

Yer Deęiřtirme Őifrelemesi Etkinlięinin Uygulanabilirlięinin İncelenmesi ve Öğrencilerin Etkinlikle İlgili Görüşleri

Elif BAHADIR*

Sarıyer İlköğretim Okulu / Sarıyer / Türkiye

Doç. Dr. Ahmet Őükrü ÖZDEMİR

Marmara Üniversitesi, Atatürk Eğitim Fakültesi, Göztepe Kampüsü
Kadıköy / İstanbul / Türkiye

Özet

Bu araştırma, “yer deęiřtirme Őifrelemesi” isimli Őifreleme teknięi ile ilgili bir Őifreleme etkinlięinin 7. sınıf matematik dersindeki permütasyon ve olasılık konusunun iřlenmesi sırasında uygulanabilirlięinin incelenmesi ve bu etkinlikle ilgili öğrencilerin görüşlerinin belirlenmesi amacıyla yapılmıřtır. Bu amaçla, araştırma 7. sınıf 72 öğrenci ile gerçekleştirilmiřtir. Öğrencilere öncelikle çalıřma kâğıtları daęıtılarak etkinlik uygulanmıř, daha sonra etkinlikle ilgili olarak her bir öğrenciden görüşleri yazılı olarak alınmıřtır. Uygulama sona erdikten sonra öğrencilere daęıtılan çalıřma kâğıtlarının incelenmesi ve öğrencilerin uygulama esnasındaki durumları göz önünde bulundurularak etkinlięin uygulanabilirlięi incelenmiřtir. Öğrencilerden

* Sorumlu Yazar. Tel: +90 505 251 14 34 E-posta: elifbahadir42@hotmail.com

alınan görüş formlarının incelenmesi ile de öğrencilerin etkinlikle ilgili görüşleri belirlenmiştir. Araştırma sonucunda, kullanılan etkinliğin ilköğretim 7. sınıf düzeyi için uygun ve kullanılabilir olduğu sonucuna ulaşılmıştır. Öğrencilerin şifreleme etkinliği ile ilgili görüşlerinin olumlu yönde olduğu görülmüştür.

Anahtar Kelimeler: Şifreleme; Etkinlik kullanımı; Matematik eğitimi.

Examining of Applicability of Encryption Activity About Substitution Cipher and Students Views on The Activity

Abstract

The aim of this study is to examine the applicability of the encryption activity about coding system named "substitution chipper" and to determine what the students' views in regard to this activity are. For that purpose this research is carried out with 72 students who are at 7th grade of primary school. Previously by handing out work sheets to the students, the activity is carried out. Then, the views of each student about the coding activity are taken in writren. After the encryption activity is completed, by examining of work sheets which handed out previously to the students and evaluating the positions of the students during the application, the applicability of activity is examined. The views of the students about the activity are determined with the examination of the feedback forms taken from students. At the end of the study, the result is that activity which is used in this study is convenient and usable for 7th grade primary school students. When it is considered that students have positive opinions about ciphering activities and all the students have not experienced such activities until 7th grade, it is thought that creating and using ciphering activities related with some mathematical subjects will be useful.

Keywords: Encryption; Using of activity; Education of mathematics.

Extended Summary

Purpose

The purpose of this study is to analyze the applicability of an activity related with a coding system which is called ‘letter substitution cipher’ with primary 7th grade level students and to specify the contributions of the activity to the permutation and combination subjects as well as to examine students’ views on this activity.

Methods

The study was carried out during the fall semester of 2011-12 academic year. In the study, an activity related to substitution cipher was implemented with 72 students from 7th grade. A qualitative method was used in the study. After the activity, some questions asked to the students about the activity and the answers of these questions were evaluated, then the effect of the activity to the learning of permutation and combination subject was mentioned.

In the first part of the study, the activity which was called as ‘letter substitution cipher’ was implemented to the students within the sample group. This activity was carried out with students during 4 course hours. The students worked in groups or individually with the worksheets which were distributed to each of them during the implementation of the activity. The steps in the activity were carried out respectively with the guidance of the teacher.

Later, students answered the questions about the activity. The qualitative data obtained at the study was composed of the answers of

the questions which were asked to the students at the end of the activity.

The activity used in this study is related to a ciphering activity which is called as ‘transposition and substitution cipher’. First of all, the students were told about the things to do during the implementation before the activity was carried out.

Later, the activity was carried out. First, there were things like Cesar cipher and decipher, examples for transposition cipher, different methods for deciphering transposition and substitution ciphers, (Using Vigenere Table and frequency analysis of the letters), being able to apply transposition cipher in a text which was supported with the clues of all the things learnt within the scope of this activity.

Then, the concept of activity and the approach the activity based on, necessary parts of the activity, the content of each part and behaviors expected from teachers during the implementation of the activity were explained. Furthermore, both the connection of this activity with the daily life was provided and whether this activity was suitable to use in the classroom or not were analyzed.

Results

In order to determine the distribution of students’ opinions, frequency (f) and percentage (%) of the answers of the each 10 question were given in tables and necessary evaluations were made.

In order to find the answers for the sub-problems of this study, worksheets were analyzed and statistical analytical results of the

answers given to the questions directed to the students at the end of the activity were listed.

The analyzed statistical results shows us the fact that the subject is met by the students with a big interest and curiosity.

As a conclusion in the broadest sense, it is also seen that the positive attitude of students towards ciphering activities reflected on the lessons of mathematics.

Discussion

When the findings obtained from the data gathered through students' views were interpreted, it was seen that using ciphering activities in teaching mathematics affected students' attitudes positively, attracted their attention, increased their motivation and their interest to the lesson. The results obtained were coherent with the results of some previous studies' results (Myerscough and others, 1996; Güler, 2007).

In this research, transposition and substitution ciphering activities related with the probability and permutation subjects were used. Analyzing whether positive results obtained in this study is parallel with the results obtained from different grades and different courses or not, will contribute to reveal more specifically the effects of ciphering activities in teaching mathematics and students' attitudes.

Taking into consideration that students have different skills and interests, evaluation scales can be prepared after implementing activities. More comprehensive studies in which activities designed for using

different mathematical subjects, in which the relationship between activities and student achievement to be analyzed and in which teachers' views to be taken should be conducted in our country.

The fact that there is only one post graduate thesis (Güler, 2007) about using ciphering activities in the lessons of mathematics in our country shows the need to carry out different studies related with this subject.

It should be paid attention to prepare activities and teaching designs which are suitable to the individual characteristics of students and which improve high order thinking skills for students to learn mathematics more fruitfully and attractively.

In order to implement activities more effectively and fruitfully, methods which are designed according to the contemporary approaches comprising a higher level of interaction should be developed.

In preparation of the activities, experts from all fields should be in the design team, because, activities which are designed without sufficient number of experts will decrease the effect of teaching.

Educational faculties by cooperating with the Ministry of Education can provide research and development support for preparing software that can be used in computer based teaching applications.

Conclusion

When it is considered that students have positive opinions about

ciphering activities and all the students have not experienced such activities until 7th grade, it is thought that creating and using ciphering activities related with some mathematical subjects will be useful. When the results such as activities performed during the study consolidate students' ability to reach concepts related with the subject and their existing knowledge are considered, it is seen that these activities can be used in various stages of a lesson such as getting attention, while lesson and evaluation. Besides, choosing texts related with the ciphering activities in accordance with Social Sciences and Turkish lessons, for example like teacher creates codes from a reading text that students used in their Turkish lessons... it is seen that it connects mathematics with other disciplines in students' minds. It is thought that by using ciphering activities in course books with related subjects, students' motivation will increase and by this way effective and permanent learning can be provided.

Giriş

Geleceğin dünyasında bireylerin etkili bir öğrenme için ihtiyaç duydukları en önemli becerilerin başında, eleştirel düşünme, sistemli düşünme, problem çözebilme, yaşamın yeni ve farklı koşullarına uyum sağlayabilme gelmektedir. Bunu sağlayabilmek için de etkili bir öğretim yönteminin bulunması gerekmektedir.

Günümüzde, ardışık soyutlama ve genellemelerle geliştirilen bağıntılardan oluşan bir sistem olarak kabul edilen matematiğin var olan yapı ve bağıntılarını geliştirmek sezgiyi gerektirir. Sezgi, tümevarımcı düşünme ve şaşırtıcı düşünme süreçlerini kapsar. "Tümeva-

rımcı düşünme, kısaca tek tek ele alınan olaylar arasındaki ilişkilerden genellemelere ulaşma süreci şeklinde tanımlanabilir. Şaşırtıcı düşünme ise herhangi bir konu hakkında, daha önce hiç ortaya atılmamış bir fikri öne çıkarma, farklı fikirlerin ansızın akla gelmesi sürecidir. Dolayısıyla öğretim esnasında, öğretmenlerin görevi, öğrencilere belli başlı kalıplaşmış birtakım kurallar yığını ezberletmek yerine, matematiksel ilke ve genellemeleri kendilerinin keşfetmesine rehberlik etmek olmalıdır.” (Baykul, 2001).

“Etkili öğrenme, öğrencinin öğrenme süreci boyunca, derslere aktif olarak katılması ve bilgiyi öğrenirken öğrenme işleminin içinde yer almasıyla olur. Matematik, zihinsel canlandırmalara ve algılara dayalı olduğu için öyle boş bir kaba su boşaltır gibi doğrudan doğruya anlatım yoluyla pasif durumdaki öğrencinin kafasına aktarılamaz. Öğrencinin aktif olabilmesinin en bilinen yolu; çözüm yolları kolayca bilinen algoritmaları içermeyen veya daha önce aynısı çözülmemiş problemleri çözme aktivitelerine katılmalarıdır.” (Bayraktar, 1998).

Altun (2006)’a göre, çocuklar fiziksel gelişmelerinin gereği olarak, oyun oynamaktan ve sportif etkinliklerden, zihinsel gelişmelerinin gereği olarak da problemler, olaylar ve meseleler üzerinde düşünmekten hoşlanırlar, hoşlandıkları için yaparlar, yaptıkları için de kendilerini geliştiklerinden (Skemp, 1986) dolayı, çocuklar matematiksel bilgiyi kendileri oluşturduklarında ondan büyük zevk alırlar. Ancak doğrudan kendilerine söylenen formül veya bilgidan hoşlanmazlar. Bundan dolayı matematik öğretimi gerçekleştirilirken öğrencinin ilgisini çeken, öğrenme istekliliklerini arttıran, onları sürekli aktif kılan etkinlikler

kullanıldığında öğrencilerin başarıları anlamlı derecede artış göstermektedir (Altun 2006; Tural, 2005; Başer, 2008; Hiçcan, 2008; Şen, 2008).

Bu nedenle, çeşitli öğrenme güçlüklerinin ortadan kaldırılacağı ve öğrencilerin motivasyonlarını artırma konusunda etkili olabileceği düşünülerek bu çalışmada matematik öğretiminde şifreleme etkinlikleri kullanılmıştır. Matematiksel kavramlar, gerçek, somut olarak var olan nesnelere değildir. Algılanmaları ve yapılandırılmalarına daima işaret ve semboller aracılık eder (Bagni, 2006). Dolayısıyla soyut kavramlardan oluşmasından dolayı matematiğin öğrenciler için genellikle zor olduğundan yola çıkarak, matematiği şifreleyerek de matematiğin daha da zor hale geldiği düşünülebilir. Şifreleme etkinlikleri içeren uygulamalar günlük hayattaki kullanımlarına birer örnek teşkil etmektedir. Bu şekilde, matematiğin şifrelenen bir bilgiyi çözmek, öğrenciler tarafından ilgi ile takip edilmekte, bu sayede matematik dersinde daha kalıcı öğrenmeler geliştirilebilmektedir. (Güler, 2007).

İnsanların herkesin bilmesini istemediği konularda haberleşme ihtiyaçlarından doğan şifreleme teknikleri, başlangıçta çeşitli kurnazlıklarla iletinin gizlenmesinden ibaretti. Dolayısıyla ilkel şifreleme tekniklerinde matematiğin kullanılmadığı, ancak daha sonraları daha karmaşık şifreleme yöntemlerine ihtiyaç duyulmasının, matematiksel şifreleme yöntemlerini de beraberinde getirdiği araştırmacılar tarafından söylenmektedir. Şifreleme ile ilgilenen bilim dalı kriptolojidir. Şifre bilim (kriptoloji), şifreleme ve şifre analizlerinden oluşur (Güler,

2007). Schneider (1996)'ya göre, kriptoloji Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir (akt; Yerlikaya, 2006).

İlk ciddi şifre (kripto) analiz çalışmaları Araplar tarafından yapıldı. Araplar şifreleme çalışmalarına edebiyatta ve matematikte çağın ilerisinde oldukları milattan sonra 600'lü yıllarda başladılar. Arapların şifreleme konusunda yazdıkları ilk eser, Abdurrahman el-Halil İbn-i Ahmed tarafından MS 718 yılında kaleme alınan *Kitabü'l-Muamma* adlı kitaptır. Bu kitapta Abdurrahman el-Halil, Bizans imparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümünü verir (Babaoğlu, 2009; akt; Güler, 2007). İlk şifre (kripto) analiz çalışması yapanlardan biri de Ebû-Yûsuf Ya'kûb ibn İshâk el-Kindî'dir. El-Kindî, şifreleme biliminde Sezar tarafından bulunan ve uygulanan tek alfabeli yerine koyma şifreleme yöntemini geliştirerek frekans analizini bulan ilk kişidir (Vikipedi, 2011). Şifre anlamına gelen İngilizce "cipher" ve Fransızca "chiffre" sözcükleri bu dillere Arapçadan (cifr ya da cifir) geçmiştir.

Şifreleme yöntemi ile ilgili olarak günlük hayattan bazı durumlar uygun konulara tatbik edilerek çeşitli şifreleme etkinlikleri geliştirilmiştir.

Bu etkinlikler farklı ders, konu ve düzeylerde uygulanarak öğrenci başarı ve tutumuna etkisi incelenmiştir. Örneğin; öğrencilerde merak uyandırarak şifreyi çözmelerini sağlayacak şifreleme aktiviteleri

uygulayarak bir çalışma yapmışlardır. Myerscough ve arkadaşlarının çalışmaları esnasında öğrencilerin şifreyi çözmeye zorlandıkları anlarda öğretmenlerin verdikleri ipuçlarıyla çocukları yönlendirerek rehber rolü üstlenmişlerdir (akt; Güler, 2007). Çalışma sonucunda araştırmacılar, bazı sınıfların şifreyi çözmeye zorlandıklarını, bazılarının öğretmen ipucu vermeden şifre hakkında yorum yapmadıklarını fakat birçoğunun şifreyi çözmeye inatçı ve başarılı olduklarını tespit etmişlerdir. Güler (2007) yaptığı çalışmada modüler aritmetik konusunun öğretiminde şifreleme etkinliklerinin kullanılmasının öğrenci tutumu ve başarısına etkisini incelemiştir. Araştırmada ön test – son test kontrol gruplu desen kullanılmış ve deney grubu öğrencilerine modüler aritmetik konusunun öğretiminde şifreleme etkinliklerine yer verilirken, kontrol grubu öğrencilerine ise geleneksel öğretim yöntemi kullanılarak dersler işlenmiştir. Araştırma sonucunda deney grubu öğrencilerin akademik başarıları kontrol grubu öğrencilerine göre anlamlı düzeyde yüksek çıkmıştır. Deney grubu öğrencilerinin şifreleme etkinliklerine yönelik tutumlarının ise olumlu olduğu belirlenmiştir.

Şifreleme etkinliklerinin uygulanabilirliğini sınamak amaçlı yaptığımız araştırmanın konusunu içeren öğrenme alanı 7. sınıfta yer alan permütasyon ve olasılık ünitesidir. Permütasyon ve olasılık öğrenme alanında öğrencinin yaşantısında en çok ihtiyaç duyacağı ve karşılaştığı kavramlar ele alınmıştır. Permütasyon ve olasılık konusu içerisinde olasılık deneylerinin yer alması, günlük yaşamdan daha fazla örnekle zenginleştirilebilecek bir konu olması bakımından ve konu içerisinde şifreleme etkinliğinde de yer alan faktöriyel kavramını

içermesinden dolayı uyguladığımız şifreleme etkinliğinde seçilebilecek bir konudur.

Matematiksel düşünme becerisinin farklı disiplinleri matematik konuları ile ilişkilendirmeleri sonucunda gelişebileceği düşüncesinden hareketle, araştırmamızda şifreleme etkinliklerinde kullandığımız şifrelerin ve metin örneklerinin 7. sınıf sosyal bilgiler ve Türkçe kitaplarından alınmasına dikkat edilmiştir. Bu sayede öğrencilerde permütasyon ve olasılık ile ilgili kavramların geliştirilmesinin yanı sıra öğrencilerin tahmin becerilerinin de geliştirilmesine ve farklı disiplinlerle matematik dersinin ilişkilendirilerek öğrenciler için daha etkili bir öğrenme alanı oluşturulmaya gayret edilmiştir.

“Mathematics Enchancement Programme” programının önerdiği “harf değiştirme şifrelemesi” etkinlikleri ve araştırmacı tarafından oluşturulan etkinlik örnekleri kullanılmıştır. Uygulanan etkinliklerin 7. sınıf düzeyindeki uygulanabilirliğinin incelenmesi ve bu etkinlikle ilgili öğrenci görüşlerinin belirlenmesi amaçlanmıştır.

Araştırmanın evrenini İstanbul ili Sarıyer ilçesinde bulunan ilköğretim devlet okullarında öğrenim gören 7. sınıf öğrencileri oluşturmaktadır. Örneklemine ise aynı ilçedeki bir ilköğretim devlet okullarındaki 72 adet 7. sınıf öğrencisi oluşturmaktadır. 10 tane 7. sınıfın bulunduğu okulda başarı durumu daha yüksek olan B ve C şubelerinden 36’şar adet öğrenci seçilmiştir. Çalışmaya katılacak öğrencilerin seçiminde amaçlı örnekleme yöntemlerinden birisi olan maksimum çeşitlilik örnekleme yöntemi kullanılmıştır. Bu örneklemedeki amaç, görelilik olarak

küçük bir örneklem oluşturmak ve bu örnekleme çalışılan probleme taraf olabilecek bireylerin çeşitliliğini maksimum derecede yansıtmaktır (Yıldırım ve Şimşek, 2005).

Alt Problemler

- Öğrenciler verilen şifreleri çözerken harflerin kaç farklı miktarda ötelenebileceğini bulabilmekte midir?
- Öğrenciler verilen bir şifrenin deşifresini yaparken harf ötelmesi konusunda Vigenere karesini kullanabilmekte midir?
- Öğrenciler verilen bir metinden yola çıkarak Türkçede en sık kullanılan harflerin analizini yapabilmekte midir?
- Öğrenciler Türkçede mümkün olan kaç tane yer değiştirme şifrelemesinin olduğunu faktöriyel olarak bulabilmekte midir?
- Öğrenciler seçilen bir paragrafın şifresi verildiğinde deşifresinin bulunması için harflerin kullanım sıklığından faydalanabilmekte midir?

Yöntem

Araştırma 2011-2012 eğitim öğretim yılının güz döneminde yürütülmüştür. Araştırmada nitel yöntem kullanılmıştır. Nitel araştırma, nitel veri toplama yöntemlerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırmalardır (Yıldırım ve Şimşek, 2006). Bu araştırmada nitel araştırma tekniklerinden olan durum çalışmasıdır. Durum, bir program, bir olay, bir aktivite veya zaman ve yerle sınırlı bir grup birey olabilmektedir (McMillan ve Schumacher,

2001). Araştırmada gözlemlerle veri toplama tekniklerinden video kaydı ile yazılı kaynaklardan yararlanılmıştır. Veri toplama araçları ve toplanan verilerin analiz ve yorumlanmasında benimsenen sürekli karşılaştırma yöntemi kullanılmıştır. Etkinlik sonrasında öğrencilere etkinlik ile ilgili sorular sorularak, bu sorulara verilen yanıtların değerlendirilmesi yapılmıştır.

Araştırmada gözlemlerle veri toplama tekniklerinden video kaydı ve yazılı kaynaklardan yararlanılmıştır. Şifreleme etkinlikleriyle faktöriyel ve permütasyon konusunu öğretme sürecini incelemek amacıyla video kayıtları tutulmuştur. Araştırma sürecinde öğrenci etkinliklerinden oluşan yazılı dokümanlar ve etkinlikle ilgili öğrencilere dağıtılan soruların cevaplarının bulunduğu dokümanlar çalışma sonunda öğrencilerden alınmıştır. Bu yazılı dokümanlar ders işleme süreci ve öğrencilerin düşünceleri hakkında genel bir fikir vermeleri amacıyla kullanılmıştır.

Etkinlikler üç başlıkta toplanmıştır. Etkinliklerde kullanılmak üzere şifreli harf çizelgeleri, Vigenere karesi, frekans çizelgeleri gibi materyallerden oluşan çalışma kâğıtları araştırmacılar tarafından hazırlanmış ve uygulama sürecinde öğrencilere dağıtılmıştır. Vigenere karesi tüm harf ötelemelerinin yer aldığı bir çizelgedir (Singh, 1999). Çalışma kâğıtlarından alıntılar bulgular bölümünde açıklanarak verilmektedir. Araştırmada uygulanan etkinliklere yönelik kazanımlar ve açıklamalar aşağıda ayrıntılı olarak verilmiştir.

Şifrelemeyle tanışalım

Kazanımlar

- Şifreleme kavramını açıklar.
- Şifrelemenin önemini ve günlük hayatta kullanımını belirler.
- Sezar (Caesar) şifrelemesiyle şifreleme ve deşifre yapar.

Uygulama

- Şifreleme kavramının ortaya çıkışı, önemi ve günlük hayatta kullanımı tartışılır.
- Sezar şifrelemesi anlatılır.
- Türk alfabesi Sezar şifrelemesine göre düzenlenir.
- Metinler Sezar şifrelemesi kullanılarak şifrelenir ve deşifre edilir.

Şifreleme ve deşifre yapalım

Kazanımlar

- Yerine koyma şifrelemesini açıklar.
- Farklı anahtarlarda şifreleme ve deşifre yapar.
- Deşifre stratejilerini tartışır.

Uygulama

- Harflerin kaç farklı miktarda ötelenebileceği tartışılır.
- Harflerin farklı miktarlarda ötelendiği yerine koyma şifrelemesi anlatılır.
- Farklı anahtarlar kullanılarak metinler şifrelenir ve şifreli metinler deşifre edilir.
- Deşifre etmedeki güçlükler ve daha kolay deşifre etme yolları tartışılır.

- Tüm ötelemeler kullanılarak oluşturulan Vigenere karesi deşifre etmek için kullanılır.
- Vigenere karesinin avantajları ve dezavantajları tartışılır.
- Şifreli metinleri deşifre ederken sesli harflerin sessiz harflerle olan ilişkilerinden nasıl faydalanılabileceği üzerine fikir yürütülür.
- Öğretmen tarafından “Türkçe metinlerde harf frekansı” ödevi verilir. Bu ödevde, Türkçe bir metinde en sık kullanılan harflerin sıralandığı bir alfabe oluşturulması istenir.

Harf sıklığı kullanarak şifreleri çözelim

Kazanımlar

- Harf sıklığının nasıl kullanıldığını tartışır.

Uygulama

- Öğrencilerin şifreleme ile ilgili bir oyun tasarımları istenir.
- İkinci etkinliğin devamı olarak, harflerin kullanılma frekanslarına göre Türkçe alfabe düzenlenir ve deşifre amacıyla bu alfabe kullanılır.
- Öğrencilerin şifreleme etkinliği ile ilgili tasarladıkları oyunlar sınıfta sergilenir.

Uygulamalar sürecinde her öğrenciye dağıtılan çalışma kâğıtları ile öğrenciler bireysel veya grup halinde çalışmışlardır. Etkinlikteki adımlar sırasıyla öğretmen rehberliğiyle uygulanmıştır.

Daha sonra ise öğrenciler, yapılan etkinlikle ilgili soruları yanıtlamışlardır.

Etkinlik ve Uygulanması

Araştırmada kullanılan etkinlik, “yer değiştirme şifreleme” şeklinde isimlendirilen bir şifreleme etkinliği ile ilgilidir. İlk olarak öğrencilere uygulama süresince yapılacaklardan bahsedilmiştir. Daha sonra, etkinlik uygulamasına geçilmiştir.

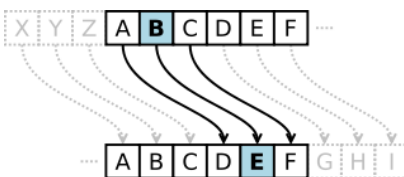
Araştırma kapsamında yer değiştirme şifrelemesinin deşifresi ile ilgili farklı metotlar ve etkinlikler yer almaktadır. Etkinliklerin öğrenciler üzerindeki uygulanabilirliği gözlemlenip, bu sayede kullanılan etkinliklerin ilköğretim 2. kademe öğrencilerine alternatif etkinlik örnekleri olarak sunulmaya uygun olup olmadığına karar verilecektir. Uygulama esnasında ilk olarak öğrencilere uygulama süresince yapılacaklardan bahsedilmiştir. Etkinliklerle ilgili her öğrenciye ayrı çalışma kâğıdı verilmiştir. Böylece, her öğrenciye kendi hızına uygun çalışma imkânı sağlanmaya çalışılmıştır. Bazı etkinlikler düzenlenirken öğrenciler arasındaki etkileşime önem verilerek, öğrencilerin ikişer kişilik gruplar halinde çalışmalarını sağlanmıştır. Öğrencilerin aktif katılımlarının sağlanması için her öğrenci tartışmalara katılma yönünde cesaretlendirilmiş, yorumlar doğru veya yanlış şeklinde öğretmen tarafından değerlendirilmemiş, ortak kararlara varılmıştır. Uygulama esnasında öğrencilerden sahip oldukları tüm bilgilerden faydalanarak etkinliklerde yer alan sorulara yönelik cevaplarını çalışma kâğıtlarına ayrıntılı olarak açıklamaları istenmiştir. Çalışma kâğıdı sonuna “Bu çalışma hakkındaki düşüncelerim” bölümü eklenerek, bu kısma öğrencilerden çalışma sonunda şifreleme, faktöriyel ve permütasyon etkinlikleriyle ilgili görüşlerini yazmaları istenmiştir.

Daha sonra, etkinlik uygulamasına geçilmiştir. Öncelikle etkinlik kapsamında kullanılan Sezar şifrelemesi ve deşifresi, yer değiştirme şifrelemesine örnekler, yer değiştirme ve harf değiştirme şifrelemesinin deşifresi ile ilgili farklı metotlar (Vigenera tablosundan faydalanma ve harflerin sıklık analizi), Vigenera tablosunu kullanabilme, bütün öğrenilenlerin ipuçları ile desteklenmiş bir metinde yer değiştirme şifrelemesini uygulayabilmeleri bulunmaktadır.

Daha sonra ise etkinlik ve etkinlik temelli yaklaşım kavramı, bir etkinlikte bulunması gereken bölümler ve her bölümün içeriği ile etkinlikler uygulanırken öğretmenlerden beklenen davranışların neler olduğuna değinilmiştir. Bu sayede uygulanan etkinliğin hem günlük hayatla bağlantısı kurulmuş, hem de sınıflarda uygulanmaya elverişli bir etkinlik olup olmadığı irdelenmiştir.

Uygulamaya başlarken şifrelemenin tarihçesinden ve ne amaçla nerelerde kullanılabileceğinden, öğrencilerin de fikirleri alınarak bahsedilmiştir. Daha sonra şifreleme türünün özellikleri verilmiştir.

Tarihin ilk kriptolojik fikirleri İngilizcede transposition and substitution cipher adını taşır, yani yer değiştirme ve harf değiştirme şifrelemesi. Bu yöntemlerden ilki bir yazıyı harflerin yerlerini değiştirerek, ikincisi ise harfleri başka harflerle değiştirerek elde edilir. Bu şifrede her harf o harften birkaç sonraki harf kullanılarak yazılır.



Öğrencilere şifrelemeyi daha önce duyup duymadıkları ve duymuşlarsa şifreleme hakkında ne bildikleri sorulmuştur. Öğrencilerden çoğunluğu şifrelemeyi daha önce duymadığını, şifrelemenin sadece bankalarda, bilgisayarlarda gizlilik için kullanıldığını belirtmişlerdir. Bir yer değiştirme şifrelemesi olan Sezar şifreleme ile ilgili olarak buluş yöntemiyle öğretim seçilmiştir ve öğrencilere bazı sorular sorulmuştur:

Neden bu metodun adının Sezar olduğunu biliyor musunuz?

Sizce neden bir şifrelemeye gerek duyulmuş olabilir?

Öğrencilerden gelen cevapların ardından Sezar şifrelemede alfabedeki bir harf kendinden üç harf sonrakiyle yer değiştirmeli olduğu ve bu şifreleme türünde bir haberi şifrelemek için kod harflerinin veya işaretlerinin kullanıldığı, kod harfleri ve işaretlerinin ise açık metindeki harflerin yerine geçtiği bilgisi verilmiştir.

A - Ç

B - ?

C -?

Ç -?

Şifreleme tekniğinde harflerin hangi harfe öteleneceği konusunda daha kullanışlı bir yöntem için harf tablosu kullanmaları öğrencilere tavsiye edilmiştir ve her öğrenciye harf kodları için Şekil 1’de gösterilen harf çizelgesi dağıtılmıştır.

HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
ŞİFRELER																													

Şekil 1. Öğrencilere dağıtılan harf çizelgesi

Bütün alfabenin şifre karşılığı olan tüm kodlarının listesinin yapılmasının daha kullanışlı olduğu öğrencilere söylenmiştir. Örneğin “**ŞİFRELER HAYATIMIZIN İÇİNDE** “ ifadesinin kodlanması aşağıdaki gibidir.

HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
ŞİFRELER	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C

“ŞİFRELER HAYATIMIZIN İÇİNDE”

“ÜLHTĞOĞT JÇBÇVKÖKCP LFLPGĞ”

Şekil 2. Birinci etkinlik için kullanılan şifre ve tablo

Bir sonraki etkinlikte ise bir deşifrenin verilir şifrenin bulunması öğrencilerden istenmiştir.

“PĞÜĞOL DLT BZC IZPĞÜOL DLT JÇAÇ ILDLGLT”

“NEŞELİ BİR YÜZ GÜNEŞLİ BİR HAVA GİBİDİR”

Şekil 3. İkinci aktivite için kullanılan şifre ve deşifresi

Her bir kodun üç harf öncesine gidilerek metin bulunabilir.

Bu etkinliğin ardından öğrencilere Türkçede Sezar şifrelemenin kaç farklı şekilde yapılabileceği sorusu sorulmuştur. Öğrencilerin bu sorunun cevabını bulmaları ve şifreleme harflerinde kullanmaları için Türkçe uygun olarak hazırlanmış Vigenere tablosu dağıtılmıştır.

TÜRK ALFABESİ VİGENERA TABLOSU

A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z
B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A
C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B
Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C
D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç
E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D
F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E
G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F
G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G
H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G
I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H
I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I
J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I
K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J
L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K
M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L
N	O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M
O	O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N
O	P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O
P	R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O
R	S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P
S	Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R
Ş	T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S
T	U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş
U	U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T
U	V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U
V	Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U
Y	Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V
Z	A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y
A	B	C	Ç	D	E	F	G	G	H	I	I	J	K	L	M	N	O	O	P	R	S	Ş	T	U	U	V	Y	Z

Şekil 4. Türkçe Vigenere Tablosu

Tablo öğrencilere fotokopi olarak dağıtılıp incelemeleri istenmiştir. Türkçe Vigenere tablosundan yararlanarak öğrenciler 29 farklı kod olduğunu fark ettiler.

Üçüncü etkinlik olarak öğrencilere bu sefer, harf atlmalı şifrelemeyi harfleri ezberlerinden sayarak değil de, Vigenere tablosundan faydalanmaları istenerek kaç harf atlmalı olduğu söylenmeyen bir şifre verilmiştir ve öğrencilerin bu şifreyi çözmeleri için 25 dakika süre tanınmıştır ancak öğrenciler bu şifrenin ne olduğunu tanınan zaman zaafında bulamamışlardır.

“AKU JK TP FKJP UIP AÖUÖLCĞ VNZKUİPAPU”

“SEN DE Mİ YEDİNCİ SINIFTA ÖĞRENCİSİN”

Şekil 5. Üçüncü etkinlikte kullanılan şifre ve deşifresi

Vigenera tablosu kullanılarak uygulanan şifreleme ve deşifreleme metodunun 29 farklı olasılığının olmasının beraberinde getirdiği dezavantajları öğrenciler de fark etmişler ve daha basit bir yolunun olup olmadığını sorgulamışlardır. Öğrencilerden alınan geri dönütler sonrasında harflerin kullanım sıklığından bahsedilmiştir.

“Türkçede hangi harfler daha sık kullanılır?” sorusu öğrencilere sorulmuş öğrencilerin tahmin yürütmeleri istenmiş.

Türkçede en sık kullanılan ilk beş harfin; **A E I N R** olduğu söylenmiştir.

Verilen bu bilgi doğrultusunda 4. etkinlik olarak öğrencilere aşağıdaki şifre dağıtılmıştır.

“ZÜFBÜLÜ FRCZAVPVF ZÜFAMFÜC ŞRAVCVPVF”

“KIRMIZI RENKLİDİR KIRLARIN GELİNİDİR”

Şekil 6. Dördüncü etkinlikte kullanılan şifre ve deşifresi

Verilen şifrede “En sık kullanılan ‘F’ harfi ‘R’ nin yerine geçmiş olabilir.” diyerek öğrencilere ipucu verilmiştir.

Daha sonraki safhada öğrenciler öğretmenlerinin kendilerine uygulama başında verdiği yaklaşık 100 harflik bir metin ve içerisinde bütün harflerin bulunduğu bir hesap çizelgesi dağıtmıştır. Dağıtılan bu

BİR KÖYLÜ KADIN BİR DANAYI DOĞAR DOĞMAZ KUCAĞINA ALIP SEVMİŞ SONRA DA BUNU ÂDET EDİN-MİŞ HER GÜN DANAYI KUCAĞINA ALIP TAŞIRMİŞ SONUNDA BUNA O KADAR ALIŞMIŞ Kİ DANA BÜYÜYÜP KOSKOCA ÖKÜZ OLDUĞU ZAMAN ONU YİNE KUCAĞINDA TAŞIYABİLMİŞ BU HİKÂYİYİ KİM UYDURDUYSA ALIŞKANLIĞIN NE BÜYÜK BİR GÜÇ OLDUĞUNU ÇOK İYİ ANLAMISŞ OLACAK GERÇEKTEN ALIŞKANLIK PEK YAMAN BİR HOCADIR VE HİÇ ŞAKASI YOKTUR YAVAŞ YAVAŞ SİNSİ SİNSİ İÇİMİZE İLK ADIMINI ATAR BAŞLANGIÇTA KUZU GİBİ SEVİMLİ ALÇAK GÖNÜLLÜDÜR AMA ZAMANLA ORAYA YERLEŞİP KÖKLEŞTİ Mİ ÖYLE AZILI ÖYLE AMANSIZ BİR YÜZ TAKINIR Kİ KENDİSİNE GÖZLERİMİZİ BİLE KALDIRMAYA İZİN VERMEZ.

Şekil 9. Ev ödevi için kullanılan metin

Yapılan etkinlikler ve ev ödevleri sonunda öğrencilere Türkçedeki harflerin kullanım sıklıklarına göre sıralanışı verilmiştir. Ayrıca öğrencilere harflerin kullanım sıklığı ve El-Kindî'nin harf sıklığı analizi ile ilgili bilgiler verilmiştir.

**A, E, İ, N, R, L, İ, D, K, M, U, Y, T, B, S, O, Ü, Ş, Z, G, Ç, H, Ğ, V,
C, Ö, P, F, J**

Şekil 10. Türkçedeki harflerin kullanım sıklıklarına göre sıralanışı

El-Kindî şifreleme ve deşifre ile ilgili bilgilerin bulunduğu el yazması kitabında sıklık analizini kullanarak deşifre yaptığı bilinen ilk kişidir. Arap alfabesinde en yaygın olarak kullanılan 'a' ve 'ı' harfle-

rinin sıklık analiziyle deşifresini yapmıştır.

Son etkinlik olarak öğrencilerden ipuçları ile bir paragrafın deşifresi istenmektedir. Öğrencilere harflerin kullanım sıklığı ile ilgili 6 tane ipucu verilmiştir. Öğrencilerden metni incelemeleri ve şimdiye kadar öğrendikleri deşifre metotlarını paragrafa uygulamaları istenmiştir.

ACA PAE NZÇ CÖŞÖH GERT SAEAE ÖSJZVZ
TE GETDÇA JARÖHTJ NFÇK FÇÖE AĞTC NFÇK
ŞLENÖSÖ LEÇLŞLH SAE AÇT ÖMHKGÖ ÖİNÖ MT
ÖUHACÖ ÖHÖIZEŞÖCA CGĞHL ÇÖHÖC CÖPKÇ
TŞAÇTE AĞTC NFÇKEKE ŞFVK AÇT PÖJZ
ÖHÖIZEŞÖCA TCFEFDAC MT CLÇJLHTÇ ÖÇ-
ZİMTHAİT GETDÇA CÖJCZÇÖHZ FÇDKİJKH

Şekil 11. 7. Etkinlikte öğrencilere verilen şifre metni

**İKİ BİN YIL KADAR ÖNCE ÇİNİN AÇTIĞI EN ÖNEMLİ
TİCARET YOLU OLAN İPEK YOLU DÜNYACA ÜNLÜDÜR
ÇİN İLE AVRUPA ASYA VE AFRİKA ARASINDAKİ KÖPRÜ
OLARAK KABUL EDİLEN İPEK YOLUNUN DOĞU İLE BATI
ARASINDAKİ EKONOMİK VE KÜLTÜREL ALIŞVERİŞE
ÖNEMLİ KATKILARI OLMUŞTUR**

Şekil 12. 7. Etkinlikte öğrencilere verilen şifrenin deşifresi

Uygulamanın son aşamasında ise öğrencilerden şifreleme ile ilgili bir etkinlik veya oyun geliştirmeleri istendi öğrencilerin geliştirdiği bir oyunun sınıf içinde oynanmasıyla uygulama sonlandırıldı.

Bulgular

Verilerin analizinde, öğrencilere dağıtılan çalışma kâğıtları incelenmiştir. Yapılan incelemeler alt problemlere göre gerçekleştirilmiştir. Ayrıca öğrencilerin yapılan uygulamaya ilişkin görüşlerinin dağılımını belirlemek amacıyla, öğrencilere sorulan 10 sorunun her birine verilen yanıtlarla ilgili frekans (f) ve yüzdeleri (%) tablolaştırılarak verilmiş ve gerekli değerlendirmelerde bulunulmuştur.

Bu bölümde araştırmanın alt problemlerine yanıt bulabilmek için çalışma kâğıtlarının incelenmesine ve uygulama sonunda öğrencilere sorulan sorulardan alınan yanıtların yüzdeler olarak sonuçlarına yer verilmiştir. Etkinliğin uygulanması ile ilgili çalışmalarda kullanılan harf-şifre çizelgesinin kullanımı öğrencilere tarif edilmiş ve öğrencilere verilen şifrelerin bu çizelge yardımıyla daha kolay çözülebileceğinden bahsedilmiştir. Şekil 13'te denek öğrencilerden birinin bu çalışma ile ilgili olarak kullandığı çalışma kâğıdı görülmektedir.

HARF- ŞİFRE ÇİZELGESİ

HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
SİFRELER																												

HARF- ŞİFRE ÇİZELGESİ

HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
SİFRELER	3	2	A	B	C	C	E	P	E	f	G	H	I	J	K	L	M	N	O	B	P	S	Ş	T	U	V		

HARF- ŞİFRE ÇİZELGESİ

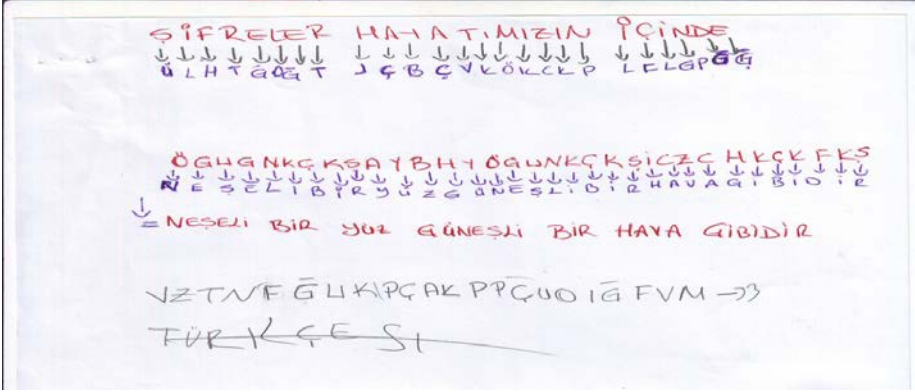
HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
SİFRELER																												

HARF- ŞİFRE ÇİZELGESİ

HARFLER	A	B	C	Ç	D	E	F	G	Ğ	H	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
SİFRELER																												

Şekil 13. Öğrencilerden birinin etkinliklerde kullandığı harf şifre çizelgesi

Daha sonra öğrencilerden şifresi verilen Şekil 14'teki deşifrenin şifresini bulmaları istendiğinde öğrencilerin bu çalışmada başarılı oldukları, sorun yaşamadan istenileni yapabildikleri görülmüştür. Şekil 14'te denek öğrencilerden birinin bu çalışma ile ilgili olarak kullandığı çalışma kâğıdı görülmektedir.



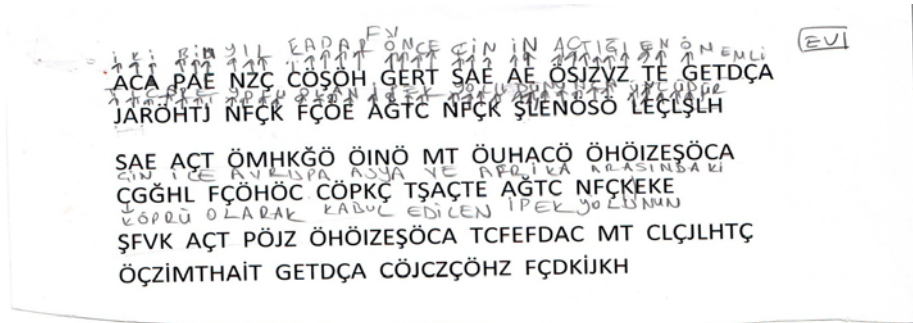
Şekil 14. Öğrencilerden birinin ilk etkinlik için kullandığı çalışma kâğıdı

Bu çalışmadan sonra öğrencilerden, kendilerine yine uygulama başında verilen Şekil 3'teki Vigenere tablosundan yararlanarak öğretmen tarafından belirlenen şifreleri çözmeleri istendiğinde öğrenciler bu çalışmayı da gerçekleştirebilmişlerdir. Ardından harf sıklığı ile şifre çözme etkinliklerine geçildiğinde öğrencilere uygulamaya başlamadan dağıtılan ve ikişerli gruplar halinde kullanmaları tavsiye edilen harf sıklığı çizelgesi ve şifreli metin verilmiştir. Öğrenciler daha önceki uygulamalara göre daha fazla zaman alan bu etkinliği de başarı ile tamamlayabilmişlerdir. Şekil 15 ve Şekil 16'da denek öğrencilerin bu çalışmalar ile ilgili olarak kullandıkları çalışma kâğıtlarından birer örnek görülmektedir.

HESAP ÇİZELGESİ

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	Ü	V	Y	Z					
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
33	12	6	5	15	23		6	7	3	25	38		27	6	15	31	15	6	4	18	13	10	7	17	7	14	16	7
TOPLAM :																												
SIKLIK :																												

Şekil 15 Öğrencilerin harf sıklığını belirlemek için ikişerli grup olarak etkinliklerde kullandıkları harf şifre çizelgesinden biri



Şekil 16. Öğrencilerden birinin 7. etkinlik için kullandığı çalışma kâğıdı

Uygulamanın bir diğer aşamasında (6. etkinlik) ise Şekil 7, Şekil 9, Şekil 9'da verilen alfabeler kullanılarak elde edilebilecek şifre kombinasyonlarının hesaplanması üzerinde durulmuştur. Bu aşamada

öğrencilerden bazılarının hesaplama yapmakta zorlandıkları görülmüştür. Bundan dolayı permütasyon konusu ile ilgili bazı hesaplamaların nasıl yapılması gerektiği hatırlatılmıştır. Bu hatırlatmadan sonra öğrenciler bu hesaplamaların nasıl yapılması gerektiğini anlamışlar ve kendi çalışma kâğıtlarına bu doğrultuda hesaplamalar yapmışlardır.

Uygulamanın son aşamasında ise öğrencilerden şifrelemenin de içinde bulunduğu bir oyun tasarımları istenmiştir. Bu oyunlardan iki tane örnek şu şekildedir:

Birinci oyun; “Öğrenciler sınıf olarak iki gruba ayrılacak, grubun belirlediği bir kişi sınıf dışına çıkacak, diğer gruptan olanlar Türkiye’deki bir ilimizin adını şifreli olarak tahtaya yazacak içeri alınan öğrenci belirlenen sürede şifreyi çözüp haritadan ilin yerini göstermesiyle grubuna puan kazandırmış olacak ve sıra diğer gruba geçecek.”

İkinci oyun; “İlk sıralara birer kişi, sonraki sıralara ikişer kişi oturtalım; birinci kişi bir kelimelik, kuralı anlamlı ve çoğaltılabilecek bir şifre belirlesin sonra arkasındakine versin, o da önceki kelime ile uygun bir şifre hazırlayıp bir sonrakine... Bu şekilde en sondaki kişiler bütün şifreyi çözüp herkese ilan etsin, yanlış kural verenler veya anlamsız kelime ekleyenler oyun dışı kalsın, en sona kalan kazansın.”

Sorulan sorulara verilen yanıtların frekans ve yüzde değerleri ile ilgili tablolar oluşturulmuştur. Öğrenciler bazı sorulara birden fazla yanıt verdikleri için, toplam yanıt sayısı bazı tablolarda öğrenci sayısı olan 72’nin üzerindedir.

Tablo 1’de öğrencilerin ilk soru olan “Bu etkinlik size matematiksel beceri açısından ne kazandırdı?” sorusuna verilen yanıtların dağılımı yer almaktadır.

Tablo 1. “Bu etkinlik size matematiksel beceri açısından ne kazandırdı?” Sorusuna Verilen Yanıtların Dağılımı

	Matematiğin eğlenceli taraflarını fark ettim.		Aslında hayat ve matematik şifrelerle gizlidir. Bizler o şifreleri çözmeliyiz.		Grup olarak çalışmayı öğrendim.		Matematikle diğer sözel derslerin bağlantısını gördüm.		Matematiğin oyunlarla anlatıldığını gördüm.		Faktöriyel ve permütasyon konularını daha iyi anladım.	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinlik size matematiksel beceri açısından ne kazandırdı?	21	29,16	17	23,6	11	15,2	14	19,4	10	13,8	5	6,94

Tablo 1’de de görüldüğü gibi, yapılan etkinliğin öğrencilere ne kazandırdığı ile ilgili soruya; öğrencilerin % 29.16’sı matematiğin eğlenceli taraflarını fark ettim, % 23.6’sı aslında hayat ve matematik şifrelerle gizlidir ve bizler o şifreleri çözmeliyiz. % 15.2’si grup olarak çalışmayı öğrendim, % 19.4’ü matematikle diğer sözel derslerin bağlantısını gördüm., % 13.8’i matematiğin oyunlarla anlatıldığını gördüm ve % 6.94’ü de faktöriyel ve permütasyon konularını daha iyi anladı-

ğın belirtmiştir. Tablo 2’de “Etkinliğin en beğendiğiniz kısmı neresidir?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 2. “Etkinliğin en beğendiğiniz kısmı neresidir?” Sorusuna Verilen Yanıtların Dağılımları

	Şifreleri çözme		Grup halinde yarışarak şifre oluşturma		Tabloyu okuyabilme		Kendime ait çizelge ve tablonun olması		Okuma parçalarından ne çıkacağını merakla beklemek	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Etkinliğin en beğendiğiniz kısmı neresidir?	32	44,44	13	18	9	12,5	5	6,94	12	16,6

Tablo 2’de de görüldüğü gibi, öğrencilere etkinliğin en beğendikleri yönü sorulduğunda, öğrencilerin % 44.44 ‘ü şifreleri çözme, % 18’i, grup halinde yarışarak şifre oluşturma % 12.5’i tabloyu okuyabilme, % 6.94’ü kendime ait çizelge ve tablonun olması, % 16.6’sı ise şekil alfabeleri ile faktöriyel bulma beğendiklerini belirtmiştir. Tablo 3’te “Bu etkinlikte zorlandığınız kısım varsa neresiydi?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 3. “Bu etkinlikte zorlandığınız kısım varsa neresiydi?” Sorusuna Verilen Yanıtların Dağılımları

	Harf sıklığı şifresini çözerken		Vigenera tablosunda harfleri sayarken		Kendim şifre ile ilgili oyun bulurken		Farklı konulardaki şifreleri tahmin ederken	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinlikte zorlandığınız kısım varsa neresiydi?	38	52,7	12	16,66	12	16,66	9	12,5

Tablo 3’te de görüldüğü gibi, öğrencilere etkinlikte zorlandıkları kısım olup olmadığıyla ilgili soruya öğrencilerin % 52.7’si harf sıklığı şifresini çözerken şeklinde yanıt vermişlerdir. % 16.66’sı vigena tablosunda harfleri sayarken, % 16.66’sı kendim şifre ile ilgili oyun bulurken, % 12.5’i ise farklı konulardaki şifreleri tahmin ederken zorlandıklarını belirtmişlerdir. Tablo 4’te “Bu etkinlik matematiğe bakış açınızda değişikliğe sebep oldu mu?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 4. “Bu etkinlik matematiğe bakış açınızda değişikliğe sebep oldu mu?” Sorusuna Verilen Yanıtların Dağılımları

	Evet matematiğe bakış açım olumlu yönde değişti.		Hiçbir değişikliğe sebep olmadı.		Matematiğin oyunlarla anlatıldığını gördüm.		Matematik dersleri şifrelerle daha zevkli geçiyor.	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinlik matematiğe bakış açınızda değişikliğe sebep oldu mu?	47	65,27	5	6,94	12	16,66	7	9,72

Yapılan etkinliğin öğrencilerin matematiğe bakış açılarında bir değişikliğe sebep olup olmadığı ile ilgili soruya öğrencilerin % 65.27’si evet matematiğe bakış açım olumlu yönde değişti şeklinde, % 6.94’ü hiçbir değişikliğe sebep olmadı, % 16.66’sı matematiğin oyunlarla anlatıldığını gördüm,, % 9.72’si matematik dersleri şifrelerle daha zevkli geçiyor şeklinde görüş bildirmişlerdir. Tablo 5’te “Bu etkinliği matematikte hangi konu ile ilişkilendirebilirsiniz?” sorusuna verilen

yanıtların dağılımları yer almaktadır.

Tablo 5. “Bu etkinliği matematikte hangi konu ile ilişkilendirebilirsiniz?” Sorusuna Verilen Yanıtların Dağılımları

	Sayı sayma		Faktöriyel		Permütasyon ve faktöriyel		Tablo ve grafikler	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinliği matematikte hangi konu ile ilişkilendirebilirsiniz?	29	40,27	18	9	15	20,83	13	18

Öğrencilere etkinlikteki şifreleme türünün matematikte hangi konu ile ilişkilendirebilirsiniz diye sorulduğunda, Tablo 5’te de görüldüğü gibi, öğrencilerin % 40,27’si sayı sayma, % 9’u faktöriyel, % 20.83’ü permütasyon ve faktöriyel ve % 18’i tablo ve grafikler şeklinde yanıt vermişlerdir. Tablo 6’da “Bu etkinlikteki barkot türünün hatırladığınız özellikleri nelerdir?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 6. “Bu etkinlikteki şifreleme türünün hatırladığınız özellikleri nelerdir?” Sorusuna Verilen Yanıtların Dağılımları

	Harf atlayarak şifreleme yapılması		Vigenera tablosundan faydalanma		Harflerin kullanım sıklığının önemi		Sezar’ın yaptığı şifreleme		Harf sayısı arttıkça yazılan şifrelerin artması	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinlikteki şifreleme türünün hatırladığınız özellikleri nelerdir?	15	20,8	18	9	13	18	18	9	8	11,1

Öğrencilere etkinlikteki şifreleme türünün hatırladıkları özellikleri sorulduğunda, Tablo 6’da da görüldüğü gibi, öğrencilerin % 20.8’i harf atlayarak şifreleme yapılması, % 9’u Vigenere tablosundan faydalanma, % 18’i harflerin kullanım sıklığının önemi, % 9’u şekillerle yazılan alfabeler bulunduğunu ve % 11.1’i harf sayısı arttıkça yazılan şifrelerin artması şeklinde yanıt vermişlerdir. Tablo 7’de “Bu etkinliğin size faydalı olduğunu düşündüğünüz yönleri nelerdir?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 7. “Bu etkinliğin size faydalı olduğunu düşündüğünüz yönleri nelerdir?” Sorusuna Verilen Yanıtların Dağılımları

	Matematiğe olan ilgilim arttı.		Eğlenceli olduğundan daha iyi anladım.		Akılda kalıcı oldu.		Dersi sevmemi sağladı.		Şifrelerin nasıl yapıldığını öğrendim.	
	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)	(f)	(%)
Bu etkinliğin size faydalı olduğunu düşündüğünüz yönleri nelerdir?	24	33,33	14	19,44	18	9	10	13,88	5	6,94

Öğrencilere bu etkinliğin faydalı olduğunu düşündükleri yönlerinin neler olduğu sorulduğunda, Tablo 7’de de görüldüğü gibi, öğrencilerin % 33.33’ü matematiğe olan ilgilerinin arttığı, % 19.44’ü konuları eğlenceli olduğundan daha iyi anladıklarını, % 9’u akılda kalıcı olduğunu, % 13.88’i dersi sevmemi sağladı ve % 6.94’ü de şifrelerin nasıl yapıldığını öğrendim yönünde görüş bildirmişlerdir. Tablo 8’de “Bu tür bir çalışma daha önce yaptınız mı?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 8. “Bu tür bir çalışma daha önce yaptınız mı?” Sorusuna Verilen Yanıtların Dağılımları

	Evet		Hayır	
	(f)	(%)	(f)	(%)
Bu tür bir çalışma daha önce yaptınız mı?	0	0	72	100

Öğrencilere daha önce bu tür bir çalışmayı yapıp yapmadıkları sorulduğunda, Tablo 8’de de görüldüğü gibi öğrencilerin tamamı hayır yanıtını vermişlerdir. Tablo 9’da “Bu tür bir çalışmayı daha sonra tekrar yapmak ister misiniz?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 9. “Bu tür bir çalışmayı daha sonra tekrar yapmak ister misiniz?” Sorusuna Verilen Yanıtların Dağılımları

	Evet		Hayır	
	(f)	(%)	(f)	(%)
Bu tür bir çalışmayı daha sonra tekrar yapmak ister misiniz?	68	94,44	4	5,55

Öğrencilere bu tür bir çalışmayı daha sonra tekrar yapmak isteyip istemedikleri sorulduğunda ise, Tablo 9’da da görüldüğü gibi öğrencilerin % 94.44’ü evet yanıtını, % 5.55’i ise hayır yanıtını vermişlerdir. Tablo 10’da “Bu şifreleme günlük hayatta nerelerde kullanılabilir?” sorusuna verilen yanıtların dağılımları yer almaktadır.

Tablo 10. “Bu şifreleme günlük hayatta nerelerde kullanılabilir?” Sorusuna Verilen Yanıtların Dağılımları

	Oyun oynarken		Gizli bilgileri saklamak için kullanılabilir.		Savaşlarda	
	(f)	(%)	(f)	(%)	(f)	(%)
Bu şifreleme günlük hayatta nerelerde kullanılabilir?	35	48,6	28	38,88	9	12,5

Tablo 10’da görüldüğü gibi öğrencilere, bu şifrelemeyi günlük hayatta nerelerde kullanılabileceği sorulduğunda, öğrencilerin % 48.62’ı oyun oynarken, % 38.88’i gizli bilgileri saklamak için kullanılabilir ve % 12.5’si ise savaşlarda kullanılabileceğini belirtmişlerdir.

Tartışma

Öğrencilerin görüşlerinden elde edilen verilerin analizi sonucu elde edilen bulgular yorumlandığında, matematik dersi öğretiminde şifreleme etkinliklerinin kullanılmasının öğrencilerin tutumlarını olumlu yönde etkilediği, dikkatlerini çektiği, derse karşı ilgi ve motivasyonlarını arttırdığı gibi elde edilen sonuçlar daha önceden yapılan bazı çalışmaların sonuçları ile uyum içerisindedir (Myerscough ve diğerleri, 1996; Güler, 2007).

Ülkemizde şifreleme etkinliklerinin matematik dersinde kullanılmasına yönelik sadece bir tane yüksek lisans tez çalışmasının (Güler, 2007) bulunması, konuyla ilgili farklı çalışmaların yapılmasına duyuru-

lan ihtiyacı göstermektedir.

Bu arařtırmada 7. sınıf düzeyinde olasılık, permütasyon konularıyla ilgili olarak yer deęiřtirme ve harf deęiřtirme řifrelemesi etkinlikleri kullanılmıřtır. Etkinlięin öęrencilerde oluřturduęu farkındalık ve motivasyonu arttırıcı özellięinin yanında öęrenciler tarafından beęenilmiř olması ve ilgiyle takip edilmesi etkinlięin bařarılı olduęu řeklinde yorumlanabilir. Arařtırmadan elde edilen olumlu sonuların farklı sınıf düzeyi ve farklı konularla iřlenen matematik derslerinde etkili bir uygulama örneęi oluřturabileceęini dūřünmekteyiz. Arařtırmamızda öęrenci görüřlerine yer vermemiz ve uygulama esnasında verdięimiz řifreleme örneklelerinin dięer disiplinlerle iliřkili oluřunun yanı sıra uygulamaların öęrenci merkezli olarak yürütölüp öęretmenin rehber konumunda yer alması yönüyle de etkili matematik öęretimi için örnekle bir uygulama olduęunu dūřünmekteyiz.

Ayrıca, etkinliklerin uygulama sürecinin öęrencilerin iletiřim becerilerinin geliřmesini de olumlu etkiledięi belirlenmiřtir. Etkinlik sonunda öęrenciler tarafından tasarlanan oyunların sınıfa oynanmasıyla da grup alıřmasındaki olumlu etkileřim sonucunda etkinliklerin iyi seviyede gerekleřtięi söylenebilir. Kaur (2008) de alıřmasında grup alıřması ve iletiřime önem vermiřtir. Tüm bu olumlu sınıf ortamının öęrenci bařarisını arttırmada önemli bir rol oynayacaęı söylenebilir.

Öęrencilerin farklı yetenek ve ilgilere sahip oldukları göz önüne alınarak, etkinlik uygulamaları sonucu deęerlendirme ölekleri hazır-

lanabilir. Şifrelemenin farklı matematik konularında kullanımını gerektiren etkinliklerin tasarlandığı, etkinlikler ile öğrenci başarısı arasındaki ilişkilerin, öğretmen görüşlerinin incelendiği daha kapsamlı araştırmalara ülkemizde de yer verilmelidir.

Hazırlanan etkinliklerin daha etkili ve verimli bir biçimde gerçekleştirilmesi için daha yüksek düzeyde etkileşim içeren çağdaş öğretim yöntemlerine göre tasarlanmış yöntemler geliştirilmelidir.

Etkinliklerin hazırlanmasında tüm alanlardan uzmanların tasarım ekibi içinde yer almaları gereklidir. Çünkü yeterli sayıda ve nitelikte uzmanın geliştirme sürecinde yer almadığı etkinlikler öğretimin etkinliğini azaltacaktır.

Öğretmen yetiştiren fakülteler ile Millî Eğitim Bakanlığı iş birliği yaparak, bilgisayar destekli öğretimin uygulamalarında kullanılmak üzere yazılımlar hazırlamak için AR-GE desteği verebilir.

Yeni araştırmalar daha uzun süreli ve çok denekli olarak uygulanabilir.

Sonuçlar

Öğrencilerin şifreleme etkinlikleri ile ilgili ortaya çıkan olumlu görüşleri ve öğrencilerin tamamının 7. sınıfa kadar böyle bir etkinlik yapmamış olmaları göz önünde bulundurulduğunda bazı matematik dersi konularıyla ilgili şifreleme etkinliklerinin oluşturulmasının ve kullanılmasının yararlı olacağı düşünülmektedir. Etkinlik sırasında yapılan aktivitelerin öğrencilerin konu ile ilgili kavramlara ulaşması ve

var olan bilgilerini pekiştirdikleri yönündeki sonuçlar dikkate alındığında dersin dikkati çekme, derse geçiş ve değerlendirme gibi birçok aşamasında kullanılabileceği görülmüştür. Ayrıca şifreleme etkinlikleri ile ilgili metinlerin sosyal bilgiler, Türkçe ve diğer derslerle ilişkili seçilmeleri, mesela öğrencilerin Türkçe dersinde okuduğu bir okuma parçasıyla şifrelerin öğretmen tarafından oluşturulması gibi... matematik dersiyle diğer disiplinlerin öğrenci zihninde de ilişkilendirilmesini sağladığı görülmüştür. Ders kitaplarında ilgili konularda şifreleme etkinliklerinin yer almasıyla öğrencilerin konuya ilgilerinin çekilerek motivasyonlarının artacağı, bu şekilde de etkili ve kalıcı öğrenmelerin gerçekleşebileceği düşünülmektedir.

Kaynakça

- Altun, M. (1998). *Matematik öğretimi*. Bursa.
- Başer, E. T. (2008). *5E modeline uygun öğretim etkinliklerinin 7. sınıf öğrencilerinin matematik dersindeki akademik başarılarına etkisi*. Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü.
- Baykul, Y. (2001). *T.C. Milli Eğitim Bakanlığı ilköğretimde etkili öğretme ve öğrenme el kitabı ilköğretim matematik kitabı*, Ankara: MEB Yayınları.
- Bayraktar, E. (1998). *Bilgisayar destekli matematik öğretimi*. Yayınlanmamış doktora tezi, A.Ü. Sosyal Bilimler Enstitüsü.
- Clark, R. C. (2005). Language teaching techniques. *Pro Lingua Associates*. 08 Ocak 2010, <http://unjobs.org/authors/raymond-c.-clark>.

- Durmuş, S. (2007). Matematikte öğrenme güçlüğü gösteren öğrencilere yönelik öğretim yaklaşımları. *Mehmet Akif Üniversitesi Eğitim Fakültesi Dergisi*, 8(13), 76-83.
- Ercan, Ö. (2005). *Çoklu zeka kuramına dayalı öğretim etkinliklerinin 8. sınıf öğrencilerinin matematik dersi "permütasyon ve olasılık" ünitesindeki akademik başarılarına etkisi*. Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü.
- Güler E. (2007). *Modüler aritmetik konusunun öğretiminde şifreleme aktivitelerinin matematik başarısına etkisi*. Yayınlanmamış yüksek lisans tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü.
- Karaçay, T. (1985). *Matematik öğretiminin bugünkü durumu ve değerlendirilmesi: Matematik öğretimi ve sorunları*, Ankara: TED Yayınları.
- Kaur, M. (2008). *Cryptography as a pedagogical tool*. (ERIC Document Reproduction Service No. EJ810999).
- Koç, S. (1996). *Matematik üzerine bir konuşma*. *Bilim ve Teknik Dergisi*, 341, 8.
- MEB. (2005). *İlköğretim matematik dersi öğretim programı ve kılavuzu*. Ankara: MEB Yayınları.
- Singh, S. (1999). *The code book: the evolution of secrecy from Mary, Queen of Scots to quantum cryptography*. NY: Doubleday.
- Yerlikaya, T. (2006). *Yeni şifreleme algoritmalarının analizi*. Yayınlanmamış doktora tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü.
- Yıldırım, A. ve Şimşek, H. (2005). *Sosyal bilimlerde nitel araştırma yöntemi*. Ankara: Seçkin Yayıncılık.
- Yıldırım, C. (2000). *Matematiksel düşünme*, İstanbul: Remzi Kitapevi.