TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Ekim Ayının Ödüllü Soru ve Cevapları

Soru 1 :

RFID (*Radio Frequency Identification*, Radyo Frekans Kimlik Belirleme) etiketleri, ucuzlukları, boyutlarının küçüklüğü, ve sınırlı da olsa bazı kriptografik işlemleri yapabilme özellikleri ile ürün takibi, envanter kontrolü gibi alanlarda giderek önem kazanmaktadırlar.

Bunu dikkate alan Ayşe, RFID konusunda geliştireceği bir projede kullanmak üzere, RFID üreticisi bir firmadan etiketler satın alıyor.

- Üretici firma, sunduğu etiketlerin hatalı olma oranının %1 olduğunu belirtiyor.
- Ayşe, satın aldığı etiketlerin hatalı olup olmadıklarını kontrol etmek için, %95 doğrulukla çalışan bir test cihazı kullanıyor. Yani,
    - Etiket aslında hatalı ise, cihaz %95 olasılıkla ”hatalı” yanıtı veriyor;
    - Etiket aslında hatasız ise, cihaz %95 olasılıkla “hatasız” yanıtı veriyor.

Bu bilgiler ışığında, aşağıdaki olasılıkları hesaplayınız:

(i) Ayşe, rastgele seçtiği bir etiketi alıp test ediyor, ve cihaz “hatalı” yanıtı veriyor. Etiketin aslında hatasız olma olasılığı nedir?

(ii) Ayşe, rastgele seçtiği bir etiketi alıp test ediyor, ve cihaz “hatasız” yanıtı veriyor. Etiketin aslında hatalı olma olasılığı nedir?

Cevap 1 :

(i) ~ % 84
(ii) ~ % 0,053

Koşullu olasılıklar için Bayes teoremini kullanarak (konu ile ilgili ayrıntılı bilgi için: "Olasılık Kuramına Bir Giriş - I: Temel Kavramlar", *BİLGEM Dergisi*, Sayı: 6, Sf. 131-141, ve "Olasılık Kuramına Bir Giriş - II: Uygulamalar", *BİLGEM Dergisi*, Sayı: 7, Sf. 94-103, kaynakları incelenebilir), sorulan olasılıkları hesaplamadan önce, şu kısaltmaları tanımlayalım:

EH: etiket aslında hatalı, ES: etiket aslında hatasız (sağlam).

CH: test cihazı "hatalı" yanıtı veriyor, CS: test cihazı "hatasız" (sağlam) yanıtı veriyor.

Bu durumda, sorulan ilk olasılık için:

$$P(\mathrm{ES} \,/\, \mathrm{CH}) = \frac{P(\mathrm{CH} \,/\, \mathrm{ES}) \cdot P(\mathrm{ES})}{P(\mathrm{CH} \,/\, \mathrm{EH}) \cdot P(\mathrm{EH}) + P(\mathrm{CH} \,/\, \mathrm{ES}) \cdot P(\mathrm{ES})} = \frac{0{,}05 \cdot 0.99}{0{,}95 \cdot 0{,}01 + 0{,}05 \cdot 0.99} \approx 0{,}84$$

tür. Yani, Ayşe etiketleri bu şekilde test ederken, kullandığı cihaz "hatalı" yanıtını verdiğinde, %84 gibi hayli yüksek bir olasılıkla, test ettiği etiket aslında hatasız olacaktır. İlk bakışta şaşırtıcı gibi gözüken bu tür çıkarımlar, ana oran yanlışlığı (*base-rate fallacy*) olarak adlandırılmakta, ağ güvenliği istatistikleri, medikal test sonuçları gibi alanlarda karşımıza çıkmaktadır.

Sorulan ikinci olasılık ise,

$$P(\mathrm{EH} \,/\, \mathrm{CS}) = \frac{P(\mathrm{CS} \,/\, \mathrm{EH}) \cdot P(\mathrm{EH})}{P(\mathrm{CS} \,/\, \mathrm{ES}) \cdot P(\mathrm{ES}) + P(\mathrm{CS} \,/\, \mathrm{EH}) \cdot P(\mathrm{EH})} = \frac{0{,}05 \cdot 0{,}01}{0{,}95 \cdot 0{,}99 + 0{,}05 \cdot 0{,}01} \approx 0{,}00053$$

olarak (yaklaşık % 0,053) bulunmaktadır.

Soru 2 : ***Sağlık Sigortası Primleri***

	Yaş	Kilo	Sigara Kullanımı	Prim
BORA	24	85	Hayır	242 TL
GÜVEN	35	70	Evet	490 TL
EROL	42	90	Hayır	306 TL
ZAFER	46	75	Hayır	?
FATİH	57	53	Hayır	277 TL

Cevap 2 :

288

Verilen isimlere karşı düşen sigorta primleri bulunurken, şu formül kullanılmıştır:

$$\text{Prim} = \begin{cases} \text{kilo} * 2 + \text{yaş} * 3, & \text{sigara kullanımı yoksa} \\ \text{kilo} * 4 + \text{yaş} * 6, & \text{sigara kullanımı varsa} \end{cases}$$

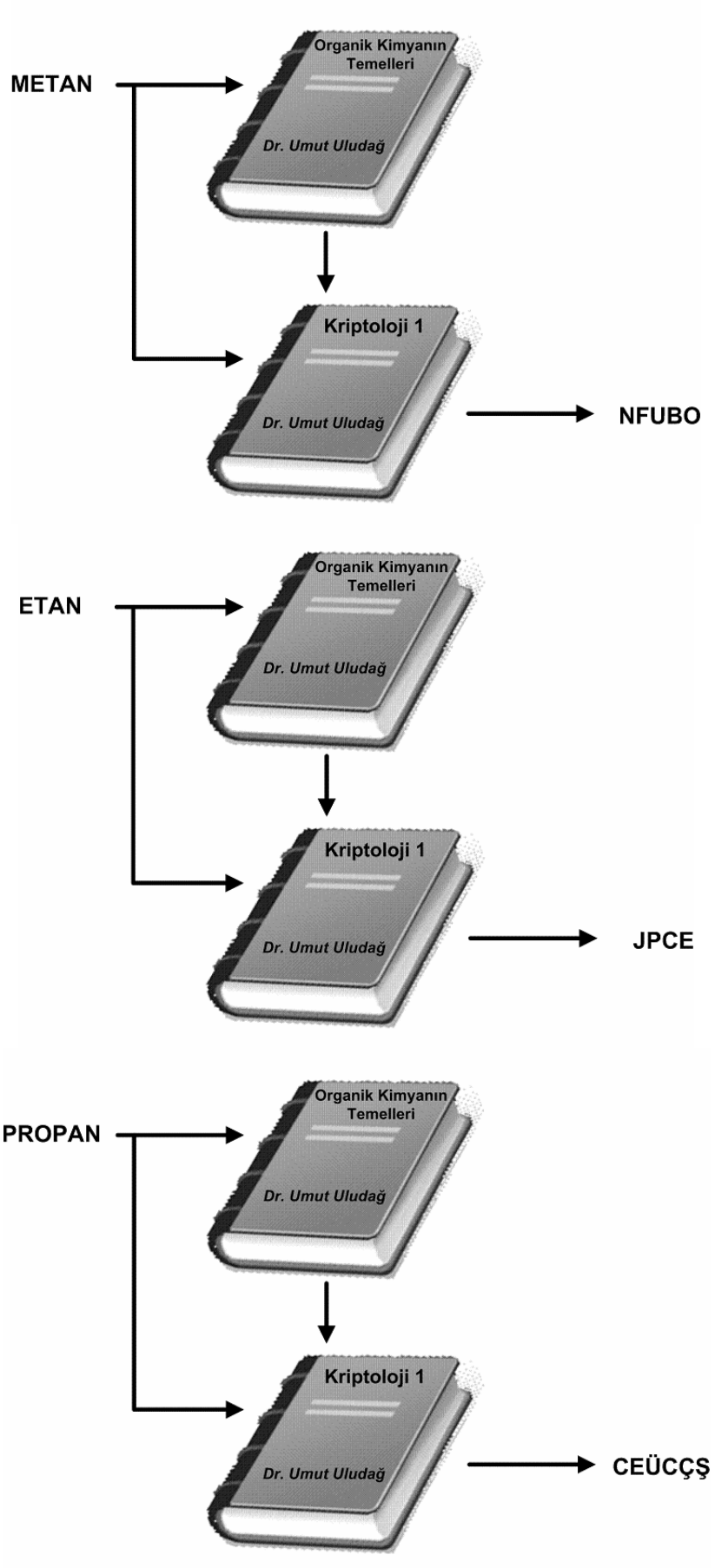
Bora için prim: 85 * 2 + 24 * 3 = 242 TL

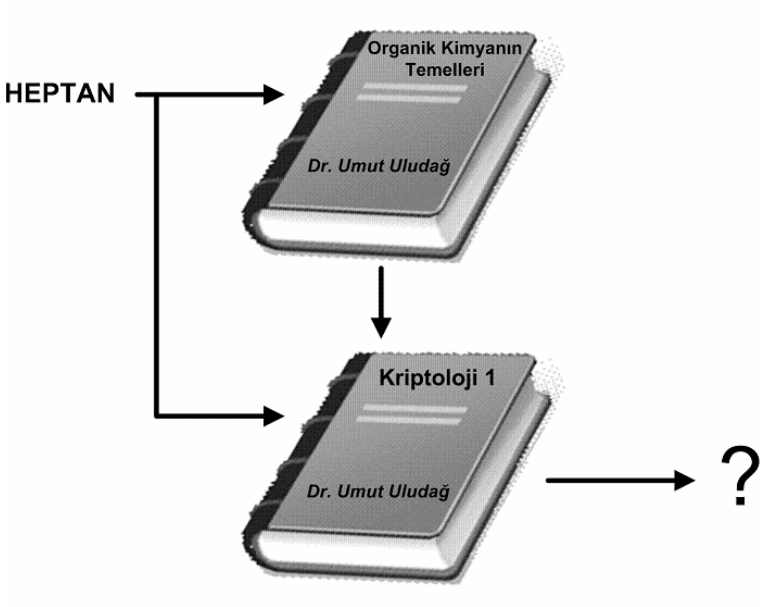
Güven için prim: 70 * 4 + 35 * 6 = 490 TL

…

Bu durumda, Zafer için prim: 75 * 2 + 46 * 3 = 288 TL olacaktır.

Soru 3 :


METAN
Organik Kimyanın Temelleri
Dr. Umut Uludağ
Kriptoloji 1
Dr. Umut Uludağ
NFUBO
ETAN
Organik Kimyanın Temelleri
Dr. Umut Uludağ
Kriptoloji 1
Dr. Umut Uludağ
JPCE
PROPAN
Organik Kimyanın Temelleri
Dr. Umut Uludağ
Kriptoloji 1
Dr. Umut Uludağ
CEÜCÇŞ


HEPTAN
Organik Kimyanın Temelleri
Dr. Umut Uludağ
Kriptoloji 1
Dr. Umut Uludağ
?

Cevap 3 :

JKUTGÇ

Soruda verilen doymuş hidrokarbon (alkan) isimleri, her bir moleküllerinde kaç adet karbon atomu bulunduğu bilgisine (*Organik Kimyanın Temelleri* kitabından gelen veri) bağlı olarak, afin (*affine*) şifrelemeye (*Kriptoloji 1* kitabından gelen veri) tabi tutulmuşlardır.

Yani:

C_nH_{2n+2} kimyasal formulü ile gösterilen alkan, bir molekülünde, n adet karbon ve (2n+2) adet hidrojen atomu içermektedir:

METAN: formül: CH_4 → n = 1 karbon atomu
ETAN: formül: C_2H_6 → n = 2 karbon atomu
PROPAN: formül: C_3H_8 → n = 3 karbon atomu
BÜTAN: formül: C_4H_{10} → n = 4 karbon atomu
PENTAN: formül: C_5H_{12} → n = 5 karbon atomu
HEKZAN: formül: C_6H_{14} → n = 6 karbon atomu
HEPTAN: formül: C_7H_{16} → n = 7 karbon atomu
OKTAN: formül: C_8H_{18} → n = 8 karbon atomu
…
...

Sorudaki afin şifrelemede, açık yazı harfi a , gizli yazı harfi g olmak üzere,
g = n*a + n kuralı uygulanmıştır (tüm işlemler A = 0, B = 1, …, Z = 28 olarak mod 29 da yapılmıştır):

METAN → şifreleme kuralı: g = 1*a + 1 = a + 1

M → N
E → F
T → U
A → B
N → O

ETAN → şifreleme kuralı: g = 2*a + 2

E → J
T → P
A → C
N → E

PROPAN → şifreleme kuralı: g = 3*a + 3

P → C
R → E
O → Ü
P → C
A → Ç
N → Ş

olmaktadır. Bu durumda, bu kuralı sorulan alkan ismine uygularsak:

HEPTAN → şifreleme kuralı: g = 7*a + 7

H → J
E → K
P → U
T → T
A → G
N → Ç

yukarıda verilen JKUTGÇ cevabına ulaşırız.

Copyright © 2010 Dr. Umut ULUDAĞ,
Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü