Eğitim ve Bilim
2012, Cilt 37, Sayı 166

Education and Science
2012, Vol. 37, No 166

Yükseköğretime Geçiş Sınavı'nda Şifreleme İddiaları ve Adayların Şifrelemeyi Kullanıp Kullanmadığını Belirleyen Bir Yöntem Önerisi

Encryption Claims in Transition to Higher Education Exam and Proposing a Method to Determine Whether the Candidates Used the Encryption

M. Kadir DOĞAN*

Ankara Üniversitesi

Öz

2011 Yılı Yükseköğretime Geçiş Sınavı'nda soruların şifrelendiği, doğru cevaba sadece cevap seçenekleri kullanılarak erişilebildiği iddiaları ortaya atılmıştır. Bu çalışmanın amacı, söz konusu iddiayı istatistiksel olarak test etmektir. Dairesel mod şifreleme yönteminin uygulanabildiği matematik bölümündeki 31 soruda beklenen başarı oranının %58.7 (18.2 doğru cevap) olduğu tespit edilmiştir. İstatistiksel olarak milyonda birin altında hata payıyla sınavda şifreleme yapıldığı, şifreleme olmadan herhangi bir yöntemin bu kadar yüksek oranda başarı sağlayamayacağı sonucuna ulaşılmıştır. Ayrıca, iddia edildiği gibi, şifrelemenin cevap seçeneklerinin sehven kaydırılarak oluşturulması sonucu ortaya çıkması olası değildir. Çalışmada şifrelemenin adaylar tarafından kullanılıp kullanılmadığını tespit etmeyi sağlayan, eğer kullanılmışsa, kimler tarafından kullanıldığını belirleyen bir yöntem de önerilmektedir.

Anahtar Sözcükler: Öğrenci Seçme ve Yerleştirme Sistemi, Yükseköğretime Geçiş Sınavı, şifreleme.

Abstract

It is claimed that the questions were encrypted in the transition to higher education exam of year 2011, and thus the correct answers can be found by using the choices given under each question. The aim of this study is to test this claim statistically. The circular mode encryption method is applicable to 31 questions in math section and its expected success rate is %58.7 (18.2 correct answers). It is determined that the exam was encrypted with a probability of error less than one millionth. It can be concluded that no method can reach such high success rate without any encryption. Also, it is not possible that encryption arises as a result of shifting the choices of questions inadvertently when forming the new choices. The study also proposes a method to determine whether the encryption is used by candidates or not, and if used, the method states the candidates have used it.

Keywords: Student selection and placement system, transition to higher education exam, encryption

Summary

Purpose

This study has two aims. The first aim is to test the claim that the questions were encrypted in the transition to higher education exam of year 2011, and thus the correct answers can be found by using the choices given under each question. The second aim is to propose a method to determine whether the encryption is used by the candidates or not, and if used, to point at the candidates using it. We tested the validity of circular mode encryption method (DMS). In this

* Yrd. Doç. Dr. M. Kadir DOĞAN, Ankara Üniversitesi, Siyasal Bilgiler Fakültesi, İktisat Bölümü, doganmk@politics.ankara.edu.tr

method, the choices are sorted in ascending order and compared with the original order. If only one choice matches, the method predicts it as the correct answer. If the entire choices match, the method predicts the choice with the lowest value as the correct answer. Otherwise, the choice at the end is shifted to the first choice and the procedure repeats.

An important fact on exam is that the choices of questions are formed by shifting them in exam booklets. Hence, if the circular mode encryption method is applied in the exam, it can be valid for all f othe booklets.

The values in choices can be ordered in 120 different ways. By taking the lowest choices as reference points, there exist 24 general orderings so that all the 120 orderings can be obtained by them by shifting the choices. We computed the predictions of DMS for the general orderings.

Results

The predictions of DMS are determined for 31 applicable questions in the math section. These predictions are compared with the correct answers and it is found that the expected success rate of DMS is %58.7 (18.2 correct answers in 31 questions). We applied a hypothesis testing procedure to determine whether this success rate can be reached without an encryption or not. The test statistics is 5.39 and the associated p-value is 0.000000036. We conclude that the exam was encrypted and no method can reach such high success rate without an encryption with a Type I error less than one millionth.

Discussion

We also propose a method to determine whether the encryption is used by candidates or not, and if used, to state the candidates using it. This method is based on the investigations of candidates' answers on questions 1, 5, 9, 16, 17 and 30. DMS predicts correct answers for some of these questions and wrong answers for some of them depending on the orderings of the choices of these questions in the exam booklets. We conclude that if a candidate answers all the questions as DMS predicts (some of them are wrong answers), he or she probably uses encryption methods to solve the questions and thus the answers of this candidate for the other questions must also be investigated.

Conclusion

This study concludes that the transition to higher education exam of year 2011 was encrypted. Also, it is not possible that encryption arises as a result of shifting the choices of questions inadvertently when forming new choices. The method that we proposed can determine whether any candidate used encryption methods to solve the exam. Also, note that our method can be used to analyze any encrypted exam just by changing the investigated questions.

Giriş

Türkiye'de üniversitelerde eğitim görecek öğrencileri seçmek ve yerleştirmek Ölçme, Seçme ve Yerleştirme Merkezinin (ÖSYM) görevidir. ÖSYM, her sene bazı sınav(lar) düzenleyerek adayları sınavlardan aldıkları puanlara, ortaöğretimdeki başarı düzeylerine, bildirmiş oldukları tercihlere ve üniversite programlarının kontenjanlarına bağlı olarak üniversitelere yerleştirmektedir. Öğrenci Seçme ve Yerleştirme Sistemi'nde (ÖSYS) sürekli yeni düzenlemeler yapılmaktadır.** 1999 yılından itibaren uygulanan tek aşamalı sınav sistemi 2010 yılında değiştirilerek iki aşamalı sınav sistemine geçilmiştir. Sınavlar Yükseköğretime Geçiş Sınavı (YGS) ile Lisans Yerleştirme Sınavı'ndan (LYS) oluşmaktadır. 2011 yılında sınav güvenliğini artırmak için YGS'de "adaya özgü sınav kitapçığı" uygulaması gerçekleştirilmiştir. Her adaya soruların ve cevap seçeneklerinin yerleri değiştirilerek farklı bir kitapçık verilmiştir. Adaya özgü sınav kitapçığı uygulamasının bazı adayların lehine, bazı adayların ise aleyhine sonuçlar doğurarak sınavın geçerliliğini ve güvenilirliğini tehlikeye attığı

** Tezbaşaran (2004), ÖSYS'de 1960-2004 arasında gerçekleşen değişimi anlatmaktadır.

eğitimbilimciler tarafından belirtilmektedir.*** Adaya özgü sınav kitapçığı uygulaması beraberinde sınavda şifreleme iddialarını gündeme getirmiştir. Soruların şifrelenmesi, doğru cevapların seçeneklerde belli bir yönteme göre yerleştirildiği ve bu yöntem kullanıldığında sadece cevap seçeneklerine bakılarak doğru cevaba erişilebilmesi anlamına gelmektedir.

Bu çalışmanın iki amacı bulunmaktadır. Bunlardan ilki, 2011 yılı Yükseköğretime Geçiş Sınavı'nda adaylara dağıtılan *tüm* kitapçıklarda bazı yöntemler kullanılarak doğru çözümlere ulaşılabileceği (yani, cevap seçeneklerinin belli bir şifreye göre yerleştirildiği) iddiasını istatistiksel olarak test etmektir. İkinci amaç ise sınavda uygulanan bir şifre varsa, şifrenin adaylar tarafından kullanılıp kullanmadığını, eğer kullanılmışsa kimler tarafından kullanıldığını tespit eden bir yöntem önermektir.

Bu çalışmada, cevap seçeneklerinin belli bir şifreye göre yerleştirilip yerleştirilmediğini araştırmak üzere sınav sonrası kamuoyunda öne çıkan dairesel mod şifreleme yönteminin en basit halinin geçerliliği test edilecektir.****

Dairesel Mod Şifreleme Yöntemi

Bu yöntem şöyle işlemektedir: "Cevap seçenekleri küçükten büyüğe dizilirler ve soru kitapçığındaki orijinal sıralama ile karşılaştırılırlar. Sadece bir seçenek kesişiyorsa, o seçenek doğru cevaptır. Eğer birden fazla çakışan cevap seçeneği varsa veya çakışan hiçbir cevap seçeneği yoksa verilen sıralamayı sağa doğru kaydırarak (yani, sondaki cevap seçeneğini en başa alarak) elde edilen sıralamayla karşılaştırma işlemi tekrarlanır. Bu şekilde sadece bir seçenek çakışıncaya kadar ilerlenir. Eğer beş seçenek birden çakışıyorsa (cevap seçeneklerinin sıralaması küçükten büyüğe doğru ise) doğru cevap en küçük değere sahip olan seçenektir."

Dairesel mod şifreleme yöntemi uygulansa bile tüm adayların kitapçıklarında geçerli olabilmesi için cevap seçeneklerinin ana (master) kitapçıktan (veya basına dağıtılan kitapçıktan) *kaydırılarak* türetilmesi gerekmektedir. Aksi halde, yani cevap seçenekleri kaydırılarak değil de tamamen tesadüfi olarak belirleniyorsa, dairesel mod şifreleme basına dağıtılan kitapçıkta geçerli olsa bile tüm kitapçıklar için geçerli olamayacaktır.

Cevap Seçeneklerinin Kaydırılarak Belirlenmesi

Cevap seçeneklerinin kaydırılarak belirlenmesini Örnek 1 aracılığıyla açıklayalım.

Örnek 1: Bir sorunun cevap seçenekleri "a)2 b)4 c)0 d)8 e)6" ise, bu sorunun cevap seçeneklerinin diğer kitapçıklarda kaydırılarak belirlenmesi, diğer kitapçıklardaki cevap seçeneklerinin ancak şu beş sıralamadan birisi olabileceği anlamına gelmektedir.

1. "a)2 b)4 c)0 d)8 e)6"
2. "a)6 b)2 c)4 d)0 e)8"
3. "a)8 b)6 c)2 d)4 e)0"
4. "a)0 b)8 c)6 d)2 e)4"
5. "a)4 a)0 b)8 c)6 d)2"

1. sıralama zaten verilen sıralamadır. 2. sıralama 1. sıralamanın 'e' seçeneğindeki 6 cevabı 'a' seçeneğine ve "a,b,c,d" seçenekleri de sırasıyla "b,c,d,e" seçeneklerine kaydırılarak oluşturulmuştur. 3. sıralama 2. sıralamanın 'e' seçeneği, 'a' seçeneğine ve 'a,b,c,d' seçenekleri de sırasıyla "b,c,d,e" seçeneklerine kaydırılarak elde edilmiştir. Benzer şekilde 4. sıralama üçüncüden, 5. sıralama da dördüncüden elde edilebilir. Öte yandan seçenekler tamamen tesadüfî olarak belirlense "2, 4, 0, 8, 6" seçenekleri 5! (yani, 120) farklı şeklide sıralanabilir. Kaydırılarak belirlemeye göre ise sadece beş farklı şekilde sıralanabilmektedir.

*** Bkz. i)Ankara Üniversitesi Eğitim Bilimleri Fakültesi'nin YGS Hakkında Görüşü, Ankara Üniversitesi (2011), ii) 2011 Yılı Yükseköğretime Geçiş Sınavı Hakkında ODTÜ Eğitim Fakültesi Görüşü, ODTÜ (2011) ve iii) 45 ölçme-değerlendirmeci akademisyenin imzalayarak kamuoyuna duyurduğu metin. (http://www.abbasguclu.com.tr/ egitim/ iste_konunun_uzmani_45_bilim_adaminin_sifre_aciklamasi.html. Erişim tarihi: 6 Mart 2012)

**** Şifreleme yöntemleri hakkında detaylı bilgi için bkz. Buchmann (2004) ve Mollin(2007).

YGS'de cevap seçenekleri kaydırılarak belirlenmektedir. Aday kitapçıkları internete yüklendikten sonra 11247.98420 ile 11314.27133 numaralar arasındaki yüzlerce kitapçık üzerinde yaptığım incelemede adayların kitapçıklarındaki cevap seçeneklerinin basına dağıtılan kopyadaki seçeneklerden kaydırılarak belirlendiği ve sadece beş farklı sıralamadan biri olduğu tespit edilmiştir. Ayrıca, ÖSYM başlangıçta bu durumu kabul etmemesine rağmen 11 Nisan 2011 tarihinde adaylara gönderdiği e-postada cevap seçeneklerinin sehven kaydırılarak belirlendiğini kabul etmiştir. Yani, seçeneklerin kaydırılarak oluşturulması ÖSYM'nin algoritmasıdır. Lakin şifrelemenin cevap seçeneklerinin kaydırılması sonucu oluştuğunu iddia etmek yersizdir; çünkü cevap seçeneklerinin kaydırılması ancak bir şifre yöntemi kullanılıyorsa onun tüm adayların kitapçıklarında geçerli olmasını sağlayabilecektir.

Cevap seçenekleri kaydırılarak oluşturulduğuna göre, eğer doğru cevaplar dairesel mod şifreleme yöntemine göre şifrelenmişe, sadece basına dağıtılan kitapçık için değil, *tüm aday kitapçıkları* için geçerli olacaktır.

Yöntem

Soruların dairesel mod yöntemine göre nasıl şifrelenebileceğini açıklayabilmek için öncelikle aşağıdaki bölümde cevap seçeneklerinin nasıl sıralanabileceği belirlenmiştir. Daha sonraki bölümde ise bu sıralamaların (kombinasyonların) her biri için dairesel mod şifreleme yönteminin tahmini hesaplanmıştır.

Cevap Seçeneklerinin Genel Sıralaması

Cevap seçeneklerinde verilecek beş değer 120 farklı şekilde sıralanabilir. Yani, cevap seçeneklerinin en küçüğüne a1, en küçük ikinci seçeneğe a2, ve bu şekilde ilerleyerek en büyük seçeneğe a5 dersek, a1, a2, a3, a4 ve a5 değerleri 120 farklı şekilde sıralanabilir. a1'i referans (ilk değer) alırsak, farklı 120 sıralama Tablo 1'de verilen 24 genel sıralamanın kaydırılmasından elde edilebilir.

Diğer bir deyişle;

i) YGS'deki her sorunun cevap seçeneklerinin Tablo 1'de verilen 24 genel sıralamadan (GS) birine denk gelen bir genel sıralaması vardır.

ii) Bir sorunun cevap seçenekleri herhangi bir adayın kitapçığında ancak ve ancak sahip olduğu genel sıralamadan kaydırılarak elde edilen beş farklı sıralamadan birisi olabilir.

Tablo 1.

Cevap Seçeneklerinin Sahip Olabileceği Genel Sıralamalar

No	Genel Sıralama (GS)					No	Genel Sıralama (GS)				
1	a1	a2	a3	a4	a5	13	a1	a4	a2	a3	a5
2	a1	a2	a3	a5	a4	14	a1	a4	a2	a5	a3
3	a1	a2	a4	a3	a5	15	a1	a4	a3	a2	a5
4	a1	a2	a4	a5	a3	16	a1	a4	a3	a5	a2
5	a1	a2	a5	a3	a4	17	a1	a4	a5	a2	a3
6	a1	a2	a5	a4	a3	18	a1	a4	a5	a3	a2
7	a1	a3	a2	a4	a5	19	a1	a5	a2	a3	a4
8	a1	a3	a2	a5	a4	20	a1	a5	a2	a4	a3
9	a1	a3	a4	a2	a5	21	a1	a5	a3	a2	a4
10	a1	a3	a4	a5	a2	22	a1	a5	a3	a4	a2
11	a1	a3	a5	a2	a4	23	a1	a5	a4	a2	a3
12	a1	a3	a5	a4	a2	24	a1	a5	a4	a3	a2

Tablo 1'deki a1, a2, a3, a4 ve a5'in ne ifade ettiğini tekrar etmek gerekirse, a1, seçeneklerdeki en küçük değeri; a2, seçeneklerdeki en küçük ikinci değeri; a3, seçeneklerdeki en küçük üçüncü değeri; a4, seçeneklerdeki en küçük dördüncü değeri ve a5, seçeneklerdeki en büyük değeri belirtmektedir.

Örnek 2: ÖSYM'nin basına dağıttığı kitapçıktaki matematik bölümünün birinci sorusunda seçenekler sırasıyla 8, 10, 6, 4 ve 2'dir. Bu soruda, a1=2; a2=4; a3=6; a4=8 ve a5=10'dur. Buna göre seçeneklerin sıralaması a4-a5-a3-a2-a1'dir. Bu sıralamayı a1'i en başa gelecek şekilde kaydırırsak Tablo 1'deki 18 no'lu a1-a4-a5-a3-a2 genel sıralamasını elde ederiz. Yani bu sorunun cevap seçeneklerinin sahip olduğu genel sıralama 18 no'lu GS'dir. Bu sorunun cevap seçenekleri tüm kitapçıklarda (kaydırılarak elde edildiği için) 18 no'lu GS'den elde edilecek sıralamalara sahip olacaktır. Herhangi bir kitapçıkta bu sorunun cevap seçenekleri şu beş sıralamadan birisine sahip olacaktır.

1. a1-a4-a5-a3-a2 (yani; 2,8,10,6,4)
2. a2-a1-a4-a5-a3 (yani; 4,2,8,10,6)
3. a3-a2-a1-a4-a5 (yani; 6,4,2,8,10)
4. a5-a3-a2-a1-a4 (yani; 10,6,4,2,8)
5. a4-a5-a3-a2-a1 (yani; 8,10,6,4,2)

Dairesel Mod Şifreleme Yönteminin Tahmininin Belirlenmesi

Dairesel mod şifreleme (DMS diyelim) yönteminin Tablo 1'de verilen genel sıralamalara verdiği tahminler hesaplanarak Tablo 2'de verilmiştir.

Tablo 2.

Genel Sıralamalar İçin DMS Tahminleri

No	Genel Sıralama					DMS Tahmini
1	a1	a2	a3	a4	a5	a1
2	a1	a2	a3	a5	a4	a5
3	a1	a2	a4	a3	a5	%60a3 - %40a4
4	a1	a2	a4	a5	a3	a3
5	a1	a2	a5	a3	a4	a5
6	a1	a2	a5	a4	a3	%20a3 - %80a5
7	a1	a3	a2	a4	a5	%60a2 - %40a3
8	a1	a3	a2	a5	a4	a1
9	a1	a3	a4	a2	a5	a2
10	a1	a3	a4	a5	a2	%60a1 - %40a2
11	a1	a3	a5	a2	a4	%20a1-%20a3-%20a5-%20a2-%20a4
12	a1	a3	a5	a4	a2	a3
13	a1	a4	a2	a3	a5	a4
14	a1	a4	a2	a5	a3	%20a1-%20a5-%20a4-%20a3-%20a2
15	a1	a4	a3	a2	a5	%20a2 - %80a4
16	a1	a4	a3	a5	a2	a5
17	a1	a4	a5	a2	a3	a1
18	a1	a4	a5	a3	a2	%20a1 - %80a3
19	a1	a5	a2	a3	a4	%40a1 - %60a5
20	a1	a5	a2	a4	a3	a2
21	a1	a5	a3	a2	a4	a4
22	a1	a5	a3	a4	a2	%80a2 - %20a5
23	a1	a5	a4	a2	a3	%80a1 - %20a4
24	a1	a5	a4	a3	a2	%20a1-%20a4-%20a2-%20a5-%20a3

Tablo 2'de belirtilen DMS tahminlerinin nasıl hesaplandıkları aşağıdaki iki örnekle anlatılmıştır.

Örnek 3: 9 numaralı GS: a1-a3-a4-a2-a5

DMS'ye göre bu sıralama, küçükten büyüğe sıralama ile karşılaştırılmaktadır. Tek bir çakışan varsa bu değer DMS tahmini olmaktadır. Aksi halde sondaki seçenek en başa kaydırılarak bu işlem tekrarlanmaktadır. DMS tahminin hesaplanması Tablo 3'te gösterilmiştir.

Tablo 3.

9 Numaralı GS İçin DMS Tahminin Hesaplanması

Küçükten Büyüğe Sıralama	a1	a2	a3	a4	a5
Sıralama 1	a1	a3	a4	a2	a5
Sıralama 2	a5	a1	a3	a4	a2
Sıralama 3	a2	a5	a1	a3	a4
Sıralama 4	a4	a2	a5	a1	a3
Sıralama 5	a3	a4	a2	a5	a1

9 no'lu GS'ye DMS'nin tek bir tahmini mevcuttur: a2. Bu tahmine soru kitapçığında sıralama, a4-a2-a5-a1-a3 olarak verilmişse direkt karşılaştırma sonucu, a3-a4-a2-a5-a1 olarak verilmişse dört yineleme (iterasyon) sonrası, a1-a3-a4-a2-a5 olarak verilmişse üç yineleme sonrası, a5-a1-a3-a4-a2 olarak verilmişse iki yineleme sonrası ve a2-a5-a1-a3-a4 olarak verilmişse bir yineleme sonrası erişilebilmektedir. Yani, 9 no'lu GS'nin cevap seçeneklerinin hangi sıralamayla verilmesi elde edilen tahmini etkilemeyecek olup sadece tahmini bulmakta yapılması gereken yineleme sayısını ve geçen zamanı etkileyecektir.

Örnek 4: 18'lu GS: a1-a4-a5-a3-a2

Tablo 4.

18 Numaralı GS İçin DMS Tahmininin Hesaplanması

Küçükten Büyüğe Sıralama	a1	a2	a3	a4	a5
Sıralama 1	a1	a4	a5	a3	a2
Sıralama 2	a2	a1	a4	a5	a3
Sıralama 3	a3	a2	a1	a4	a5
Sıralama 4	a5	a3	a2	a1	a4
Sıralama 5	a4	a5	a3	a2	a1

18 numaralı GS için DMS tahmininin hesaplanması Tablo 4'te verilmiştir. DMS'nin bu genel sıralama için muhtemel iki tahmini vardır. Eğer sıralama a1-a4-a5-a3-a2 olarak verilirse, direk karşılaştırma sonucunda a1 tahminine ulaşılmaktadır. Bunun dışındaki muhtemel dört sıralamadan biri olarak verilmesi halinde ise DMS'nin tahmini a3 olacaktır. Eğer sıralama a2-a1-a4-a5-a3 olarak verilmişse üç yineleme sonrası, a3-a2-a1-a4-a5 olarak verilmişse iki yineleme sonrası, a5-a3-a2-a1-a4 olarak verilmişse bir yineleme sonrası ve a3-a2-a1-a4- a5 olarak verilmişse direkt karşılaştırma sonucu a3 cevabına erişilebilmektedir. Yani, DMS muhtemel beş sıralamanın dördünde a3 tahmin ederken, birisinde a1 tahmin etmektedir. O halde, DMS herhangi bir kitapçıkta bu genel sıralamada gelen bir soruya 4/5 (%80) ihtimalle a3 ve 1/5 (%20) ihtimalle a1 seçeneğini doğru cevap olarak tahmin edecektir.

Tablo 2'ye göre DMS'nin tahmini 1, 8 ve 17 no'lu GS'lerde a1; 9 ve 20 no'lu GS'lerde a2; 4 ve 12 no'lu GS'lerde a3; 13 ve 21 no'lu GS'lerde a4; 2, 5 ve 16' no'lu GS'lerde a5 olmaktadır. Yani, DMS yöntemi 24 genel sıralamanın 12'si için kitapçıklardaki muhtemel farklı sıralamalarına bağlı olmaksızın tek bir cevap seçeneğini doğru cevap olarak tahmin etmektedir.

3, 6, 7, 10, 15, 18, 19, 22 ve 23 no'lu genel sıralamalar için DMS'nin tahmini, genel sıralamaların verilebileceği muhtemel beş sıralamaya göre iki değerden birini almaktadır. Örneğin, 3 no'lu GS eğer a1-a2-a4-a3-a5 veya a5-a1-a2-a4-a3 olarak verilirse, DMS a4

seçeneğini tahmini etmekte; diğer sıralamalarda (a3-a5-a1-a2-a4, a4-a3-a5-a1-a2, a2-a4-a3-a5-a1) verilirse, DMS a3 seçeneğini tahmin etmektedir. Dolayısıyla, herhangi bir kitapçıkta 3 no'lu GS'den bir soru için DMS tahmini %60 ihtimalle a3 ve %40 ihtimalle a4 olacaktır. 11, 14, ve 24 no'lu GS'lerde DMS tahmini tam olarak verilen sıralamaya bağlıdır. Yani, beş muhtemel sıralamanın her bir için ayrı bir cevap seçeneğini tahmin etmektedir.

YGS Matematik Testinin Değerlendirilmesi

Bu bölümde YGS matematik testindeki soruların her biri için DMS tahmini belirlenmektedir. Daha sonra her soru için elde edilen DMS tahmini doğru cevap ile kıyaslanarak tahminin başarı oranı hesaplanmaktadır. Sorular ÖSYM'nin basına dağıttığı kitapçıktaki sırayla değerlendirilmektedir. Ancak, dikkat ediniz ki DMS tahmininin elde edilen başarı oranı ÖSYM'nin basına dağıttığı kitapçık için değil, YGS'de adaylara dağıtılan rasgele bir kitapçık için olacaktır. Çünkü, DMS tahmininin başarı oranı hesaplanırken, ÖSYM'nin basına dağıttığı kitapçıktaki sıralama değil, o sıralamadan kaydırılarak oluşturulabilecek tüm sıralamaları kapsayan genel sıralama kullanılmıştır.

Sorular Tablo 5'te sırasıyla incelenmiştir. Tablo 5'te öncelikle her sorunun seçenekleri, daha sonra bu seçeneklerin en küçüğü a1, ..., en büyüğü a5 ile ifade edilerek bu terimlere göre seçeneklerin sıralaması verilmiştir. Üçüncü olarak bu sıralamanın bağlı olduğu genel sıralama, daha sonra genel sıralamanın Tablo 2'deki numarası ve DMS'nin söz konusu genel sıralama için Tablo 2'de belirtilen tahmini verilmiştir. Son olarak sorunun doğru cevabı ve DMS tahmininin başarı oranı verilmiştir. Tablo 5'te 31 adet soru değerlendirilirken dokuz adet soru (6, 10, 18, 20, 25, 37, 38, 39 ve 40 numaralı sorular) cevap seçeneklerindeki değerlerden ötürü DMS yöntemi uygulanamadığı için değerlendirme dışı bırakılmıştır.

Bulgular

Tablo 5 incelendiğinde, YGS matematik bölümünde de cevap seçeneklerinin dağılımı muhtemel 24 genel sıralamadan on ikisine (5, 6, 7, 9, 11, 12, 14, 15, 16, 21, 22 ve 24 numaralı olanlar) uyan hiç soru çıkmadığı görülmektedir. Öte yandan 1 ve 18 no'lu GS'lerden altışar soru sorulmuştur. Sınavda 10 no'lu GS'den dört soru; 23 no'lu GS'den üç soru; 3, 4,17 ve 19 no'lu GS'lerden ikişer soru ve 2, 8, 13 ve 20 no'lu GS'lerden birer soru bulunmaktadır.

31 sorudan aynı genel sıralamaya sahip altı soru olma ihtimali binde 1.33 olup, iki farklı genel sıralamadan altışar soru çıkma ihtimali oldukça düşüktür. Kaldı ki 1 no'lu GS'den çıkan altı sorunun tamamının doğru cevabı DMS tahmini olan a1 seçeneği ve 18 no'lu GS'den çıkan altı sorunun tamamının doğru cevabı da DMS'nin %80 ihtimalle öngördüğü a3 seçeneğidir. Bunların her birinin tesadüfi olup olamayacağı hakkında yapılan istatistiksel testleri vermek yerine, DMS tahmininde beklenen doğru cevap sayısına tesadüfi erişilip erişilemeyeceği hakkında yapılan test alttaki bölümde verilmiştir. Ancak bu noktada şu konuyu vurgulamak isterim: ÖSYM Başkanı'nın 11 Nisan 2011 tarihinde adaylara gönderdiği ve şifreyi kısmen kabullendiği e-postada, sınavda aslında şifre kullanılmadığı ama cevap seçeneklerinin "sehven" kaydırılarak oluşturulduğu, bunun sonucunda da bazı soruların yanıtına sadece cevap seçenekleri kullanılarak erişilebildiği belirtilmiştir. Halbuki, cevap seçeneklerinin kaydırılarak elde edilmesi sadece eğer bir şifre varsa, bunun tüm kitapçıklar için geçerli olmasını sağlayabilir; eğer şifre kullanılmamışsa, cevap seçenekleri sehven kaydırılarak da elde edilse, doğru cevaplara bir yöntem aracılığıyla erişilmesi mümkün olmayacaktır. Örneğin, 1 no'lu GS'den çıkan altı sorunun doğru cevaplarının tamamı a1 olmayıp tesadüfi olarak dağılsa veya 18 no'lu GS'den çıkan altı sorunun doğru cevaplarının tamamı a3 olmayıp tesadüfi olarak dağılsa, cevap seçenekleri sehven kaydırılarak elde edilse dahi şifre yöntemleri kullanılarak bu sorularda doğru cevaplara erişmek mümkün olmayacaktır.

Tablo 5.

YGS Matematik Bölümündeki Soruların İncelenmesi

Soru No	Seçenekler (a)	(b)	(c)	(d)	(e)	Sıralama					Genel Sıralama					GS No	DMS Tahmini	Doğru Cevap	Başarı Oranı
1	8	10	6	4	2	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (6)	80%
2	0.1	0.2	0.5	1	2	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (0.1)	100%
3	2	6	-1	0	-2	a4	a5	a2	a3	a1	a1	a4	a5	a2	a3	17	a1	a1 (-2)	100%
4	1004	1008	1000	1006	1002	a3	a5	a1	a4	a2	a1	a4	a2	a3	a5	13	a4	a4 (1006)	100%
5	15	16	9	8	4	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (9)	80%
7	21	7	5	10	14	a5	a2	a1	a3	a4	a1	a3	a4	a5	a2	10	%60a1-%40a2	a2 (7)	40%
8	8	9	6	3	4	a4	a5	a3	a1	a2	a1	a2	a4	a5	a3	4	a3	a3 (6)	100%
9	2	4	1	1/2	1/4	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (1)	80%
11	-2	-1	0	1	4	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (-2)	100%
12	Y1	Y3	1v2	1v3	2v3	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (Y1)	100%
13	12	9	15	13	11	a3	a1	a5	a4	a2	a1	a5	a4	a2	a3	23	%80a1-%20a4	a4 (13)	20%
14	9	10	8	12	15	a2	a3	a1	a4	a5	a1	a4	a5	a2	a3	17	a1	a5 (15)	0
15	1v3	Y1	1v2	Y3	1,2v3	a4	a1	a3	a2	a5	a1	a3	a2	a5	a4	8	a1	a3 (1v2)	0
16	8	9	6	5	4	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (6)	80%
17	8	9	7	6	5	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (7)	80%
19	2/3	-1	-1/2	0	2	a4	a1	a2	a3	a5	a1	a2	a3	a5	a4	2	a5	a1 (0)	0
21	1v2	Y1	1,2v3	1v3	Y2	a3	a1	a5	a4	a2	a1	a5	a4	a2	a3	23	%80a1-%20a4	a4 (1v3)	20%
22	50	30	45	40	20	a5	a2	a4	a3	a1	a1	a5	a2	a4	a3	20	a2	a2 (30)	100%
23	10	11	12	13	14	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (10)	100%
24	60	40	30	45	55	a5	a2	a1	a3	a4	a1	a3	a4	a5	a2	10	%60a1-%40a2	a2 (40)	40%
26	180	60	45	90	120	a5	a2	a1	a3	a4	a1	a3	a4	a5	a2	10	%60a1-%40a2	a2 (60)	40%
27	3	5	1	2	4	a3	a5	a1	a2	a4	a1	a2	a4	a3	a5	3	%60a3-%40a4	a2 (2)	0
28	12	14	15	16	18	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (12)	100%
29	1v3	Y1	1,2v3	2v3	1v2	a3	a1	a5	a4	a2	a1	a5	a4	a2	a3	23	%80a1-%20a4	a4 (2v3)	20%
30	2.5	3	2	1.5	1	a4	a5	a3	a2	a1	a1	a4	a5	a3	a2	18	%20a1-%80a3	a3 (2)	80%
31	17.5	17.6	18	17	18.6	a2	a3	a4	a1	a5	a1	a5	a2	a3	a4	19	%40a1-%60a5	a5 (18.6)	60%
32	32	24	21	28	30	a5	a2	a1	a3	a4	a1	a3	a4	a5	a2	10	%60a1-%40a2	a2 (24)	40%
33	30	40	20	25	35	a3	a5	a1	a2	a4	a1	a2	a4	a3	a5	3	%60a3-%40a4	a2 (25)	0
34	105	110	115	120	125	a1	a2	a3	a4	a5	a1	a2	a3	a4	a5	1	a1	a1 (105)	100%
35	7/2	8/3	2	5/2	3	a5	a3	a1	a2	a4	a1	a2	a4	a5	a3	4	a3	a4 (3)	0
36	10	12	14	9	15	a2	a3	a4	a1	a5	a1	a5	a2	a3	a4	19	%40a1-%60a5	a5 (15)	60%

Dairesel Mod Sistemi (DMS) Tahmininin Başarısı

Tablo 5'in son sütununda her soru için verilen DMS tahmininin başarı oranları kullanılarak DMS'nin tahmin edeceği doğru cevap sayısının beklenen değeri 18.2 ve DMS tahmininin beklenen başarı oranı 58.7% olarak hesaplanmıştır. Yani, rasgele seçilen herhangi bir kitapçıkta DMS yöntemine göre soruları cevaplayan bir adayın 31 soruda elde edeceği doğru cevap sayısının beklenen değeri 18.2'dir. Herhangi bir kitapçıktaki yöntemin uygulanabildiği herhangi bir soru DMS yöntemine göre cevaplandığında, doğru cevaplanma olasılığı %58.7'dir.

Öte yandan rasgele seçilen bir kitapçıkta soruları rasgele cevaplayan bir adayın elde edeceği doğru sayısının beklenen değeri 6.2'dir. Herhangi bir soru rasgele cevaplandığında doğru cevaplanma olasılığı (beş cevap seçeneği olduğu için) %20'dir.

DMS yönteminin yüksek başarı oranı tesadüfi olabilir mi? (Yani, sınavda bir şifreleme olmadan bir yöntem bu oranda başarıyla doğru cevabı bulabilir mi?)

DMS yönteminin tahmininin beklenen değerinin, tesadüfi cevaplamanın beklenen değerinden farklı olup olmadığı istatistiksel olarak şöyle test edilebilir: n tane sorunun k tanesini doğru cevaplama olasılığı Binom olasılık dağılımına göre hesaplanır. Tesadüfi yöntemle başarı elde etme (doğru cevaplama olasılığı) p=0.2'dir. n yüksek olduğunda (yirmiden büyük olması) ve np ile $n(1-p)$ değerlerinin beşten büyük olması durumunda Binom dağılım, ortalaması np ve varyansı $np(1-p)$ olan normal dağılıma $[N(np, np(1-p))]$ tam bir şekilde yakınsar. (Daha detaylı bilgi için bkz. Walpole ve Myers, 1993: 158-164.) Buna göre n=31 >20 ; np=6.2 >5; $n(1-p)$=24.8 >5 olduğundan 31 soruda elde edilecek doğru cevap sayısının dağılımı, ortalaması np=6.2, varyansı $np(1-p)$=4.96 (standart sapması=2.227) olan normal dağılıma göre dağılır.

"H_0: DMS yöntemiyle elde edilen doğru cevap sayısı tesadüfi olabilir" boş hipotezini, "H_a: DMS yöntemiyle elde edilen doğru cevap sayısı tesadüfi olamaz" alternatif hipotezi ile test edelim. Eğer boş hipotez reddedilirse, sınavda bir şifreleme olduğu; şifreleme olmadan (tesadüfen) bu kadar doğru cevap sayısının elde edilmesinin mümkün olamayacağı anlaşılacaktır. Eğer boş hipotez reddedilemezse, sınavda bir şifreleme olmasının istatistiksel olarak iddia edilemeyeceği sonucu çıkacaktır.

Test istatistiği $Z = (18.2 - 6.2)/2.227 = 5.39$ olarak hesaplanmıştır. Yani, DMS'nin başarısının beklenen değeri, tesadüfen cevap verildiğinde elde edilecek başarı dağılımının beklenen değerinden 5.39 standart sapma daha yukarıdadır. Bu test istatistiğine göre p-değeri ise 0.000000036 (yani, $0.036*10^{-6}$) olarak bulunmaktadır. Sonuç olarak, milyonda bir anlamlılık düzeyinde dahi boş hipotez reddedilmektedir. Yani, istatistiksel olarak milyonda birin altında (1. Tip) hata payıyla sınavda şifreleme yapıldığı, şifreleme olmadan DMS'nin bu kadar yüksek oranda başarı sağlayamayacağı söylenebilir.

Tartışma

Herhangi bir sınavda şifrenin adaylar tarafından kullanılması, elbette şifrenin varlığından daha önemlidir. ÖSYM, 2011 YGS'de adaya özgü soru kitapçığı uygulamasını ilk (ve belki de son) defa gerçekleştirmiş, bunun sonucunda 1.7 milyon civarında soru kitapçığı üretmiştir. Sınavda şifre kullanılmasının sebebi, bu kitapçıkların cevap anahtarlarının kontrol edilebilirliğini sağlamak olabilir. Öte yandan kullanılan şifreleme yönteminin son derece basit olması sınavın güvenilirliği hakkında şüpheler doğurmuştur. Eğer bu yöntem sınavda bazı adaylar tarafından kullanılmışsa, sınavın adil ve güvenilir olamayacağı kesindir.

Bu bölümde amacımız YGS'de uygulanan şifrenin adaylar tarafından kullanılıp kullanmadığını tespit etmeyi sağlayan, eğer kullanılmışsa, kimler tarafından kullanıldığını belirleyen bir yöntem önermektir. Bu yöntem incelenilen sorular değiştirilerek şifre uygulanan herhangi bir sınava da uyarlanabilir. Öncelikle belirtmek isterim ki YGS'de tüm soruları doğru cevaplayan veya ilk 1000'e giren adayların kitapçıklarını ve cevaplarını incelemek, şifrenin adaylar tarafından kullanılıp kullanılmadığını belirlemede faydalı olmayacaktır. Çünkü şifre tüm soruları doğru cevaplamaya yönelik olmayıp, bazı sorularda yanlış cevap öngörmektedir.

Önerilen yöntem, sınav sorularından Tablo 1'de verilen 18 numaralı genel sıralamaya sahip olan altı soruya adayların verdiği cevapların incelenmesi üzerine kuruludur. Bu sorular ÖSYM'nin basına dağıttığı kitapçıktaki numaralamayla 1, 5, 9, 16, 17 ve 30 numaralı sorulardır.

18 numaralı genel sıralama a1-a4-a5-a3-a2 olarak verilmiştir. Örnek 4'te açıklandığı gibi, DMS yöntemini kullanan bir aday bu genel sıralamaya sahip olan bir sorunun cevap seçenekleri eğer kitapçıkta a1-a4-a5-a3-a2 sırasıyla verilmişe a1 seçeneğini işaretlemektedir. Aksi halde (yani cevap seçenekleri kitapçıkta a2-a1-a4-a5-a3; a3-a2-a1-a4-a5; a5-a3-a2-a1-a4 veya a4-a5-a3-a2-a1 sıralarıyla verilmişse) a3 seçeneğini işaretlemektedir. İncelediğimiz altı sorunun her birinin doğru cevabı a3'tür. Yani, şifre kullanan bir aday, bu altı sorudan her biri için, sorunun cevap seçenekleri kitapçıkta eğer a1-a4-a5-a3-a2 olarak verilmişse a1 seçeneğini işaretleyerek yanlış cevap verecek; ama eğer diğer dört sıralamada verilmişse a3 işaretleyerek doğru cevabı verecektir.

Önerilen yöntem, bu altı sorudan şifrenin doğru cevabı öngördüğü soruları doğru cevaplayıp, yanlış cevabı öngördüğü sorularda da şifrenin öngördüğü yanlış cevabı işaretleyen adayları belirlemeye yöneliktir. Bu altı sorunun tamamını doğru yanıtlayan adayları belirlemeyi amaçlamamaktadır; çünkü bir aday hakkıyla da bu soruların tamamını doğru yanıtlayabilir

Yöntemin uygulanabilmesi için gerekli veriler şunlardır: i) Her adayın 1, 5, 9, 16, 17 ve 30 numaralı sorular için cevaplamış olduğu seçenekler, ii) Adayların kitapçıklarında bu soruların (a) seçeneklerindeki değerler. Soruların (a) seçeneklerindeki değerler bilindiğinde, cevap seçeneklerinin dizilimi genel sıralamadan kaydırılarak oluşturulduğu için diğer seçenekler de kolaylıkla bulunabilir.

İnceleyeceğimiz soruların seçenekleri ve doğru cevapları Tablo 6'da özetlenmiştir.

Tablo 6.

Önerilen Yöntemde İncelenen Sorular Hakkında Bilgiler

Soru No	Seçenekler					Doğru Cevap
	(a)	(b)	(c)	(d)	(e)	
1	8	10	6	4	2	6
5	15	16	9	8	4	9
9	2	4	1	1/2	1/4	1
16	8	9	6	5	4	6
17	8	9	7	6	5	7
30	2.5	3	2	1.5	1	2

Örneğin, 1 numaralı sorunun cevap seçenekleri şu sıralamalarda çıkabilir:

1. a)2 b)8 c)10 d)6 e)4

2. a)4 b)2 c)8 d)10 e)6

3. a)6 b)4 c)2 d)8 e)10

4. a)10 b)6 c)4 d)2 e)8

5. a)8 b)10 c)6 d)4 e)2

Şifre kullanan bir aday eğer kitapçığında bu sorunun 'a' seçeneği 2 ise, 2 cevabını işaretleyerek yanlış cevap verecektir; aksi halde ('a' seçeneği 2'den farklıysa) 6 cevabını işaretleyerek doğru cevap verecektir. Şifre kullanan bir adayın 5, 9, 16, 17 ve 30 numaralı sorulardaki cevapları ise şöyle olacaktır: 5 no'lu soruda eğer 'a' seçeneği 4 ise, 4 cevabını işaretleyip yanlış cevap; aksi halde 9 işaretleyip doğru cevap verecektir. 9 no'lu soruda eğer 'a' seçeneği 1/4 ise, 1/4 cevabını işaretleyip yanlış cevap verecek; aksi halde 1 işaretleyip doğru cevap verecektir. 16 no'lu soruda eğer 'a' seçeneği 4 ise, 4 cevabını işaretleyip yanlış cevap verecek; aksi halde 6 işaretleyip doğru cevap verecektir. 17 no'lu soruda eğer 'a' seçeneği 5 ise, 5 cevabını işaretleyip yanlış cevap verecek; aksi halde 7 işaretleyip doğru cevap verecektir. 30 no'lu soruda eğer 'a' seçeneği 1 ise, 1 cevabını

işaretleyip yanlış cevap verecek; aksi halde 2 işaretleyip doğru cevap verecektir.

Aşağıda belirtilen algoritma, adayların belirtilen soruları şifrenin öngördüğü biçimde cevaplayıp cevaplamadığını belirleyecektir.

Algoritma

Aday i için: (i=1'den sınava giren aday sayısı kadar)

{ X=0; Y=0;

i'nci adayın soru kitapçığında:

Eğer soru 1'in 'a' seçeneği 2 ise ve adayın cevabı 2 ise: X=X+1;Y=Y+1;

Eğer soru 1'in 'a' seçeneği 2 değilse ve adayın cevabı 6 ise: X=X+1;

Eğer soru 5'in 'a' seçeneği 4 ise ve adayın cevabı 4 ise: X=X+1; Y=Y+1;

Eğer soru 5'in 'a' seçeneği 4 değilse ve adayın cevabı 9 ise: X=X+1;

Eğer soru 9'un 'a' seçeneği 1/4 ise ve adayın cevabı 1/4 ise: X=X+1; Y=Y+1;

Eğer soru 9'un 'a' seçeneği 1/4 değilse ve adayın cevabı 1 ise: X=X+1;

Eğer soru 16'nın 'a' seçeneği 4 ise ve adayın cevabı 4 ise: X=X+1; Y=Y+1;

Eğer soru 16'nın 'a' seçeneği 4 değilse ve adayın cevabı 16 ise: X=X+1;

Eğer soru 17'nin 'a' seçeneği 5 ise ve adayın cevabı 5 ise: X=X+1; Y=Y+1;

Eğer soru 17'nin 'a' seçeneği 5 değilse ve adayın cevabı 7 ise: X=X+1;

Eğer soru 30'un 'a' seçeneği 1 ise ve adayın cevabı 1 ise: X=X+1; Y=Y+1;

Eğer soru 30'un 'a' seçeneği 1 değilse ve adayın cevabı 2 ise: X=X+1;}

Bu algoritma sonunda her aday için değeri 0 ile 6 arasında değişebilecek bir X değeri ve yine değeri 0 ile 6 arasında değişebilecek bir Y değeri saptanacaktır. Eğer bir aday için X<6 ise, aday soruları şifre kullanarak çözmemiştir; en azından bir soruda şifrenin öngördüğü cevap seçeneğini işaretlememiştir.

Eğer bir aday için X=6 ise bu aday soruların tamamını şifrenin öngördüğü gibi cevaplamıştır. Bu durumda eğer Y=0 ise şifrenin öngördüğü tüm cevaplar doğru cevaplardır. ***** Yani X=6 ve Y=0 ise aday şifre kullanarak soruları doğru cevaplayabildiği gibi hakkıyla da tüm soruları doğru cevaplamış olabilir.

Eğer X=6 ve Y>0 ise şifrenin öngördüğü cevapların bir kısmı doğru bir kısmı yanlış olmasına rağmen aday soruları tam anlamıyla şifrenin öngördüğü gibi cevaplamıştır. Bu durumdaki adayların şifre kullanmış olması çok yüksek olasılığa sahiptir ve bu adayların diğer sorulara verdiği cevaplar da incelenmelidir. Eğer diğer soruları da şifrenin öngördüğü gibi cevaplamışlarsa sınavda şifre kullandıklarını söyleyebiliriz.

Bu yöntemin uygulanması oldukça kolaydır. Sadece altı soruya verilen yanıtlar ve adayların kitapçığında bu soruların 'a' seçeneklerindeki değerlerinin bilinmesi yeterlidir. Elbette bu yöntem, daha farklı sorular ve/veya daha fazla sayıda soru seçilerek daha net sonuçlar verecek şekilde geliştirilebilir. Burada amacımız inceleme yapılırken izlenmesi gereken yöntemde, şifrenin doğru cevap öngördüğü soruların bir kısmı ile yanlış cevap öngördüğü soruların bir kısmının bir araya getirilerek, adayların bu soruların tamamına şifrenin öngördüğü cevapları verip vermediğine bakılması gerektiğini vurgulamaktır. Öte yandan, böyle bir yöntem yerine tüm sorulara doğru cevap veren adayların kitapçıklarının veya cevaplarının incelenmesi bir sonuç vermeyecektir; çünkü şifre kullanan adaylar tüm soruları doğru cevaplayamayacaklardır.

***** Bu durumda Y=0 olma ihtimali, cevap seçenekleri kaydırılarak elde edildiği için $[1-(4/5)^6]$, yani yaklaşık %26.2'dir. Şifrenin her sıralama için yanlış cevap öngördüğü bir soru (örneğin 19. soru) incelenen sorulara katılarak bu ihtimal sıfıra çekilebilir.

Önerilen Yöntemin Uygulanmasına Bir Örnek

Rasgele seçilen bir kitapçığı (11281.10715 numaralı kitapçık) ele alalım. Önerdiğimiz yöntemde incelenmesi öngörülen 1, 5, 9, 16, 17 ve 30 numaralı soruların bu kitapçıktaki soru numaraları ve 'a' seçenekleri Tablo 7'de verilmiştir. Bu tabloda ayrıca şifre kullanan bir adayın işaretleyeceği cevaplar ve soruların doğru cevapları da verilmiştir.

Tablo 7.

11281.10715 Numaralı Kitapçıkta İncelenen Sorular Hakkında Bilgiler

Soru No	11281.10715 no'lu Kitapçıktaki Soru Numarası	(a) Seçeneği	Şifrenin Öngördüğü Cevap	Doğru Cevap
1	2	4	6	6
5	17	16	9	9
9	5	1/4	1/4	1
16	16	8	6	6
17	7	6	7	7
30	28	2	2	2

11281.10715 no'lu kitapçığı çözen aday eğer matematik bölümünden 2, 7, 16, 17 ve 28 numaralı soruları doğru cevaplamışsa ve 5 numaralı soruyu 'a' seçeneğini (1/4) işaretleyerek yanlış cevap vermişse muhtemelen şifre kullanmıştır. (Bu durumda yukarıda belirtilen algoritmada bu aday için X=6 ve Y=1 olur.) Bu adayın diğer sorulara verdiği cevaplar şifrenin öngördüğü cevaplarla karşılaştırılarak şifre kullanıp kullanmadığı kesinleştirilebilir. Bu altı soruya belirtilen cevaplardan farklı cevaplar vermişse şifre kullanmadığı sonucuna varılabilir.

Sonuç

Bu çalışmada ilk olarak 2011 yılı Yükseköğretime Geçiş Sınavı'nda adaylara dağıtılan tüm kitapçıklarda bazı yöntemler kullanılarak doğru çözümlere ulaşılabileceği iddiası, yani sınavda bir şifreleme yapılıp yapılmadığı araştırılmıştır. Bu amaçla kamuoyunda öne çıkan çok basit bir şifreleme yönteminin (DMS) geçerliliği incelenmiştir. Şifrelemenin herhangi bir kitapçık (basına dağıtılan kopya veya ana kitapçık) için değil de tüm kitapçıklarda geçerliliğini belirleyebilmek için cevap seçeneklerinin kaydırılarak elde edebileceği 24 genel sıralama belirlenmiş ve bunların her birinde DMS tahmini hesaplanmıştır.

YGS matematik bölümünden yöntemin uygulanabileceği 31 soru için DMS tahminleri belirlenmiş ve doğru cevaplarla kıyaslanmıştır. Buna göre adaylara dağıtılan kitapçıklardan herhangi birinde DMS yöntemiyle cevaplanacak doğru cevap sayısının beklenen değeri 18.2 ve DMS yönteminin başarı oranı %58.7 olmaktadır.

Sınavda bir şifreleme yapılmadan DMS yönteminin başarısının bu kadar yüksek olup olamayacağı istatistiksel yöntemlerle test edilmiştir. Test sonuçları milyonda birin altında bir hata payıyla sınavda şifreleme olmadan bu kadar yüksek oranda doğru cevap elde edilemeyeceğini, yani sınavda bir şifreleme olduğunu göstermektedir. Bu çalışmanın sonuçları sadece bir kitapçık için değil, sınavda adaylara dağıtılan tüm kitapçıklar için geçerli olduğu için istatistiksel olarak milyonda birin altında bir hata payıyla adaylara dağıtılan tüm kitapçıklarda şifreleme olduğu sonucuna ulaşılmıştır.

ÖSYM adaylara 11 Nisan 2011'de gönderdiği e-postada, cevap seçeneklerinin sehven kaydırılarak belirlendiğini ve bunun sonucunda şifreleme gibi bir durumun ortaya çıktığını belirtmiştir. Fakat cevap seçeneklerinin kaydırılarak elde edilmesi, sadece eğer bir şifre kullanılmışsa, bunun tüm kitapçıklar için geçerli olmasını sağlayabilir. Eğer sınavda bir şifre kullanılmamışsa, cevap seçenekleri sehven kaydırılarak da elde edilse, doğru cevaplara erişilmesi mümkün olmayacaktır. Sonuç olarak, sınavdaki şifre uygulaması sehven olmamıştır.

Ayrıca, bu çalışma YGS'de uygulanan şifrenin adaylar tarafından kullanılıp kullanmadığını tespit etmeyi sağlayan, eğer kullanılmışsa, kimler tarafından kullanıldığını belirleyen bir yöntem de önermektir. Bu yöntem, incelenen sorular değiştirilerek şifre uygulanan herhangi bir sınava da uyarlanabilir. Yöntemin uygulaması oldukça kolay olup adayların sadece altı soruya verdiği yanıtlar ile adayların kitapçıklarında bu soruların 'a' seçeneklerindeki değerlerin bilinmesi uygulama için yeterlidir.

Bu yöntemi önerirken amacımız, inceleme yapılırken izlenmesi gereken yöntemde, şifrenin doğru cevap öngördüğü soruların bir kısmı ile yanlış cevap öngördüğü soruların bir kısmının bir araya getirilerek, bu soruların tamamına adayların şifrenin öngördüğü cevapları verip vermediğine bakılması gerektiğini vurgulamaktır. Öte yandan, böyle bir yöntem yerine tüm sorulara doğru cevap veren adayların kitapçıklarının veya cevaplarının incelenmesi bir sonuç vermeyecektir; çünkü şifre kullanan adaylar tüm soruları doğru cevaplayamayacaklardır.

Kaynakça

Ankara Üniversitesi (2011). Ankara Üniversitesi Eğitim Bilimleri Fakültesi'nin YGS Hakkında Görüşü. [Online]: http://www.ankara.edu.tr/dyr.php?id=1170 adresinden 06 Temmuz 2011 tarihinde indirilmiştir.

Buchmann, J. A. (2004). *Introduction to Cryptography (*2nd Ed.). New York: Springer.

Mollin, R.A. (2007). *An Introduction to Cryptography* (2nd Ed.). New York: Chapman & Hall / CRC.

ODTÜ (2011). 2011 Yılı Yükseköğretime Geçiş Sınavı Hakkında ODTÜ Eğitim Fakültesi Görüşü. [Online]:http://www.fedu.metu.edu.tr/web/documents/other/YGS2011hkEgitimFakultesiGorusu_28_4_2011_v2.pdf adresinden 06 Temmuz 2011 tarihinde indirilmiştir.

ÖSYM (2011). Basına Dağıtılan YGS Soru Kitapçığı. [Online]: http://osym.gov.tr/belge/1-12470/2011-osys-ygs-sorulari-ve-cevaplari-29032011.html) adresinden 06 Nisan 2011 tarihinde indirilmiştir.

ÖSYM (2011). 11247.98420 ile 11314.27133 numaralar arasındaki YGS Soru Kitapçıkları. [Online]: ftp://2011ygs-kitapcik.osym.gov.tr/063%20-%20ANKARA-KUZEY/ adresinden 06 Nisan 2011 tarihinde indirilmiştir.

ÖSYM (2011). ÖSYM Başkanı Prof. Dr. Ali Demir'in 2011-YGS'ye girmiş ve 2011-LYS'ye girecek adaylara göndermiş olduğu e-posta. [Online]: http://www.osym.gov.tr/dosya/1-57598/h/osym-mektup.pdf adresinden 06 Temmuz 2011 tarihinde indirilmiştir.

Tezbaşaran, A. (2004). Yükseköğretime Geçişin Kısa Öyküsü ve Öğrenci Seçme ve Yerleştirme Sistemindeki Değişmeler (1960-2004). *Eğitim Bilim Toplum*, 6, 108-113.

Walpole, R.E & Myers, R.H. (1993). *Probability and Statistics for Engineers and Scientists* (5th Ed.). New Jersey: Prentice-Hall, Inc.