RSA Şifrelemesi Yardımıyla Modüler Aritmetik Konusunun Pekiştirilmesi

Arş. Gör. Yasemin KATRANCI*

Kocaeli Üniversitesi, Eğitim Fakültesi, İlköğretim Bölümü, Matematik Öğretmenliği ABD, Kocaeli / Türkiye

Doç. Dr. Ahmet Şükrü ÖZDEMİR

Marmara Üniversitesi, Atatürk Eğitim Fakültesi, İlköğretim Bölümü, Matematik Öğretmenliği ABD, İstanbul / Türkiye

Özet

Kriptoloji kelimesi, köken olarak eski Yunancada yer alan "kryptos" ve "logos" kelimelerinden gelmektedir. Kryptos kelimesi "gizli"; logos ise "sebep-sonuç ilişkisi kurma, mantıksal çözümleme alanı" anlamı taşımaktadır. Günümüzde kriptoloji, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini kullanan bir matematik bilimidir ve genelde sayılar teorisi üstüne kuruludur. Bu araştırmada, RSA şifreleme yöntemi kullanılarak, öğrencilerin modüler aritmetik konusunu pekiştirmeleri amaçlanmıştır. RSA şifrelemesi yöntemine göre hazırlanan etkinlikler Kocaeli ili Körfez İlçesi'ndeki bir devlet okulunda öğrenim görmekte olan 19 on birinci sınıf öğrencisiyle iki ders saati içerisinde çalışılmıştır. Etkinlik kâğıtlarından elde edilen veriler betimsel analiz yöntemi ile analiz edilmiş ve yorumlanmıştır. Günlük hayatta pek çok şifre ile karşılaşan öğrencilerin değişik bir yöntem öğrenmenin hazzını

* Sorumlu Yazar. Tel: +90 262 303 24 46 E-posta: yaseminkatranci@gmail.com
 ISSN: 2146-5606

yaşadıkları gözlenmiş, modüler aritmetik konusunda zorlandıkları noktaları aştıkları, eksik oldukları noktaları tamamladıkları sonuçlarına ulaşılmıştır.

Anahtar Kelimeler: Şifreleme; RSA şifreleme yöntemi; Modüler aritmetik.

Strengthening the Subject of Modular Arithmetic With the Help of RSA Encryption

Abstract

The word of Cryptology is originated from the words of "crypto" and "logos" in An? Greek. The word "crypto" means that "secret"and the word "logos" means that "establishing relationship between cause and effect and the field of logical analysis". Today cryptology is a mathematical science which uses various sciences like electronics, optic and computer and in general it is based on the theory of numerals. The aim of this research is to let students to strengthen their knowledge on the subject of modular arithmetic in mathematics by using RSA encryption method. The activities which are prepared according to RSA encryption method have been studied together with 19 students from 11^{th} grade at a public school at Körfez district of the city of Kocaeli within two course hours. The data obtained from the activity worksheets have analyzed and interpreted by using descriptive analysis method. It is observed that students who faced with many cryptos in their daily lives have the pleasure to learn a different method and the results that they overcame the difficulties that they have about modular arithmetic and they completed the missing points in their knowledge at present.

Keywords: Cryptology; RSA cryptology system; Modular arithmetic.

Extended Summary

Purpose

Math teachers frequently search for different ways for teaching important mathematical subjects to their students. Field of Cryptology

presents very different subjects to teachers in their teaching. In this study it will be analyzed how students can strengthen modular arithmetic with the help of cryptology / encryption will be analyzed. Cryptology is originated from the Greek words of "crypto" and "logos". The word of "crypto" means "secret" and the word of "logo" means "establishing relationship cause and effect and the field of logical analysis". Cryptology is a science of encryption. The algorithms of cryptology are totally composed of mathematical functions. The functions that are used in mono alphabetical cryptology systems always work with modes corresponding to prime numbers. As we take into consideration the basic elements of cryptography, when a sender wants to send a message to a receiver via open networks, such a message which is sent via open network are always under the threat of being listened or changed by third persons. The said message we mention here is a normal text. In some usage it is called as plaintext. Encryption is something to hide the content of a message. This process converts the plaintext into the encrypted text and the content of information became something that nobody can understand. This content can be a message which is encrypted to be sent to someone else or to be stored. An encrypted message is a ciphertext. Deciphering is converting an encrypted text into a plaintext. In this study, RSA encryption method is chosen and the application has been conducted.

*RSA (**R**ivest, **S**hamir, **A**delman) Encryption*

RSA Encryption was defined first by Ronald Rivest, Adi Shamir and Leonard Adleman in August 1977, but subsequent investigations

revealed the fact that it was discovered in GCHQ by Clifford Cocks in 1973. A RSA process is an exponentiation process which requires repeated modular multiplications (Bahçetepe, 2006). The mode of RSA encryption "m" is consisted of multiplication of two big prime numbers. Unclosed force "e" and reserve force "d" are related to each others as being prime numbers (Dujella, 2009). Since we use large numbers in RSA which is a factorization problem that can easily be applied, its solution is not easy.

Modular Arithmetic

The subject of Modular Arithmetic was removed from primary school curriculum which was revised lastly in 2005 and added into secondary school curriculum. It has been seen that the subject of modular arithmetic which is used as part of cryptology methods was not mentioned in our country's educational programs. If remainder r as a result of an x number which is divided by a d number and if division is shown by the letter of q, then x can be expressed as follows:

$$X=q^* d+ r \qquad 0 \leq r < d$$

The remainder of a number which is divided by d number is r < d. The numbers of d's remainder equivalence class set have the values between {0,…,d-1}. This d's remainder equivalence class set is called as d – base mode and expressed as follows.

$$a \equiv b \pmod{d}$$

The problem sentence of this study is determined as follows: "How and what is the roy of RSA encryption method in strangthening the subject of modular arithmetic as and when utilized in secondary

school education?"

Method

This study is a case study. Case studies can be both qualitative and quantitative but in both cases the purpose is to give results related with a specific condition. This is a qualitative case study. The observations during the application of activities and document analysis methods have been used in the study. The study group is composed of 19 students from 11^{th} grade at a public high school at Körfez district in Kocaeli. Data collection instruments are worksheets used during the study and observations. The data is analyzed and evaluated by using descriptive analysis method.

Results

The data collected from study booklets are presented and evaluated in four parts. In the first part the students are expected to construct RSA encryption structure by using their prior knowledge. In this part, the students are also expected to use prime number knowledge, relatively prime knowledge and exponent/power concepts. From the findings, it has been concluded that almost all of the students participated in the study have constructed these concepts previously. In the study it has also been seen that most of the students can find exponentiation and remainder operations successfully. In the decryption part of the booklets the students are expected to make operations such as exponentiation and mode as in the encryption part. In the encryption part students are provided to remember the subject of modular arithmetic and it has been seen that students remembered the subject of modular arithmetic

which they have learned before. In this part, it has been aimed that both students can strengthen the knowledge they learned before and do decryption of the encrypted text. It has been seen that students participated in the study managed to do remainder operations fastly as in the first section. In the fourth part of the booklets a large mode value has been selected in order make the students to strenghten their knowledge with the subject of modular arithmetic. Before asking students to solve the example given in the booklet, $7^{11} \equiv x(\mathrm{mod}\,9)$ example has been given in order to check and remind their existence knowledge. The mode value which was selected as 10 in the previous examples, has been preferred as 9 in this example and it has been explained to them how to operate in finding the value of 7^{11} expression. It has been observed that all the students participated in the study has easily understood the given example.

Discussion

The main purpose of this study is to analyze how 11^{th} grade students will strengthen their knowledge with the subject of modular arithmetic which they learned before with the help of encryption activities. The results of the study can be analyzed in four parts by considering the study process.

Conclusion

(i) Establishing RSA Encryption Algorithm

The whole teaching in this study is activity based. All of the students showed great interest to every part of the study. In the first part

of the study, they used prime number knowledge appropriately while establishing RSA encryption algorithm. They solved the difficulties that appeared in finding the necessary value for decryption which was the last step of algorithm by using peer assistance. At this stage of the study they got fun and learned by using peer assistance. The findings of the study presented that the activities prepared were suitable to produce targeted mathematical knowledge. In this part of the study, student discussed about the selection of prime numbers, finding the mode value, finding the necessary values for encryption and decryption operations and expressed their views freely and openly. Since the study environment provided them to express their ideas freely, it has been concluded that all the students established RSA encryption algorithm successfully.

(ii) Encryption of Selected Plain Texts

It has been seen that as and when students got difficulties in operating exponentials during encryption activities, they asked peer assistance or used calculators. Consequently, it has also been seen that students correctly encrypted the plaintexts they selected. It can be said that as a result of the observations where they do not have difficulties in using modular arithmetic knowledge during encryption, their modular arithmetic knowledge structure was strengthened with the help of encryption activities (Dreyfus et al., 2006).

(iii) Decryption of Encrypted Texts

Using the structures constructed in a learning situation provide strengthening in these structures. In this part of the study, the modular

arithmetic knowledge that students used while decrypting activities for the encrypted plaintexts can also help them to consolidate strengthen these structures.

Students decrypted the encrypted plaintexts with the help of the algorithm that they constructed in the first part of the study. During decrypting activities, they used again exponential and modular arithmetic knowledge. This also allows them to strengthen their knowledge structures.

(iv) Finding the Remainder in Expressions with Large Mode Value

The purpose of this part of the study is to provide further enhancement and strengthening of the existing knowledge structures of the students. It has been seen that students understood the operations which were explained by more simple systems in this section, they tried to compensate their shortage of knowledge about modular arithmetic and they strengthened their existing knowledge structures.

Giriş

Matematik öğretmenleri sıklıkla, önemli matematik konularını öğrencilere öğretmek için değişik yollar ararlar. Kriptoloji alanı, öğretmenlere öğretme yapabilecekleri çok değişik konular sağlar. Bu çalışmada kriptoloji yardımıyla öğrencilerin modüler aritmetik konusunu nasıl pekiştirecekleri incelenecektir.

Şifreleme, köken olarak Yunancada yer alan “kryptos” ve “logos” kelimelerinden gelmektedir. Kryptos kelimesi “gizli” anlamına

gelmektedir. Logos ise "sebep-sonuç ilişkisi kurma, mantıksal çözümleme alanı" anlamı taşımaktadır. Kriptoloji, şifre bilimidir. Klasik kriptoloji, sırları saklamakla ilgili iken, 1975'ten beri modern kriptoloji, düşmanların varlığındaki iletişimle ilgilidir (Lucks, 2003).

İlk kriptolog, 4000 yıl önce yaşamış Mısırlı bir kâtiptir. Efendisinin hayatını anlatmak için hiyeroglifler kullanmış ve bu hiyeroglifleri şifreli bir şekilde oluşturmuştur. Bu şekilde başlayan kriptografi, hayatının ilk 3000 yılında neredeyse hiç gelişmemiştir. Dünyanın farklı yerlerinde en temel biçimlerde ve bağlantısız bir şekilde kullanılmasına rağmen sonraki adımlara geçilememişti. Daha sonraları (M.Ö. 5.–6. yüzyıl) askerî istihbaratta gizlilik gerekmesi sebebiyle, kriptografi askerî alana girdi.

Günümüzde şifreleme, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini kullanan bir matematik bilimidir ve genelde sayılar teorisi üstüne kuruludur. Şifreleme, bilgiyi matematiksel işlemleri kullanarak veya bilgiyi belli bir algoritmaya göre yer değiştirme işlemi yaparak karmaşık hale getirerek gerçekleştirilir (Yılmaz, 2010). Kriptoloji algoritmaları tamamen matematiksel fonksiyonlardan oluşur. Mono alfabetik kriptolama sistemlerinde kullanılan fonksiyonlar, asal sayılara karşılık gelen modlarla her zaman çalışırlar.

Buna göre, 29 harften oluşan Türk alfabesi şifreleme için uygun olmasına karşın 26 harften oluşan İngiliz alfabesi ya da 10 elemanlı rakamlar kümesi için bazı kısıtlar söz konusudur. Kriptolojinin iki temel alt dalı vardır: Kriptografi ve kriptoanaliz. Kriptoanaliz, krip-

tografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır. Ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya koymak için kriptoanaliz kullanılır. İlk kriptoanaliz yapanlardan biri de 700'lü yıllarda yaşamış olan el-Kindi'dir. Al Kindi'nin yerine koyma usullü şifreyi kırma tekniği harflerin kişiliklerine ki bu kişilikler onların frekanslarıydı bağlıdır. Bazı harfler diğerlerine göre daha yaygındır. Al Kindi'nin tekniği frekans analizi olarakda bilinmekteydi (Wikipedi, 2008). el-Kindi'nin devrimsel kriptanaliz sistemi iki kısa paragrafta özetlenmektedir:

> *"Eğer yazıldığı dili biliyorsak şifreli bir mesajı çözmenin bir yolu, aynı lisana ait yaklaşık bir sayfayı dolduracak kadar bir metin bulup sonra her bir harfin metindeki sayısını bulmaktır. En çok kullanılan harfe 'ilk', ondan sonra en çok bulunan harfe 'ikinci', sonrakine 'üçüncü' diyerek bütün harfleri numaralandırırız. Sonra çözmeye çalıştığımız şifre metnin içindeki sembolleri de aynı şekilde numaralandırırız. En çok geçen sembolü düz metinden bulduğumuz en çok kullanılan harfle, ikinciyi ikinciyle vs. değiştiririz. Sonuçta çözmeye uğraştığımız metin içindeki her harfe karşılık normal alfabeden bir harf bulana kadar bunu tekrarlarız."*(Güler, 2007).

Kriptografi bir anahtar yardımı ile verinin (düz metin olarak bilinir) kodlanmış bir şekle ("cipher-text") getirilmesi işlemidir. Kriptografi genellikle bilginin gizliliğini korumak için kullanılır. Örneğin o bilgiye ulaşabilen insanlar anahtarı bilenler olarak sınırlandırılmıştır

(Kalaycı, 2003). Yani, ileti güvenliğini sağlamaktır. Şifreleme algoritmalarını kullanarak yapılan gizli mesajlaşma, onaylama, dijital imzalar, elektronik para ve diğer uygulamaların tüm yönleriyle ilgilidir (Şen, 2006). Askerî alanda, kriptografiyi kullanan ilk ulus Ispartalılardır (Aksuoğlu, 2010). M.Ö. 5. yüzyılda geliştirdikleri ilk yer değiştirme sistemi olarak askeriye tarafından kullanılan cihaz belli bir kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs veya ince, deri bir şeritten oluşuyordu. Gönderilmek istenen gizli mesaj silindir boyunca silindire sarılı papirüse veya şeride yazılıyor ve sonrasında da papirüs veya şerit silindirden çözülüyordu (Aksuoğlu, 2010).

Şekil 1: Ispartalıların Kripto Cihazı (Aksuoğlu, 2010)

Kriptografi genel olarak şu ana konularla ilgilenir:

Gizlilik: Bilgi istenmeyen kişiler tarafından anlaşılamamalı.

Bütünlük: Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememeli.

Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra

bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkâr edememeli. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.

Kimlik belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.

Kriptografinin uygulama alanları olarak;

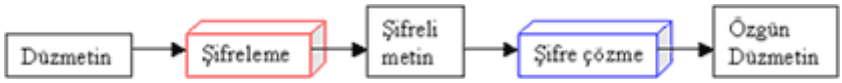
• Kablolu ve kablosuz ağlarda ses ve/veya veri aktarımının istenmeyen kişilerce izlenmesinin önlenmesi,

• Bilgisayar sistemlerinde bulunan verilere yetkisiz erişimlerin engellenmesi,

• Güvenli bir şekilde e-ticaret işlemlerinin yapılabilmesi örneklenebilir (Yerlikaya ve diğ., 2006)

Kriptolojinin (şifrelemenin) temel elemanları göz önüne alındığında, bir göndericinin bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar. Burada söz konusu ileti düz metindir. Bazı kullanımlar *plaintext* adı da verilir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (*encryption*). Bu işlem düz metni şifreli metne dönüştürür. Bilginin içeriği başkalarının anlamayacağı hâle gelir. Bu bilgi bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir

bilgi olabilir. Şifrelenmiş bir ileti şifreli metindir (*ciphertext*). Şifreli metni düz metne geri çevirme işlemi şifre çözümüdür (*decrypt*). Bu işlemler Şekil 1'de gösterilmektedir.



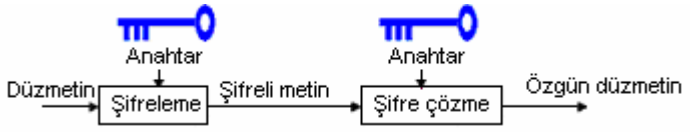
Şekil 2: Şifreleme ve şifreyi çözme işlemleri (Kodaz ve Botsalı, 2010)

Kriptolojinin genel olarak kullanılan iki yöntemi vardır. Bunlar:

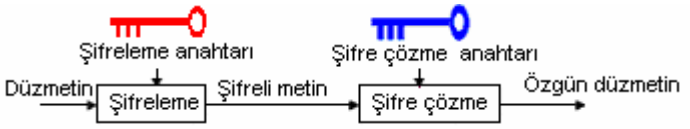
Paylaşılmış/Simetrik Anahtar Şifreleme (Shared Key Cryptography): Veriyi değiştiren iki tarafta anahtara sahiptir. Bu başkalarınca bilinmeyen anahtar verinin iletimden önce şifrelenmesi; iletildikten sonra karşı tarafta şifresinin çözülmesi için kullanılmaktadır (Kalaycı, 2003). Kullanım alanları ise, veri oturum şifrelemesi, banka sistemleri (pin şifreleme).

Açık Anahtar Şifreleme (Public Key Cryptography): İki tarafta da bir gizli anahtar ve açık anahtar bulunur. Gizli anahtarlar sadece sahipleri tarafından bilinmektedir. Açık anahtarlar ise herkese açıktır (telefon numaraları gibi). Gönderen mesajı alıcının açık anahtarı ile şifreler ve alıcı şifreli-mesajı, gizli anahtarı ile çözer. Bu Diffie ve Hellman (Stanford Üniversitesi, 1975 Sonbahar) tarafından yapılan, algoritmaların ve bir anahtarın şifrelemek, bir başka anahtarın çözmek için kullanılabileceği keşifleri sayesinde mümkün olmaktadır. Açık ve gizli anahtar bir anahtar çiftini oluşturur. Bu şifreleme yöntemleri gerçekten çözülmesi zor olan sonlu alanların logaritmalarını almak

(Diffie - Hellman), büyük sayıları asal çarpanlarına ayırmak (RSA) gibi matematiksel yöntemlerle tek-yönlü fonksiyonlardan yararlanır. Bu tip fonksiyonlarda tek yönde hesaplama diğer yönde hesaplamaya göre daha kolaydır. Bugünün işleme gücü ve bilgisayarlarıyla bile brute-force kullanarak kırmak sanal olarak imkânsızdır.



Şekil 3: Tek anahtar ile gizli anahtar (simetrik) şifreleme (Abken ve Subaşı, 2005)



Şekil 4: Çift anahtar ile açık anahtar (asimetrik) şifreleme (Abken ve Subaşı, 2005)

Bu çalışmada da yukarıda belirtilen açık anahtar şifreleme yöntemlerinden birisi olan RSA şifreleme yöntemi seçilmiş ve uygulama yapılmıştır.

*RSA (**R**ivest, **S**hamir, **A**dleman) Şifreleme*

İlk olarak Ağustos 1977'de Ronald Rivest, Adi Shamir, ve Leonard Adleman tarafından tanımlanmış olup, aslında 1973 yılında GCHQ içerisinde Clifford Cocks tarafından keşfedildiği daha sonraki incelemelerde açığa çıkmıştır. Bir RSA işlemi, tekrarlanan modüler

çarpımlar gerektiren bir modüler üst alma işlemidir (Bahçetepe, 2006).

RSA Algoritmasının içeriği ve çalışması aşağıdaki gibidir:

RSA Public Key Sistemi	***Örnek***
Hem p'nin hem de q'nun asal olduğu p ve q seçilir.	*P =11; q=13;*
Mod alınacak değer hesaplanır ***m*** *=* ***pq***	***m*** *= 11*13 = 143.*
Euler's totient fonksiyonu uygulanır ***A*** *= (****p****-1)(****q****-1).*	***A****= (11-1)*(13-1) = 120.*
A değeri ile en büyük ortak böleni 1 olan bir e değeri hesaplanır.	***e*** *= 7. (7<120, ve 7 ve 120'nin en büyük ortak böleni 1'dir*
e*d *= 1 mod****(m)*** *olacak şekilde d değeri hesaplanır*	*7****d*** *= 1 mod 120 =>* ***d*** *= 103,* *çünkü* *7*103 = 721 = 1 mod 120.*
*public key (****e****,* ***m****).*	*public key (7, 143).*
*Private key (****d****,* ***m****).*	*private key (103, 143).*
Plaintext ***M*** *olsun.*	***M*** *= 5 kabul edelim.*
ciphertext ***C*** *=* ***M^e*** *mod****m****.*	*Ciphertext:* ***C*** *= 5^7 mod 143= 47*
Şifre çözme işlemi => *plaintext =* ***C^d*** *mod* ***m*** *=* ***(M^e)^d*** *mod* ***m*** *=* ***M****.*	*Plaintext:* *47^103 mod 143 = 5* *47^103 = (5^7)^103 = 5^721* *=5*[5^720]=5*[(5^120)^6]* *= 5*[1^6] = 5.* *5^120 = 5^t = 1 mod 143 (Euler teoremi) veya, daha basitçe,* ***x^(e*d) = x****; bu sebepten,* *5^721 = 5'tir.*

RSA şifrelemesinin modu "m" iki büyük asal sayının çarpımından meydana gelmektedir. Açık kuvvet "e" ve saklı olan kuvvet "d" aralarında asal olacak şekilde ilişkilidirler (Dujella, 2009).

$$e.d \equiv 1 \ (\text{mod } \varphi(n))$$

Bu algoritmada iki asal sayının çarpımını kullanarak anahtar oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmak asal olmayan sayıları ayırmaktan daha zor olmasıdır (Yılmaz, 2010). Günümüz kripto analistlerinin asıl hedefi, kriptografinin temel

taşlarından biri olan RSA'yı kırabilmektir. RSA en önemli askerî, diplomatik, ticarî ve suç örgütlerinin iletişimlerini korumakta kullanılmaktadır (Çimen, Akyelek ve Akyıldız, 2008). Uygulaması basit bir çarpanlara ayırma problemi olan RSA'da çok büyük sayılar kullanıldığı için çözümü basit değildir.

Modüler Aritmetik

Modüler aritmetik konusu son olarak 2005 yılında düzenlenen ülkemiz ilköğretim programından çıkarılmış ve ortaöğretim konuları içerisine dâhil edilmiştir. Şifreleme yöntemlerinin bir kısmında da kullanılan modüler aritmetik konusuna ülkemiz programlarında bu yönüyle değinilmediği görülmektedir.

Bir x sayısının d sayısına bölümünde kalan r ve bölüm q ile gösterilirse x şöyle ifade edilebilir.

$$x = q*d + r$$

d sayısına bölünen bir sayının kalanı $r < d$ 'dir. d'nin kalan denklik sınıfı kümesindeki sayılar {0,...,d-1} arasındaki değerlerdir. Bu d'nin kalan denklik sınıfı kümesine d tabanına göre mod denir ve şöyle ifade edilir.

$$a \equiv b \pmod{d}$$

a'nın d'de modu b'ye denktir diye okunur ve şu kuralları sağlar.

$a \equiv b \pmod{d}$ ise $a=b+d*k$ (k=0, 1, ...)

$a \equiv b \pmod{d}$ ve $c \equiv e \pmod{d}$ ise $a+c \equiv d+e \ (mod\ d)$

$a \equiv b \pmod{d}$ ve $c \equiv e \pmod{d}$ ise $a*c \equiv d*e \pmod{d}$

Örnek; $25 \equiv 25 \pmod{52}$

$3 + 5 \equiv 2 \pmod{6}$

$4 \times 7 \equiv 3 \pmod{25}$

$1156 \equiv 6 \pmod{10}$

Aşağıda mod 7 ye göre toplama, çarpma ve üs alma işlem sonuçları görülmektedir:

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

^	**0**	**1**	**2**	**3**	**4**	**5**	**6**
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1
4	1	4	2	1	4	1	2
5	1	5	4	6	2	3	1
6	1	6	1	6	1	6	1

Eğer çarpma tablosundan hepsi 0 olan satır ve sütunu kaldırırsak, her satır ve sütundaki sayıların birbirinden farklı olduğunu görürüz. Bu 7'nin asal sayı olmasından kaynaklanan bir durumdur. Üs tablosunda üs olarak 6'ya geldiğimizde sonucun tekrar ettiğini görüyoruz. Buradan mod 7'de iken üssün mod 6'ya göre düşünülmesi gerektiği sonucunu çıkarırız. Bu sonuçlar bütün asal tabanlar için geçerlidir. Eğer biz bir sayının 5 ve 7 ile bölündükten sonra kalanını biliyorsak 5

ve 7 nin çarpımı olan 35 sayısından kalanını da buluruz. Bu demektir ki mod 35 aritmetiği, mod 5 ve mod 7 aritmetiğinin bir kombinasyonundan oluşmaktadır. Fakat üs almada mod 34 yerine mod 24 tür. Çünkü üste mod 5'in yerine mod 4, mod 7'nin yerine mod 6, böylece mod 35'in yerine de 6*4 =mod 24 olmaktadır. Bu (p-1)(q-1) sayısının RSA daki rolünü çok az da olsa açıklayacaktır. Ama sadece (p-1)(q-1)'e göre asal olan sayılar RSA'da şifrelemek ve çözmek için kullanılır. Bütün asal sayılar değil ayrıca RSA da güvenli olabilmek için çok yüksek (geniş) modüler gerektirir. RSA algoritması, elektronik dokümanlar için dijital imza üretilmesi ve şifreli mesajların gönderilmesi amacıyla kullanılır. Bu algoritma, dijital dokümanların imzalanması için prosedür sağlar ve bir imzanın gerçek olup olmadığını tespit eder (Bahçetepe, 2006).

Problem Durumu

Modüler aritmetik konusu son kez 2005 yılında düzenlenen ilköğretim müfredatından çıkarılarak ortaöğretim müfredatı içerisine dâhil edilmiştir. Çoğunlukla modüler aritmetiğe bağlı olan şifreleme etkinlikleri bu sebeple ilköğretim okullarında uygulanmamaktadır. Bu durum Türkiye'de bu şekilde iken, birçok dünya ülkesinde içerisinde modüler aritmetiğin kullanılmadığı, basit alfabeye yönelik şifreleme etkinlikleri tasarlanmıştır veya ayrı bir "kriptoloji ve kodlama" dersi olarak veya matematik dersi kapsamında uygulanmaktadır.

Modüler aritmetik bilgisini içeren RSA şifreleme yönteminin ise ülkemiz ortaöğretim okullarında bu konunun öğretilmesinde kullanılmadığı dikkat çekmiştir. Bu sebeple bu çalışmanın problem cümlesi

"Ortaöğretimde modüler aritmetik konusunun öğretilmesinde RSA şifreleme yönteminin kullanılması ile bu konunun pekiştirilmesi nasıldır?" şeklinde belirlenmiştir.

Araştırmanın Amacı

İlgili literatür incelendiğinde modüler aritmetik konusunun hem öğretilmesinde hem de pekiştirilmesinde, şifreleme etkinliklerinden yararlanılmadığı görülmektedir. Bu çalışma için belirlenen çalışma grubundaki öğrencilerin modüler aritmetik konusunu daha önceden öğrenmiş/yapılandırmış olmaları sebebiyle, çalışmada konunun öğretiminden ziyade konu ile ilgili eksikliklerin giderilmesine ve konunun pekiştirilmesine odaklanılmıştır. Bu bağlamda çalışmada, ortaöğretim on birinci sınıf öğrencilerinin RSA şifreleme yöntemini kullanarak, modüler aritmetik konusundaki eksikliklerini gidermeleri ve bu konu ile ilgili pekiştirme yapmaları amaçlanmıştır. Literatürde modüler aritmetik konusunun öğretilmesi ve pekiştirilmesinde şifreleme etkinliklerinin kullanılmaması ve ortaöğretim düzeyinde modüler aritmetik konusuna yönelik bir çalışma olması bakımından bu çalışmanın alana katkı getireceği öngörülmektedir.

Yöntem

Araştırma Modeli

Bu çalışma bir durum çalışması olan *"örnek olay incelemesi"*dir. Durum çalışmaları hem nitel hem de nicel olabilirken her iki durumda da amaç belirli bir duruma ilişkin sonuçları ortaya koyabilmektir. Bu çalışmada ise nitel bir durum çalışması yapılmıştır. Nitel araştırma gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntem-

lerinin kullanıldığı, algıların ve olayların doğal ortamda, gerçekçi ve bütüncül bir biçimde ortaya konulmasına yönelik nitel bir sürecin izlendiği araştırmadır (Yıldırım ve Şimşek, 2006). Bu çalışmada, hazırlanan etkinliklerin uygulanması sırasında yapılan gözlemler ve doküman analizi yöntemleri kullanılmıştır.

Örnek olay incelemesinde ve nitel araştırmalarda araştırmacı nicel çalışmalarda olduğu gibi sadece araştırma konusunu gözleyen değil, aynı zamanda konuyu ve katılımcıları daha iyi anlayıp analiz edebilmek için çalışmaya bizzat katılan, katılımcılarla birebir görüşen kişi konumundadır, yani sürecin bir parçasıdır (Yıldırım ve Şimşek, 2006). Bundan dolayı araştırmacı çalışmaya *katılımcı gözlemci* konumunda dâhil olmuştur.

Çalışma Grubu

Kocaeli ili Körfez İlçesine bağlı bir devlet okulunda öğrenim görmekte olan 19 on birinci sınıf öğrencisi çalışma grubunu oluşturmaktadır. Ortaöğretim programlarının düzenlenmesi ile daha önceden var olan bölüm uygulaması kaldırılmıştır. Daha önceden Fen, Sosyal veya Türkçe-Matematik sınıfı olarak öğrencilerin bölümlere ayrılması şeklinde olan uygulama bu yeni sisteme göre yoktur. Çalışmanın gerçekleştirildiği okulda herhangi bir bölüm uygulaması olmamasına karşın çalışmaya katılan öğrencilerin üniversite seçimlerinde sayısal ağırlıklı bölümleri seçecekleri öğretmenleri ve öğrenciler ile yapılan görüşmelerle belirlenmiştir.

Veri Toplama Araçları ve Verilerin Toplanması

Çalışmanın üzerinde yürütüldüğü etkinliklerin bulunduğu çalışma kâğıtları ve çalışma ortamında yapılan gözlemler çalışmanın veri toplama araçlarını oluşturmaktadır. Çalışmanın yürütüldüğü bu çalışma kâğıtları araştırmacılar tarafından daha önceden gözden geçirilerek gerekli düzenlemeler yapılmıştır. Her bir çalışma fasikülü dört sayfadan oluşmaktadır. İlk sayfada öğrencilerin RSA şifreleme yönteminin yapısını oluşturmaları amaçlanmıştır. İkinci sayfada ise mod'u 10 olacak şekilde düzenlenen sistemin devamı olan şifreleme etkinliği bulunmaktadır. Bazı harflerden oluşan bir sistemi içeren bu sayfada, öğrencilerin daha önceden belirlenmiş bu harflerden yeni kelimeler oluşturmaları beklenmektedir. Bu harfler, öğrencilerin rahatça kelime üretebilmelerine olanak sağlayacak şekilde ayarlanmıştır. Öğrencilerin, oluşturmuş oldukları RSA şifreleme yöntemi çalışma sistemine göre daha önceden belirlenmiş harflerden oluşturdukları bir kelimeyi şifrelemeleri bu sayfada beklenmektedir. Üçüncü sayfada ise şifreledikleri metinlerin deşifresini yapmaları istenmektedir. İkinci ve üçüncü sayfalarda öğrencilerin modüler aritmetik konusu ile ilgili daha önceden yapılandırmış oldukları bilgileri hatırlamaları ve kullanmaları beklenmektedir. Son bölüm olan dördüncü sayfada ise mod değerinin değişmesi ile şifrelemenin gücünün artırılması ve öğrencilerin daha önceden yapılandırmış oldukları modüler aritmetik konusunu pekiştirmeleri amaçlanmıştır.

Verilerin toplanmasında bu dört sayfadan oluşan çalışma fasikülleri kullanılmıştır. İlk olarak öğrencilere "Günlük hayatınızda kullandığınız şifreler nelerdir?" şeklinde bir soru yöneltilmiştir. Öğrenci-

lerden “cep telefonu şifresi, bilgisayar şifresi, apartman kapısı şifresi, banka kartı şifresi vb. gibi” cevaplar alınmıştır. Bir tane kız öğrenci ise en yakın arkadaşı ile aralarında bir alfabe oluşturduklarını ve bu alfabeyi kullanarak sohbet ettiklerini belirtmiştir. Böylece öğrencilerin şifre ile ilgili genel bir bilgiye sahip oldukları belirlenmiştir. Daha sonra, hiç “Facebook şifrenizi kıran oldu mu?” şeklinde bir soru yöneltilerek konuya ilgileri çekilmiştir. “Şifrelerinizin kırılmaması için neler yapılabilir?” diye bir soru yöneltilerek şifreleme hakkındaki bilgileri yoklanmıştır. Şifrelerin çalınmaması veya kırılmaması için büyük-küçük harf, sayı, sembol gibi ifadelerin şifrelerde kullanılması gerektiğini belirttikleri görülmüştür. “Şifrelemenin nasıl yapıldığını biliyor musunuz?” diye sorularak “RSA” ifadesi tahtaya yazılmıştır. Bu ifadenin ne anlama gelebileceği sorulmuş ve öğrencilerin ilgilerinin arttığı gözlemlenmiştir. “Reel Şifreleme Aygıtı, Rastgele Seçilen Algoritma” şeklinde tahminlerde bulunmuşlardır. RSA’nın bir şifreleme tekniği olduğu ve bu tekniği geliştirenlerin isimlerinin baş harflerinin kodlanması ile adlandırıldığı bilgisi verildikten sonra fasiküllerin ne şekilde uygulanacağı anlatılmıştır. Fasiküllerin öğrencilere dağıtılmasının ardından, ilk sayfadaki işlemlerin yapılması ile çalışmaya başlanılmıştır. Çalışma için herhangi bir süre verilmemiş, öğrencilerin sayfalardaki işlemleri bitirmelerine göre çalışma sonlandırılmıştır. Daha sonra öğrencilerin sıra arkadaşlarına göstermeden bir kelime şifrelemeleri istenmiştir. Şifrelenen kelimeler sıra arkadaşlarına verilerek deşifre etmeleri sağlanmıştır. Böylece öğrencilerin hem ne olduğunu bilmedikleri bir şeyi deşifre etmeleri sağlanmaya hem de modüler aritmetik konusu ile ilgili daha çok işlem yapmaları sağlanmaya çalı-

şılmıştır. Son olarak, öğrencilerin şifrelemiş oldukları kelime ya da metinleri ne şekilde şifrelediklerini birkaç örnek ile tahtada göstermeleri istenmiştir. Çalışma sonunda bütün fasiküller toplanmıştır. Bu çalışma fasiküllerinin her bir sayfası çalışma kâğıtları şeklinde analiz edilmiş ve yorumlanmıştır.

Verilerin Analizi

Elde edilen veriler betimsel analiz yöntemi ile değerlendirilmiştir. Betimsel analizde, görüşülen ya da gözlenen bireylerin görüşlerini çarpıcı bir biçimde yansıtmak amacıyla doğrudan alıntılara sık sık yer verilir. Bu tür analizde amaç, elde edilen bulguları düzenlenmiş ve yorumlanmış bir biçimde okuyucuya sunmaktır (Yıldırım ve Şimşek, 2006). Elde edilen veriler araştırmacı tarafından dört başlık altında ayrı ayrı değerlendirilmiş, bulgular düzenlenmiş ve yorumlanmıştır.

Çalışmanın Geçerlik ve Güvenirliği

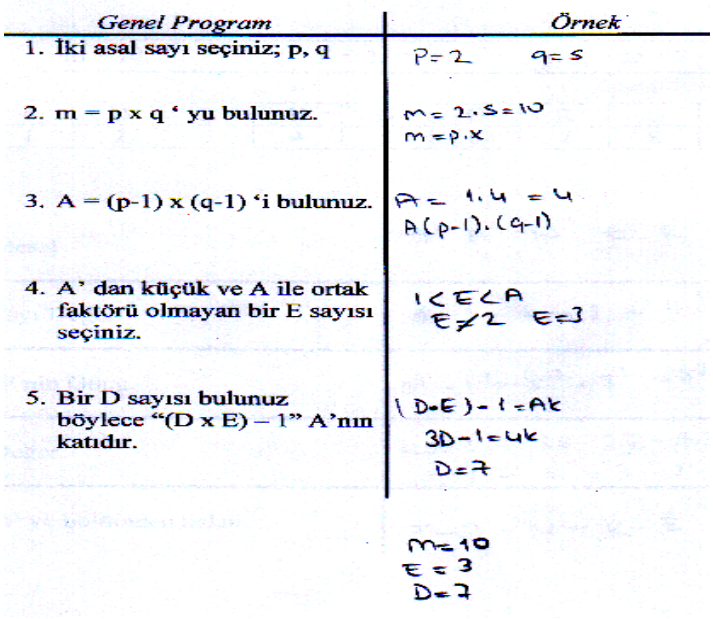
Nitel araştırmalarda kullanılan geçerlik ve güvenirlik açıklamaları farklılık göstermektedir. Nicel araştırmada geleneksel olarak kullanılan "geçerlik" ve "güvenirlik" kavramları yerine nitel araştırmalarda "iç geçerlik" yerine "inandırıcılık", "dış geçerlik" yerine "aktarılabilirlik", "iç güvenirlik" yerine "tutarlık" ve "dış güvenirlik" yerine "teyit edilebilirlik" kavramları önerilmektedir (Yıldırım ve Şimşek, 2006). Nitel araştırmada geçerlik araştırmacının araştırdığı olguyu, olduğu biçimiyle ve olabildiğince yansız gözlemesi anlamına gelmektedir (Kirk ve Miller, 1986).

Bu araştırmada, araştırma boyunca sağlanan uzun süreli etkile-

şim, derin odaklı veri toplama, çeşitleme, uzman incelemesi ve katılımcı teyidi ile iç geçerlik, ayrıntılı betimleme ve amaçlı örnekleme ile dış geçerlik sağlanmıştır. Çalışmada güvenirlik için çalışma bittikten sonra elde edilen veriler şifrelemenin ve modüler aritmetik konularının gözlenebilirliği bakımından farklı iki uzman tarafından yorumlanmış ve yorumların birbirleri ile tutarlı olduğu görülmüştür. Ayrıca güvenirliği sağlamak için çalışma içerisinde öğrencilerin çalışma fasikülleri-nden elde edilen verilere sıkça yer verilmiştir.

Bulgular ve Yorumlar

Çalışma fasiküllerinden elde edilen veriler dört ayrı bölümde sunulmuş ve yorumlanmıştır. Birinci bölümde, öğrencilerin daha önceki bilgilerini kullanarak RSA şifrelemesinin yapısını oluşturmaları beklenmiştir. Bu bölümde öğrencilerin, asal sayı bilgisi, aralarında asal olma bilgisi ve üs / kuvvet kavramlarını da kullanmaları beklenmektedir. Çalışmaya katılan öğrencilerin hemen hemen hepsinin bu kavramları daha önceden yapılandırmış oldukları bulgusuna ulaşılmıştır. Aşağıda RSA şifrelemesinin alt yapısının kuruluşuna yönelik bir örnek verilmiştir.



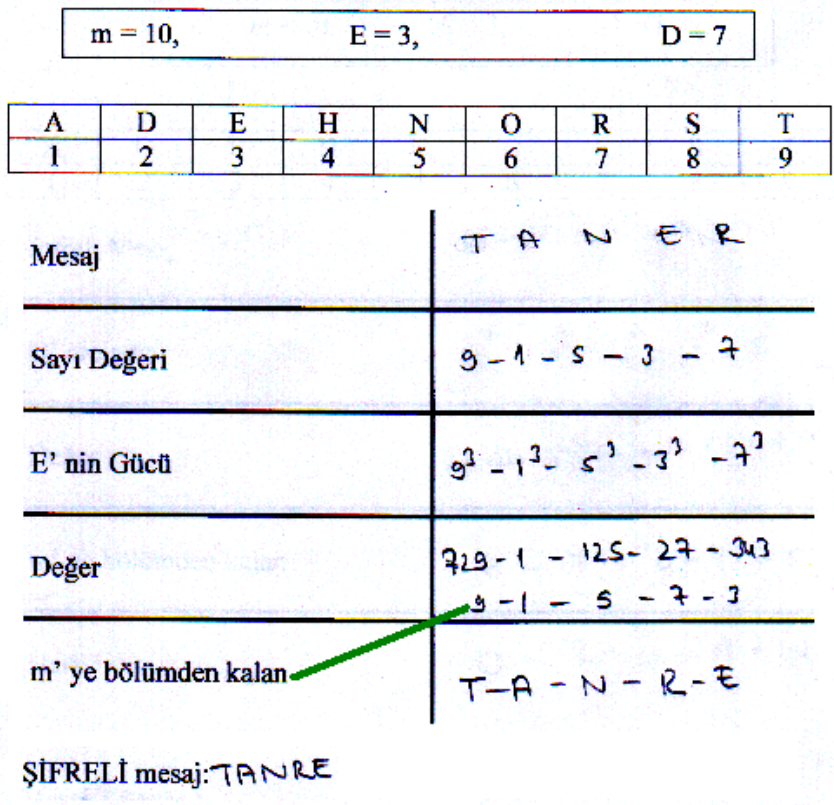
Örnek 1: RSA şifrelemesi yönteminin kurulması

Örnek 1'de görülen m = 10, RSA şifrelemesi için gerekli olan mod değerini, E = 3, seçilecek olan kelimeyi ya da metni şifrelerken kullanılacak olan sayıyı, D = 7 ise deşifre işlemi sırasında kullanılacak olan sayıyı ifade etmektedir. Örnek 1'de görüldüğü üzere, seçilen asal sayılar doğrudur. Buradan öğrencinin asal sayı bilgisini daha önceden yapılandırmış olduğu görülmektedir. Çalışmaya katılan diğer öğrencilerin çalışma kâğıtları da incelendiğinde, her öğrencinin doğru asal sayılar seçtikleri fakat sayıları seçerken mümkün olan en küçük asal sayıları tercih ettikleri görülmüştür. Özellikle mod değerinin "10" olması gelecek işlemleri kolaylaştıracağından p için 2'yi, q için ise 5'i tercih ettikleri görülmüştür. Seçilen asal sayıların çarpımı ile mod değeri ikinci aşamada doğru bir şekilde bulunmuştur. Diğer çalışma

kâğıtlarında da öğrencilerin 2. ve 3. aşamaları doğru bir şekilde hesapladıkları belirlenmiştir. Dördüncü aşamada belirtilen ifadeyi öğrencinin doğru bir şekilde eşitsizlik haline getirdiği ve olası E değerlerinden "2"nin üzerini çizmiş olduğu görülmektedir. Buradan öğrencinin ortak çarpan bilgisini daha önceden yapılandırmış olduğu ortaya çıkmaktadır. Çalışmaya katılan diğer öğrencilerden sadece iki tanesinin E değeri için nasıl bir tercih yapacaklarını bilmedikleri gözlenmiş, bu konudaki zorluk arkadaşlarından yardım almaları sağlanarak ortadan kaldırılmıştır. Ortak çarpan olan bir değerin seçilmeme nedeni açıklanmış ve bu iki öğrencinin doğru E değerini seçerek işlemlerine devam etmeleri sağlanmıştır. Kongrüans denklemleri yardımıyla da bulunabilen E sayısının tersi, öğrencilerin bu konuyu üniversitede öğrenecekleri düşüncesi ile, beşinci adımdaki şekilde buldurulmuştur. Öğrencinin beşinci adımda gerekli D değerini bulabilmek için verilen ifadeden yola çıkarak denklemi doğru bir şekilde kurduğu ve D değerini doğru bir şekilde bulduğu görülmektedir. Bu noktada çalışmaya katılan öğrencilerden bir tanesinin D değeri için farklı birçok sonuç olabileceğini belirttiği, hangisini seçeceği konusunda kararsız kaldığı gözlenmiştir. Sıra arkadaşının *"E ile aynı olmayan en küçük değeri seç"* şeklindeki ifadesi üzerine öğrenciye herhangi bir müdahalede bulunulmamış, işlemlerine devam etmesi sağlanmıştır. Örnek 1'de görülen ve RSA şifrelemesinin alt yapısının kurulmasına yönelik adımın bütün öğrenciler tarafından başarılı bir şekilde tamamlandığı belirlenmiştir. Çalışma kâğıtlarının tamamının incelenmesi ile de öğrencilerin, asal sayı, aralarında asal olma, üs/kuvvet, eşitsizlik, mod ve ortak faktör kavramlarını yapılandırdıkları görülmüştür. Ayrıca mod

değerinin 10 olarak seçilmesinin işlem kolaylığı sağladığını ifade ettikleri çalışma esnasında gözlemlenmiştir.

Fasiküllerin ikinci aşamasında öğrencilerin, üs alma ve belirlenen mod değerine göre kalanı bulmaları beklenmektedir. Çalışmada öğrencilerin çoğunun üs alma ve kalan bulma işlemlerini sorunsuz bir şekilde buldukları görülmüştür.



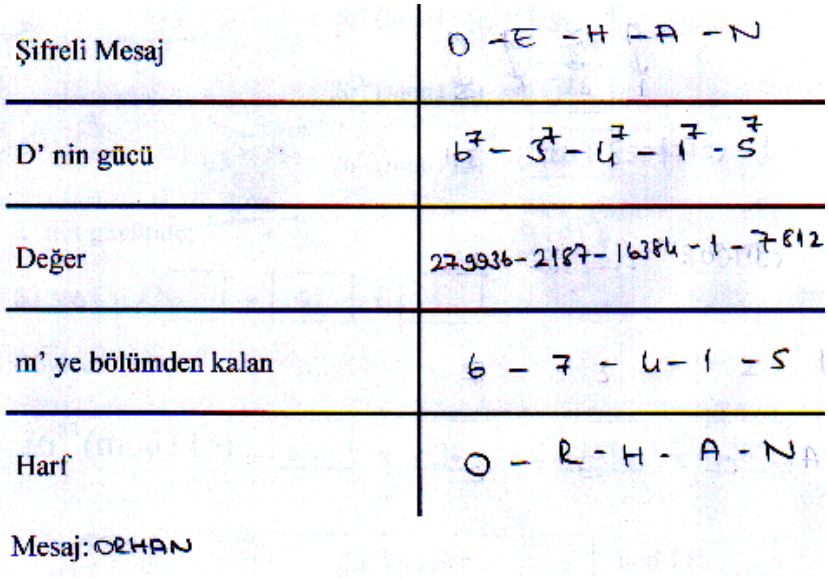
Örnek 2: RSA şifrelemesi kullanılarak şifreli metnin oluşturulması

Fasikülün ikinci bölümünde öğrencilerin daha önceden seçilmiş

harflerden yeni kelimeler oluşturarak şifrelemeleri beklenmektedir. Örnek 2'de mod = 10, şifrelemede kullanılacak E değeri 3 ve deşifre etmede kullanılacak olan D değeri 7 olarak belirlenmiştir. Öğrenci; A, D, E, H, N, O, R, S ve T harflerinden "TANER" kelimesini seçmiş ve şifrelemiştir. Seçtiği kelimenin ilk önce sayı değerlerini bulmuş, daha önceden belirlemiş olduğu E değerine göre de gerekli bütün değerleri hesaplamıştır. En son adımda m = 10 olacak şekilde 10'a bölümden kalanları hesaplamıştır. Mod 10'a bölümden kalanları bulmak için sadece son rakamları almak yeterlidir. Örnek 2'de öğrencinin kalanları doğru bir şekilde bulduğu görülmektedir. Kalan değerlerin harf karşılıkları yerine yazıldığında şifreli metin "TANRE" olarak bulunmuştur. Öğrencinin hem üs alma hem de mod'a göre kalan bulma işlemlerini doğru bir şekilde yaptığı görülmüştür. Çalışmaya katılan diğer öğrencilerin de gerekli olan bütün işlemleri sorunsuz bir şekilde tamamladığı görülmüştür. Mod değerini 10 olarak belirlemeyen iki öğrencinin "m'ye bölümden kalan" değerleri bulmak için uğraştıkları görülmüştür. Bu bağlamda mod'u 10 olarak seçen öğrencilerin "değer" sırasında buldukları sonuçların son rakamlarını direkt olarak yazdıkları, diğer iki öğrencinin ise modüler aritmetik işlemleri yaptıkları görülmüştür. Bu noktada her iki öğrencinin de zorlanmadığı, buldukları değerleri mod değerine bölerek kalanları kolayca buldukları belirlenmiştir.

Fasiküllerin deşifre yapılan bölümünde öğrencilerin şifreleme bölümünde olduğu gibi üs alma ve mod alma işlemlerini yapmaları beklenmektedir. Şifreleme bölümünde öğrencilerin modüler aritmetik konusunu hatırlamaları sağlanmıştır. Öğrenciler daha önceden öğren-

miş oldukları modüler aritmetik bilgisini hatırlamıştır. Özellikle mod değerini 10'dan farklı olarak belirleyen iki öğrencinin bulunan değerleri direk mod değerine bölerek kalanı buldukları görülmüştür. Bu bölümde ise hem hatırlanan bilgilerin pekiştirilmesi hem de şifreli metnin deşifresi amaçlanmaktadır. Çalışmaya katılan öğrencilerin ilk bölümdeki gibi kalan bulma işlemlerini hızlıca yapabildikleri görülmüştür.

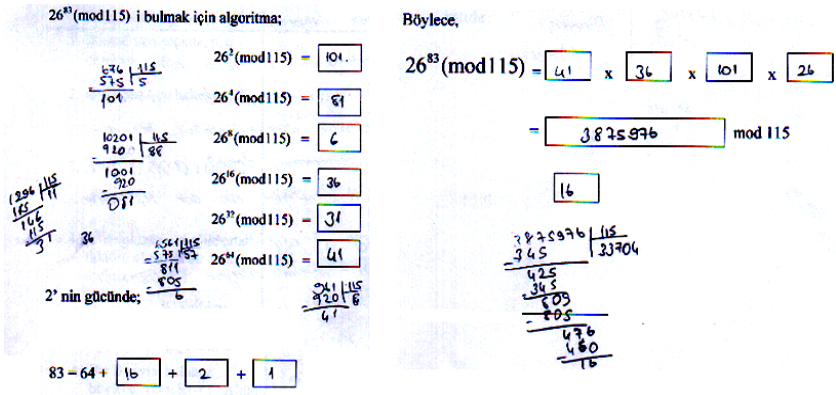


Örnek 3: Şifreli metnin deşifre edilmesi

Şifreli metin olan "OEHAN" deşifre edilmiştir ve şifrelenmiş olan metnin "ORHAN" olduğu bulunmuştur. Deşifrenin yapılabilmesi için RSA şifrelemesi için kurulan alt yapıdan D değerine göre işlemler gerçekleştirilmiş ve m'ye bölümden kalan değerlerinin örnek 3'te yanlışsız bir şekilde bulunduğu görülmüştür. Örnek 3'te de mod değe-

rinin 10 seçildiği, buna göre de kalanların direkt yazıldığı görülmüştür. Çalışmaya katılan diğer öğrencilerin de şifrelemiş oldukları metinleri doğru bir şekilde deşifre ettikleri belirlenmiştir. Böylece öğrencilerin modüler aritmetik bilgisini pekiştirdikleri söylenebilir. Ayrıca öğrenciler, şifreleme ve deşifre etme ile fasiküllerin dördüncü bölümünde yer alan ve büyük sayılardan oluşan modüler aritmetik işlemlerini kolaylıkla yapabilmeleri için de hazırlanmışlardır.

Fasiküllerin dördüncü bölümünde ise öğrencilerin modüler aritmetik bilgisini iyice pekiştirmeleri için mod değeri oldukça büyük seçilmiştir. Öğrencilerden fasikülde verilen örneği çözmelerini istemeden önce, var olan bilgilerini yoklamak ve hatırlatmak için, şifreleme ve deşifre etme bölümlerindekinden ayrı, $7^{11} \equiv x(\mathrm{mod}\,9)$ örneğini çözmeleri istenmiştir. Daha önceki örneklerde 10 olarak seçilen mod değeri (iki öğrenci önceki çalışmalarda mod değerini 10'a farklı seçmiştir) bu örnekte 9 seçilmiş ve 7^{11} ifadesinin değerini bulmada nasıl işlem yapabilecekleri gösterilmiştir. Çalışmaya katılan öğrencilerin tamamının verilen örneği kolaylıkla anladığı gözlenmiştir.



Örnek 4: Mod değeri büyük bir ifadenin sonuçlandırılması

Dördüncü bölümde beklenen, öğrencilerin mod değeri büyük bir ifadeyi çözümleyebilmeleridir. Örnek 4'te de görüldüğü gibi işlemler kolaylıkla yapılmış ve sonuç doğru bir şekilde bulunmuştur. Çalışmaya katılan diğer öğrencilerin de işlemleri doğru ve sorunsuz bir şekilde yaptıkları, sonuca sorunsuzca ulaştıkları görülmüştür. İşlemlerin bazı noktalarında zorluk çeken öğrencilerin ise arkadaşlarından yardım aldıkları ve işlemleri nasıl yapacakları yönünde tartıştıkları gözlenmiştir. Arkadaşlarının anlamalarını kolaylaştırmak için daha küçük sayıları seçerek örnek üzerinden zorlanılan noktaları açıklığa kavuşturdukları görülmüştür. Böylece öğrencilerin modüler aritmetik konusu ile ilgili mod gücü yükseltildiğinde karşılaştıkları zorlukları arkadaşlarından yardım alarak aştıkları ve konu ile ilgili olan eksikliklerini tamamladıkları görülmüştür.

Öğrencilerin sıra arkadaşlarının hazırladıkları şifreli mesajları deşifre etme sürecinde hem heyecanlandıkları hem de çalışmadan hoşlandıkları gözlenmiştir. Fasiküllerin en sonunda yer alan çalışma hakkındaki düşünceleriniz bölümünde ise öğrencilerin, daha önce böyle bir etkinlikle karşılaşmadıklarını, dersin eğlenceli geçtiğini, bundan sonra bilgisayarlarına veya cep telefonlarına daha zor şifreler üreteceklerini, hatta kendi isimlerine özgü bir şifreleme tekniği geliştireceklerini belirttikleri görülmüştür.

Sonuçlar ve Tartışma

Bu çalışmanın ana hedefi ortaöğretim on birinci sınıf öğrencilerinin daha önce öğrenmiş oldukları modüler aritmetik konusunu şifreleme etkinlikleri yardımıyla pekiştirmelerini incelemekti. Bu amaçla dört bölümden oluşan ve RSA şifreleme yöntemini içeren çalışma kâğıtları ile iki ders saatinde çalışma gerçekleştirilmiştir. Çalışma sürecinde öğrencilerin hâl ve hareketleri de gözlemlenmiştir. Çalışma süreci dikkate alınarak çalışmanın sonuçları dört başlık altında incelenebilir.

(i) RSA Şifreleme Algoritmasının Kurulması

Bu çalışma ile yapılan öğretimin tamamı etkinlik tabanlıdır. Çalışmanın her bölümüne öğrencilerin tamamı büyük ilgi göstermiştir. Etkinliğin ilk bölümünde RSA şifreleme algoritmasını kurmaya çalışırken asal sayı bilgisini doğru kullanmışlardır. Algoritmanın son adımı olan deşifre için gerekli değerin bulunması sırasında gözlenen zorlukları akran yardımı ile çözmüşlerdir. Bu esnada hem eğlenmişler hem de akran desteği alarak öğrenmişlerdir. Çalışmanın bu bölümünde öğrencilerin asal sayıların seçiminde, mod değerinin bulunmasında, şifreleme ve deşifre etme işlemleri için gerekli değerlerin bulunmasında tartışmışlar, fikirlerini açıkça ve özgürce ortaya koyabilmişlerdir. Böylece RSA şifrelemesinin algoritmasını bütün öğrenciler sorunsuz bir şekilde oluşturmuşlardır. Yılmaz'ın (2010) yaptığı "Kriptolojik Uygulamalarda Bazı İstatistiksel Testler" adlı tez çalışmasında RSA algoritmasının kurulum şeması detaylı bir şekilde verilmiştir. Yapılan bu çalışmada RSA algoritmasının bilgisayar uygulaması yer almakta-

dır. Yapılan bu çalışmada ise RSA algoritmasının modüler aritmetik konusunun hatırlanmasında ve pekiştirilmesinde kullanılmıştır. Bu yönüyle bu çalışmanın matematik eğitimi açısından önemli olduğu düşünülmektedir. Bahçetepe'nin (2006) yaptığı çalışmasında modüler çarpma işlemi ve kullanılan yöntemlerin sınıflandırılması üzerinde durulmuştur. Sayı sistemleri ve uygulama olarak seçilen RSA kripto sistemi ile ilgili temel bilgiler verilmiştir. Bu bağlamda yapılan bu çalışma ile benzerlikler göstermektedir. Fakat Bahçetepe'de RSA algoritmasının ortaöğretim düzeyinde analizini yapmamıştır. Aksuoğlu'nun (2010) çalışmasında asimetrik şifrelemenin en önemli sistemi olan RSA incelenmiştir. Yapılan çalışmada RSA sisteminin anahtar havuzunu genişleten fakat şifre açma (decryption) kısmını zaman bakımından yavaşlatan "Verimli RSA Şifreleme Şemasını" hızlandırmak için bazı şifre açma algoritmaları zaman karmaşıklıklarıyla (Büyük-O) beraber incelenmiş ve yeni bir algoritma önerilmiştir. Önerilen bu RSA algoritmasının nesne tabanlı programlama ile uygulaması yapılmış ve sonuçları birkaç RSA algoritması ile karşılaştırılmıştır. Yapılan bu çalışmada da herhangi bir eğitim uygulaması bulunmamaktadır.

(ii) Seçilen Açık Metinlerin Şifrelenmesi

Çalışma, etkinlik-çalışma kâğıtlarında daha önceden belirlenmiş olan (A, D, E, H, N, O, R, S, T) harfleri arasından oluşturulacak açık metin şifrelenmesi üzerine kurulmuştur. Öğrencilerin belirlenen harflerden çeşitli kelimeler/açık metinler türettikleri (örneğin, Taner, Hande, Orhan, Oda, Son, Ters, Arda, …v.b.) görülmüştür. Belirlemiş oldukları bu açık metinleri RSA şifreleme algoritmasına göre şifrele-

mişlerdir (Örneğin; Orhan – Oehan). Öğrencilerin şifreleme etkinliği esnasında üs alma işlemlerinde zorlandıkları noktalarda akranlarından yardım aldıkları veya hesap makinesi kullandıkları görülmüştür. Sonuç olarak, öğrencilerin seçtikleri açık metinleri doğru bir şekilde şifreledikleri görülmüştür. Şifreleme esnasında modüler aritmetik bilgisini kullandıkları bölümlerde zorlanmadıkları belirlenmiştir. Şifreleme işlemlerinin kolaylıkla yapılabilmesinin gözlemlenmesi sonucunda öğrencilerin, bu konu ile ilgili bilgi yapılarında bir derinleşme olduğu söylenebilir.

(iii) Şifreli Metinlerin Deşifre Edilmesi

Bir öğrenme durumunda oluşan yapıların kullanılması o yapıların pekişmesine yol açmaktadır. Çalışmanın bu bölümünde öğrencilerin, şifreledikleri açık metinleri deşifre etme esnasında kullanacakları modüler aritmetik bilgisi de bu yapılarının pekişmesine olanak sağlamaktadır.

Öğrenciler şifrelemiş oldukları açık metinleri çalışmanın ilk bölümünde oluşturmuş oldukları algoritma yardımıyla deşifre etmişlerdir. Deşifre etme esnasında yine üs alma ve modüler aritmetik bilgisine başvurmuşlardır. Bu da onların bu bilgi yapılarını pekiştirmelerine olanak sağlamıştır. Güler'in (2007) yaptığı çalışmada modüler aritmetik konusunun öğretiminde şifreleme aktivitelerinin matematik başarısına etkisini incelemiştir. Şifreleme aktiviteleri ile işlenen matematik dersi ile doğrudan anlatım yöntemi ile işlenen arasında şifreleme ile işlenen lehine anlamlı bir farklılık ortaya çıkmıştır. Şifreleme aktivitelerinin hatırlamayı kolaylaştırdığı görülmüştür. Öğrencilerin tutum-

larında da pozitif yönde değişiklikler bulunmuştur. Yapılan bu çalışma ile Güler'in çalışması öğrencilerin derse katılma durumları ve matematiğe karşı pozitif tutum sergileme açılarından benzerlikler göstermektedir. Çünkü yapılan bu çalışmada da öğrencilerin, etkinlikten hoşlandıkları ve olumlu tutum sergiledikleri görülmüştür. Bahadır ve Özdemir' in (2012) yaptıkları çalışmalarında da öğrencilerin olumlu tutum sergiledikleri belirlenmiştir.

(iv) Mod Değeri Büyük İfadelerde Kalan Bulma

Çalışmanın bu bölümünde öğrencilerin var olan bilgi yapılarının daha derinleşmesini ve pekişmesini sağlamak amaçlanmıştır. Daha basit sistemlerle açıklanan bu bölümdeki işlemleri öğrencilerin rahatlıkla kavradıkları, modüler aritmetik konusundaki bilgi eksikliklerini gidermeye çalıştıkları ve daha önceden oluşturmuş oldukları bilgi yapılarını pekiştirdikleri görülmüştür.

Kaynakça

Abken, S. B. ve Subaşı, A. (2005). RSA ve eliptik eğri algoritmasının performans karşılaştırması. *KSÜ Fen ve Mühendislik Dergisi, 8*(1), 35-40.

Aksuoğlu, A. (2010). *Rsa algoritmasının iyileştirilmesi için yeni bir yaklaşım*. Yayınlanmamış yüksek lisans tezi, Anadolu Üniversitesi Fen Bilimleri Enstitüsü.

Bahadır, E. ve Özdemir, A. Ş. (2012). Yer değiştirme şifrelemesi etkinliğinin uygulanabilirliğinin incelenmesi ve öğrencilerin etkinlikle ilgili görüşleri. *KALEM Uluslararası Eğitim ve İnsan*

Bilimleri Dergisi, 2(2), 51-90.

Bahçetepe, H. (2006). *Modüler çarpma algoritmalarinin incelenmesi ve kriptolojide uygulamalari*. Yayınlanmamış yüksek lisans tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü.

Çinem, C., Akyelek, S. ve Akyıldız, E. (2008). *Şifrelerin matematiği kriptografi*. Ankara: Odtü Yayıncılık.

Dujella, A. (2009). A variant of Wiener's attack on RSA. *Computing, 85*(1-2), 77–83.

Güler, E. (2007). Modüler aritmetik konusunun öğretiminde şifreleme aktivitelerinin matematik başarısına etkisi. Yayınlanmamış yüksek lisans tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü.

Kalaycı, T. E. (2003). *Bilgi teknolojilerinde güvenlik ve kriptografi*. Yayınlanmamış lisans tezi, Ege Üniversitesi Mühendislik Fakültesi.

Kirk, J. ve Miller, M. (1986). *Reliablity and validity in qualitative research*. Beverly Hills, CA: Sage Puplication.

Kodaz, H. ve Botsalı, F. M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Teknik - Online Dergi*, 9(1), 10-23.

Lucks, S. (2003). What is Cryptology? *Talk at the Summer School on*

"Datensicherheit",University of Mannheim. 04.02.2011, http://th.informatik.uni-mannheim.de/people/lucks/papers/SS1.pdf.

Şen, Ş. (2006). *İndirgenmiş spn (substitution permutation network) algoritması için lineer kriptanaliz uygulaması*, Yayınlanmamış yüksek lisans tezi. Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Yerlikaya, T., Buluş, E. ve Buluş, N. (2006, Şubat). *Asimetrik şifreleme algoritmalarında anahtar değişim sistemleri*. Akademik Bilişim, Denizli.

Yıldırım, A. ve Şimşek, H. (2006). *Sosyal bilimlerde nitel araştirma yöntemleri* (5. baskı). Ankara: Seçkin Yayıncılık.

Yılmaz, R. (2010). *Kriptolojik uygulamalarda bazı istatistik testler*. Yayınlanmamış yüksek lisans tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü.

http://en.wikipedia.org/wiki/Brute_force_attack, Encyclopedia of Wikipedia, "Brute force attack". (2008). siteye son erişim tarihi: 23.Mayıs.2013