İletişim ve Şifreleme

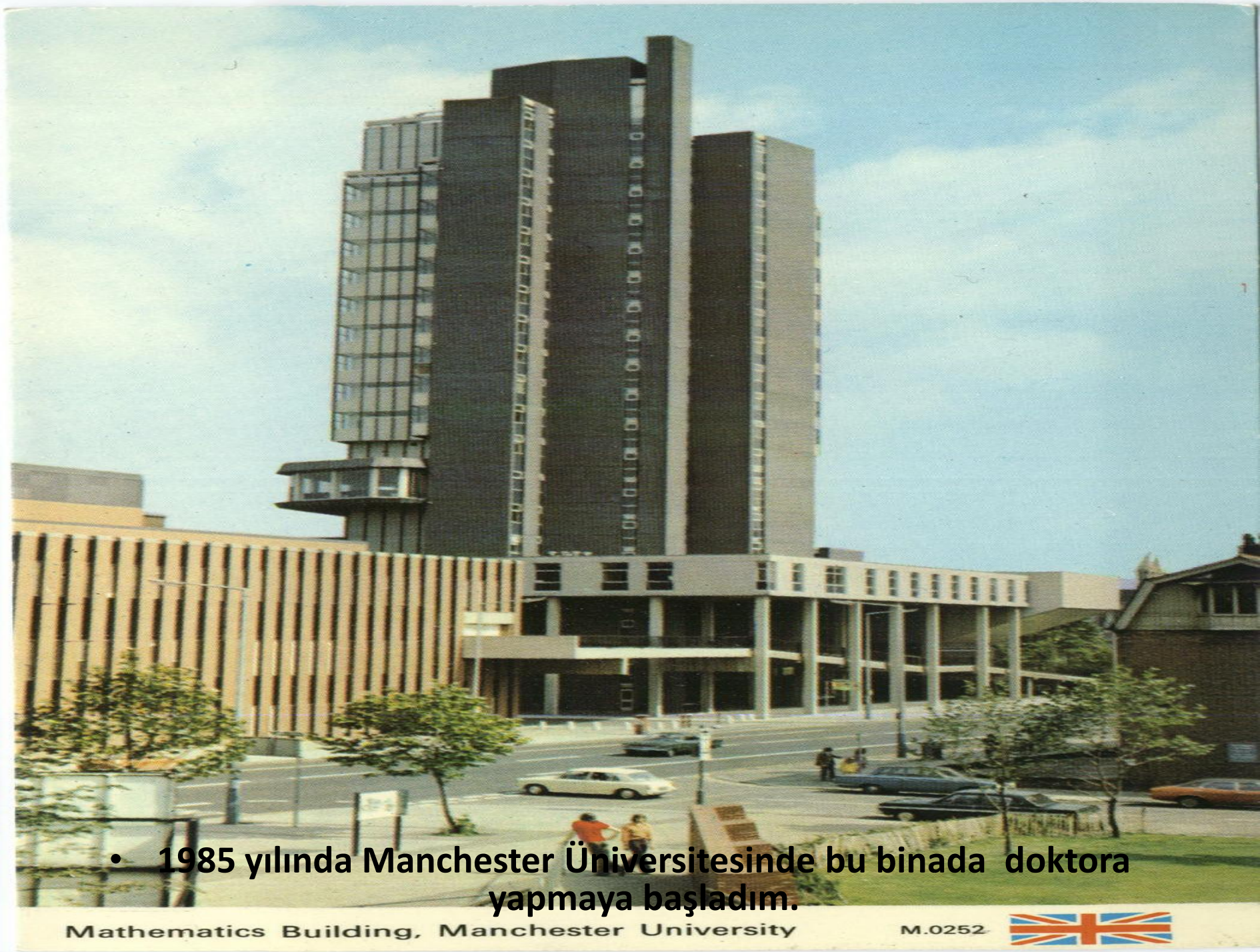
Mahmut KUZUCUOĞLU
Orta Doğu Teknik Üniversitesi
Matematik Bölümü
Ankara
matmah@metu.edu.tr

İlkyar-2014
$June 17, 2014$
19- Haziran 2012

Ben Kimim

- Denizli’nin Çal Ortaköy köyünde bu evde doğdum.

- 1984 yılında Amerikanın Toledo Üniversitesine Asistan olarak gittim . Amarikanın Başkenti wahington'daki Beyaz Saray.



- **1985 yılında Manchester Üniversitesinde bu binada doktora yapmaya başladım.**

- **3 Ay Ailecek Rusya da kaldık.**

ALMANYA OBERWOLFACH MATEMATİK ENSTİTÜSÜ

ISCHIA GROUP THEORY 2012

İletişim ve Şifreleme

Mahmut KUZUCUOĞLU
Orta Doğu Teknik Üniversitesi
Matematik Bölümü
Ankara
matmah@metu.edu.tr

İlkyar-2014
$June 27, 2014$
19- Haziran 2012

Neler Öğreneceğiz:

İletişim nedir?

Neler Öğreneceğiz:

İletişim nedir?

İletişim yolları nelerdir ?

Neler Öğreneceğiz:

İletişim nedir?

İletişim yolları nelerdir ?

Hayvanların iletişimi?

Neler Öğreneceğiz:

İletişim nedir?

İletişim yolları nelerdir ?

Hayvanların iletişimi?

İletişimde gizlilik ?

Neler Öğreneceğiz:

İletişim nedir?

İletişim yolları nelerdir ?

Hayvanların iletişimi?

İletişimde gizlilik ?

Gizli bilgilerin emniyetli bir şekilde alıcıya iletilmesi?

İletişim ve Şifreleme

- İletişim duygu, düşünce ya da bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması, bildirişim, haberleşme, komünikasyon demektir.
- İletişim telefon, telgraf, televizyon, radyo gibi aygıtlarla yürütülen bilgi alışverişi, bildirişim, haberleşme, komünikasyon.

İletişim ve Şifreleme

- İletişim iki ya da daha çok kişi arasında bir anlaşma, uzlaşma doğmasını sağlayan karşılıklı konuşma, diyalog şeklinde de tanımlanabilir .

  İletişimde kişinin konuşma biçimi, seçtiği sözcükler, ses tonu, beden duruşu, jest ve mimikler önemlidir.

  İletişimde en önemli faktörlerden birisi de dinlemek ve empati kurabilmektir.

  Empati Kurma; dış dünyayı karşımızdaki insanın penceresinden, yani onun penceresinden görmeye çalışmak demektir.
  Bir başka deyişle kendimizi onun yerine koymak demektir.

İletişim ve Şifreleme

Başlıca İletişim Yolları:

- Sözlü İletişim: Karşılıklı konuşmaya dayalı iletişimdir.
- Yazılı İletişim: yazı yoluyla sağlanan iletişimdir.
- Hareketlerle İletişim: Jest, mimik ve çeşitli hareketlerle sağlanan iletişimdir.

İletişim ve Şifreleme

- Hayvanlar arası iletişim için kuşların ötüşü, aslanların, kaplanların, çıtaların, idrar koklaması, kükremesi; kedilerin miyavlamasını örnek verebiliriz.
- Köpeklerde koklayarak ve havlayarak iletişim kurar.

İletişim ve Şifreleme

- Hayvanlar arası iletişim için keklikle kafes avcılığı da verilebilir.
  Bu yöntemde avcılar kendi kekliklerini dağa götürüp kafes içinde bir çalının kenarına bırakırlar.
  Keklik öterek çevredeki kekliklerle iletişime geçer ve onları yanına çağırır.
  Tabi avcı da bu durumdan yararlanarak gelen keklikleri avlar.

İletişim ve Şifreleme

- Tarihte güvercinlerle iletişim sağlanmıştır. Özellikle savaşlarda ve zor zamanlarda yardım istemek veya durumlarını belirtmek için yazdıkları küçük notları güvercinlerin ayaklarına bağladıkları küçük kağıt parçalarıyla diğer kişilere veya gruplara iletmişlerdir.
- Karadeniz insanları cep telefonundan önce ıslık çalarak komşuları ile haberleşirlerdi.

İletişim ve Şifreleme

- Elektronik posta (e-mail) ve telefon numaraları da bir çeşit şifreli habeleşmedir zira herkesin bir telefon numarası var ve numaranızı konuşmak istediğiniz kişilere verirsiniz.

- Aynı şekilde elektonik postalar (e-mail) için bir e-mail posta adresi ve ayrıca şifresi vardır.

- Bunun sayesinde iletişim sadece istenen kişiler arasında sağlanır ve istenmeyen kişilerin mesajları okuması veya telefonları dinlemesi önlenir.

İletişim ve Şifreleme

- Başkalarının duymasını veya görmesini istemediğimiz bilgileri gizli olarak bildiririz. Örneğin yazdığımız bir mektubu başkaları okumasın diye zarfa koyarız.
- Savaş sırasında düşmanların bizim haberleşmemizi dinlemesin diye şifreler geliştirir ve bilgilerin düşmanın eline geçmesini engellemeye çalışırız.

İletişim ve Şifreleme

- Bunların yanısıra bir de işleri kolaylaştırmak ve zaman kazanmak için bilgisayarlardan yararlanırız. Örneğin mektupların, paket servislerin üzerine bölge isimleri yani posta kodu yazılarak bilgisayarların bunları ayrı bölgeler için gruplara ayırması ve bu sayede dağıtımın hızlanması sağlanmaktadır.
- Aynı şey kitaplar için de konularına ve basıldıkları ülkeye göre numaralandırılmaktadırlar. Buna ISBN (International Standard Book Number) numarası denir.

İletişim ve Şifreleme

- Benzer bir yöntem marketlerde alış veriş sırasında ürünlerin üzerine barkod denilen bir çeşit şifre ile de yapılmaktadır. Ürünü alırken makineden çıkan bir kağıdı ürün paketinin üzerine yapıştırırlar. Bu kağıtta bir çeşit şifre vardır. O ürünün adı, firması gibi bilgiler içerir. Ürünün fiyatını kasadaki makine okumakta yani bir çeşit şifre kırma yapmakta ve daha sonra bu üründen ne kadar satış yapıldığı belirlenmektedir.

İletişim ve Şifreleme

- Gizli kodlarla şifrelerin oluşturulmasına Kriptoğrafi denir.
- Gizli kodlarla şifrelerin kırılmasına da kripto analiz denir.
- Kriptoloji ise hem kriptografiyi hem de kripto analizi içine alır.

İletişim ve Şifreleme

- Gizli yazışmaların tarihi M.Ö. 1900 lü yıllara kadar uzanır. Mısırlı yazı uzmanlarının mezar taşlarına yazmalarına bazı bilgi ve mesajları harf sıralarını değiştirerek yazdıkları belirlenmiştir.

İletişim ve Şifreleme

- Daha sonraları bazı metinleri silindir biçimindeki skytale adı verilen şerit şeklindeki bir parşümen yada papilus adı verilen bir çeşit kağıdı önce bu silindir şeklindeki nesneye düzenli bir şekilde sarılır. Daha sonra metinler soldan sağa doğru yazılır. Bu durumda metin şeritin üzerinde yukarıdan aşağıya ama çok karışık bir biçimde görünür. Şerit slindirden ayrılınca yazdığımız metni okuyabilmek mümkün olmaz. Ancak bu silindir biçimindeki nesneyi mesajın iletileceği kişiye de vererek bir iletişim sağlıklı bir şekilde kurulur.
  Bu sayede şifreli mesajlarını karşı tarafa güvenli bir şekilde ulaştırmışlardır.

İletişim ve Şifreleme

- Tarih boyunca çeşitli şifreler kullanılmış, zira insan var olduğu müddetçe şifreye (gizliliğe) ihtiyaç olmuştur. ikinci dünya savaşında Manchester Univertsitesi Profesörlerinden Alan Turing ve ekibinin şifreleri çözmesi ile savaşın sonucunu ciddi şekilde etkilemişlerdir.

İletişim ve Şifreleme

- Bugün banka kartları, uydudan yayın yapan şifreli kanallar, cep telefonları şifreleri kullanarak insanların biribirleri ile daha emniyetli bir şekilde haberleşmeleri sağlanmaktadır. Bu işler için kullanılan yöntemler daha çok matematikçiler tarafından geliştirilmektedir.
  Bu konulara devletlerin de destek vermesinden ve ihtiyaç olmasından dolayı bu konulardaki teknoloji hem çok hızlı gelişmekte hemde bu gelişmeler sayesinde daha çok matematikçiye ihtiyaç bulunmaktadır. Bu uygulamalarda matematiğin gelişmesine yardımcı olmaktadır. Yani gelişme iki taraflı olarak devam etmektedir.

İletişim ve Şifreleme

İlk kriptoloji sistemlerinden olan Caesar şifresi Julius Caesar tarafından Galya (Gallic) savaşlarında kullanılmıştır.

Julius Casear MÖ 100-MÖ 44 yıllarında yaşamış 56 yaşında ölmüştür. Galya savaşları MÖ 58-50 yılları arasında olmuştur.

İletişim ve Şifreleme

Julius Caesar şifresi alfabedeki her harfi (İngiliz alfabesinde 3 Türkçe alfabede 4 harf) sağa kaydırarak oluşturulan bir şifre sistemidir. Yani a yerine d harfi konmuştur.

İletişim ve Şifreleme

Julius Caesar şifresi:

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m
D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P

n	o	ö	p	r	s	ş	t	u	ü	v	y	z
R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç

İletişim ve Şifreleme

Kelimemiz MUTLULUKLAR olsun. Şimdi bu kelimeyi şifreleyelim.

M	U	T	L	U	L	U	K	L	A	R
P	Z	Y	Ö	Z	Ö	Z	O	Ö	D	U

İletişim ve Şifreleme

Yeni kelimemiz ATATÜRK olsun.

A	T	A	T	Ü	R	K
D	Y	D	Y	A	U	O

İletişim ve Şifreleme

Yeni kelimemiz CUMHURİYET olsun.

İletişim ve Şifreleme

C	U	M	H	U	R	İ	Y	E	T
F	Z	P	K	Z	U	M	C	H	Y

İletişim ve Şifreleme

Şimdi şifrelenmiş olarak verilen şu kelimenin gerçek anlamını bulalım.

İletişim ve Şifreleme

Şimdi şifrelenmiş olarak verilen şu kelimenin gerçek anlamını bulalım.

v d ı d o y d ü d ö ğ l u

İletişim ve Şifreleme

Şimdi şifrelenmiş olarak verilen şu kelimenin gerçek anlamını bulalım.

v d ı d o y d ü d ö ğ l u

Ne yapmamız gerekir. Bu noktada şifre üretirken

kullandığımız metod da İşlemlerin tersinin olması gerektiğini kavramamız gerekir.

İletişim ve Şifreleme

Kelimemizin Şafakta saldır olduğunu buluruz.

ş	a	f	a	k	t	a	s	a	l	d	ı	r
v	d	ı	d	o	y	d	ü	d	ö	ğ	l	u

İletişim ve Şifreleme

Şimdi aşagıdaki şifreye karşılık gelen metni bulalım.
O Z U E D R E D C U D P L

İletişim ve Şifreleme

Kelimemizin KURBAN BAYRAMI olduğunu görürüz.

K	U	R	B	A	N		B	A	Y	R	A	M	I
O	Z	U	E	D	R		E	D	C	U	D	P	L

Şu kelimeleri de siz şifreleyin:

(a) PARA YOLLA

(b) MATEMATİĞİ SEVİYORUM

İletişim ve Şifreleme

- Her şifre kırılabilir.
- Ancak bir şifrenin ne kadar zamanda kırılabileceğine dair tahminler ve hesaplamalar vardır.
- Bütün bu hesaplamalar bu günkü teknolojik aletlere göre yapılır. Bu yıl yapılan bir şifre kırma süresi gelecek yıl için geçerli değildir.
- Zira gelecek yıl çok daha donanımlı ve çok daha hızlı bilgisayarlar çıkabilir.
- Bu durumda şifrenin kırılma süresi de azalır.

İletişim ve Şifreleme

- Örneğin savaşta bir şifre kullanacaksınız. Bu şifre kullanarak pilotunuzla haberleşeceksiniz. Hesaplanması gereken süre sizin uçağınız hareket ettikten sonra düşman sizin şifrenizi kırmadan önce uçağınızın bombasını bırakıp ülkenize dönmesi gerekir.
- Bu arada bu şifre ile siz de en güvenli şekilde pilotunuzla haberleşebilmeniz ve gerekli iletişimi kolayca yapabilmeniz gerekmektedir.
- Düşman güçlerin ortamı kirlendirmesine karşı (telefonlardaki jammer sistemi gibi) sizin pilotunuzun sizin ne dediğinizi doğru anlamasını sağlayacak ve yanlış anlamayı giderici şifreler yazmalıyız.

İletişim ve Şifreleme

Örneğin saatlerdeki gibi modulo 24 e göre hesap yapmak istesek ve benim bu işlemi yapmak için 2 saniyem olsa ve şu soruya yanıt arasam:

2019 saat sonra saat kaç olur?
Burada 3 saati 2019 ile şifrelemekten bahsediyoruz.

Yapılması gereken şey 2019 u 24 e böleriz ve sonucu 84 gün 3 saat olarak buluruz. Biz saati merak ettiğimize göre şu andaki saate 3 saat ekler 2019 saat sonraki saati söyleyebiliriz.

Bunu 2 saniyede yapamayız.

Dolayasıyla süre şifre için önemli bir kavramdır.

İletişim ve Şifreleme

Şimdi size gerçek bir şifrenin hikayesini anlatayım.
AYŞE TATİLE ÇIKSIN

İletişim ve Şifreleme

1974 yılında yapılan Kıbrıs Barış harekatı için o dönemin Dışişleri bakanı Turan Güneş tarafından bizzat kullanılan ve gerçeğe çok uygun olan bir şifrelemedir.
Turan Güneş'in Ayşe isminde bir kızı olduğu bilinir.
Kıbrıs barış harekatı ile ilgili olarak Dışişleri bakanı Turan Güneş İsviçrenin Cenevre şehrine gitmiştir ve bu ilgili ülkelerle yapılan son görüşmedir.

İletişim ve Şifreleme

Cenevre'de sürdürülen görüşmeler sırasında anlaşmanın mümkün olmadığı kanaati kesinleşince harekâtın yeniden başlatılacağı anlamına gelen "Ayşe Tatile Çıksın" parolasını Türk Dışişleri Bakanı Turan Güneş, Başbakan Bülent Ecevit'e bildirdi.
Bu mesajla işlerinin uzayacağını ve kızı Ayşe'nin tatile çıkmasını ve kendisini beklememesi mesajı iletilmiştir. Ancak asıl verilmek istenen mesaj Türk Askerinin Kıbrıs'a gitmesini yani harekatın başlama mesajını iletmiştir.

İletişim ve Şifreleme

Öteleme şifresi Casear dan sonra da kullanıldı. Bu şifrenin daha geliştirilmiş olanlarını incelemek için biraz matematiksel hazırlık yapalım.

İletişim ve Şifreleme

Harflerin yerine rakamlar koyarak da şifrelemeler yapılmıştır.
Bunun için İngiliz alfabesi kullanarak yapılan şu şifrelemeyi Türkçe alfabeye uygulayarak inceleyelim.
Alfabemizde 29 harf vardır. Bu harfleri 0 dan başlayarak numaralandıralım ve boşluk için de 29 yazalım.
Sıfırdan başladığımız için toplam 28 rakam kullanmış olduk yanı a için sıfır yazıyoruz ve listemiz şöyle.

İletişim ve Şifreleme

şifre2

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

o	ö	p	r	s	ş	t	u	ü	v	y	z	
17	18	19	20	21	22	23	24	25	26	27	28	29

İletişim ve Şifreleme

Şimdi bu yöntemle Para yolla metnini şifreleyelim.

P	A	R	A		Y	O	L	L	A
19	0	20	0	29	27	17	14	14	0

İletişim ve Şifreleme

Aynı şifreleme metoduyla Fenerbahçe yi şifreleyelim.

F	E	N	E	R	B	A	H	Ç	E
6	5	16	5	20	1	0	9	3	5

İletişim ve Şifreleme

S	E	V	G	i	L	i		i	L	K	Y	A	R	L	I	L	A	R
21	5	26	7	11	14	11	29	11	14	13	27	0	20	14	10	14	0	20

H	O	Ş	G	E	L	D	İ	N	İ	Z
9	17	22	7	5	14	4	11	16	11	28

İletişim ve Şifreleme

S	E	V	G	İ	L	İ		A	Y	N	U	R
21	5	26	7	11	14	11	29	0	27	16	24	20

İletişim ve Şifreleme

ŞİMDİ AŞAĞIDAKİ ŞİFRENİN KELİMESİNİ BULALIM.

7	0	14	0	23	0	21	0	20	0	27

İletişim ve Şifreleme

BU KELİMENİN GALATASARAY
olduğunu bulabiliriz.

İletişim ve Şifreleme

Kaynaklar

Introduction to Criptology ; Elementary Number Theory, Sayfa, 121–125

http://www.metu.edu.tr/∼matmah/

BENİ DİNLEDİĞİNİZ İÇİN TEŞEKKÜRLER