TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Mart Ayının Ödüllü Soru ve Cevapları

Soru 1 :

Ayşe ile Bora, mesajlarını şifrelemek için kullanacakları simetrik anahtarları karşı tarafa (yani, Ayşe'den Bora'ya ve Bora'dan Ayşe'ye) iletmek sorunuyla karşı karşıyadırlar. Asimetrik şifreleme yöntemleri ile yokedilebilecek bu anahtar dağıtımı (key distribution) sorunu, simetrik şifreleme algoritması ne kadar güvenli olursa olsun, var olacak bir sorundur.

Melahat, bu iki arkadaş arasındaki haberleşme kanalını dinlediği bir günde,

9773304579879 …

başka bir günde:

1964304579879 …

ve başka bir günde de:

3564304579879 …

kanal değerlerini gözlüyor. Buna göre, Ayşe ve Bora, nasıl bir anahtar dağıtımı sistemi kullanıyor olabilirler?

Cevap 1 :

ISBN numaraları ile tanımlanan kitaplar

Soruda verilen ve mesajların en başında gözüken sayılar, aşağıdaki kitaplar için standart 13 rakamlık ISBN kodlarının tersyüz edilmiş halleridir:

ISBN: 9789754033779:
Emrehan Halıcı, *Zeka Oyunları 2*, TÜBİTAK Popüler Bilim Kitapları, No: 219, 2005.

ISBN: 9789754034691:
Lewis Thomas, *Bir Tıp Gözlemcisinin Notları*, TÜBİTAK Popüler Bilim Kitapları, No: 288, 2008.

ISBN: 9789754034653:
Walter G. Vincenti, Mühendisler: *Ne Bilirler, Nasıl Bilirler?*, TÜBİTAK Popüler Bilim Kitapları, No: 285, 2008.

Yani, Ayşe ve Bora, bu şekilde tanımladıkları kitapların, örneğin ilk cümlelerini, son cümlelerini, belirli bir sayfadaki X numaralı cümlesini vb. uyguladıkları simetrik şifrelerin gizli anahtarı olarak kullanıp, bu bilgiyi karşı tarafa, mesajların en başına ISBN numaralarını yazarak iletiyor olabilirler (ayrıca, kitap seçimlerinden görüldüğü üzere, TÜBİTAK Popüler Bilim Kitapları' nı çok beğenmektedirler).

Soru 2 :

$$3e + 2\pi = \text{TİVNK} \quad \Rightarrow \quad 5\pi - 5e = \ ?$$

Cevap 2 :

Z M T M E

Öncelikle, sayılar ile Türkçe'deki harflerin bağıntısını gösteren tabloyu yazalım:

0 A	1 B	2 C	3 Ç	4 D	5 E
6 F	7 G	8 Ğ	9 H	10 I	11 İ
12 J	13 K	14 L	15 M	16 N	17 O
18 Ö	19 P	20 R	21 S	22 Ş	23 T
24 U	25 Ü	26 V	27 Y	28 Z	

Daha sonra, formülde geçen iki aşkın (transcendental) matematiksel sabiti yazalım (virgülden sonra 5 basamağa kadar):

$$\pi = 3{,}14159$$
$$e = 2{,}71828$$

Şimdi de, bu sabitlerle skaler (örneğin, 2) gibi sayıların çarpımını, her bir rakamın ayrı ayrı bu skalerle çarpımı olarak yazalım:

$$3e = 6,\ 21\ 3\ 24\ 6\ 24$$
$$2\pi = 6,\ 2\ 8\ 2\ 10\ 18$$

Toplamı da ayrı ayrı basamakların toplamı (mod 29, alfabemizdeki harf sayısına bağlı) olarak yapalım, virgülden sonraki kısmı, yukarıdaki harf bağıntı tablosundan okuyalım:

$$3e + 2\pi = 12,\ 23\ \ 11\ \ 26\ \ 16\ \ 13 = \text{T İ V N K}$$

Gizli kuralı bu şekilde bulduktan sonra:

$$5\pi = 15,\ 5\ 20\ 5\ 25\ 45$$
$$5e = 10,\ 35\ 5\ 40\ 10\ 40$$

$$5\pi - 5e = 5,\ 28\ \ 15\ \ 23\ \ 15\ \ 5 = \text{Z M T M E}$$

Soru 3 :

836105446162 → KARTAL

0172133252 → ?

Cevap 3 :

SERÇE

Rakamlar kümesi, karşı düştükleri kelimeye dönüştürülürken:

(i) Arka rakaya dizilmiş 2' li rakam kümelerinin her biri $r_1\ r_2$ olmak üzere,

1. küme: 83
2. küme: 61
3. küme: 05
…
6. küme: 62

(ii) r_1 ' in harflerle yazımının, soldan r_2 ' inci sıradaki harfi, çıktı olarak yazılmıştır:

1. küme: 83 → $r_1 = 8,\ r_2 = 3$ → "S E **K** İ Z" → çıktı: K

2. küme: 61 → $r_1 = 6,\ r_2 = 1$ → "**A** L T I" → çıktı: A

3. küme: 05 → $r_1 = 0,\ r_2 = 5$ → "S I F I **R**" → çıktı: R

…

Aynı kural, verilen diğer rakamlar kümesine uygulanırsa:

1. küme: 01 → $r_1 = 0,\ r_2 = 1$ → "**S** I F I R" → çıktı: S

2. küme: 72 → $r_1 = 7,\ r_2 = 2$ → "Y **E** D İ" → çıktı: E

3. küme: 13 → $r_1 = 1,\ r_2 = 3$ → "B İ **R**" → çıktı: R

4. küme: 32 → $r_1 = 3,\ r_2 = 2$ → "Ü **Ç**" → çıktı: Ç

5. küme: 52 → $r_1 = 5,\ r_2 = 2$ → "B **E** Ş" → çıktı: E

yukarıda verilen SERÇE cevabına erişilir.