

9. SINIF ALGORİTMA VE BİLİŞİM-2

ŞİFRELEME ALGORİTMALARI

Verilerin, bilgilerin güvenliğini sağlamak için kullanılan matematiksel yöntemlerdir.

Bu algoritmalar verileri şifrelere dönüştürür.

Şifreleme=Kriptografi

Şifre çözme=Kriptoanaliz

Olmak üzere iki bölümden oluşur.

Klasik şifreleme yöntemlerinde alfabedeki harflere sırayla sayısal değerler verilir. Bu değerler üzerinden şifreler oluşturulur.

A	B	C	Ç	D	E	F	G	Ğ	H
1	2	3	4	5	6	7	8	9	10

I	İ	J	K	L	M	N	O	Ö	P
11	12	13	14	15	16	17	18	19	20

R	S	Ş	T	U	Ü	V	Y	Z
21	22	23	24	25	26	27	28	0

Türkçe harfler ve değerleri

Sezar şifrelemesi:

Anahtar 4 ise her harf kendisinden sonraki 4. harf olarak yazılır.

Anahtar -4 ise her harf kendisinden önceki 4. harf olarak yazılır.

Örneğin: KALE kelimesi anahtarı 3 olan bir Sezar şifrelemesi ile NÇOĞ olmaktadır.

Bunun dışında

- Vegenere şifrelemesi
- Affine şifrelemesi

gibi şifrelemeler vardır. Bunları araştırmak isterseniz araştırabilirsiniz.

- Sizde kendinize göre şifre oluşturabilir ve buna göre veriler elde edebilirsiniz.

Ö: KEMAL

A → 1, B → 2, C → 3,, Z → 0

- Harf kodu tek ise 2 ile çarp bulunan sayıyı 29'a böl kalanın sayı değerine karşılık gelen harfi bul
- Harf kodu çift ise 3 ile çarp bulunan sayıyı 29'a böl, kalanın sayı değerine karşılık gelen harfi bul.

Buna göre yukarıda verilen kelimeye karşılık gelen 5 harfli kodu bulalım.

A	B	C	Ç	D	E	F	G	Ğ	H
1	2	3	4	5	6	7	8	9	10

I	İ	J	K	L	M	N	O	Ö	P
11	12	13	14	15	16	17	18	19	20

R	S	Ş	T	U	Ü	V	Y	Z
21	22	23	24	25	26	27	28	0

ÇİZGE KURAMI

Çizgeler nesnelere arasındaki ilişkileri göstermek için kullanılan yapılardır.

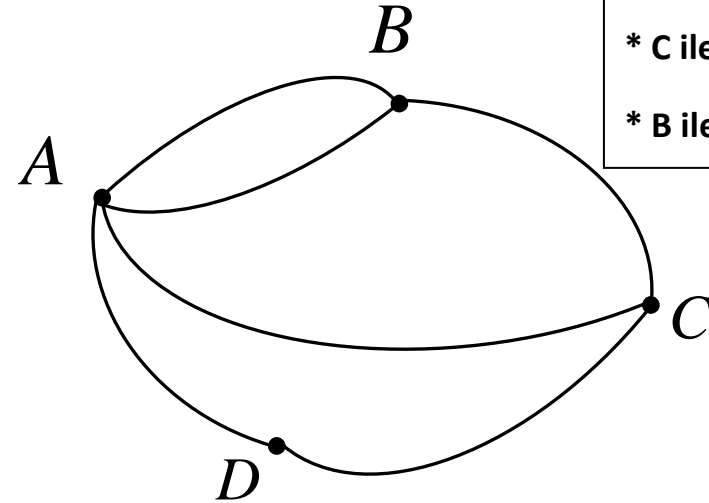
Bir çizge, düğümler ve bu düğümleri birbirine bağlayan kenarlardan oluşur.

Temel kavramlar

- I. Düğüm: Nesnelere gösteren noktalardır.
- II. Kenar: Düğümler arasındaki bağlantıyı gösteren çizgilerdir.
- III. Komşuluk: İki düğüm birbirine bağlı ise bu düğümler komşudur.
- IV. Derece: Bir düğümün derecesi o düğüme bağlı kenar sayısıdır.

V. Tek dereceli düğüm: Bir düğümün derecesinin tek sayı olması durumudur.

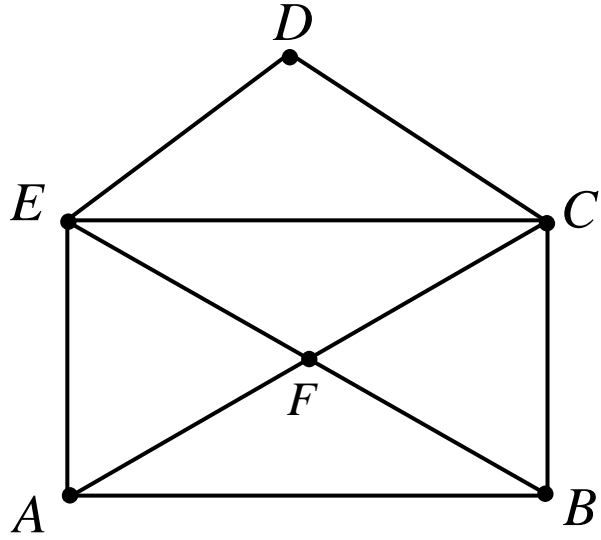
VI. Çift dereceli düğüm: Bir düğüme derecesinin çift sayı olması durumudur.



- * A ile B komşudur.
- * C ile D komşudur.
- * B ile C komşudur.

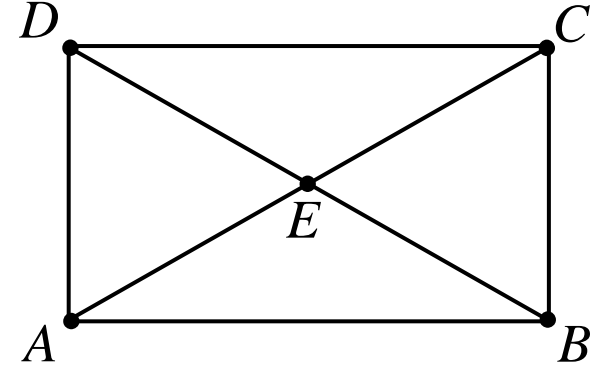
- A düğümünün derecesi: 4
- B düğümünün derecesi: 3
- C düğümünün derecesi:
- D düğümünün derecesi:

Ö:



Yukarıdaki döngüyü çizgiler üzerinden birer defa giderek tamamlayabilir miyiz?

Ö:



Yukarıdaki döngüyü çizgiler üzerinden birer defa giderek tamamlayabilir miyiz?

EULER DÖNGÜSÜ

Bu çizge, her kenar üzerinden sadece bir defa geçilmesi ile başladığı düğüme geri dönen kapalı bir yoldur.

- Çizgedeki her düğümün derecesi çift ise Euler döngüsüdür.
- Elimizi kaldırmadan her kenardan sadece bir kez geçerek bu çizgeyi çizebilir ve çizmeye başladığımız noktada bitirebiliriz.

EULER YOLU

Bir çizge her kenardan bir kere geçilerek çizilebiliyor fakat başlangıç düğümünden farklı bir düğüme bitiyorsa Euler yolu denir.

- Çizgedeki sadece iki düğümün derecesi tek, diğerleri çift ise Euler yoludur.
- Elimizi kaldırmadan her kenardan sadece bir kez geçerek tamamlamak için, tek dereceli bir düğümden başlanır ve diğer tek dereceli düğümlerde bitirilir.