TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Şubat Ayının Ödüllü Soru ve Cevapları

Soru 1: *Kriptopara*

Aşağıda, 3 sorudan oluşan bir yarışmada sorulan sorular, ve yarışmacı Ayşe' nin, o soruda elinde olan paranın hangi oranını hangi seçeneğe yerleştirdiği bilgisi yer almaktadır.

3. sorunun sonunda, Ayşe ne kadar bir ödülle (TL) yarışmayı tamamlayacaktır?

Ayşe'nin başlangıç parası = 1.000.000 TL

Soru 1: Hangisi asimetrik şifreleme sistemidir?

MAC	DES	RSA	AES
%10	**%50**	**%30**	**%10**

Ayşe' nin 1. soru sonunda parası =

Soru 2: Sezar şifreleme sisteminde, "SEZAR" açık yazısı, Türkçe alfabede, hangi gizli yazıya dönüşür?

RDYZP	UĞCÇT	ŞFABS	BRÜTÜS
%20	**%40**	**%30**	**%10**

Ayşe' nin 2. soru sonunda parası =

Soru 3: Hangisi mükemmel sayıdır?

543	488	502	496
%0	**%60**	**%0**	**%40**

Ayşe' nin 3. soru sonunda parası = ?

Cevap 1:

48.000 TL

Soru 1’ in doğru cevabı RSA dır. Bu durumda, Ayşe’ nin elinde, 1. soru sonrasında:

1.000.000 x 0.30 = 300.000 TL

kalacaktır.

Soru 2’ nin doğru cevabı UĞCÇT dır. Bu durumda, Ayşe’ nin elinde, 2. soru sonrasında:

300.000 x 0.40 = 120.000 TL

kalacaktır.

Soru 3’ nin doğru cevabı 496 dır. Bu durumda, Ayşe’ nin elinde, 3. soru sonrasında:

120.000 x 0.40 = 48.000 TL

kalacaktır.

Soru 2:

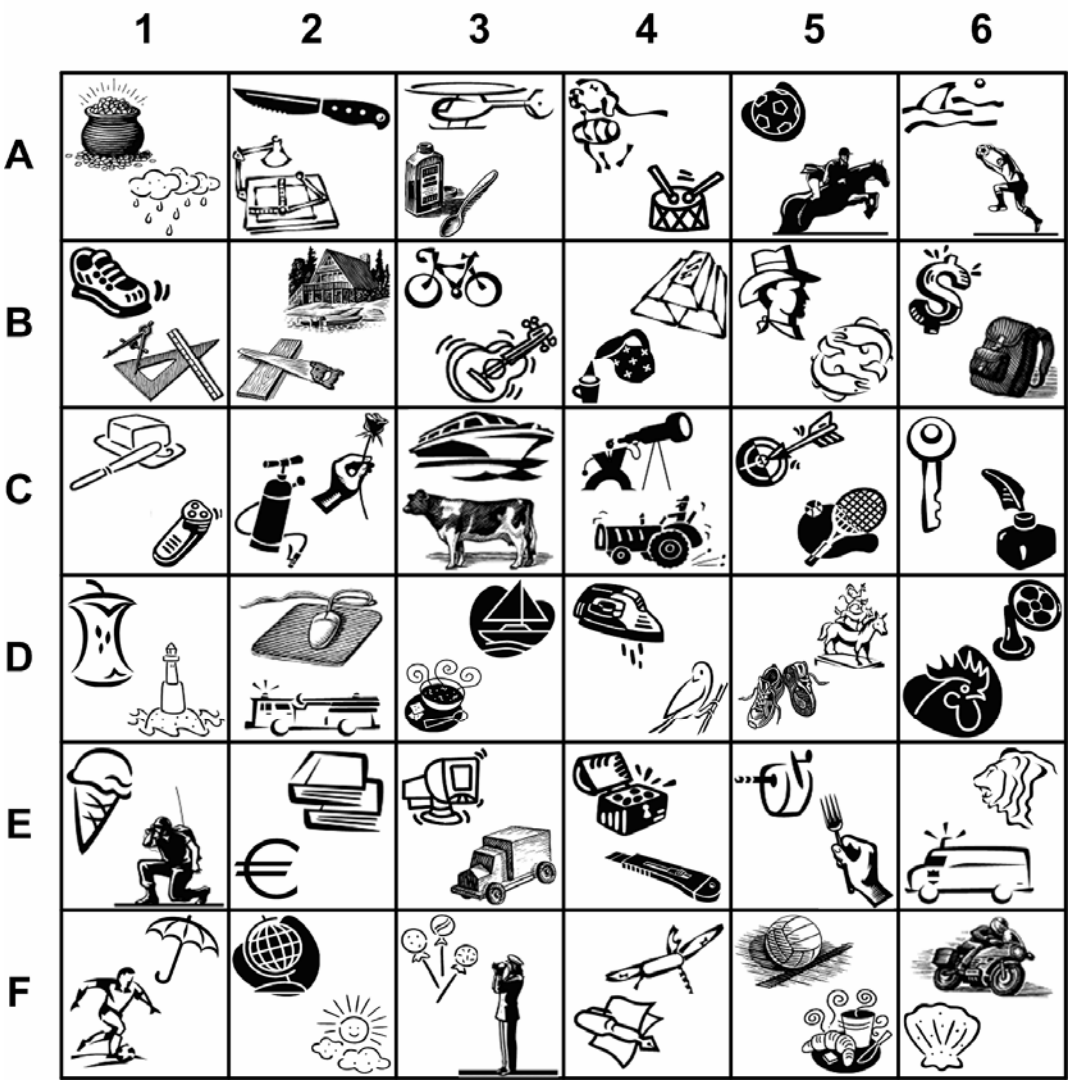
Aşağıdaki gibi, kullanıcılara gösterilen bir resim tablosundan 4 adet sıralı koordinat bilgisi (ör. B3–E1–C6–A3) seçimi temeline dayanan bir parola sistemi, kullanıcıların, hayli yüksek güvenliğe sahip şifreleri hafızalarında daha rahat tutmalarını sağlayabilir.

Koordinat bilgileri yerine, koordinatlarla ilgili resimler hafızalarda rahatlıkla tutulabilir (ör. yukarıda verilen koordinatlar için: "bisiklet" – "dondurma" – "anahtar" – "helikopter" sırası).

Bu sistemde,

(i) Koordinatlarda tekrarlara da izin verildiğinde (ör. B3 – D1 – C6 – D1 parolasındaki gibi), toplam kaç adet parola olasılığı vardır?

(ii) Koordinatlarda hiçbir tekrara izin verilmediğinde (ör. B3 – E1 – C6 – A3 parolasındaki gibi), toplam kaç adet parola olasılığı vardır?



Cevap 2:

(i) ~ 1.7 milyon
(ii) ~ 1.4 milyon

Koordinatlar, 36 elemanlı

{A1, A2, A3, A4, A5, A6, B1, B2, … , E5, E6, F1, F2, F3, F4, F5, F6}

kümesinden seçilmektedir.

Bu durumda, tekrarlara izin verildiğinde, 4 koordinat bilgisi,

36^4 ~ 1.7 milyon

farklı şekilde seçilebilir.

Tekrarlara izin verilmediğinde, 4 koordinat bilgisi,

36 x 35 x 34 x 33 ~ 1.4 milyon

farklı şekilde seçilebilir.

Karşılaştırma olarak, yaygın olarak kullanılan ATM makinelerinin, sıralı 4 adet rakam {0, 1, 2, 3, … , 8, 9} dan oluşan parolalarının toplam sayısı, yalnızca 10.000 dir:

ATM parola kümesi = {0000, 0001, 0002, 0003, 0004, … , 9995, 9996, 9997, 9998, 9999}

Soru 3:

Eğer, hem p sayısı, hem de (p-1)/2 sayısı, asal sayılar ise, p' ye güvenli asal (*safe prime*) denmektedir.

Bu durumda, aşağıdaki asal sayılardan kaç tanesi güvenli asaldır?

1091	1697	607	113	587	1321
1439	1871	277	419	619	1019

Cevap 3:

3

Verilen sayıları inceleyelim:

(1091 – 1) / 2 = 545 → asal değil

(1637 – 1) / 2 = 818 → asal değil

(607 – 1) / 2 = 303 → asal değil

(113 – 1) / 2 = 56 → asal değil

(587 – 1) / 2 = 293 → ASAL → 587 güvenli asaldır.

(1321 – 1) / 2 = 660 → asal değil

(1439 – 1) / 2 = 719 → ASAL → 1439 güvenli asaldır.

(1871 – 1) / 2 = 935 → asal değil

(277 – 1) / 2 = 138 → asal değil

(419 – 1) / 2 = 209 → asal değil

(619 – 1) / 2 = 309 → asal değil

(1019 – 1) / 2 = 509 → ASAL → 1019 güvenli asaldır.

Bu durumda, verilen asal sayılardan, sadece 3 tanesi güvenli asaldır.