Anahtarlı ve Yer Değiştirmeli Şifreler

Çalışma Kâğıdı · 30 Soru · Kolaydan Zora

Ad Soyad _____ Sınıf / No _____ Tarih _____

KONU ÖZETİ

- **Anahtarlı (Vigenere tipi) şifreleme:** Anlamlı bir kelime anahtar olarak seçilir ve metnin harflerine döngüsel olarak uygulanır. Anahtar harfi X ise metindeki harf, alfabesi X ile başlayan satıra göre şifrelenir; yani **(X'in sayısı - 1)** kadar kaydırılır. (A anahtarı harfi değiştirmez, B 1 kaydırır, C 2 kaydırır ...)
- Vigenere tipi şifrelemede **aynı harf farklı harflere** dönüşebilir; bu yüzden sıklık analiziyle çözmek zordur. Anahtar bilinirse her harf aynı miktarda geri kaydırılarak çözülür.
- **Yer değiştirme yöntemi:** Harfler değişmez, yalnızca yerleri değişir. Metni ters yazma, n'li bloklara ayırıp bloklar içinde yer değiştirme, harfleri satırlara yazıp sütun sütun okuma bu yönteme örnektir.
- **Yerine koyma yöntemi:** Harfler başka harf, sayı ya da sembollerle değiştirilir (Sezar, doğrusal, Vigenere). **Polybius tablosunda** her harf, bulunduğu satır ve sütunun numarasıyla (iki basamaklı sayı) gösterilir.
- Şifreli metin ile gerçek metin arasındaki benzerlikler (aynı harfler mi kullanılmış, harf sayısı, tekrar eden harfler) hangi yöntemin kullanıldığını tahmin etmeye yardım eder.

KOLAY Isınma Soruları (1–10)

1. Vigenere tipi şifrelemede anahtar yalnızca **D** harfinden oluşuyorsa
a) Her harf kaç kaydırılır?
b) Bu şifreleme hangi şifreleme yöntemiyle aynıdır?

2. **BC** anahtarıyla Vigenere tipi şifreleme yapılacaktır. (B: 1 kaydırma, C: 2 kaydırma, döngüsel) **OKUL** kelimesini şifreleyiniz.

3. **BC** anahtarıyla Vigenere tipi şifreleme ile şifrelenmiş **BŞBÇB** kelimesini çözünüz.

4 Bir şifrelemede kelimeler **tersten** yazılmaktadır. **ÇUVAH** şifreli kelimesini çözünüz. Bu hangi tür şifreleme yöntemidir?

5 Bir şifrelemede kelime **ikişerli bloklara** ayrılıyor ve her bloktaki iki harfin yeri değiştiriliyor. **SERGİLER** kelimesini şifreleyiniz.

6 **KAR** kelimesinin harflerinin yerleri değiştirilerek kaç farklı şifreli yazım elde edilir? (Kelimenin kendisi hariç) Hepsini yazınız.

7 Aşağıdakilerden hangisi **DENİZ** kelimesinin **yer değiştirme** yöntemiyle şifrelenmiş hâli olabilir?

A) GĞPLC B) ZİNED C) DDNİZ D) ÇDMHY E) DEMİZ

8 Aşağıdaki şifrelemelerin **yerine koyma** mı, **yer değiştirme** mi olduğunu belirtiniz.

a) KALEM → MELAK b) KALEM → NÇOĞÖ c) KALEM → AKELM ç) KALEM → 14-1-15-6-16

9 Polybius tablosunda her harf önce satır, sonra sütun numarasıyla yazılır (örneğin G → 22). **SU** kelimesini şifreleyiniz.

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

10 Polybius tablosuna göre **12 11 33** ile şifrelenmiş kelimeyi bulunuz.

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

ORTA Pekiştirme Soruları (11–20)

11 **YOL** anahtarıyla Vigenere tipi şifreleme yapılacaktır. **KİTAP** kelimesini şifreleyiniz.

12 **ET** anahtarıyla Vigenere tipi şifreleme ile şifrelenmiş **UTDTÜ** kelimesini çözünüz.

13 **BD** anahtarıyla Vigenere tipi şifreleme yapılıyor.
a) **AAAA** metni nasıl şifrelenir?
b) Bu sonuç, Vigenere tipi şifrelemenin sıklık analiziyle çözülmesini neden zorlaştırır?

14 Bir mesaj her satıra **3** harf gelecek biçimde satır satır yazılıyor, sonra **sütun sütun** (yukarıdan aşağı) okunarak şifreleniyor. **SAATBEŞTE** mesajını şifreleyiniz.

…	…	…
…	…	…
…	…	…

15 Bir şifrelemede kelime **üçerli bloklara** ayrılıyor ve her blok ters yazılıyor (son blok eksik olabilir). **KALEMLİK** kelimesini şifreleyiniz.

16 Harfleri birbirinden farklı **4** harfli bir kelimenin harflerinin yerleri değiştirilerek kelimenin kendisi dışında kaç farklı yazım elde edilir?

A) 11 B) 12 C) 16 D) 23 E) 24

17 **EVET** kelimesi iki harfli bir anahtarla Vigenere tipi şifreleme sonucunda **ÖVÖT** olmuştur. Anahtarı bulunuz.

18 Polybius tablosuna göre **GÖL** kelimesini şifreleyiniz.

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

19 Satırlara 3'er harf yazılıp sütun sütun okunarak şifrelenmiş **DSTEBTRİİ** mesajını çözünüz.

20 Aşağıdaki şifreleme yöntemlerinden hangisi **sıklık (frekans) analiziyle** çözülmeye karşı en dayanıklıdır?

A) Anahtarı 3 olan Sezar şifreleme
B) 2n + 1 kuralıyla doğrusal şifreleme
C) Uzun bir anahtar kelimeyle Vigenere tipi şifreleme
D) Her harfi sabit bir sembolle değiştirme
E) Anahtarı 10 olan Sezar şifreleme

ZOR Düşünme Soruları (21–30)

21 **BİR** anahtarıyla Vigenere tipi şifreleme yapılıyor. **ANKARA** kelimesinin şifreli hâli aşağıdakilerden hangisidir?

A) BYDBCR B) BYDBCS C) CZEÇDT D) BİRBİR E) ÇNKÇRA

22 **DENEME** kelimesi iki harfli bir anahtarla Vigenere tipi şifrelenerek **OŞAŞZŞ** elde edilmiştir. Anahtar aşağıdakilerden hangisidir?

A) JO B) KÖ C) LO D) OK E) KO

23 Bir kelime önce anahtarı **3** olan Sezar şifrelemeyle şifreleniyor, sonra **tersten** yazılıyor. Sonuç **ÇUÇÖ** olduğuna göre kelime hangisidir?

A) MASA B) KASA C) ASAM D) MASAL E) SAMA

24 **ANNA** kelimesinin harflerinin yerleri değiştirilerek (kendisi de dahil) kaç farklı dizi yazılabilir?

A) 4 B) 6 C) 8 D) 12 E) 24

25 Polybius tablosuna göre **14 26 14 16 32** ile şifrelenmiş kelime hangisidir?

A) ÇIÇEK B) CİCEK C) ÇİÇEK D) ÇİÇEL E) ÇİZEK

26 **KUŞ** anahtarıyla Vigenere tipi şifreleme yapılan uzun bir metinde **A** harfleri hangi harflere dönüşebilir?

A) Yalnız K B) Bütün harflere C) L, Ü ve T D) A, K ve U E) K, U ve Ş

27 İkişerli bloklarda harflerin yeri değiştirilerek **KİTAPLAR** kelimesi **İKATLPRA** olarak şifrelenmiştir. Aynı yöntemle **AKELLMRE** şifresi çözülürse hangi kelime elde edilir?

A) KALMELER B) KLALEMER C) LKALMERE D) KALEMLER E) KELAMLER

28 Bir mesaj satırlara 4'er harf yazılıp sütun sütun okunarak şifrelenmiştir. Şifreli metin **YNİAGYREOILR** olduğuna göre gerçek mesaj hangisidir?

A) YARINGELİRİM
B) YARINGİDİYOR
C) YARINGELİYOR
D) YARINGELİYOM
E) YANIRGELİYOR

29 **AAAAAA** metni Vigenere tipi şifreleme ile **BCDBCD** olmuştur. Kullanılan anahtar hangisidir?

A) BCD B) BC C) B D) ABC E) CDE

30 **EN** anahtarıyla Vigenere tipi şifreleme ile şifrelenmiş **JJSSYBN** kelimesi hangisidir?

A) GÜNDÜZE B) GÜZELCE C) GÜNLÜKÇ D) BÜYÜKLÜ E) GÜNEŞLİ

Takıldığın soruyu işaretle, konu özetine tekrar göz at. Başarılar!
Diğer konuların çalışma kâğıtları ve deneme sınavları: **maarifpdf.com.tr**