14: 1110

23: 10111

$$14 + 23 = \text{ondalık}(111010111) = 471$$

olmaktadır. Bu durumda,

26: 11010

9: 1001

$$26 + 9 = \text{ondalık}(110101001) = 425$$

cevabına erişilir.