

BULUŞ ATÖLYESİ

Şifreli mesajlar yazmak ve bunları çözmek tam bir eğlencedir. Gerçekte, gizlilik ve güvenlik gerektiren alanlarda şifreli mesajlar çok işe yarar. Ancak biz, atölyemizde şifreli mesajların düşünce üretmeyi gerektiren yanıyla ilgileniyoruz. Çünkü, buluş yapmanın bir yönü de yeni düşünce üretmektir. O zaman şifre hazırlamak ve çözmek, buluşçular için iyi bir alıştırmaya olabilir. Üstelik yoğun sınav döneminde olanlar da, bu alıştırmayla küçük bir mola verebilirler.



İşte Sorumuz

Bora ve arkadaşı Doğa, birbirlerine şifreli mesajlar yazmayı çok seviyorlar. Doğa'nın son yazdığı şifreli mesaj şöyle: "Khriaüj okjnü vgugi bşab vrröüfi."

Bora, bunun eski şifre yazımı yöntemlerinden biri olduğunu hemen anlıyor ve çözmeye başlıyor. Sizden de bu şifreli mesajı çözmenizi istiyoruz. Dedektifler iş başına...

Eda'nın Denge Sorununu Çözenler

Mart ayı Buluş Atölyesi'ne yanıt olarak Elif Nazlı, ağırlık merkezimizin yere yakın olmasının denge açısından önemini hatırlatıyor. "Eda, yere yakın dönüşler yaparsa daha iyi dengede durur" diyor. Aslı da, buz patencilerini gözlemlediğini, kolları yana açık döndüklerinde ağırlık merkezlerinin yerden uzaklaştığını, bu nedenle dengede durmalarının zorlaşacağını ekliyor. Aslı, Özenç ve Nihal arabanın bizi neden tuttuğunu açıklıyorlar: Arabada giderken, koltukta hareketsiz olduğumuz halde gözlerimizin beynimize hareket halinde olduğumuza ilişkin uyarılar ilettiğini, bunun da algı karışıklığına neden olduğunu söylüyorlar. Elif ve Gökçe, den-

ge organımızın iç kulakta olduğunu, ancak beynimizin gözler ve kaslardan gelen uyarıları da dikkate alarak hareketlerimize karar verdiğini belirtiyorlar. Böylece Aslı, Özenç, Nihal, Elif ve Gökçe sorumuzun yanıtına yönelik önemli ipuçları yakalıyorlar. Eda, baleda dönüşler yaparken gözlerini sabit bir noktaya dikerse dengesini koruyarak daha iyi dönüşler yapmaz mı? Gözlerimizi sabit bir noktaya dikip dönüşler yaptığımızda, iç kulaktan ve gözlerimizden beynimize mümkün olduğunca aynı uyarılar iletilir ve algı karışıklığı daha az yaşanır. Sorumuzun yanıtı, ne kadar basitmiş gerçekte, değil mi? Selin, Eda'ya dönüşler hakkında birkaç bilgi

Şifre Yazımı (Kriptografi)

Şifreli mesajların kullanımı, büyük olasılıkla gizlilik ve güvenlik gerektiren işlerin ortaya çıkmasıyla başladı. Örneğin, Roma imparatorlarından biri olan Sezar, askerlerine şifreli mesajlar gönderdi. Bu, en eski şifre yazımı yöntemlerinden biridir. Örneğin, "İlerleyin" mesajı, bu yöntemle "ıkdpkdvım" biçiminde şifrelenir. Bu şifredeki harflerin, gerçek mesajdaki harflerden bir önceki harfler olduğuna dikkat edin. İşte, bir şifreyi yapmak ya da çözmek için uygulanan kurallar dizisine algoritma denir. Örneğimizdeki algoritmada, "önceki harfi kullan" olmalı. Ancak, kaçınıcı önceki harf kullanılacak? Burada da bize şifreyi yapmak ya da çözmek için kullanılacak sayı dizisi, yani anahtar gerekir. Bu durumda, anahtarın "1" olduğunu kestirebilirsiniz.

Günümüzde, iletişimde kullandığımız teknoloji şifre kullanımını özellikle gerektiriyor. Örneğin, bir arkadaşınıza elektronik posta gönderdiğinizizi düşünelim. Gerçekte, mesajınız birçok bilgisayardan geçiyor. Mesaj, başkaları tarafından okunmaması için şifreleniyor. Bu, basit bir örnek. Elektronik dünyanın yaşamımıza ne kadar çok girdiğini düşünenecek olursanız, birçok bilginin gizlilik ve güvenlik nedeniyle şifrelendiğini anlayabilirsiniz.

Hangi Etkinliği Yapabilirim?

Şifre kullanmadan da bilgi gizli tutulabilir ve

güvenlik altına alınabilir mi? Bunun yapılabildiğini şu örnekten göreceksiniz: Nisan ve Beril birbirlerine mektup göndermek istiyorlar. Ancak, bu mektubun kimse tarafından okunmamasını istiyorlar. Güneş, onlara kilit takılabilecek bir kutu ve anahtarları üzerinde olan iki de kilit veriyor. Bu malzemeleri kullanarak, mektuplarını kimsenin okumamasını sağlayabileceklerini söylüyor. Bunun nasıl olabileceğini bulmanızı istiyoruz. Zor gibi görünüyor, ancak çok kolay! Çözerseniz, sizi "şifre uzmanı" olarak ilan edeceğiz.

Nereden Araştırabilirim?

İnternet'te arama yaparak şifre yazımıyla (kriptografi) ilgili bilgilere ulaşabilirsiniz. Ancak, sorumuzun doğrudan yanıtını bulmanıza olanak yok. Ulaşacağınız bilgiler, şifreyi çözmek için gereken algoritma ve anahtarı bulmanıza yardımcı olabilecek ipuçlarını verebilir.

Kim Buldu?

Amerikalı bir matematikçiyi soruyoruz. Modern kriptografinin babası olarak kabul ediliyor. Elektronik iletişim onunla başladı diyebiliriz. 1949 yılında yayımlanan bir kitabıyla ünlendiğini de söyleyelim.

Tuğba Can

Adres

TÜBİTAK Bilim Çocuk Dergisi Buluş Atölyesi Köşesi Atatürk Bulvarı
No:221 06100 Kavaklıdere/Ankara

de vermek istemiş. "Kolları yana açık biçimde daha yavaş, kapalı biçimde daha hızlı dönebilir" diyor. Arda'nın da önerileri var. "Eda bale yaparken kendisini çok sıkmamalı, ancak gereğinden fazla da rahat bırakmamalı" diyor.

"Kim Buldu?" sorumuzda dengeyi altıncı duyu olarak duyuran İngiliz cerrahı sormuştuk. Yanıt alamamışız. Sabrican, "Bilimadamlarını ve buluşçula-

rı çok zor sormaya başladınız" diye yakınıyor. Tamam, Sabrican bunu dikkate alacağız. Sorumuzun yanıtı, Terence Cawthorne olacaktı. Şu an yoğun bir sınav dönemi geçiriyorsunuz, farkındayız. Arda'nın Eda'ya önerdiğini, biz de size söylüyoruz. Ne kendinizi çok sıkın ne de çok rahat bırakın. Gelecek ay buluştuğumuzda tatile gireceğinizi de hatırlayın. Hepinize kolay gelsin.

Katkıda Bulunanlar

Abdullah Kurtuluş Melike Pinar İÖO 7-A Bursa
Arda Demirkale Çorlu, Tekirdağ
Aslı Göltekin Altınova Merkez İÖO 7-A Ayvalık, Balıkesir
Büşra Arıkan Melike Pinar İÖO 7-A Bursa
Canberk Taşkı/Hatice Uğur/Nur Aktepe/Verda Şen Altınova Merkez İÖO 7-A Ayvalık, Balıkesir
Elif Nazlı Güler Melike Pinar İÖO 7-A Bursa
Gökçe Peker Melike Pinar İÖO 7-A Bursa
Gözde Atay/Buğra Levent/Özlem Kılınç/Melike Aytasgin/Esma Kaya/Sezen Onet/Sibel Daşcı/Yusuuf Emre Bulut/Okay Mercan Karlıtepe İÖO 6-D İstanbul

İşık Sena Akgün Ambarlı İÖO 6-D İstanbul
Konuralp Hayat Melike Pinar İÖO 7-A Bursa
Levent Yurt/Velcan Dalkırmaz Cumhuriyet İÖO 8-B İstanbul
Mehmet Temel Melike Pinar İÖO 7-A Bursa
Nihal Dur Merkez İÖO 6-B Milas, Muğla
Orhun Burak Kara Melike Pinar İÖO 7-A Bursa
Özenci Mutfak Suphi Koyuncuoğlu İÖO 7-A Bornova, İzmir
Özgür Sarık 2001 İÖO 2. sınıf İstanbul
Sabrican Sarık Cumhuriyet İÖO 8-B İstanbul
Selin Bengü Ediz Melike Pinar İÖO 7-A Bursa
Sevde Üçpınar Melike Pinar İÖO 7-A Bursa /
Yusuufcan Kurs Cumhuriyet İÖO 7-E İstanbul