9 ve 10. Sınıflar

Yarıyıl Tatili

Matematik Dersi

ÖĞRETMEN EL REHBERİ

KRİPTOLOJİ SERÜVENİ

HAZIRLAYANLAR

Editör
Doç. Dr. Burak KARABEY

Yazarlar
Dr. Rukiye GÖKCE
Dr. Sibel TAŞCI
Abdullah BALCI
Ayşe YAŞAR PIRTI
Ceren TUNALI
Özcan EKEN

Program Geliştirme Uzmanı
Bilgen KERKEZ

Dil Uzmanı
Soner SAVAK

Ölçme ve Değerlendirme Uzmanı
Dr. Mustafa KANDIRMAZ

Görsel Tasarım
Enes Malik TEKİN
İnci YILMAZ ŞİMŞEK
Saliha TÜRK
Serdar KULABOĞA
Şükrü Ufuk NAYMAN

Kapak Tasarım
Esra ÇALHAN

ISBN: 978-975-11-0730-5

İÇİNDEKİLER

Etkinlik Adı	:	Kriptoloji Serüveni	**Sınıf**	:	9-10
Ders	:	Matematik	**Konu**	:	Kriptoloji
Süre	:	10 ders saati (400 dakika)			

Kazanımlar :

1. Matematiğin şifrelemedeki rolünü açıklar.

a) Şifrelemenin dil, veri, bilişim vb. alanlardaki örneklerine yer verilir.

b) Şifrelemenin tarihsel gelişim süreci içinde matematiksel kavramların nasıl kullanıldığına yönelik çalışmalara yer verilir.

2. Şifrelemede kullanılan teknikleri açıklar.

a) Sezar, doğrusal şifreleme gibi tekniklere yönelik çalışmalara yer verilir..

Araç-Gereçler : Kağıt, kalem, bilgisayar, internet.

Uygulayıcı İçin Ön Hazırlık : Öğretmen aşağıdaki kare kodlarda verilen çalışmaları okuyarak etkinliğe hazırlık yapar.

Etkinliğe başlamadan önce ***Etkinlik Formu 1-2-3-4***'ün öğrenci sayısı kadar çıktısını alır.

ÖĞRENME ÖĞRETME SÜRECİ

I) GİRİŞ

5 dakika

Görsel 1: Enigma

Öğretmen **Görsel 1**'i gösterir ve ***"Görseldeki makine hangi amaçla kullanılmış olabilir?"*** sorusunu sorar ardından öğrencilerin yorumlarını alır.

ÖĞRENME ÖĞRETME SÜRECİ

II) SORU SORMA

10 dakika

Öğretmen öğrencilerin tahminlerini aldıktan sonra **Görsel 1'**de verilen makine görselinin mesajları şifrelemek amacıyla kullanılan tarihi bir makine olduğunu ifade eder ardından şu soruları sorar:

1) ***Şifrelemeye neden ihtiyaç duyulmuş olabilir?***
2) ***Şifreleme geçmişten günümüze hangi alanlarda kullanılmıştır?***
3) ***Görsel 1'deki şifreleme makinesi hangi tarihlerde kullanılmış olabilir?***

III) DERİNLEŞME

25+40+40+40+80 dakika

Öğretmen soruların yanıtlarını öğrencilerden aldıktan sonra şifreleme bilimi ve şifreleme yöntemleriyle ilgili çalışmalara yer verir. Bu amaçla şu bilgileri öğrencilerle paylaşır:

"'Kriptoloji, şifreleme bilimi olarak tanımlanmaktadır. Kriptografi, adını antik Yunancada "gizli" anlamına gelen kryptos ve "yazı" anlamına gelen graphein kelimelerinin birleşiminden almaktadır. Kriptoloji, gönderilen iletilerin güvenliğini sağlamak için gönderici ve alıcı arasına üçüncü kişilerin girmesini engellemeyi amaçlayan matematiksel yöntem ve yaklaşımlara dayalı bir disiplindir.

Günümüzde olduğu kadar tarihsel süreçte de iletilerin ve bilgilerin korunması ve güvenliğinin sağlanması her zaman önemli bir konu olmuştur. Bu nedenle kriptoloji biliminin ortaya çıkışının çok eski zamanlara dayandığı söylenebilir. Kriptoloji ile ilişkili ilk çalışmalara, MÖ 1900'lü yıllarda Mısır hiyerogliflerinde rastlanmıştır. Efendisinin hayatını gizli simgeler kullanarak anlatan söz konusu kişi, tarihin ilk kriptologlarından biri olarak sayılabilir. Spartalılar MÖ 500'lü yıllarda yer değiştirme yöntemine dayanan ilk şifreleme aracını geliştirerek askeri amaçlı haberleşmede kriptolojiyi kullanan ilk şehir devleti olmuştur. Scytale adı verilen şifreleme aracında belirli bir kalınlıktaki tahta silindirin yan yüzeyine bir papirüs ya da ince bir deri eğik biçimde sarılıyor ve gizli mesaj bu şeritin üstüne yazılıyordu. Sonrasında ise şerit silindirden sökülüyor ve alıcıya gönderiliyordu. Gizli mesajın yazılı olduğu papirüs, alıcı tarafından aynı kalınlıkta bir silindire sarılmazsa ileti anlaşılmaz oluyordu. Kriptolojiyi askeri amaçlı kullananlardan biri de Büyük Roma İmparatoru Julius Caesar'dır (Jul Sezar). Julius Caesar'ın komutanlarıyla haberleşmek için kullandığı ve kendi adıyla anılan yerine koyma yönteminde ise alfabedeki her harf kendisinden sonra gelen üçüncü harf (sayı değiştirilebilir) ile yer değiştirmektedir. Örneğin Sezar şifreleme yöntemine göre kendi alfabemizdeki harfleri kullanarak "MATEMATİK" sözcüğünü "ÖÇVĞÖÇVLN" sözcüğü olarak şifreleyebiliriz."

ETKİNLİK 1

40 dakika

Öğretmen **Etkinlik Formu 1**'i dağıtır ve açıklamayı öğrenciler ile paylaştıktan sonra öğrencilere formda yer alan şu soruları sorar:

ÖĞRETMENE NOT

Sezar yöntemi gibi alfabedeki harflerin yer değiştirmesine dayandırılan şifreleme yöntemlerinde şifrelemede kullanılan dilin özellikleri dikkate alınarak şifreli metinlerin çözümü yapılabilmektedir. Sıklık analizi olarak adlandırılan bu yöntem, El Kındî tarafından geliştirilmiştir. Örneğin Türkçe'deki harflerin kullanım sıklıkları Tablo 1'de verilmiştir. Alfabedeki harflerin kullanım sıklıkları, yer değiştirmeye dayalı şifreleme yöntemlerinde önemli bir ipucudur. Buna göre şifreli metinde geçen harflerin sıklıkları, Tablo 1'deki sıklıklarla karşılaştırılarak harflerin olası karşılıkları belirlenebilir.

El Kındî ile ilgili daha detaylı bilgiye bu karekoddan ulaşabilirsiniz.

Tablo 1. Türkçe'deki Harflerin Kullanım Sıklıkları

Harf	Sıklık	Harf	Sıklık	Harf	Sıklık	Harf	Sıklık
A	%11,92	Ğ	%1,125	N	%4,487	U	%3,235
B	%2,844	H	%1,212	O	%2,476	Ü	%1,854
C	%0,963	I	%5,114	Ö	%0,777	V	%0,959
Ç	%1,156	İ	%8,6	P	%0,886	Y	%3,336
D	%4,706	J	%0,034	R	%6,722	Z	%1,5
E	%8,912	K	%4,683	S	%3,014		
F	%0,461	L	%5,922	Ş	%1,78		
G	%1,253	M	%3,752	T	%3,014		

Tablo 1' deki Türkçe harflerin kullanım sıklıklarını dikkate alarak aşağıdaki soruları yanıtlayınız.

1. Aşağıda verilen şifrelenmiş metinleri çözünüz. Şifreli metin oluşturma yönteminde harflerin hangi kurala göre değiştirildiğini açıklayınız.

Şifreli Metin		Türkçe Karşılığı	
ĞIĞ VAONG ĞIĞ	BMOR		
ĞIĞ VAONG ŞA	VİRG		
ŞA VAONG BMOR	LKĞIĞ		
ĞIĞ VAONG VİRG	LKĞIĞ		

ÖĞRETMENE NOT

Yukarıdaki tablonun Türkçe karşılığı aşağıda verilmiştir.

Şifreli Metin		Türkçe Karşılığı	
ĞIĞ VAONG ĞIĞ	BMOR	İKİ ÇARPI İKİ	DÖRT
ĞIĞ VAONG ŞA	VİRG	İKİ ÇARPI ÜÇ	ALTI
ŞA VAONG BMOR	LKĞIĞ	ÜÇ ÇARPI DÖRT	ON İKİ
ĞIĞ VAONG VİRG	LKĞIĞ	İKİ ÇARPI ALTI	ON İKİ

2. *"FNÜ SŞÖZEHES VŞSVAD HŞKÜA JIĞIÜ." olarak şifrelenen metni çözümleyiniz. Şifreli metin oluşturma yönteminde harflerin hangi kurala göre değiştirildiğini açıklayınız.*

ETKİNLİK 2

40 dakika

Öğretmen Sezar şifreleme yönteminin, bir doğrusal şifreleme yöntemi olduğunu belirtir ardından öğrencileri üçerli gruplara ayırarak **Etkinlik Formu 2'**yi öğrencilere dağıtır. Aşağıdaki açıklamayı öğrenciler ile paylaştıktan sonra öğrencilere formda yer alan şu soruları sorar:

ÖĞRETMENE NOT

Doğrusal Şifreleme Yöntemi: Cebirsel ifadeler ile Sezar şifrelemenin birlikte kullanıldığı bir yöntemdir. Bu yöntemde bir cebirsel ifadeye dayalı olarak şifreleme yapılır. Harfler sırasıyla 0'dan 28'a kadar numaralandırılır. Harflerin alfabedeki sıra numaraları cebirsel ifadedeki değişkenin yerine yazılarak elde edilen değere karşılık gelen sıradaki harf ile şifrelenir.

1. *3x - 2 cebirsel ifadesini kullanarak bir doğrusal şifreleme yapılacaktır. Buna göre;*

   a) x değişkeni ne ifade etmektedir?
   b) 3 sayısı neyi ifade etmektedir?
   c) -2 değeri neyi ifade etmektedir?

ÖĞRETMENE NOT

3x - 2 ifadesindeki;

a) x değişkeni harfin alfabedeki sıra numarasını ifade etmektedir (Örneğin A = 0, B = 1, C = 2 gibi).

b) Değişkenin katsayısı

c) Öteleme için sabit değer

2. *4x + 5 cebirsel ifadesini kullanarak doğrusal şifreleme yöntemini kullanarak aşağıdaki soruları cevaplayınız.*

   a) *a,b,c harflerini şifreleyiniz.*

ÖĞRETMENE NOT

'a' harfi alfabenin birinci harfi olduğundan 'a' harfini 0 ile eşleştirildiğine 4x + 5 cebirsel ifadesinde x yerine 0 yazılır;

4x + 5 ifadesinde x = 0 için

4.0 + 5=5 değeri bulunur.

Alfabedeki beşinci harf 'd' harfidir. 'a' harfi şifreli metinde 'd' harfine karşılık gelir.

b) *Alfabemiz 29 harften oluştuğuna göre 49 sayısının karşılığını bulmak için nasıl bir yöntem izlemek gerekir*?

ÖĞRETMENE NOT

49 - 5 = 44

44 : 4 = 11

49 sayısı alfabemizdeki 11. harf olan "ı" ya karşılık gelir.

Görsel 2: Sürdürülebilir Kalkınma Amaçları

3. *Görsel 2'de verilen Sürdürülebilir Kalkınma Amaçlarına yönelik yapılan ulusal ve uluslararası projeler ile ilgili araştırma yapınız.*

ÖĞRETMENE NOT

Öğretmen sıfır atık projesi ile ilgili öğrencilere bilgi verir. Benzer ulusal ve uluslararası projeleri incelemelerini sağlar.

Sıfır atık ile ilgili daha detaylı bilgilere bu karekoddan ulaşabilirsiniz.

4. *Grup arkadaşlarınız ile Görsel 2'de verilen Sürdürülebilir Kalkınma Amaçlarından birine yönelik en az on kelimeden oluşan bir slogan hazırlayınız.*
   a) Sloganlarınızı doğrusal şifreleme yöntemi ile şifreleyiniz.
   b) Sloganlarınızı şifrelerken kullandığınız doğrusal yöntemin cebirsel ifade karşılığını yazınız.
   c) Diğer gruplardan biriyle şifrelenmiş sloganlarınızı paylaşınız. Şifrelenmiş sloganları çözünüz ve çözdüğünüz metnin doğruluğunu aldığınız grup ile karşılaştırınız.

ÖĞRETMENE NOT

Grup öğrencileri farklı grupların oluşturduğu şifreli mesajları çözerler.

ETKİNLİK 3

40 dakika

Öğretmen öğrencileri üçerli gruplara ayırdıktan sonra tüm öğrencilere **Etkinlik Formu 3**'ü dağıtır ve formda yer alan soruları sorar:

Bir şifreleme sisteminde 15 adet sembol kullanılmaktadır. Sembollerin 10 tanesi rakamlarla (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), geri kalan 5 tanesi harflerle (Ü, Ç, G, E, N) temsil edilmektedir. 0'dan 9'a kadar olan sayılar aynen kullanılıyor. 10,11,12,13,14 sayıları ise birer harf sembolü ile ifade edilmektedir.

0 1 2 3 4 5 6 7 8 9 ÜÇGEN
Ü = 10, Ç = 11, G = 12, E = 13, N= 14 gösterir.

A	B	C	Ç	D	E	F	G	Ğ	H
0	1	2	3	4	5	6	7	8	9
I	İ	J	K	L	M	N	O	Ö	P
10	11	12	13	14	15	16	17	18	19
R	S	Ş	T	U	Ü	V	Y	Z	
20	21	22	23	24	25	26	27	28	

Alfabemizdeki harfler 0'dan başlayarak numaralandırılmıştır. Alfabemizdeki harfleri kodlayabilmek için rakam veya sembollerden üç tanesi yan yana yazılır. Rakamlar ile sembollere karşılık gelen sayı değerlerinin toplamı alfabemizdeki harflere karşılık gelen numaraları vermektedir. Toplam 28'i geçtiğinde toplamın 29 ile bölümünden kalana bakılır. Bu kodlama sistemine göre harflerin birden fazla kodlaması yapılabilir. Aşağıdaki tabloda alfabemizin 24. harfi olan U için birkaç örnek kodlama verilmiştir:

U			
9	OLUŞAN KOD 9N1	Ü = 10	OLUŞAN KOD ÜG2
N = 14		G = 12	
1		2	
9 + 14 + 1 = 24		10 + 12 + 2 = 24	

1. *Bu sisteme göre "EN3G60Ü22ÜE2G31ÜÇEEN3NEEG20E21NE7" kodu ile verilen kelimeyi bulunuz.*

ÖĞRETMENE NOT

Birinci sorunun cevabı BÖLÜNEBİLME'dir.

2. *"ÇABA" kelimesi için 3 farklı şifrelenmiş kelime yazınız.*

ÖĞRETMENE NOT

İkinci sorunun cevabı

"NN4Ü81NN29Ç9

EG7Ç99NÜ61Ü8

Ü9EG89EG5NÜ5" gibi olabilir.

3. *Bu kodlama sistemine göre <u>en fazla</u> kod hangi harf için oluşur?*

ÖĞRETMENE NOT

Üçüncü sorunun cevabı Z harfidir.

4. *Grup arkadaşlarınız ile bu sistemdeki yöntemi değiştirerek farklı bir şifreleme sistemi oluşturunuz. Oluşturduğunuz şifreleme sistemi ile en az dört kelimeden oluşan bir metni şifreleyiniz. Şifreli metninizi farklı gruplar ile paylaşarak diğer grupların geliştirdiği sistemin nasıl işlediğini bulunuz.*

ETKİNLİK 4

80 dakika

Öğretmen yer değiştirme yöntemi ile yapılan şifrelemelerin şifreli metindeki harflerin sıklıklarındaki farklılıklardan dolayı şifre kırıcılara (kriptoanalistler) ipuçları sağladığını ifade eder. Bu nedenle kriptologların zaman içerisinde daha güvenli bir şifreleme yöntemi geliştirmek için çalışmalar yaptığını söyleyerek Enigma ile ilgili şu açıklamayı yapar:

> *"Kriptoloji bilimi açısından önemli sayılabilecek dönüm noktalarından biri de 1920'li yıllarda siyasi ve ticari amaçlı haberleşmede kullanılması için geliştirilen ve İkinci Dünya Savaşı sırasında Almanlar tarafından askeri amaçlı haberleşme aracı olarak kullanılan Enigma şifreleme makinesi olmuştur. Alman orduları arasında hassas askeri bilgileri içeren metinler, enigma makinesi ile şifreledikten sonra radyo dalgaları üzerinden Mors kodları kullanılarak gönderilmiştir. Radyo dalgaları sayesinde şifreli metinlerin uzak mesafeler arasında iletimi kolaylaşmış olsa da bu durum İngiliz kuvvetleri tarafından dinlenerek şifrelerin çözülmesine yönelik çalışma fırsatı sağlamıştır.. Enigma şifreleme makinesinde her 24 saatte bir değişen bir şifreleme anahtarı kullanılmıştır. Enigma kodu da adı verilen bu anahtarı kısa bir zaman dilimi içerisinde bulmak matematiksel açıdan neredeyse imkansızdır. İngiliz matematikçi Alan Turing ve çalışma arkadaşları, Enigma makinesindeki bir şifreleme zayıflığından/kusurundan yola çıkarak oluşturdukları bir matematiksel model ile Bombe adını verdikleri elektromekanik bir cihaz geliştirmişlerdir. Bombe sayesinde Alman ordularının birbirlerine gönderdikleri mesajların Enigma kodları kırılabilmiştir. Enigma kodlarının kırılması ile İkinci Dünya Savaşı'nın seyri değişmiştir."*

Öğretmen Enigma şifreleme makinesi ile ilgili açıklama yaptıktan sonra Etkinlik Formu 4'ü dağıtır ve öğrencilere formda yer alan soruları sorar:

Enigmadan esinlenerek bir şifreleme makinesi geliştiren Selim'in makinesi, klavye, santral, çarklar ve ampul tablosu adı verilen dört temel parçadan oluşmaktadır.

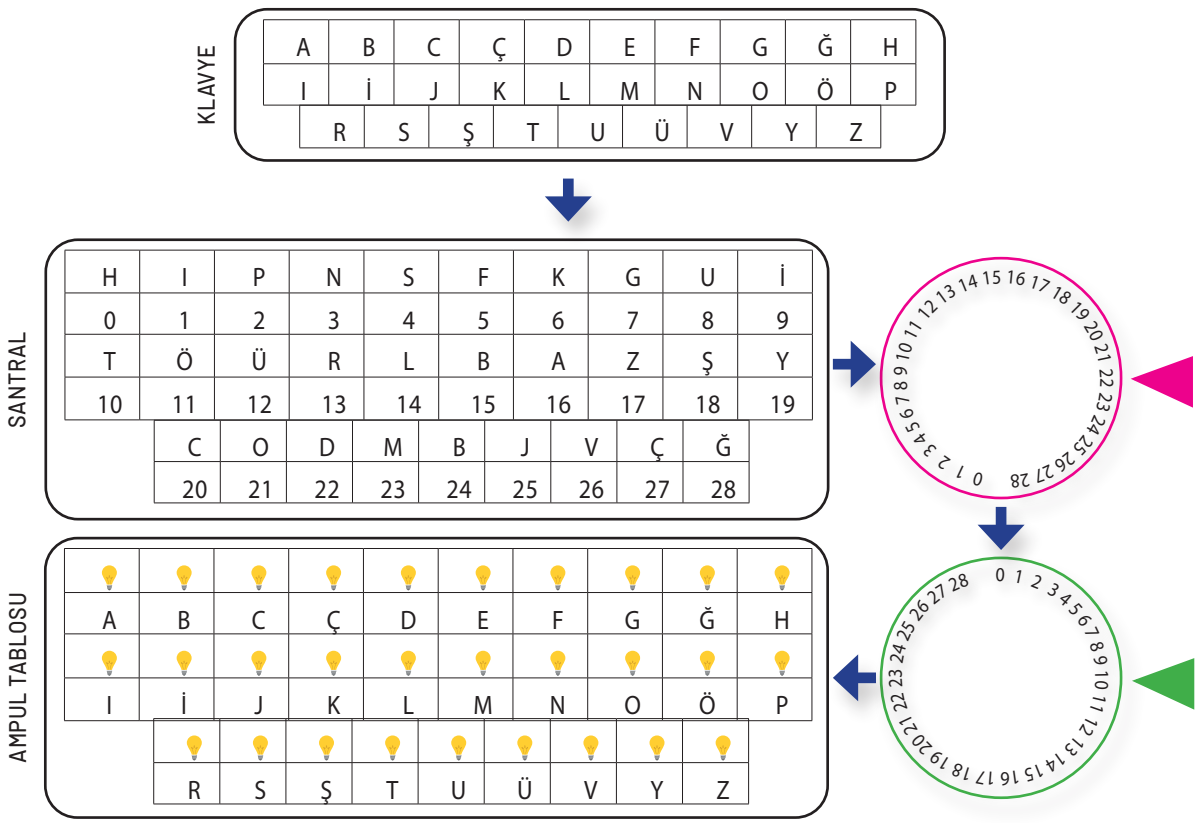
Bu parçaların işleyişi şu şekildedir:

- *Klavye, şifrelenecek mesajları yazma amacı ile kullanılmaktadır. Klavyede alfabemizdeki 29 harfin yer aldığı tuşlar bulunmaktadır.*
- *Santral adı verilen parçada klavyede bulunan harfler rastgele numaralandırılmış numaraları ile birlikte yer almaktadır. Santralde bulunan tuşlar ile klavyedeki tuşlar kablolar ile birebir eşleştirilerek şifreleme başlamaktadır. Böylelikle klavyede basılan tuşlardaki harfler, santral üzerinde bağlı bulunduğu kablonun diğer ucundaki harfe dönüşmektedir.*

- *Makine iki hareketli çark ile çalışmaktadır.*
- *Hareketli çarklar istenilen bir başlangıç konumu ile makinedeki yerlerine yerleştirilebilmektedir. Birincisi saat yönünde bir birim dönmekte, ikincisi ise saat yönünün tersine bir birim dönmektedir. Çarkların her birinde 0 ve 28 dahil olmak üzere bu aralıktaki tam sayılar bulunmaktadır.*
- *Oluşturulan algoritmaya göre hareketli çarka gelen numara ile çarkın üzerindeki numara toplanmaktadır. Elde edilen toplam 29'dan küçük ise bu sayının karşılığı olan harf (varsa) bir sonraki çarka aktarılmaktadır. Eğer elde edilen toplam 28'den büyük ise bu sayıdan 29 çıkarılmakta ve elde edilen sayının karşılığı olan harf (varsa) bir sonraki çarka aktarılmaktadır. Örneğin santralden 16 numaralı harf 25 sayısını gösteren hareketli çarka aktarılıyor olsun. Bu durumda 16+25=41 sayısı 28'den büyük olduğu için 41-29=12 numaralı harf bir sonraki çarka aktarılır.*
- *Birinci çarktan çıkan sayı belli olduktan sonra ikinci çark çalışmaktadır.*
- *Işık tablosu şifreleme makinesinin (klavyenin her bir harfine karşılık) 29 adet ışıklı harften oluşan parçasıdır. Işık tablosunda, klavyede basılan her bir harfin çarkların dönmesi sonucunda elde edilen şifrelenmiş karşılığı ışık vererek şifreli kelimeler oluşturulmaktadır.*

Şifreli bir mesaj gönderebilmek için ilk olarak santraldeki harflerin nasıl sıralandığı ile hareketli çarkların nasıl konumlandırıldığına ilişkin bilgiler verilmelidir.

Selim'in geliştirdiği makinenin görsel temsili Görsel 3'te verilmiştir.



Görsel 3: Şifreleme Makinesinin Çalışma Sistemi

ÖĞRENME ÖĞRETME SÜRECİ

Örneğin: ***Görsel 3***'te verilen makine sistemi ile S harfinin şifrelemesi şu şekilde yapılmaktadır:

- *Klavyeden S harfine basıldığında santralde yer alan S harfinin karşılık geldiği 4 sayısını sistem Çark 1' e göndermektedir.*
- *Çark 1' e sayı geldiğinde rastgele yerleştirilmiş çark konumuna göre saat yönünde dönerek 21 sayısını göndermektedir.*
- *Çark 1' den sayı gelince Çark 2 çalışmaktadır. Rastgele yerleştirilmiş çark konumuna göre saat yönünün tersine dönerek 11 sayısını göndermektedir.*
- *Sistem sayıları toplayarak (4 + 21 + 11) 36 sayısına ulaşmaktadır. 36 sayısına karşılık gelen bir harf olmadığı için 36 sayısından 29 çıkararak 7 sayısına ulaşmaktadır. Sistem santralde 7 sayısına karşılık gelen harfi yani G harfini ampul tablosunda yakmaktadır.*

Selim'in şifreleme makinesi ile ilgili verilen bilgilerden yararlanarak aşağıdaki soruları yanıtlayınız.

1. ***Şifreleme makinesinin harfleri ve çarkları Görsel 3' te olduğu gibi konumlandırılmıştır. Buna göre "YARDIM" kelimesi harfleri sırası ile şifreli olarak gönderildiğinde hangi harflerin ampullerinin sırası ile yandığını bulunuz.***

ÖĞRETMENE NOT

Öğrenciler sorunun cevabını şu şekildeki bir tablo ile bulabilirler:

Y	19 + 21 + 11 = 51, 51-29=22 → D	D
A	16 + 20 + 12 = 48, 48-29=19 → Y	Y
R	13 + 19 +13 = 45, 45-29=16 → A	A
D	22 + 18 + 14 =54, 54-29=15 → B	B
I	1 + 17 + 15 = 33, 33-29=4→ S	S
M	23 + 16 + 16 = 55, 55-29=26 → V	V

2. ***Şifreleme makinesinin harfleri ve çarkları Görsel 3' te olduğu gibi konumlandırılmıştır. Buna göre ampul tablosunda sırası ile "B, E, Y ,İ, N" harflerinin ampulleri yandığına göre hangi harf dizisinin mesaj olarak gönderildiğini bulunuz.***

ÖĞRETMENE NOT

Öğrenciler sorunun cevabını şu şekildeki bir tablo ile bulabilirler:

B	15+29=44, 44-21-11=12 → Ü	Ü
E	24+29=53, 53-20-12=21 → O	O
Y	19+29=48, 48-19-13=16→ A	A
İ	9+29=37, 37-18-14=6→ K	K
N	3+29=32, 32-17-12=3 → N	N

3. *Şifreleme makinesinin harfleri ve çarkları **Görsel 3**'te olduğu gibi konumlandırılmıştır. Makinenin çarkları sistemsel bir sorundan dolayı arıza yapmış ve saat yönünde dönmesi gereken çark saatin tersi yönünde, saatin tersi yönünde dönmesi gereken çark saat yönünde dönmeye başlamıştır.*

"ACİL" mesajını şifreyle göndermek isteyen bir kişi sırası ile klavyeden tuşlara bastığında arızadan dolayı giden şifreli harf dizisini bulunuz.

ÖĞRETMENE NOT

Öğrenciler sorunun cevabını şu şekildeki bir tablo ile bulabilirler:

A	16 + 23 + 9 = 48, 48-29=19 → Y	Y
C	20 + 24 + 8 = 52, 52-29=23 → M	M
İ	9 + 25 + 7 = 39, 39-29=10 → T	T
L	14 + 26 + 6 = 46, 46-29=17 → Z	Z

IV) PROJELENDİRME

155 dakika

Öğretmen projelendirme aşamasında tasarım odaklı düşünme yaklaşımı çerçevesinde öğrencilerin şifreleme ile ilgili bir proje çalışması ortaya koymalarını sağlar. Bunun için öğrencilere kendi şifreleme sistemlerini oluşturmalarını ve bir prototip ortaya koymaları gerektiğini ifade eder. Bu çalışma için şu uygulama adımları takip edilir:

1 Sorun Belirleme	Mevcut bir soruna yönelik araştırma yapılan bölümdür. Öğrencilerin şifreleme sistemlerine yönelik literatür taraması yapmaları sağlanır. Bu literatür taramasında geçmişten günümüze kadar geliştirilen şifreleme sistemlerinin özellikleri, güçlü ve zayıf yönleri vs incelenir.	**40 dk**
2 Empati	Bu bölüm üç aşamadan oluşmaktadır: • Bir sorunu anlama • Araştırma • İlham alma Araştırma sonuçlarından yola çıkarak öğrencilerin kendi şifreleme sistemleri ile ilgili düşüncelerini/fikirlerini/hayallerini ve bu doğrultuda neler yapabileceklerini belirlemeleri istenir. Kendi şifreleme sistemlerinin kullanıcılarını ve ihtiyaçlarını tanımlamaları, bu doğrultuda sahadan bilgi ve veri toplamaları sağlanır.	

3 *Problem*	Bu aşamada öğrencilerden şifreleme ile ilgili mevcut araştırma bulgularından ve sahadan elde ettikleri verilerden yola çıkarak problem durumunu ifade etmeleri istenir.	
4 *Fikir Üretme*	Bu bölüm üç aşamadan oluşmaktadır: • Hikayeleştirme • Anlamlandırma • Fırsatları belirleme Problem durumuna yönelik farklı çözüm yollarının üretilmesi sağlanır. Örneğin; kendi şifreleme sistemlerinin özellikleri, hangi yönden farklılık ve yenilik getireceği gibi. Bu aşamada çok sayıda çözüm yollarının üretilmesi önemlidir. Çözüm yollarının her biri, güçlü ve zayıf yönleri ile ele alındıktan sonra en iyi ve en uygun çözüm belirlenir.	**40 dk**
5 *Prototip Oluşturma*	Bu bölüm iki aşamadan oluşmaktadır: • Prototip Üretme • Geri Bildirim Alma Öğrenciler kendi şifreleme sistemleri ile ilgili problem durumlarına yönelik en uygun çözümü belirler ve kendi şifreleme sistemlerini ortaya koyan bir prototip geliştirirler. Tasarım odaklı düşünme sürecinde prototip ortaya konan çözümü tanımlayan bir model, akış şeması, eylem planı, algoritma, maket gibi ürünler içerebilir.	**40 dk**
6 *Test Etme*	Bu aşamada oluşturulan prototipin ilgili kullanıcılar tarafından test edilmesi söz konusudur. Öğrenciler kendi şifreleme sistemlerini, hedef kullanıcılar ile test ederler.	**35 dk**
7 *Değerlendirme*	Bu aşamada test sonuçlarına göre prototipin değerlendirmesi, revize edilmesi ve yeniden tanımlanması yapılır. Öğrenciler kendi şifreleme sistemlerinin güçlü ve zayıf yönlerini belirleyerek prototiplerini ve çözüm yaklaşımlarını revize ederler.	

ÖĞRENME ÖĞRETME SÜRECİ

V) ÖZ DEĞERLENDİRME

5 dakika

1. Etkinlikte şifrelemeye dair .....
.....
.....
.....
..... öğrendim.

2. Etkinlikte sezar şifreleme ile ilgili .....
.....
.....
.....
..... öğrendim.

3. Etkinlikte doğrusal şifreleme ile ilgili .....
.....
.....
.....
..... öğrendim.

4. Etkinlikte enigma şifreleme makinesi ile ilgili .....
.....
.....
.....
..... öğrendim.

5. Etkinlik sırasında en zorlandığım kısım .....
.....
.....
.....
.....

6. Etkinlik sırasında en çok ilgimi çeken kısım .....
.....
.....
.....
.....

7. Etkinlik sonrasında şifreleme ile ilgili farklı olarak .....
.....
.....
.....
..... öğrenmek istiyorum.

KAYNAKÇA

Karekod 1: https://services.tubitak.gov.tr/edergi/yazi.pdf;jsessionid=vdg0x9YADSyPLe-4AOHTrE7j?dergiKodu=4&cilt=42&sayi=638&sayfa=28&yaziid=28093

Karekod 2: https://bilimteknik.tubitak.gov.tr/system/files/makale/kripto.pdf

Karekod 3: https://bilimgenc.tubitak.gov.tr/makale/kriptografi-bilginin-anahtari

Karekod 4: https://bilgem.tubitak.gov.tr/sites/images/bilgem/dergi/01_UEKAE.pdf

Karekod 5 https://sifiratik.gov.tr/

Görsel 1: www.shutterstock.com ID:719004559

Görsel 2: http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Yoksulluga-Son.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Saglikli-ve-Kaliteli-Yasam.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Nitelikli-Egitim.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Erisilebilir-Temiz-Enerji.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Sanayi-Yenilikcilik-ve-Altyapi.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Surdurulebilir-Sehirler-ve-Topluluklar.svg

http://www.surdurulebilirkalkinma.gov.tr/wp-content/uploads/2020/03/Iklim-Eylemi.svg

EKLER

ETKİNLİK FORMU 1

80 dakika

Tablo 1. Türkçe'deki Harflerin Kullanım Sıklıkları

Harf	Sıklık	Harf	Sıklık	Harf	Sıklık	Harf	Sıklık
A	%11,92	Ğ	%1,125	N	%4,487	U	%3,235
B	%2,844	H	%1,212	O	%2,476	Ü	%1,854
C	%0,963	I	%5,114	Ö	%0,777	V	%0,959
Ç	%1,156	İ	%8,6	P	%0,886	Y	%3,336
D	%4,706	J	%0,034	R	%6,722	Z	%1,5
E	%8,912	K	%4,683	S	%3,014		
F	%0,461	L	%5,922	Ş	%1,78		
G	%1,253	M	%3,752	T	%3,014		

Tablo 1'deki Türkçe harflerin kullanım sıklıklarını dikkate alarak aşağıdaki soruları yanıtlayınız.

1. *Aşağıda verilen şifrelenmiş metinleri çözünüz. Şifreli metin oluşturma yönteminde harflerin hangi kurala göre değiştirildiğini açıklayınız.*

Şifreli Metin		Türkçe Karşılığı	
ĞIĞ VAONG ĞIĞ	BMOR		
ĞIĞ VAONG ŞA	VİRG		
ŞA VAONG BMOR	LKĞIĞ		
ĞIĞ VAONG VİRG	LKĞIĞ		

2. *"FNÜ SŞÖZEHES VŞSVAD HŞKÜA JIĞIÜ." olarak şifrelenen metni çözümleyiniz. Şifreli metin oluşturma yönteminde harflerin hangi kurala göre değiştirildiğini açıklayınız.*

ETKİNLİK FORMU 2

40 dakika

1. *3x - 2 cebirsel ifadesini kullanarak bir doğrusal şifreleme yapılacaktır. Buna göre;*

   a) **x** değişkeni ne ifade etmektedir?

   b) **3** sayısı neyi ifade etmektedir?

   c) **-2** değeri neyi ifade etmektedir?

2. *4x + 5 cebirsel ifadesini kullanarak doğrusal şifreleme yöntemini kullanarak aşağıdaki soruları cevaplayınız.*

   a) **a,b,c** harflerini şifreleyiniz.

   b) Alfabemiz **29** harften oluştuğuna göre **49** sayısının karşılığını bulmak için nasıl bir yöntem izlemek gerekir?

Görsel: Sürdürülebilir Kalkınma Amaçlarından Bazıları

3. *Görselde yer verilen Sürdürülebilir Kalkınma Amaçlarına yönelik yapılan ulusal ve uluslararası projeler ile ilgili araştırma yapınız.*

4. *Grup arkadaşlarınız ile görselde verilen Sürdürülebilir Kalkınma Amaçlarından birine yönelik en az on kelimeden oluşan bir slogan hazırlayınız.*

   a) Sloganlarınızı şifrelerken kullandığınız doğrusal yöntemin cebirsel ifade karşılığını yazınız.

   b) Diğer gruplardan biri ile şifreli sloganlarınızı birbiriniz ile paylaşınız. Şifreli sloganları çözünüz ve şifreli slogan aldığınız grup ile çözdüğünüz metnin doğruluğunu karşılaştırınız.

ETKİNLİK FORMU 3

40 dakika

Bir şifreleme sisteminde sembollerden 10 tanesi rakamlarla (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), geri kalan 5 tanesi harflerle (Ü, Ç, G, E, N) temsil edilir. Bu sistemdeki sayı sınırı 0-14 arasındadır. 0 'dan 9 'a kadar olan sayılar aynen kullanılıyor. 10,11,12,13,14 sayıları ise birer harf sembolü ile ifade edilir.

0 1 2 3 4 5 6 7 8 9 ÜÇGEN
Ü = 10, Ç = 11, G = 12, E = 13, N= 14 gösterir.

A	B	C	Ç	D	E	F	G	Ğ	H
0	1	2	3	4	5	6	7	8	9
I	İ	J	K	L	M	N	O	Ö	P
10	11	12	13	14	15	16	17	18	19
R	S	Ş	T	U	Ü	V	Y	Z	
20	21	22	23	24	25	26	27	28	

Alfabemizdeki harfler 0'dan başlayarak numaralandırılmıştır. Alfabemizdeki harfleri kodlayabilmek için rakam veya sembollerden üç tanesi yan yana yazılır. Rakamlar ile sembollere karşılık gelen sayı değerlerinin toplamı alfabemizdeki harflere karşılık gelen numaraları vermektedir. Toplam 28'i geçtiğinde toplamın 29 ile bölümünden kalana bakılır. Bu kodlama sistemine göre harflerin birden fazla kodlaması yapılabilir. Aşağıdaki tabloda alfabemizin 24. harfi olan U için birkaç örnek kodlama verilmiştir:

U			
9	OLUŞAN KOD **9N1**	Ü = 10	OLUŞAN KOD **ÜG2**
N = 14		G = 12	
1		2	
9 + 14 + 1 = 24		10 + 12 + 2 = 24	

1. *Bu sisteme göre "EN3G60Ü22ÜE2G31ÜÇEEN3NEEG20E21NE7" kodu ile verilen kelimeyi bulunuz.*

2. *"ÇABA" kelimesi için 3 farklı şifrelenmiş kelime yazınız.*

   1.

   2.

   3.

3. *Bu kodlama sistemine göre en fazla kod hangi harf için oluşur?*

4. *Grup arkadaşlarınız ile bu sistemde üçlü grup sayısını veya karakter sayısını değiştirerek farklı bir şifreleme sistemi oluşturunuz. Oluşturduğunuz şifreleme sistemi ile en az dört kelimeden oluşan bir metni şifreleyiniz. Şifreli metninizi farklı gruplar ile paylaşarak diğer grupların geliştirdiği sistemin nasıl işlediğini bulunuz.*

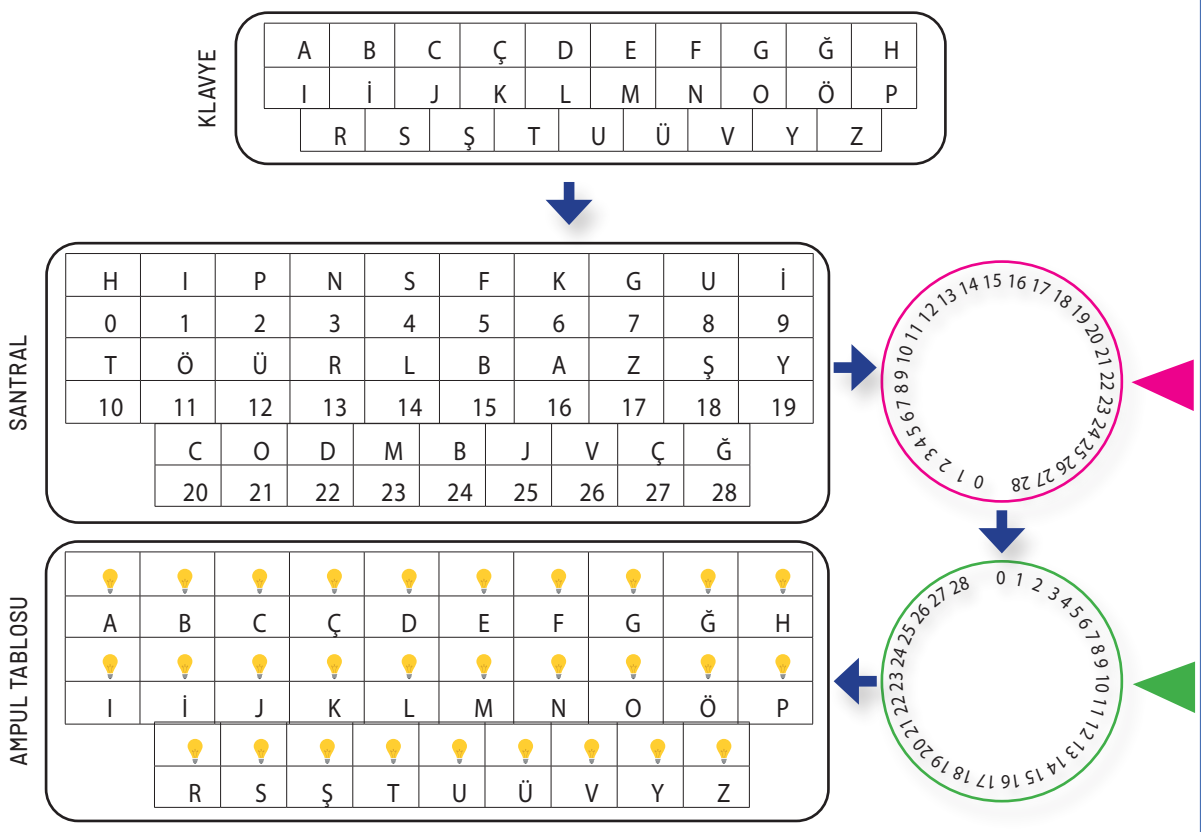
ETKİNLİK FORMU 4

80 dakika

Enigmadan esinlenerek bir şifreleme makinesi geliştiren Selim'in makinesi, klavye, santral, çarklar ve ampul tablosu adı verilen temel parçalardan oluşmaktadır. Bu parçaların işleyişi şu şekildedir:

- *Klavye, şifrelenecek mesajları yazma amacı ile kullanılmaktadır. Klavyede alfabemizdeki 29 harfin yer aldığı tuşlar bulunmaktadır.*
- *Santral adı verilen parçada klavyede bulunan harfler rastgele numaralandırılmış numaraları ile birlikte yer almaktadır. Santralde bulunan tuşlar ile klavyedeki tuşlar kablolar ile birebir eşleştirilerek şifreleme başlamaktadır. Böylelikle klavyede basılan tuşlardaki harfler, santral üzerinde bağlı bulunduğu kablonun diğer ucundaki harfe dönüşmektedir.*
- *Makine iki hareketli çark ile çalışmaktadır.*
- *Hareketli çarklar istenilen bir başlangıç konumu ile makinedeki yerlerine yerleştirilebilmektedir. Birincisi saat yönünde bir birim dönmekte, ikincisi ise saat yönünün tersine bir birim dönmektedir. Çarkların her birinde 0 ve 28 dahil olmak üzere bu aralıktaki tam sayılar bulunmaktadır.*
- *Oluşturulan algoritmaya göre hareketli çarka gelen numara ile çarkın üzerindeki numara toplanmaktadır. Elde edilen toplam 29'dan küçük ise bu sayının karşılığı olan harf (varsa) bir sonraki çarka aktarılmaktadır. Eğer elde edilen toplam 28'den büyük ise bu sayıdan 29 çıkarılmakta ve elde edilen sayının karşılığı olan harf (varsa) bir sonraki çarka aktarılmaktadır. Örneğin santralden 16 numaralı harf 25 sayısını gösteren hareketli çarka aktarılıyor olsun. Bu durumda 16+25=41 sayısı 28'den büyük olduğu için 41-29=12 numaralı harf bir sonraki çarka aktarılır.*
- *Birinci çarktan çıkan sayı belli olduktan sonra ikinci çark çalışmaktadır.*
- *Işık tablosu şifreleme makinesinin (klavyenin her bir harfine karşılık) 29 adet ışıklı harften oluşan parçasıdır. Işık tablosunda, klavyede basılan her bir harfin çarkların dönmesi sonucunda elde edilen şifrelenmiş karşılığı ışık vererek şifreli kelimeler oluşturulmaktadır.*
- *Şifreli bir mesaj gönderebilmek için ilk olarak santraldeki harflerin nasıl sıralandığı ile hareketli çarkların nasıl konumlandırıldığına ilişkin bilgiler verilmelidir.*

Selim'in geliştirdiği makinenin görsel temsili görselde verilmiştir.



Görsel: Şifreleme Makinesinin Çalışma Sistemi

Örneğin: Görselde verilen makine sistemi ile S harfinin şifrelemesi şu şekilde yapılmaktadır:

- *Klavyeden S harfine basıldığında santralde yer alan S harfinin karşılık geldiği 4 sayısını sistem Çark 1' e göndermektedir.*
- *Çark 1' e sayı geldiğinde rastgele yerleştirilmiş çark konumuna göre saat yönünde dönerek 21 sayısını göndermektedir.*
- *Çark 1' den sayı gelince Çark 2 çalışmaktadır. Rastgele yerleştirilmiş çark konumuna göre saat yönünün tersine dönerek 11 sayısını göndermektedir.*
- *Sistem sayıları toplayarak (4 + 21 + 11) 36 sayısına ulaşmaktadır. 36 sayısına karşılık gelen bir harf olmadığı için 36 sayısından 29 çıkararak 7 sayısına ulaşmaktadır. Sistem santralde 7 sayısına karşılık gelen harfi yani G harfini ampul tablosunda yakmaktadır.*

Selim'in şifreleme makinesi ile ilgili verilen bilgilerden yararlanarak aşağıdaki soruları yanıtlayınız.

1. ***Şifreleme makinesinin harfleri ve çarkları görselde olduğu gibi konumlandırılmıştır. Buna göre "YARDIM" kelimesi harfleri sırası ile şifreli olarak gönderildiğinde ampul tablosundaki hangi harflerin ampullerinin sırası ile yandığını bulunuz.***

2. ***Şifreleme makinesinin harfleri ve çarkları görsel'de olduğu gibi konumlandırılmıştır. Buna göre ampul tablosunda sırası ile "B, E, Y ,İ, N" harflerinin ampulleri yandığına göre hangi harf dizisinin mesaj olarak gönderildiğini bulunuz.***

3. ***Şifreleme makinesinin harfleri ve çarkları görselde olduğu gibi konumlandırılmıştır. Makinenin çarkları sistemsel bir sorundan dolayı arıza yapmış ve saat yönünde dönmesi gereken çark saatin tersi yönünde, saatin tersi yönünde dönmesi gereken çark saat yönünde dönmeye başlamıştır. "ACİL" mesajını şifreyle göndermek isteyen bir kişi sırası ile klavyeden tuşlara bastığında arızadan dolayı giden şifreli harf dizisini bulunuz.***