

İçindekiler

24

İnsanoğlunun gizli haberleşmeye gereksindiği günden beri şifreleme teknikleri var. Binlerce yıllık gizli haberleşme tarihinde teknolojinin gelişimiyle şifreleme sistemleri ve cihazlar da değişti. Ancak bir ilke binlerce yıldır geçerliliğini koruyor: Kırılan bir şifre tarihin tozlu sayfalarında yerini alır ve onun yerine daha gelişmiş tasarlanır. Diğer bir deyişle, bir şifre kırılmadığı sürece varlığını korur. Kriptoloji bu ilkeyle gelişerek günümüze kadar geldi. İnsanoğlu Alberti diskini ya da Jefferson tekerleğini binlerce yıl daha önce icat edecek teknolojiye sahipti. Antik çağda şifre kırma teknikleri iki yüzyıl önceki kadar gelişmiş olsaydı, belki şimdi o dönem insanların Alberti diskini de Jefferson tekerleğini de kullandıklarından bahsediyor olacaktık.



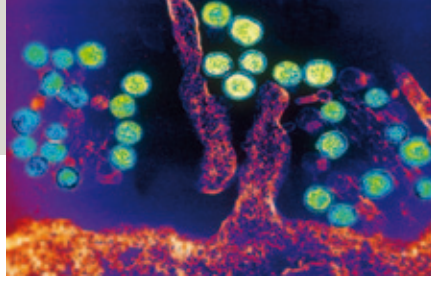
42

Düşmandan bilgi saklama ve gizli haberleşme insanoğlunun kafasını binlerce yıldır meşgul eden bir problem. Çok eski zamanlarda ilkel haberleşme teknolojilerinden ve okuryazar oranının düşük olmasından faydalanılarak bu problemlere kolay çözümler getirilebilmiş. Oysa günümüzün son derece karmaşık ve gelişmiş bilgi ve haberleşme teknolojilerinde, kimlik doğrulama, gizliliği sağlama, bilginin kaynağını doğrulama, verinin bütünlüğünü sağlama gibi bilgi güvenliği problemlerini çözmek o kadar kolay değil. Öyle ki, bu problemleri çözmek için bir bilim dalı doğmuş: Kriptoloji



72

Geçtiğimiz Nisan ayında bir grup bilim insanı, çiftlik hayvanlarından sığırın gen haritasını çıkardıklarını bildirdi. Bu gelişme hayvancılıkta yepyeni bir çağa, gen çağına girişimizin de habercisi oldu. Bu bilgi sayesinde yüz yılı aşkın bir sürede elde edilen verim artışını belki on yıldan dahi kısa bir sürede gerçekleştirebilmek söz konusu olacak. Bu bilimsel ilerleme sayesinde çiftlik hayvanlarının seçimi artık onların ölçülen verimlerine göre değil, doğdukları anda genlerine bakılarak yapılacak. Hayvancılığın çok önemli olduğu ülkemiz için ise bu gelişme tarihi bir fırsat.



Haberler	4
Türkiye'den Haberler / <i>Duran Akca</i>	16
Tekno-Yaşam / <i>Osman Topaç</i>	18
Ctrl+Alt+Del / <i>Levent Daşkiran</i>	22
Kriptolojinin Geçmişi: Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın! / <i>Alparslan Babaoğlu</i>	24
II. Dünya Savaşı'ndan Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme / <i>Orhun Kara</i>	28
Kriptografinin Yapıtaşları: Kriptografik Algoritmalar ve Protokoller / <i>Orhun Kara</i>	34
Kriptonun Olmazsa Olmazı Anahtar / <i>Uğur Kaşif Boyacı</i>	36
Bilgi Güvenliği Problemlerine Matematiksel Yaklaşım Getiren Bir Bilim Dalı: Kriptoloji / <i>Uğur Kaşif Boyacı - Orhun Kara</i>	42
Gündelik Hayatta Kriptoloji / <i>A. Murat Apohan</i>	48
Kara Kutu mu, Şeffaf Kutu mu? / <i>Deniz Karakoyunlu</i>	50
İletişimde Mutlak Güvenlik İçin Kuantum Kriptografi / <i>Tekin Dereli</i>	54
Kuantum Bilgisayarları / <i>Zafer Gedik</i>	58
Tıbbi Uygulamalarda Uzakları Yakınlaştırmak: Teletıp / <i>Yüksel Yazıcı</i>	60
Hanta Virüsü / <i>Nursel Aşan -Damla Ateş</i>	66
Doku Mühendisliği ile Yedek Organlara Doğru / <i>Mustafa Özgür Güler</i>	70
Hayvancılıkta Gen Çağı / <i>Bahri Karaçay</i>	72
Adli Araştırmalarda Yeni bir Pencere: Adli Jeofizik / <i>Şebnem Elbek</i>	78
Yeni Bir Güneş Enerjisi Teknolojisi: Nano Kaplama / <i>Figen Kadırgan</i>	82
TÜBİTAK Bilim ve Teknik Dergisine Gönderilen Yazı ve Görsellerin Sahip Olması Gereken Özellikler	96

84

Doğa
Bülent Gözcelioğlu

86

Sağlık
Ferda Şenel

88

Gökyüzü
Alp Akoğlu

92

Zekâ Oyunları
Emrehan Halıcı

94

Yayın Dünyası
Adem Uludağ