

T.C.
Marmara Üniversitesi
Eğitim Bilimleri Enstitüsü
İlköğretim Ana Bilim Dalı
İlköğretim Matematik Öğretmenliği Bilim Dalı

**MODÜLER ARİTMETİK KONUSUNUN ÖĞRETİMİNDE
ŞİFRELEME AKTİVİTELERİNİN MATEMATİK
BAŞARISINA ETKİSİ**

Yüksek Lisans Tezi

Enes GÜLER

İstanbul, 2007

T.C.
Marmara Üniversitesi
Eğitim Bilimleri Enstitüsü
İlköğretim Ana Bilim Dalı
İlköğretim Matematik Öğretmenliği Bilim Dalı

**MODÜLER ARİTMETİK KONUSUNUN ÖĞRETİMİNDE
ŞİFRELEME AKTİVİTELERİNİN MATEMATİK
BAŞARISINA ETKİSİ**

Yüksek Lisans Tezi

Enes GÜLER

Danışman: Yrd. Doç. Dr. Ahmet Ş. Özdemir

İstanbul, 2007

T.C.
Marmara Üniversitesi
Eğitim Bilimleri Enstitüsü
İlköğretim Ana Bilim Dalı
İlköğretim Matematik Öğretmenliği Bilim Dalı

Enes GÜLER tarafından hazırlanan “Modüler Aritmetik Konusunun Öğretiminde Şifreleme Aktivitelerinin Matematik Başarısına Etkisi” başlıklı bu çalışma, 06.12.2007 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans tezi olarak kabul edilmiştir.

İmzalar

Danışman : Yrd. Doç. Dr. Ahmet Ş. ÖZDEMİR

Üye : Yrd. Doç. Dr. Emin AYDIN

Üye : Yrd. Doç. Dr. Sare ŞENGÜL

ÖNSÖZ

“ Tm evren eleman ve faktrleri birbiriyle baēlantılı kendi iinde birok fonksiyonel aılıma sahip matematiksel bir Őfre-dizin olaylarına baēlı olarak sreēendir ya da olmaktadır.”

Bu tez alıřmam sresince, bana her trl desteēi vererek Kriptoloji gibi muazzam bir konuda beni alıřmaya teřvik eden ve bu alıřmanın ortaya ıkmasını saēlayan hocam Sayın Yrd. Do. Dr. Ahmet Ő. ZDEMİR’e, yksek lisansa bařlamamı canı gnlden isteyip maddi ve manevi katkıda bulunan anneme, hayatıma bir anlam katan babama, byklerin szn dinlemenin nemini hatırlatan kardeřime ve tm arkadařlarıma sonsuz teřekkrlerimi sunarım.

ARALIK 2007

Enes GLER

ÖZET

MODÜLER ARİTMETİK KONUSUNUN ÖĞRETİMİNDE ŞİFRELEME AKTİVİTELERİNİN MATEMATİK BAŞARISINA ETKİSİ

Matematiği yaparak, yaşayarak öğrenen öğrenciler günlük hayatlarındaki karşılaştıkları problemlere karşı daha güçlü, çözüm üreten bir yapıya sahip olurlar. Öğrencilerin güvenli bireyler olarak yetişmesini sağlayan bir matematik eğitiminin gelişimi, sınıf ortamlarındaki etkili matematik öğretimini gerektirir.

Bu çalışma Modüler Aritmetik konusunun öğretiminde Şifreleme aktivitelerinin kullanılmasından yola çıkarak, benzer matematik konularının da bu şekilde daha zevkli, daha kalıcı öğretilebileceğini/öğrenilebileceğini göstermek bakımından önemlidir. Aynı zamanda matematikte geliştirilebilecek farklı standartların uygulanışları ve bunların eğitim-öğretime etkisini ortaya koyacak projelere örnek bir kaynak oluşturması muhtemeldir.

Bu çalışmanın araştırma modeli “ön test-son test kontrol grubu model” dir. Seçilen öğrencilerin kişisel özelliklerini, ailelerinin içinde bulundukları sosyoekonomik durumlarını, anne babalarının eğitim düzeylerini tespit etmek amacıyla kişisel bilgi anketi uygulanmıştır.

Deney ve kontrol grubu matematik öğretmeni aynı olmak şartı üzere iki gruba da “Modüler Aritmetik” konusu öğretildi. Kontrol grubu öğrencilerle yapılan öğretimde öğretmen geleneksel öğretim metoduyla öğretimi gerçekleştirirken deney grubu öğrencilerle yapılan öğretimde kaynak olarak önceden dağıtılmış şifreleme aktiviteleriyle ders akışı uygulanırken materyaldeki gerek sınıf içi etkinlikler gerek bulmacalarla grup çalışmalarına yer verilmiştir. Araştırma bulguları, Modüler Aritmetik konusunun öğretiminde şifreleme aktivitelerini kullanıldığı öğretimde; öğrenci matematik başarılarının pozitif yönde etkilendiğini

geleneksel öğretim metoduna göre başarının daha olumlu yönde olduğunu göstermiştir.

Ayrıca iki gurubun matematiğe karşı tutumlarına ve kalıcılığına bakıldı. Şifreleme aktiviteleriyle ders işlemenin daha eğlenceli olduğu ve öğrencilerin bu tür öğrenme hakkındaki görüşlerinin olumlu olduğu tespit edilmiştir.

Anahtar Kelimeler: Matematik Öğretimi, Modüler Aritmetik, Şifreleme, Aktivite.

ABSTRACT

THE EFFECT OF CODING ACTIVITY ON THE SUCCESS OF MATH PERFORMANS IN TEACHING MODULAR ARITHMETIC

Students learning math by solving and living have a stronger and more creative mind (brain) against to difficulties in their daily lives. To be educated and self-confident students needs an effective math teaching with a progressive development of math education.

In this study, coding activities had used in teaching modular arithmetic subject. This method is important to show that teaching the other math subjects is more permanents and pleasant for students who don't like math. Moreover, this study may be a prototype source for the other concerned projects and studies.

In this study, “first-last test control grouped” applies by searching model. In addition, a personal information survey which consisted of personal characteristic, social and economical conditions of students, education level of parents and concerned different questions, applied to the students group.

Same teachers thought the modular arithmetic subject to two groups which are experimental and control group, teacher used traditional method of the teaching modular arithmetic in the class of control group. In the class of experimental group, coding activities, materials about coding and puzzles used by teacher.

At the end of study, if it's compared with traditional and coding method, in the coding method, the students are more successful than the students in the traditional method. In additional, it's observed that performance and attitude of two groups against mathematics. Teaching with the method of coding is more funny. As a

result of, it's determined that student's comments are positive about the method of coding.

Key words: Mathematics Education, Modular Arithmetic, Coding, Activity.

İÇİNDEKİLER

ÖNSÖZ.....	I
ÖZET.....	II
ABSTRACT	IV
İÇİNDEKİLER	VI
TABLO LİSTESİ	X
KISALTMALAR	XIII
ŞEKİL LİSTESİ.....	XIV
BÖLÜM I: GİRİŞ	1
1.1. Problem.....	2
1.2. Araştırmanın Amacı	3
1.2.1. Alt Problemler	3
1.2.2. Hipotezler	4
1.3. Araştırmanın Önemi	4
1.4. Varsayımlar	5
1.5. Sınırlılıklar.....	5
1.6. Tanımlar	5
BÖLÜM II: LİTERATÜR ÇALIŞMASI.....	7
2.1. Kriptografi Tanımı ve Kısa Tarihi.....	7

2.2. Kriptografinin İçerdiği Konular	8
2.3. Şifrelenmiş Sistemlerin Özellikleri	8
2.4. İlk Kriptografi Sistemler.....	9
2.4.1. Sezar Şifresi	11
2.4.2. Mesajın Sayılarla Gösterilmesi.....	14
2.4.3. Anahtar Şifre.....	14
2.4.4. Frekans Tablosu.....	16
2.4.5. Osmanlıda Gizli Yazı	20
2.4.6. Kod Sözcükler	20
2.4.7. Pigpen Şifresi.....	21
2.4.8. Mors Kodu	22
2.4.9. Bayraklar	24
2.4.10. Hiyeroglif.....	24
2.4.11. Isbn	25
2.4.12. Ebced Hesabı	27
2.4.13. Vigenere Şifresi	28
2.4.14. Modüler Aritmetik	29
2.4.15. Affine Şifresi	30
2.5. Asal Sayılar	30

2.6. Halka Açık Kriptoloji	31
2.6.1. Rsa	32
2.7. Dünya Savaşları Sırasında Kriptografi	32
2.8. Enigma.....	33
2.9. Modern Çağda Kriptografi	34
2.10. Kriptografinin Uygulandığı Alanlar	35
2.11. Yapılan Çalışmalar	36
BÖLÜM III: YÖNTEM.....	38
3.1. Araştırmanın Modeli	38
3.2. Veri Toplama Araçları.....	38
3.2.1. Matematik Başarı Testi.....	38
3.2.2. Tutum Ölçeği.....	38
3.2.3. Kişisel Bilgiler Anketi	39
3.3. Deneklerin Seçimi	39
3.4. Uygulama Süreci	40
3.5. Verilerin Çözümü	43
BÖLÜM IV: BULGULAR VE YORUMLAR.....	44
4.1. Normal Dağılıma Uygunluk Analizi	44

4.2. Modüler Aritmetik Konusunun Öğretiminde Şifreleme Aktivitelerinin	
Başarıya Etkisini Test Eden Hipotezler, Bulgu ve Yorumları	52
BÖLÜM V: SONUÇLAR VE ÖNERİLER	67
5.1. Sonuçlar.....	67
5.2. Öneriler.....	68
KAYNAKÇA	69
EKLER.....	74

TABLO LİSTESİ

Tablo 2.1: Sezar Şifresinin 4 Harf Kaydırılmış Hali.....	13
Tablo 2.2: Mesajın Sayılarla Gösterilmesi	14
Tablo 2.3: Şifreli Alfabe	15
Tablo 2.4 : Türkçede Harflerin Kullanım Sıklığı	19
Tablo 2.5 : Mors Alfabesi Gösterimi	22
Tablo 2.6 : Vigenere Tablosu	29
Tablo 3.1: Deney Grubunun Çalışma Programı	40
Tablo 4.1: Deney ve Kontrol Grubuna Ait Ön Test Kolmogorov-Smirnov Testi Sonuçları.....	44
Tablo 4.2: Deney ve Kontrol Grubuna Ait Ön Tutum Ölçeği Kolmogorov-Smirnov Testi Sonuçları.....	45
Tablo 4.3: Ön Test Sonuçlarına Göre Aritmetik Ortalamalarının Karşılaştırılması	46
Tablo 4.4: Paired-Sample t-testine Göre Çalışma Gruplarının Homojenliği	46
Tablo 4.5: Deney ve Kontrol Grubu Matematik Ön Tutum Ölçeği Verileri	47
Tablo 4.6: Deney ve Kontrol Grubu Öğrencilerinin Cinsiyetlerine Göre Dağılımları	48

Tablo 4.7: Deney Grubu Öğrencilerinin Öğretim Sonrası

Başarılarının Cinsiyetlerine Göre Farklılaşmasına İlişkin t-testi Sonuçları..... 49

Tablo 4.8: Deney ve Kontrol Grubu Öğrencilerin

Annelerinin Eğitim Düzeyine Göre Dağılımları 49

Tablo 4.9: Deney ve Kontrol Grubu Öğrencilerin

Babalarının Eğitim Düzeyine Göre Dağılımları 50

Tablo 4.10: Deney ve Kontrol Grubu Öğrencilerinin

Ailelerinin Aylık Ortalama Gelir Seviyelerine Göre Dağılımları..... 51

Tablo 4.11: Kontrol Grubunun Son Test Puanlarına ait

Kolmogorov-Smirnov Testi Sonuçları..... 52

Tablo 4.12: Kontrol Grubunun Ön Test ve Son Test

Puanlarına İlişkin Eşlenik Çift t-Testi Sonuçları 53

Tablo 4.13: Deney Grubunun Son Test Puanlarına ait

Kolmogorov-Smirnov Testi Sonuçları..... 54

Tablo 4.14: Deney Grubunun Ön Test ve Son Test

Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları..... 55

Tablo 4.15: Kontrol ve Deney Grubunun Son Test Puanlarına

İlişkin ilişkisiz t-testi Sonuçları..... 56

Tablo 4.16: Deney ve Kontrol Grubunun Öğretim Sonrası Matematik

Tutum Puanlarının Normalliğine İlişkin Kolmogorov-Smirnov Testi Sonuçları 57

Tablo 4.17: Deney Grubunun Uygulama Öncesi ve Sonrası Matematik Tutumlarının Farklılaşmasına İlişkin Eşlenik Çift t-testi Sonuçları	58
Tablo 4.18: Kontrol Grubu Öğretim Sonrası Matematik Tutum Puanlarının Normallğine İlişkin Kolmogorov-Smirnov Testi Sonuçları	59
Tablo 4.19: Kontrol Grubu Öğrencilerinin Öğretim Sonrası Tutum Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları	60
Tablo 4.20: Deney ve Kontrol Gruplarının Tutum Ölçeği Ön Testi İçin Yapılan İlişkisiz Grup t-testi Sonuçları	61
Tablo 4.21: Deney ve Kontrol Gruplarının Tutum Ölçeği Son Testi İçin Yapılan İlişkisiz Grup t-testi Sonuçları	61
Tablo 4.22: Kontrol Grubu Öğrencilerinin Hatırlama Testi Puanlarına Ait Kolmogorov-Smirnov Testi Sonuçları.....	62
Tablo 4.23: Kontrol Grubu Öğrencilerinin Son Test ve Hatırlama Testi Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları.....	63
Tablo 4.24: Deney Grubu Öğrencilerinin Hatırlama Testi Puanlarına Ait Kolmogorov-Smirnov Testi Sonuçları.....	64
Tablo 4.25: Deney Grubu Öğrencilerinin Son Test ve Hatırlama Testi Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları.....	65
Tablo 4.26: Deney ve Kontrol Grubu Öğrencilerinin Hatırlama Testi Puanları Arasındaki Farka İlişkin İlişkisiz t-testi Sonuçları.....	66

KISALTMALAR

?: yüzde

k.s.z: Kolmogorov-Smirnov Z

O.K.S.: Ortaöğretim Kurumlar Sınavı

n: veri sayısı

p: anlamlılık değeri

s.d: serbestlik derecesi

s.s: standart sapma

t: hesaplanan t değeri

X: ortalama

ŞEKİL LİSTESİ

Şekil 1: Jül Sezar	11
Şekil 2: Şifre Diski.....	13
Şekil 3: Pigpen Şifresi	21
Şekil 4: Telgraf.....	23
Şekil 5: Hiyeroglif Yazısı	24
Şekil 6: Hiyeroglif Yazısı	25
Şekil 7: ISBN	26
Şekil 8: Sayıların Gösterimi.....	27
Şekil 9: Enigma Makinesi	33

BÖLÜM I: GİRİŞ

Matematiğin en heyecanlı konularından biri şifreleme ve şifre çözümdür. Eski Mısır'dan beri insanlık şifrelemeyle ilgilenmiştir. İnsanlar herkesin bilmesini istemediği konularda haberleştikçe de bu ilgi sürecektir.

Tarihte ilk şifre yazan kişi Sezar'dır. Yaya ulakları pusuya düşürölüp taşıdıkları mesajlar çalınmaya başladığında, Sezar emirlerini iletmek için yeni bir yol buldu. Mesajlarından oluşan metni, yazdıkları anlamsız görünecek bir şekilde yeniden düzenliyordu. Metin anlamsız değildi elbet. Bu yöntemde her harf yerine alfabetik sıralamada kendisinden üç sonra gelen harf kullanılır. Emrindeki görevlilere, kendilerine rastgele, anlamsız gibi görünen bir mesaj ulaştığında mesajdaki harfleri kendinden 3 önce gelen harflerle yer değiştirmelerini söylemişti gizlice. Görevliler bunu yaptıklarında sihirli bir değnek değmiş gibi gizli bir mesaj ortaya çıkıyordu.

Önceleri, şifreleme yöntemlerinde matematiğin kullanıldığı pek söylenemez. Yapılan bir takım kurnazlıklarla iletinin gizlenmesinden ibaretti. Zamanla Sezar'ın metni yeniden düzenleme kavramı başkaları tarafından da benimsendi ve çözölmesi daha güç bir hale getirildi. İkinci Dünya savaşı sırasında "bilgisayar temelli olmayan şifreleme" doruk noktasına ulaştı. Naziler Enigma adında şaşırtıcı bir şifreleme makinesi yaptılar. Bu makine eski moda daktilolara benziyordu. Karmaşık biçimlerde dönen ve temiz metni görünüşte anlamsız karakter gruplarından oluşan diziler haline getiren, birbirine geçmiş pirinçten çarkları olan bir makineydi. Elinde ancak tamamen aynı biçimde ayarlanmış başka bir Enigma makinesi olan bir alıcı şifreyi çözebiliyordu.

Alan Turing, II. Dünya Savaşı'nda Almanların "çözölmez dediği" şifrelerini çözen çok zeki bir matematikçi ve bir kahramandı. 1938 yılında, II. Dünya Savaşı'na bir yıl kala Turing, Bletcley Parkı'na gizli bir göreve katılması için davet edildi. Görevi, Nazi askerî şifrelerini çözmekti. Sonuçta Turing ve meslektaşları "Clossus " adlı bir makine ürettiler. Bu cihaz Avrupa'daki savaşı iki yıl kısalttı ve sayısız yaşam kurtardı. Zafer

matematikçilerindi. Almanlar ne olduğunu dahi anlayamadan İngilizler savaşı lehlerine çevirmeyi başardılar. Bu da kriptolojinin ve şifreleme mekanizmalarının önemi üzerine sizlere bir fikir verebilir.

Şifre bilim (kriptoloji), şifreleme ve şifre analizlerinden oluşur. Literatürde kriptoloji için değişik tanımlamalar mevcuttur. Kriptoloji kod üretme ile kod kırma bilimi ve sanatıdır. Kriptoloji kriptografi ve kriptanalizi içeren matematik branşlarıdır. Yunanca gizli yazma anlamına gelen kriptoloji, depolanması ve iletilmesi sırasında bilginin güvenliğini sağlamak amacıyla bilgiyi farklı hale dönüştürme bilimi ve sanatıdır. Kriptoloji, kriptografi ve kriptanalizden meydana gelmiş bir disiplindir.

Kriptografi; Kriptolojinin bilgi güvenliği teknikleri ile ilgilenen dalıdır. Kriptanaliz ise kriptografik tekniklerinin güvenliğini ölçmek üzere onların açıklarını araştıran matematik ağırlıklı bir daldır. Kriptoloji denilince ilk akla gelen şifreleme algoritmaları olduğundan şifreleme ile ilgili temel kavramların ele alınması gereklidir.

1.1. PROBLEM

Matematikçiler için sezgiler matematiksel düşünme açısından önemli rol oynar. Bir problem üzerinde uzun zaman çalıştıktan sonra birden bire çözüm yakalanır ve çözüm sonucunu bilinen formüllerle ispatlanır. İyi matematikçiler ise hızlı tahminler yapan ve çözüm üreten kişilerdir. Bruner (1983) sezgilerin matematikçi ve fizikçiler tarafından sıklıkla kullanılmasının kendi disiplinlerine duydukları güvenden kaynaklanabileceğini düşünmektedir. Gardner'e (1983) göre üstün bilim adamlarını (Newton, Einstein gibi) özel yapan sezgilerdir ve onların sezgilerinin nasıl bir özellik taşıdığı araştırılmalıdır.

Matematiksel düşünme aslında kodlama esasına dayanır. Fakat kodlar başlangıçta ne sözel ne de grafiksel, temel de önce sezgiseldir. Bu bakımdan matematikçilerin sezgilerinin güçlü olması onlar için bir ayrıcalık taşır. Aslında bir matematikçi kavramları ve onların ilişkilerini keşfederken sezgileri tarafından yönlendirilebiliyorsa ilerleyebilir. (Dossey,1992)

Yapılan bu çalışmada modüler aritmetik konusunun öğretiminde şifreleme aktivitelerinin matematik başarısına etkisi var mıdır? Sorusu araştırmanın problemi oluşturmuştur.

1.2 ARAŞTIRMANIN AMACI

İlköğretim 8. sınıflarda Modüler aritmetik konusunun öğretiminde Şifreleme Aktivitelerinin kullanılmasının öğrencilerin matematik dersi başarısına ve kalıcılık düzeyine etkisinin incelenmesi bu araştırmanın amacının oluşturmaktadır.

1.2.1 Alt Problemler

Bu amaç kapsamında aşağıdaki alt problemlere çözüm aranmıştır.

1. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında kontrol grubunun başarısı farklılık gösterir mi?
2. Geleneksel Öğretim Metodu uygulanan kontrol grubunun başarısı farklılık gösterir mi?
3. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında kontrol grubu öğrencileri ile deney grubunun başarısı farklılık gösterir mi?
4. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında deney grubundaki öğrencilerin matematiğe karşı tutumları farklılık gösterir mi?
5. Deney-kontrol grubunun başarısı farklılık gösterir mi?
6. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Kontrol grubu öğrencilerinin hatırlamalarında farklılık gösterir mi?
7. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Deney grubu öğrencilerinin hatırlamalarında farklılık gösterir mi?
8. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında öğrencilerinin hatırlamalarında farklılık gösterir mi?

1.2.2. Hipotezler

Araştırmanın esas problemi ve alt problemi için kurulan hipotezler aşağıda belirtilmiştir.

1. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Kontrol grubu öğrencilerinin uygulama öncesi ve sonrası başarıları arasında anlamlı bir fark yoktur
2. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Deney grubu öğrencilerinin uygulama öncesi ve sonrası başarıları arasında anlamlı bir fark vardır.
3. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Kontrol grubu öğrencileri ile deney grubu öğrencilerinin öğretim sonrası başarıları arasında anlamlı bir fark vardır.
4. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Deney ve Kontrol grubu öğrencilerinin ön ve son matematik tutumları arasında anlamlı bir fark vardır.
5. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Kontrol grubu öğrencileri ile deney grubu öğrencilerinin son matematik tutumları arasında anlamlı bir fark vardır.
6. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Kontrol grubu öğrencilerinin hatırlamaları arasında anlamlı bir fark yoktur.
7. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında Deney grubu öğrencilerinin hatırlamaları arasında anlamlı bir fark yoktur.
8. Şifreleme aktivitelerinin Modüler aritmetik konusuna uygulanmasında öğrencilerinin hatırlamaları arasında anlamlı bir fark yoktur.

1.3 ARAŞTIRMANIN ÖNEMİ

Matematiği yaparak, yaşayarak öğrenen öğrenciler günlük hayatlarındaki karşılaştıkları problemlere karşı daha güçlü ve çözüm üreten bir yapıya sahip olurlar. Öğrencilerin güvenli bireyler olarak yetişmesini sağlayan bir matematik eğitiminin gelişimi, sınıf ortamlarındaki etkili matematik öğretimini gerektirir.

Bu araştırma matematikte geliştirilebilecek farklı standartların uygulanışları ve bunların eğitim-öğretime etkisini ortaya koyacak araştırmalara örnek bir kaynak oluşturması bakımından önemlidir. Etkinlikler planlanırken öğrencilerde merak uyandırması önemlidir. Merak uyandıran etkinliklerle matematiğin de merak uyandırması olasıdır. Son zamanlarda günlük yaşamda şifrelemenin olmadığı bir konu hemen hemen yok gibi. Bu yüzden konunun öğretiminde güdüleme açısından son derece önemlidir.

1.4 SAYIL TILAR

1. Araştırmaya katılan öğrenciler, kullanılan aktivitelere samimi ve doğru cevaplar vermişlerdir.
2. Araştırmanın örneklemini oluşturan 8. sınıf öğrencilerinin zekâ seviyeleri normal dağılım göstermektedir.
3. Deney ve kontrol grubu öğrencilerinin zekâ seviyeleri arasında anlamlı bir farklılık bulunmamaktadır.

1.5. SINIRLILIKLAR

1. Araştırma, Ağrı ili, Doğubayazıt ilçesi, Ş. Ö. Gürhan Yardım İlköğretim Okulunun 8. sınıflarında okuyan öğrencilerle sınırlıdır.
2. Araştırma, Ş. Ö. Gürhan Yardım İlköğretim Okulunun 8-A ve 8-B sınıfı öğrencileri ile sınırlıdır.
3. Araştırma, 2006-2007 öğretim yılının II. Kanaat dönemi Mayıs ayı (3 hafta) ile sınırlıdır.
4. Araştırma, ilköğretim 8.sınıflarının “Modüler Aritmetik” konusu ile sınırlıdır.
5. Araştırma, uygulamacının hazırladığı öğretim materyalleri ve uygulama okulunun olanakları ile sınırlıdır.

1.6. TANIMLAR

Kod: Bilgi parçasını benzer karakterler olması gerekmeksizin başka nesnelerle değiştiren kural.

Kriptoanaliz: Şifreleri çözme bilimi; kriptografik teknikleri alt etmek için yapılan matematiksel çalışmalar.

Kriptanalizci: Kriptanaliz işini yapan kişi.

Kriptografi: Kriptografi ve kriptanaliz çalışmalarıdır.

Kriptoloji: Yunanca Cryptos (Gizli) ve Logos (Anlam, Mantık) kelimelerinden türemiştir. Gizli yazışmalarla ilgili sistemlerle ilgili yapılan çok dallı matematik çalışmalarıdır.

Kriptosistem: Güvenliği ve gizliliği sağlamak için kullanılan şifreleme sistemi.

Düzmetin: Şifrelenecek metin veya kaynak bilgi.

Kriptometni: Düz metnin şifrelenmiş hali.

Şifreleme: Düz metni veya açık metni şifreli hale dönüştürme işlemi.

Deşifreleme: Şifreyi düz metin haline geri getirme işlemi.

Anahtar: Şifreleme ve deşifreleme işlemlerinde kullanılan çözümleyici gizli metin veya gönderici ve alıcının sahip olduğu gizlilik bilgisi.

Monoalfabetik yerine koyma: Düz metindeki bir karakteri değişmeyen başka bir karakterle eşleştiren bir şifreleme yöntemi.

Polialfabetik yerine koyma: Düz metindeki bir karakteri değişen başka bir karakterle eşleştiren bir şifreleme yöntemi.

SSL (Secure Socket Layer): Şifreli bilgiyi TCP/IP üzerinden aktaran bir protokoldür.

Protokol: Sistemler arası iletişim biçimini belirleyen kural.

BÖLÜM II: LİTERATÜR

2.1 KRİPTOGRAFİNİN TANIMI VE KISA TARİHİ

Kriptografi bilgiyi şifrelemek ve deşifrelemek için matematiksel teknikleri kullanan bir bilimdir. Kriptografi sözcüğü, Yunanca gizli anlamına gelen “kryptos” ve söz anlamındaki “logos” sözcüklerinden oluşmuştur. Ayrıca şifre sözcüğü “sayı vermek” anlamındaki İbranicede saphar sözcüğünden gelir. (Candiker, 2007)

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 kullanımlarda plaintext adı da verilir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (encryption). Bu işlem düz metni şifreli metne dönüştürür ve bilgi içeriği başkalarının anlayamayacağı hale 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 çözümdür (decrypt). Kriptografide kullanılan iki yöntem vardır. Simetrik ve asimetrik. Simetrik kriptografi aynı bilgiyi hem kriptolama hem de dekriptolama işlemi için aynı anahtarı kullanır. Bu yöntem gizli(simetrik) anahtarlı kriptografi olarak bilinir. Burada amaç, iki kullanıcının da üzerinde anlaştığı anahtarın istenmeyen kişilerin eline geçmesini engellemektir. Simetrik kriptografi aynı zamanda Özel Anahtar Kriptografi olarak da bilinir.

Asimetrik kriptografi yada açık anahtar kriptografi sistemi ise kriptolama ve dekriptolama için bir çift anahtar kullanır. Bir anahtar (açık anahtar) mesajı kriptolamak için kullanılır ve diğer anahtar (özel anahtar) dekriptolamak için kullanılır. Bilgiyi kriptolamada kullanılan anahtara açık anahtar (public key) adı verilir. Açık anahtar sahibi tarafından herkese yayımlanabilir. Bilgiyi dekriptolamada kullanılan anahtara özel anahtar (private key) denir ve gizli tutulur. Anahtarların üretilmesi, iletilmesi ve

saklanması anahtar yönetimi olarak bilinir. Gizli anahtarlı yapılarda, genelde güvenli anahtar yönetimi sağlamada problem yaşanır (Burnett ve Paine, 2001; Schneier,1996).

2.2. KRİPTOGRAFİNİN İÇERDİĞİ KONULAR

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.

Güvenirlik: Bilgi hedefi dışındakilerin eline geçmemeli (Menezes, Ooscot ve Vanstone, 1996).

2.3. ŞİFRELENMİŞ SİSTEMLERİN ÖZELLİKLERİ

Güvenlik derecesi: Bu aslında zor ölçülebilen bir unsurdur. Genellikle bilgiyi ele geçirme amaçlı olarak bilinen en iyi yöntemlerin kesin sonuç alınıncaya dek uygulanmasındaki işlem sayısı olarak verilir. Tipik bir sistemin güvenlik derecesi bu en yüksek sayıdaki işlem ataklarından (saldırılarından) daha çok işlem yapılmasını gerektirir. Buna bazen işlem unsuru denir.

Fonksiyonellik: Kriptografik sistemin güvenliği sağlayan kısımları birbirleriyle tümleşik bir yapıda olmalıdır. Sistemin tüm kısımları iletilen çeşitli türdeki bilgileri güvenli bir şekilde çözümleyebilmelidir.

İşlem yöntemleri: Kriptografi sisteminin temel yapılarının, uygulama sırasında değişik girişlerle değişik şekillerde çalışması tipik karakteristikler olarak farklılık gösterecektir.

Başarım: Bir şifreleme algoritmasının bir saniyede şifreleyebileceği bit sayısıdır.

Uygulamada kolaylık: Temel bir kriptografik sistem yapısının zor durumlarda uygulanabilirliği önemlidir. Bu yapılar karmaşık bir yazılım ya da donanım ortamını içerebilir. Sistemin yazılım veya donanım bölümüyle ilgili karmaşıklık derecesi işlem gücünü etkiler (Menezes, Ooscot ve Vanstone, 1996).

2.4. İLK KRİPTOGRAFİ SİSTEMLER

Romalı filozof ve devlet adamı Cícero'ya göre en eski gizli yazıların bazıları "tarihin babası" Herodotos'un zamanına kadar gitmektedir. Herodotos, Tarihler adlı yapıtında M.Ö. 5. yüzyılda Yunanistan (Grekler) ve İran (Persler) arasındaki, özgürlükle kölelik, bağımsız Yunan devletleri ile baskıcı Persler arasındaki karşılaşmalar olarak gördüğü, çatışmaların tarihsel kayıtlarını çıkardı. Herodotos'a göre Yunanistan'ı Perslerin zorba lideri, Krallar Krallı Xerxes tarafından istila edilmekten kurtaran şey, gizli yazı yazma sanatıydı.

Herodotos şöyle yazmıştır:

“Yakalanma tehlikesi çok büyük olduğu için mesajı öbür tarafa gönderebilmenin yalnızca tek bir yolu vardı: bir çift odun tablet üzerindeki balmumunu kazıyıp Xerxes'in planları ile ilgili mesajı tabletler üzerine yazdıktan sonra tekrar balmumu ile kaplamak. Bu sayede yoldaki nöbetçiler görünürde boş olan bu tabletlerden hiç şüphelenmeyeceklerdi. Anladığım kadarıyla, mesaj hedefine ulaştığında, aynı zamanda Leonidas'ın karısı da olan, Kleomenes'in kızı Gorgo'nun dışında hiç kimse tabletlerin gizemini çözememişti. Gorgo, odun tabletler üzerindeki balmumu kazınırsa altından bazı yazılar çıkacağı fikrini ortaya attı. Hemen balmumu kazındı, mesaj açığa çıkarılıp okunduktan sonra diğer bütün Yunanlılara bildirildi.” (Singh, 1999)

Demaratus'un gizli haberleşme stratejisi aslında yalnızca mesajın saklanması dayanıyordu. Mesajı saklayarak sağlanan gizli iletişim Steganografi' dir. Yunancada "gizlenmiş yazı" anlamına gelir ve bilgiyi gizleme bilimine verilen addır. Steganografi'nin şifrelemeye göre en büyük avantajı bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu fark edemiyor olmasıdır, böylece içinde bir bilgi aramaz.

İkinci Dünya Savaşı sırasında, New York'taki bir Japon ajanı (Velvalee Dickinson) oyuncak bebek pazarlamacısı kılığı altında saklanmaktaydı. Bu ajan, Amerikan ordusunun hareketlerini bebek siparişi içeren mektuplar içine saklayarak Güney Amerika'daki adreslere gönderiyordu.

Özellikle 1960'larda mor ötesi boya ile yazı yazabilen spreylere ve kalemlere moda idi. Bu kalemlerin yazdığı yazılar, sadece bir mor ötesi ışıkla görülebiliyordu (wikipedia, 2007).

İtalyan bilim adamı Giovanni Porta, on altıncı yüzyılda, iki gram alüminyum ve bir litre sirke karışımından yaptığı mürekkep ile iyice haşlanmış bir yumurtanın kabuğuna yazarak nasıl gizli mesajları sakladığını tarif etmişti. Bu çözelti, gözenekli kabuktan geçerek katılaşmış yumurta akının yüzeyine mesajı yazıyordu. Bu mesaj ancak yumurtanın kabuğu soyulunca okunabiliyordu. M.S. birinci yüzyıl civarlarında Bilge Plinius, thithy-mallus bitkisinin "süt"ünün nasıl görünmez mürekkep olarak kullanılabilceğini yazmıştır. Kuruyunca saydamlaşan bu mürekkep ısıtılınca koyulaşır kahverengileşir. Birçok organik akışkan aynı şekilde "kullanılabilir: karbon zengini oldukları için ısıtılınca kararır. Gerçekten de günümüz casuslarının standart yöntemlerle görünmez mürekkep kullanamadıkları durumlarda kendi idrarlarını kullandıkları bilinmektedir (Singh, 1999).

Günümüze kadar gelebilen gelişmiş ve içinde Mısırlıların da bulunduğu taş yazıtlara bakılırsa insanların güvenli bilgi arayışında olduklarını varsaymak akla uygundur. Kriptografinin kullanımının ilk kaydı Spartanlar'ın (M.Ö. 400) askeri komutanları arasında gizli yazışmaları için çalıştırdığı "Scytale" denen bir şifreleme aracıdır. Scytale,

etrafına, birinin üzerinde deliklerin olduğu, biri de anlaşılma ifade veya rastgele harflerin yazılı olduğu parşömenlerin sarıldığı, uçları sivriltilmiş sopalardan oluşuyordu. Yazılı parşömenin üzerine deliklerin bulunduğu diğer parşömen, sopaların sivri uçları üst üste gelecek şekilde açılır ve deliklerin alttaki parşömende gösterdiği harfler sırasıyla yan yana getirildiğinde açık metin elde edilirdi (Pell, 2006).

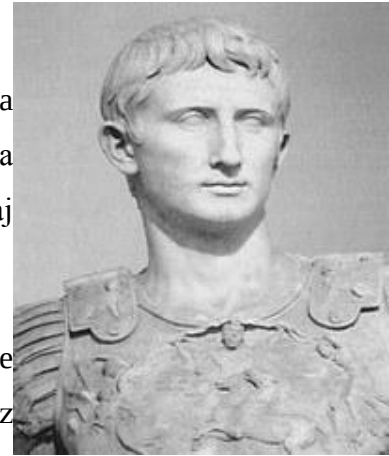
2.4.1. Sezar Şifresi

Yunanlılar'dan Aeneas Tacticus, MÖ 400. yy'da, ilk değişik sıralamaya sahip şifrelemeyi keşfetmiş ve bunu Yunan yazılarına savunmayı geliştirme çalışmalarının bir bölümü olarak uygulamıştır. Başka bir Yunanlı Polybius, "Polybius damatahtası" denen, sonraki şifreleme sistemleri için bilinen birçok benzer eleman içeren bir cihaz kullanarak metin şifrelemenin temellerini ortaya koydu. Ayrıca, Yunanlılar benzer konularda, diğer ulusların ve Romalıların kullandığı ilkel şifreleme tekniklerini de kullanıyorlardı.

"Polybius damatahtası", alfabenin harflerini içeren beşe beşlik bir ızgaradan oluşuyordu. Her harf, ilki harfin bulunduğu satır ve ikincisi de sütun olmak üzere iki sayıya dönüştürülüyordu. Şu halde A için 11, B harfi için 12 ve sonrakiler için ilgili sayılar eşleşirdi. (Eskici, 2005).

Askeri amaçlarla kullanılan belgelenmiş ilk yerine koyma şifresi, Galya Savaşları'nda görünür. Sezar, kuşatma altında ve teslim olmak üzere olan Cicero'ya nasıl mesaj gönderdiğini anlatmıştır.

Buradaki yerine koyma yöntemiyle, Latin harflerinin yerine Yunan harfleri konularak mesaj düşman için anlaşılma duruma getiriliyordu. Sezar mesajın heyecan verici gönderilişini şöyle anlatmıştır:



Şekil 1: Jül Sezar
(MÖ 100 - MÖ 44)

"Haberciye, eğer kampa yaklaşamazsa mesajı bir mızrağın ucuna bağlayıp kampın içine fırlatma talimatı verilmişti. Korkudan kampa çok yaklaşmadığı için mızrağı kimseye

fark ettirmeden kampa doğru fırlattı, ama mızrak kulelerden birine takılı kaldı. Ancak üç gün sonra askerlerimizden biri tarafından görülen mızrak hemen Cicero'ya ulaştırıldı. Cicero mesajı okuduktan sonra sevinç içinde bütün bölüklere bizim yolda olduğumuzu müjdeleyip savunmaya devam emri verdi.” (Singh, 1999).

Bilinen en eski şifreleme yöntemi Sezar şifrelemesidir. Komutanlarına göndereceği mesajların düşmanları tarafından okunmasını istemeyen İmparator, mesajlarında "harf atlama" yöntemi kullanmıştır. Her harfin yerine bir başka harf kullanan Sezar'ın mesajlarını, sadece yöntemi bilen komutanları okuyabiliyordu(Coşkun, 2006).

Sezar'ın yöntemini alfabemize uygulayalım. $M_A = 0, M_B = 1, M_C = 2, \dots, M_Z = 28$ olsun.

Atlama değerini $p \in \mathbb{N}$ kabul edersek (yukarıdaki Örnekte $p = 1$ idi; p 'yi 1'den 28'e kadar herhangi bir tamsayı alabiliriz), o zaman, şifreleme algoritması olan E,

$$E(M_i) = M_i + p \pmod{29} \text{ kuralıyla yazılabilir.}$$

Deşifreleme algoritması da aynı biçimde açıklanabilir. Yukarıdaki p 'yi $q = 29 - p$ ile değiştirin:

$$D(M_i) = M_i + q \pmod{29} \text{ olsun.}$$

Böylece, her i harfi için,

$$D(E(M_i)) = M_i \pmod{29} \text{ olur.}$$

Bu yöntemle en fazla 28 farklı şifreleme yapılabilir. Ama her dilde daha çok kullanılan harflerin ve bazı kalıpların olduğunu düşünürsek, bu Şifreleme yöntemini çözmek o kadar zor değildir.

Sezar Şifresi kırmak, görece kolay olmaktadır. Bir filolog, bir dilde en çok geçen harfleri bulabilir. O harfler ile mesajda en sık geçen harfleri karşılaştırarak hangi harfin

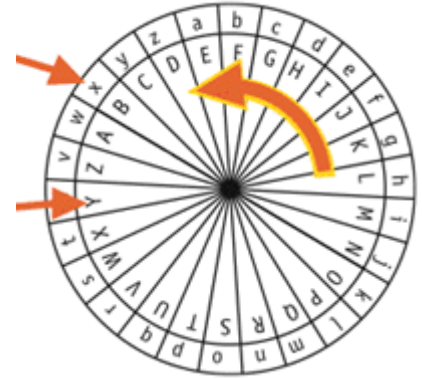
hangi harf ile değiştirildiğini bulabilir. Bu adımların ardından mesaj çözülmüş olur. (wikipedia, 2007).

Tablo 2.1 Sezar Şifresinin 4 Harf Kaydırılmış Hali.

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç

Sezar Şifresi'ni kullanmanın basit bir yolu, alfabenin bütün harflerini bir kâğıt şeridi üzerine yazıp, şeridin başını sonuna yapıştırmaktır. Normal alfabeği 10 kere kaydırarak elde edilen şifre alfabetine göre şifrelenmiş bir mesajda örneğin ITOÖH dizisi SEZAR kelimesinin yerine geçmektedir. Bu format, alfabenin her kaydırılışında farklı sonuçlar vermektedir (Dede, 2007).

İlk gerçek şifre makinesi, on beşinci yüzyılda yaşayan bir şifreci yani Leon Alberti tarafından icat edilmişti. Birden fazla şifre alfabeti kullanan ve şifre oluşturmak için ilk makineyi icat eden de Alberti'ydı.



Şekil 2: Şifre Diski

Alberti'nin şifre diskleri iki bakır diskten oluşuyordu. Bu disklerden birisi büyük, diğeri küçüktü. Merkezlerinden birbirlerine bağlanmışlardı ve ortadaki küçük disk dönebiliyordu. Büyük diskin kenarında normal alfabe, küçük diskin üzerinde de şifreli alfabe bulunuyordu.

Alberti'nin fikri o kadar başarılı oldu ki, şifre diskleri yüzyıllarca kullanıldı. Diskler üzerindeki semboller ve sembollerin dizilişi değişse de, temel prensip aynı kaldı. Hepsinde her zaman iki disk vardı (Kimpton, 2005).

2.4.2. Mesajın Sayılarla Gösterilmesi

Tablo 2.2 Mesajın Sayılarla Gösterilmesi

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

a,1 b,2 c,3... Olacak şekilde eşleştirme yapılır.

A S U

0 21 24

K=5 alarak ve mod 29'a göre «*Öğrenmenin yaşı yoktur.*» cümlesini öteleme şifrelemesini kullanarak şifreleyelim.

Bu durumda $e_k(x)=x+5 \pmod{29}$ ve $d_k(y)=y-5 \pmod{29}$ şeklinde olur.

2.4.3. Anahtar Şifre

Sezar, bu şifreleme yönteminin yeterli olmadığını düşünerek, başka bir yöntem geliştirme çabasına girmiştir. Bulduğu ikinci yöntem, ilkinde göre daha güvenli olan, bir anahtar kullanarak metni şifrelemektir. Örneğin, anahtar 265314 olursa, birinci harfi ikinci konuma, ikinci harfi altıncı konuma, üçüncü harfi beşinci konuma... Koyarak mesaj şifrelenecektir.

Düz alfabe şifre alfabenin üstüne konulduğunda şifre alfabenin üç sıra kaydırıldığı açık şekilde görülür ve bu yüzden bu yerine koyma biçimi çoğunlukla, Sezar'ın kaydırma şifresi, ya da basit bir adlandırmayla, Sezar şifresi olarak bilinir. 1 ile 25 arasında değişen kaydırmalarla 25 farklı şifre elde edileceği açıktır. Aslında eğer kendimizi salt alfabenin kaydırılmasıyla sınırlı tutmayıp, şifre alfabenin, düz alfabenin karıştırılmış herhangi bir şekline konulabileceğini kabul edersek çok daha fazla sayıda birbirinden

farklı şifre elde edebiliriz. Sonuçta 400.000.000.000.000.000.000.000 sayıda farklı sıralama ve dolayısıyla aynı sayıda farklı şifre elde edilebilir.

Hollandalı dilbilimci August Kerckhoffs von Nieuwenhof, *La Cryptographie Mili-teire* (Askeri Kriptografi) adlı kitabında 1883 yılında "Kerck- hoffs İlkesi" olarak şöyle yazıyor: "Bir kriptu sistemin güvenliği, kriptu-algoritmayı gizli tutmaya dayanmamalıdır. Güvenlik, yalnızca anahtar gizli tutmaya dayanır."

Örneğin, gönderici metni göndermek için Sezar şifresi kullanırsa, yalnızca olası 25 farklı anahtar olduğu için şifreleme görece olarak zayıf kalır. Bu durumda düşman, mesajı ele geçirip kullanılan algoritmanın Sezar kaydırması olduğunu tahmin edebilirse yalnızca 25 olasılığı kontrol etmesi yetecektir. Bir taraftan da eğer gönderici, şifre alfabenin düz alfabenin herhangi bir düzenlemesi olabileceği daha genel bir yerine koyma algoritması kullanırsa, olası anahtar sayısı 400.000.000.000.000.000.000.000 olacaktır (Eskici, 2005).

Aslında eğer gönderici, olası anahtarların sayısında küçük bir azalmayı kabullenebilirse daha da basit bir anahtar kullanmak mümkündür. Düz alfabeyi rasgele yeniden sıralamak-tansa, gönderici bir anahtar sözcük ya da anahtar cümlecik seçer. Örneğin, JÜL SEZAR anahtar cümlecik olarak kullanmak için önce bütün boşluklar ve tekrarlanan harfler atılır (JÜL SEZAR) ve bu, karıştırılmış şifre alfabenin başı olarak kullanılır. Şifrenin geri kalanı, alfabenin geri kalan harflerinin sıralarını koruyarak bu anahtar cümlecığının sonuna eklenmesiyle oluşturulacaktır. Dolayısıyla şifre alfabe şöyle olacaktır:

Tablo 2.3 Şifreli Alfabe

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
j	ü	l	s	e	z	a	r	ş	t	u	v	y	b	c	ç	d	f	g	ğ	h	ı	i	k	m	n	o	ö	p

Bu yolla şifre alfabe üretmenin avantajı, anahtar kelime ya da cümlecüğün, dolayısıyla şifre alfabenin kolay hatırlanabilmesidir.

2.4.4. Frekans Tablosu

Devletin gizli bilgilerinin şifrelemesinin yanı sıra, vergi kayıtlarının resmi yetkililerce şifrelendiğinin belgelenmesi de kriptografinin yaygın ve düzenli olarak kullanıldığını göstermektedir. Bu konudaki diğer kanıtlar, onuncu yüzyılda yazılmış ve kriptografiye adanmış bir bölüm içeren Adab El-Küttab (Sekreterin El Kitabı) gibi çeşitli yönetim rehberlerinde bulunabilir.

Yöneticiler genellikle, normal alfabenin harflerinin yer değiştirmiş formu olan şifreli alfabeyi kullanıyorlardı. Ama bunun yanında diğer bazı sembolleri içeren şifreli alfabeleri kullandıkları da oluyordu. Örneğin, normal alfabedeki a harfi # ile, b harfi + ile yer değiştirebiliyordu. Arap bilimciler şifreleri kullanmanın yanı sıra şifreleri kırmada da başarılıydılar. Aslında, anahtara sahip olmadan bir mesajı bulma bilimi olan kriptanalizi bulanlar araplardır. Kriptografi gizli yazı için yeni teknikler geliştirirken, gizli mesajları çözebilmek için bu yöntemlerin zayıf yanlarını bulmaya çalışan da kriptanalisttir. Arap kriptanalistler, yüzyıllarca kıramamış bir şifre olan tek alfabeli yerine koyma şifresini kırmayı başardılar.

Kriptanalizin keşfi, dünyevi birçok konuyu daha iyi kavrayabilmenin yanında din bilimciliğinin de gelişmesine dayanıyordu. Basra, Kûfe ve Bağdat'ta ilâhiyatçıların Hz. Muhammed'e inen ve Kuran'da yer alan vahiylerin ayrıntılı analizlerini yaptıkları, ilahiyat okulları kuruldu. İlahiyatçılar her bir vahiyde geçen sözcük sayısı yoğunluğuna (kelime frekansı) bakarak vahiylerin geliş sırasını bulmaya çalışıyorlardı. Bu kurama göre bazı sözcükler sonradan dile girmişlerdi. Bu yüzden bir vahiy içinde daha sık görünüyorlarsa bu, sözü geçen vahyin kronolojik olarak daha sonra indirildiği anlamına geliyordu. İlahiyatçılar aynı zamanda Peygamber'in gündelik söylemlerinden oluşan Hadisleri de çok yakından incelediler. Her bir hadisin gerçekten de Peygamber tarafından söylenmiş olduğunu göstermeye çalıştılar. Bu, sözü geçen metinlerin Hz.

Muhammed'in kullandığı dilsel kalıplara uygun olup olmadığını sınavabilmek amacıyla, sözcük kökleri ve cümle yapılarının ayrıntılı analiziyle yapılmaktaydı.

Din bilimciler incelemelerini sözcük düzeyinde bırakmadılar. Tek tek bütün harfleri mercek altına aldılar ve özellikle bazı harflerin diğerlerinden daha çok kullanıldığını keşfettiler.

Biraz da tanımlayıcı El, ön ekinin kullanımından dolayı e ve l harfleri en yaygın kullanılan harfler olurken, c harfi bunların onda biri sıklıkta kullanılmıştı. İlk bakışta önemsiz gibi görünen bu gözlem, kriptanalizde İlk büyük sıçramanın gerçekleşmesini sağladı. Harflerin frekansındaki değişimlerin şifreleri kırmak için kullanılabileceğinin ilk olarak kim tarafından fark edildiği bilinmiyorsa da, bu tekniğin tarifini ilk yapan dokuzuncu yüzyıl bilim adamı Ebu Yusuf Yakup İbni İshak İbni Es-Sabbah İbni Ümran İbni İsmail El-Kündi'dir. "Arapların Filozofu" olarak da bilinen El-Kündi; tıp, astronomi, matematik, dilbilimi ve müzik hakkında toplam 290 kitap yazmıştır. En büyük araştırması, Kriptografik Mesajların Deşifre Edilmesi Üzerine bir Yazı, İstanbul'da 1987 yılında kamuoyuna açılan Süleymaniye Osmanlı Arşivinde ortaya çıkarılmıştır. Arapça söz dizimi, ses bilimi ve istatistik hakkında oldukça ayrıntılı tartışmaları içermesine karşın El-Kündi'nin devrimsel kriptanaliz sistemi iki kısa paragrafta özetlenmektedir:

“Eğer yazıldığı dili biliyorsak şifreli bir mesajı çözmenin bir yolu, aynı lisana ait yaklaşık bir sayıyı 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, ikinciye ikinciyle vs. değiştiririz. Sonuçta çözmeye uğraştığımız metin içindeki her harfe karşılık normal alfabeden bir harf bulana kadar bunu tekrarlarız.”

El-Kindi'nin yukarıda da belirtilen bütün alanlara özgün katkılar yapmış olması şaşırtıcıdır. Nitekim Matematikte, sayı sistemi üzerine dört kitap yazmıştır ve modern aritmetiğin büyük bir bölümünün kuruluşunu hazırlamıştır. Arap sayılar sistemi'nin büyük ölçüde el-Harizmi tarafından geliştirilmiş olduğunda şüphe yoktur, ancak El-Kindi de bu konu üzerine zengin katkılarda bulunmuştur. Aynı zamanda, astronomi ile ilgili çalışmalarında yardım etmesi için küresel geometriye de katkıda bulunmuştur (fizik semineri, 2007).

Bilinen kayıtlı ilk kriptanaliz açıklaması 9.yy da Matematikçi olan Ebu Yusuf Yakup tarafından “A Manuscript on Deciphering Cryptographic Messages. ” eserinde yer alıyor. Bu yöntem frekans analizine dayanıyor (Örencik, 2006).

1412'de Al-Kalk-Shandi ansiklopedisi Subh Al-A'Sha adında birkaç kriptosistemin özellikleri hakkında oldukça nitelikli bilgiler veriyordu. Bu ansiklopedi birkaç örnekle harf kullanım sıklığı tekniğinin kriptanalizde nasıl kullanılacağı konusunda ilk açıklamaları da içeriyordu.

Avrupa kriptografi tarihi Orta Çağ'da Papalık İtalyası'nın şehirlerinde gelişmeye başlamıştır. İlk şifrelerin karmaşıklığı yalnızca ünlü harflerin yerine koyma yöntemiyle değiştirilmesi düzeyindeydi. Avrupa'nın kriptografide ilk klavuzu olan Circa 1379, Parma'da, Papa VII. Clement adına çalışan Gabriele de Lavinde tarafından yazılan, şifrelerden oluşan bir derlemeydi. Bu klavuz yazışmalar için bir anahtar serisi, harfler ve boşluklar için kullanılan semboller ile kelimeler ve isimlere karşılık gelen iki karakter kodu içeriyordu. Nomenclators denen ilk kod sözlüğü yavaş yavaş gelişti ve birkaç yüzyıl boyunca bütün yakın Avrupa devletleri ile yazışmaların en büyük destekçisi oldu. 1470'de Trattati ve Traicté'de ilk şifreleme sistemini açıklayan Leon Battista Alberti'ye atıfta bulunan Blaise de Vigenère, 1586'da yayınladığı eserinde, ilk otomatik anahtar sistemine sahip şifreleme ve düzmetnin oluşturulmasında kullanılan ortak sembol tablosunu içeren şifrelemeyi onun kadar iyi anlatmıştır (Pell, 2006).

1860'larda diplomatik iletişim ve şifre sistemleri için ortak olarak kullanılmış birçok kod askeri iletişim için de ender bulunan uygulamalardan biri haline gelmiştir. Birleşik Devletler Sivil Savaşları sırasında şifreleme sıkça kullanılmıştır. Konfederasyon Ordusu, Vigenère ve bazen de mono alfabetik şifreleme sistemlerini öncelikle kullandı. Daha sonraları Roma orduları iletişimlerinde Sezar'ın (alfabede 3 harf kaydırma) şifrelemesini kullanmışlardır.

Böylece bu andan itibaren şifreleme sistemlerinin bu ihtiyaçlarla buluşması beklenirdi. 19.yüzyılda Kerchoffs modern şifrelemenin prensiplerini yazdı. Bu ölçüm araçlarından yoksunlardı. Birisi en sonunda şifrelemenin nihai hedefine erişecek ve %100 güvenli sistemi bulacaktı. 1948 ve 1949 yıllarında Claude Shannon 'un "A Mathematical Theory of Communication" ve "The Communication Theory of Secrecy Systems" isimli yazılarıyla şifrelemeye bilimsel altyapı eklendi. Bu yazılar bütün umut ve önyargıları süpürüp götürdü. Shannon, bir kaç yıl öncesine ait olan Vernam 'ın şifrelemesinin (One Time Pad olarak isimlendirilen şifreleme) varolan tek koşulsuz güvenli sistem olduğunu ispatladı. Ne yazık ki Vernam 'ın şifrelemesi de pratikte kullanışlı değildi... Bugünlerde güvenlik sistemlerinin değerlendirilmesinde sayısal güvenliğin temel alınmasının nedeni budur (Pell, 2006).

Tablo 2.4 Türkçede Harflerin Kullanım Sıklığı

A	%12
E	%8
İ,K,L	%7
R	%6
N,T	%5
I,M	%4
O,S,U	%3
B,D,Y,Ü	%2
Ç,Ş,Z	%2
H,G,P	%1
F,Ö,V	%1
Ğ	%2
Yazım Hataları	%2

2.4.5. Osmanlıda Gizli Yazı

OSMANLI Devleti'nde maliye, vakıf ve tapu kayıtları gibi gizlilik isteyen evrakta, "siyakat" adı verilen bir yazı kullanılırdı. Siyakat yazısı süratli yazıldığı için harfler küçülmüş ve noktalar konulmamıştır. Kelimeler, klişe haline gelmiştir. Siyakat yazısıyla birlikte normalde kullanılan rakamlar kullanılmaz; "Divan rakamları" denilen sayıların Arapça yazılışının stilize edilmiş biçimi tercih edilirdi. Bunları sadece, özel ihtisası olanlar okuyabilirdi. III. Selim zamanında, Avrupa'da daimi elçilikler kurulunca, gizli yazışmalarda şifre kullanılmaya başlandı. Bu şifrelerde her harfin bir rakam karşılığı vardı. Kullanılan şifre her zaman aynı olmaz, zaman zaman değiştirilirdi. Yazılar ya tamamen rakamla şifrelenir, ya da bazen rakamların arasına önemli olmayan bazı kelimelerin aslı yazılırdı. Bazen de elçiler yazıların gizlilik arzeden kısımlarını yine harflerle şifrelerlerdi. Bu tür yazılarda harfler alfabedeki anlamlarından farklı manalarda kullanılırlardı. Elçilerin şifreli yazıları İstanbul'a geldiğinde şifre odasında çözüldükten sonra, ilgili yere gönderilirdi (Bilallar, 2005).

2.4.6. Kod Sözcükler

Tek alfabeli yerine koyma şifresini destekleyecek bir diğer girişim de kod sözcüklerin kullanımıydı. Kod terimi genellikle gizli iletişim için kullanılan herhangi bir yöntemi tanımlamakta kullanılır ve günlük dilde oldukça geniş anlamlar içerir.

Teknik olarak kod, sözcükler düzeyinde yerine koyma olarak tanımlanırken, şifre harf düzeyinde yerine koyma olarak tanımlanır. Bu yüzden, şifreleme terimi, bir mesajı şifre kullanarak, kodlama ise kod kullanarak karmaşık hale getirmek anlamına gelir. Aynı şekilde, deşifre etme terimi şifreli bir mesajı yeniden düzenlemeyi, kod çözme terimi ise kodlanmış bir mesajı özgün biçimine çevirmeyi anlatır.

İlk bakışta kodlar şifrelerden daha iyi güvenlik sağlıyor gibi görünür; çünkü frekans analizine karşı daha dayanıklıdırlar. Bir kodu deşifre edebilmek için yüzlerce ve hatta binlerce sözcüğün gerçek değerini bulmak gerekirken tek alfabeli bir şifreyi çözmek için

yalnızca alfabedeki harflerin her birinin değerini bulmak yeterli olacaktır. Kodları daha yakından incelersek, şifrelerle karşılaştırıldıklarında, uygulamada iki temel noktada zayıf kaldıklarını görürüz. Birincisi, gönderici ve alıcı şifre alfabede 29 harfin yeri (anahtar) konusunda anlaştıktan sonra herhangi bir mesajı şifreleyebilirler; ama bir kod kullanarak aynı esneklik düzeyine ulaşabilmek için düz metindeki olası binlerce sözcüğün her birinin yerine kullanılacak kod sözcükler üzerinde anlaşmaları gerekir. Kod kitabı yüzlerce sayfalık bir sözlük gibi olacaktır. Başka bir deyişle, bir kod kitabı derlemek başlı başına görev, bunu sağa sola taşımaksa yine başlı başına bir sorundur. İkincisi, bir kod kitabının düşman eline geçmesi yıkımdır (Singh, 1999).

2.4.7. Pigpen Şifresi

Eski Yunan'da savaşlar ve ticaret yoğunluğuydu. Bu nedenle askeri ve ticari bilginin güvenilir şekilde iletilmesini sağlamak için Yunanlılar bazı şifreleme sistemleri geliştirdiler. Yunanlı Polybius, Polybius damatahtası denen, sonraki şifreleme sistemleri için bilinen birçok benzer eleman içeren bir cihaz kullanarak metin şifrelemenin temellerini ortaya koydu. Ayrıca, Yunanlılar benzer konularda, diğer ulusların ve Romanların kullandığı ilkel şifreleme tekniklerini de kullanıyorlardı. Polybius damatahtası alfabenin harflerini içeren beşe beşlik bir ızgaradan oluşuyordu. Her harf, ilki harfin bulunduğu satır ve ikincisi de sütun olmak üzere iki sayıya dönüştürülüyordu. Şu halde A için 11, B harfi için 12 ve sonrakiler için ilgili sayılar eşleşirdi. Örnek: Polybius şifrelemede kullanılan ızgara yukarıda ifade edildiği gibi 5×5 birimlik değil, kullanılan alfabe hatta şifrelenecek metnin içerdiği alfabe harfleri sayısına bağlı olarak istenen boyutta tasarlanabilir (Eskici, 2005).



Şekil 3: Pigpen Şifresi

2.4.8. Mors Kodu

1830'larda telgrafın icat edilmesiyle mesaj göndermek için yeni bir yöntem ortaya çıktı. Sistem çok kapsamlı değildi. Sadece iki alternatif söz konusuydu. Tel boyunca ya elektrik akımı vardı ya da yoktu. Akımın büyüklüğü belirlenemiyordu ancak, akımın süresi değiştirilebiliyordu. Telgrafın mucidi, Samuel MORSE, nokta ve çizgilerden oluşan yeni bir alfabe ortaya koydu (Kimpton, 2005).

Tablo 2.5 Mors Alfabeti Gösterimi

Mors Alfabeti					
A	.-	N	-.	0	----
B	---.	O	---	1	.----
C	-.-. .	P	.-.-.	2	..---
D	-. .	Q	--.-	3	...--
E	.	R	.-.	4	-
F	..-. .	S	...	5	
G	--.	T	-	6	-....
H		U	..-	7	--...
I	..	V	...-	8	---..
J	.-.-.	W	.-.-	9	-----.
K	-.-	X	-.-.-	Nokta	.-.-.-
L	.-..	Y	-.-.-	Virgül	--..--
M		Z		Soru İşareti	..-
--		--..		..	

Mors alfabesi basitçe iki çeşit sinyalin (kısa ve uzun sinyal) farklı kombinasyonlarının harfleri, sayıları ya da noktalama işaretlerini oluşturduğu bir haberleşme dilidir. Genellikle elektrik ya da radyo sinyali kullanılarak uzak bir noktaya yazılı bir metnin ulaştırılmasında kullanılır.

Kısa ve uzun sinyallerin dışında aralardaki sessizlikler de anlam taşımaktadır. Kısa aralık harfler arasında, orta uzunlukta aralık kelimeler arasında ve uzun aralıklar ise cümleleri birbirinden ayırmakta kullanılır.



Şekil 4: Telgraf

Örneğin:

-- --- .-. ... / -. --- -. ...-

M O R S (boşluk) K O D U

Mors alfabesi, ilk kez 1832'de telgraf ile ilgilenmeye başlayan Samuel Morse tarafından 1835 yılında oluşturuldu. 1837'de ise ilk kez kullanıma başlandı. İlk hat Baltimore, Maryland ile başkent Washington arasında kuruldu. İlk mesaj incilden bir cümleyi içerirken, gönderim tarihi ise 24 Mayıs 1844 idi.

Orjinal mors kodu kısa ve uzun sinyallerin kombinasyonunun bir sayıya karşılık gelmesinden oluşmuştu. Her sayı da bir harfe karşılık geliyordu.

Ancak Morse'un bulduğu sistemin kullanımı kolay değildi. Alfred Veil ile bu konu üzerine ortaklaşa çalışmaya başlayan Morse, bir süre sonra Veil'in önerdiği sistemin daha basit bir sistem olduğuna ikna oldu. Veil'in sisteminde kısa ve uzun sinyallerin yanı sıra duraklamalar da kullanılıyordu. Bu sistem daha sonra Amerikan Mors Kodu olarak isimlendirildi.

Mors kodu birçok değişik metod ile iletilebilir. Mors alfabesi sesli olarak iletilebilmesinin yanı sıra, radyo sinyallerinin açılıp kapatılmasıyla, telegraf tellerinden geçen elektrik akımıyla, mekanik yolla ya da görsel (ışıkların yanıp sönmesi gibi) yollarla da iletilebilmektedir.

Bunun dışında mors alfabesi ile haberleşme yazılı mesajlaşmadan daha hızlıdır. Hatta bazı cep telefonu üreticileri mors alfabesi uyumlu cep telefonu üretiyorlar.

Günümüzde amatör ve askeri radyoculardan yarı otomatik ve tam otomatik cihazlar sayesinde dakikada 40 kelime anlayan cihazlar yapılmıştır. Bu cihazlara "bugs" yani Türkçe'siyle "böcek" adı veriliyor.

24 Mayıs 2004 tarihinde ise ilk telgrafın 160. yıl dönümünde Uluslararası Telekomünikasyon Birliği(ITU), "@" işaretini de Mors alfabesine ekledi. @ işareti (AT COMMERCIAL) kelimesinin baş harfleri olan "AC" harflerinin karşılığı ile ifade ediliyor (mors.gen.tr, 2007).

2.4.9. Bayraklar

Bayraklar sadece insanların kollarına dikkat çekmek için kullanılmaz. Yüzlerce yıldır bir gemiden diğerine mesaj iletmek için bayraklar kullanılmıştır. Eskiden her ülkenin kendi sistemi vardı ancak 1855 yılından itibaren uluslar arası bir kod kabul edilmiş ve böylece dünyanın her yanından gelen gemiler birbirlerinin mesajlarını anlayabilir hale gelmiştir. Bu kodda alfabenin her harfi ve önemli mesajlar için farklı bir bayrak kullanılmaktadır (Kimpton, 2005).

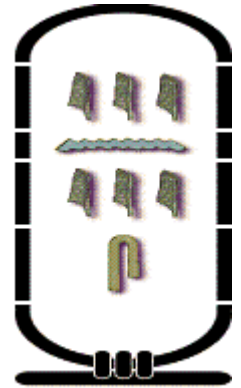
2.4.10. Hiyeroglif

Hiyeroglif, Yunanca “Hieros (Kutsal) + Glypho (Yazıt)” kelimelerinden oluşur ve “Kutsal Yazıt” demektir. Hiyeroglif yazısı altında şematik şekillerden oluşan bir yazı anlaşılır. Şu tür hiyeroglifler vardır:

1. Mısır Hiyeroglifleri

2. Luv Hiyeroglifleri

3. Urartu Hiyeroglifleri



Şekil 5: Hiyeroglif Yazısı

Mısır hiyeroglif yazısı birbirinden kolaylıkla ayırt edilebilecek yüzlerce sembolden oluşur. Her işaret belli bir sesi veya nesneyi temsil eder. Bu yazı soldan sağa veya sağdan sola ya da yukarıdan aşağı yazılabilir, okumak için ölçüt sembollerdeki insan ya da hayvan figürlerini baktıkları yöndür.



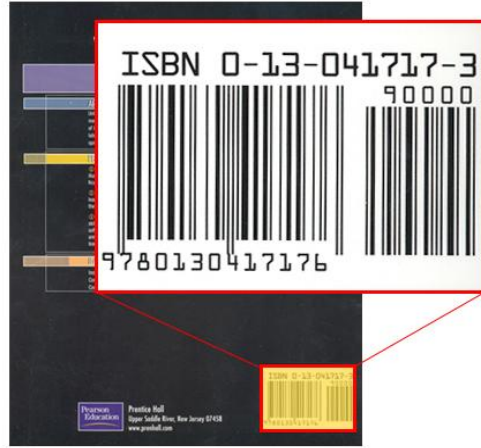
Kimi işaretler 1 harfe, kimileri 2, kimileri de 3 harfe karşılık gelir. Buna örnek olarak latin kökenli dillerde 'x' işaretinin Türkçe deki 'ks' harflerine karşılık gelmesi verilebilir. Ayrıca yazılan kelimenin anlamını güçlendiren ve tamamlayan çizimler de vardır. Mesela bastonlu adam çiziminin yaşlı kelimesini tamamlaması gibi (wikipedia, 2007).

Şekil 6: Hiyeroglif Yazısı

2.4.11. Isbn

ISBN (International Standard Book Number), hızla değişen ve gelişen dünyamızda artan bilgi üretimini izleyebilmek ve geniş çapta kullanıma sunmak için 1972 yılında Uluslararası Standartlar Organizasyonu (ISO) tarafından hazırlanan ve üye ülkelerin onayı ile yürürlüğe giren bir kitap numaralama sistemidir.

Amaç, kitap numaralarının uluslararası bir yöntemle düzenlenerek standardize edilip, Uluslararası Standart Kitap Numarası (ISBN) verilerek belirli bir yayımcının yayınladığı bir materyalin kimliğini tanımlamaktır.



Şekil 7: ISBN

ISBN sistemi, yayınlanan her materyale bir tanımlama numarası verir. Bu numara dört grup ve on haneden oluşur. Birinci grup yayının yapıldığı ülkeyi, ikinci grup yayımcıyı, üçüncü grup materyale ait sıra numarasını belirler. Dördüncü grup da ISBN' nin doğruluğunun denetimini sağlayan tek haneli bir rakamdır.

Örneğin; ISBN 1995 Türkiye Yayımcı Kataloğunun numarası “ISBN 975-17-1627-6”dır. Bu numarada 975Türkiye’yi, 17Kültür ve Turizm Bakanlığı’nı, 1627 Kültür ve Turizm Bakanlığı’nın ISBN alan yayını (1995 Türkiye Yayımcı Kataloğu), 6 ise denetim numarasını göstermektedir (Kültür turizm, 2007)

2.4.12. Ebced Hesabı

“Ebced” kelimesi, Arap alfabesindeki harflerin kolay ezberlenebilmesi için, harflerin birleştirilmesiyle meydana gelen 8 anlamsız kelimenin ilkidir. Ebced, ilk kelimenin adı olduğu gibi, aynı zamanda diğer kelimelerin tümünün de adıdır.

Ebced’in en büyük özelliği “Ebced hesabı” adı verilen bir işlemde kullanılmasıdır. Buna göre, ebced ifadesindeki her harfin bir sayı değeri vardır ve bu değerlerden istifadeyle birçok konuda pek çok işlemler yapılmıştır. İşte bunların her birine bu hesabın adı verilir. Ebced alfabe düzeninin harfleri 1’den 9’a, 10’dan 90’a, 100’den 1000’e doğru

numaralandırılır. Ayrıca bu alfabede gözükmeyen “pe” harfi “be ” gibi, “çe” harfi de “cim” gibi kabul edilerek onların sayı değerlerini alır.

Eskilerin “hisâb el-cümel” dedikleri, ebced hesabının 4 çeşidi vardır: “Büyük”, “en büyük”, “küçük” ve “en küçük” ebced hesabı.

Küçük ebced hesabı ebced hesaplarının esasını teşkil eden yöntemdir. Diğer yöntemler daha çok falcılık, cifr veya cefr (gaipten haber verme), büyüculük, ilm-i hurûf (harflerden anlam çıkarıp yorumlama bilimi) gibi alanlarda kullanılmıştır (Coşan, 1978 ve Oral, 2003)

Ebced hesabı günlük haberleşmelerde, büyü ve muska olarak, simgesel anlam yükleyerek, doğan çocuklara isim vermede, resmi devlet kayıtlarında ve tarih düşürmede kullanılmıştır.

1	ا
2	ب
3	ج
4	د
5	هـ
6	و
7	ز
8	ح
9	ط
10	ي
20	ا
30	ل
40	م
50	ن
60	س
70	ع
80	ف
90	ص
100	ظ
200	ر
300	ش
400	ت
500	ث
600	خ
700	ذ
800	ض
900	ظ
1000	ع

Şekil 8: Sayıların Gösterimi

2.4.13 Vigenere Şifresi

1460 yılında bir gün, Alberti, Vatikan'ın bahçesinde dolaşırken arkadaşı ve aynı zamanda papalığın sekreteri olan Leonardo Dato'ya rastladı. Leonardo kendisine kriptografinin bazı inceliklerini anlatmaya başladı. Yaptıkları bu ayaküstü konuşma, Alberti'nin yeni bir şifreleme biçimi olduğuna inandığı bir yöntemin ana hatlarını ortaya koyacak bir deneme yazmasına yol açtı. O zamanlarda bir mesajı şifrelemek için, bütün yerine koyma şifreleri tek bir şifre alfabesi gerektiriyordu.

Alberti, şifreleme sırasında iki ya da daha fazla alfabe kullanılmasını ve bu yolla potansiyel kriptanalistlerin aklını karıştırmayı önerdi. Alberti şifrelemede son bin yılın en önemli keşfine çok yaklaşmasına karşın, bu kavramı bütün bir şifreleme sistemi şeklinde geliştiremedi. 1523 doğumlu Fransız diplomat Blaise de Vigenere, bu görevi üstlendiler. Vigenere, yirmi altı yaşındayken Roma'ya iki yıllığına diplomatik bir görevle atandığı za man, Alberti'nin, Trithemius'un ve Porta'nın çalışmalarını gördü. İlk başlarda kriptografiye olan ilgisi tümüyle pratik ne denlerden. yani diplomatik görevinden kaynaklanıyordu. Yirmi dokuz yaşında, yeterince para biriktirdiğine inanıp kendi ni tümüyle akademik çalışmalara verme kararı aldı. İşte tara bu noktadan sonraAlberti, Trithemius ve Porta'nın çalışmalarını daha derinden inceleyip bir araya getirerek tutarlı v güçlü bir yeni şifre sistemi ortaya koydu.

Alberti, Trithemius ve Porta'nın çok büyük katkıları olmasına karşın, bulunan bu şifre ona son şeklini veren Vigenenin adı ile anılmaktadır. Vigenere şifresinin gücü bir mesajı şifrelemek için bir değil, birbirinden farklı 26 şifre alfabesi kullanmasından kaynaklanır (Singh, 1999).

Tablo 2.6 Vigenere Tablosu

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

Çok alfabelilik özelliği, vigenere şifresini güçlü kıldığı halde, uygulamasındaki zorluk yaygın kullanılmasını engellemiştir. Vigenere şifresini uygulamak için gerekli yük birçok kişiyi bu şifreyi kullanma düşüncesinden vazgeçirmiştir.

2.4.14. Modüler Aritmetik

$a, b, m \in \mathbb{Z}$, $m > 0$ olsun. Bu takdirde, $a \equiv b \pmod{m} \leftrightarrow m \mid a - b$.

2.4.15. Affine Şifresi

Simetrik (Sezar şifreleme metodu) şifreleme yöntemi ile yazı üzerinde 27 farklı dönüşüm yapılabiliyordu. Biz İngiliz alfabesini göz önünde tutarsak $26-1=25$ dönüşümden söz etmemiz gerekir. Buda simetrik şifreleme yönteminin güvenli olmadığını gösterir. Afin yöntemi ile simetrik şifreleme yöntemi biraz daha genelleştirilmiştir ve güvenlik azda olsa simetrik şifreleme yöntemine göre daha güçlüdür. Tabi bu kağıt kalem kriptolojisinin bir örneği olduğundan bunu günümüz koşullarına göre düşünürsek. Çok çok zayıf bir yöntem olduğunu görürüz. Fakat bu bize kriptolojinin temel mantığını kavratmak için güzel bir örnek teşkil etmektedir.

$y=(ax+b), \text{mod}(m)$ fonksiyonunu göz önüne alalım.

Burada x düz metindeki harflerin sayısal karşılığı, m düz metinde kullanılan alfabenin karakter sayısı, a ve b gizli sayılarımız ve y de fonksiyonumuzun işlem sonucunda aldığı değerdir. Y nin x e geri dönüşümü ise $x=\text{ters}(a)(y-b), \text{mod}(m)$ formülü yardımıyla hesaplanır. $\text{Ters}(a)$, a ile çarpımının modülo m e göre sonucu 1 olan sayıdır. Bunun kısaca şöyle ifade edebiliriz.

$$(a * \text{ters}(a)) \text{mod} m = 1$$

Aşağıdaki örnekte gördüğümüz gibi $y=11x+4, \text{mod}(26)$ şifreleme fonksiyonunu kullandığımız da E ve S harfleri W ve U şeklinde şifreli hallerini alır. Hesap modülü 26 aritmetiğini içerdiğinden, eğer çarpan 26 ile en büyük ortak bölene sahip ise bazı karakterler beklenen sonucu vermeyebilir. Bu yüzden m ve a nın en büyük ortak böleni 1 olmalıdır. Yani aralarında asal olacak şekilde seçmeliyiz. (Demir, 2007)

2.5. ASAL SAYILAR

$\pm 1,0$ dan farklı olan ve triviyal bölenlerinden başka hiçbir böleni bulunmayan bir tamsayıya asal sayı denir. (Özdemir, A.Ş, 2001)

Asal sayılar, yalnız ve yalnız iki böleni olan doğal sayılardır. Kendisinden ve 1 sayısından başka böleni olmayan, 1'den büyük pozitif tam sayılar biçiminde de tanımlanmaktadır. Yüzden küçük asal sayılar 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 ve 97'dir.

Öklid (Euklides)'ten beri asal sayılar sonsuz olduğu bilinmektedir, fakat asal sayılar hakkında pek çok başka soru hala daha cevapsızdır. Bunlardan en ünlü ikisi aralarındaki fark iki olan asal sayılar (örneğin 11 ve 13, veya 29 ve 31) hakkındaki ikiz asallar konjektürü ve asal sayıların doğal sayılar içersindeki dağılımı hakkındaki Riemann Hipotezidir. Sayılar teorisi'nin en önemli uğraşı asal sayılar hakkındaki bu tür sorulardır. Asal sayılar ayrıca kriptografi alanının da yapı taşlarıdır (Nesin, 2006).

2.6. HALKA AÇIK KRİPTOLOJİ

Açık anahtarlı sistemler karakteristik olarak, birisi gizli tutulan, diğeri ise genel kullanım için açılmış olan iki anahtarla çalışan kriptografik algoritmalar kullanırlar. Uygulamaya bağımlı olarak, gönderici, ya kendisinin özel anahtarını, ya alıcının genel anahtarını ya da ikisini birden, kimi kriptografik fonksiyonları gerçeklemek için kullanır. Geniş bir bakış açısı ile, açık anahtarlı kripto sistemlerin kullanımını üç kategoride incelenir:

Şifreleme/DeŞifreleme: Gönderici, bir mesajı alıcının genel anahtarı ile şifreler.

Dijital İmza: Gönderen, mesajı kendi özel anahtarı ile imzalar. Bu imzalama, mesajın tamamını yada önemli görülen belirleyici bir kısmını şifrelemek ile yapılır.

Anahtar Değişimi: İki taraf ortaklaşa bir oturum anahtarını değiş tokuş ederler.

Kimi algoritmalar, bu özelliklerden sadece bir yada iki tanesini gerçekleştirebilirken, bazıları bunların tümünü gerçekleştirebilir (Menezes, Ooscot ve Vanstone 1996)

2.6.1. Rsa

RSA bir tür Açık anahtarlı şifreleme yöntemidir. Güvenliği, tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanır. Hem mesaj şifreleme hem de elektronik imza amacıyla kullanılabilir.

RSA algoritması 1977'de Ron Rivest, Adi Shamir ve Len Adleman tarafından yaratılmıştır ve RSA da bu üç kişinin soy isimlerinin ilk harflerinin bir araya getirilmesi ile oluşturulmuştur.

2.7. DÜNYA SAVAŞLARI SIRASINDA KRİPTOLOJİ

İlk dünya savaşı sırasında müttefiklerin çift taraflı çalışan şifreleme sistemleri hemen hemen sadece taktik iletişimi için kullanılırken, kodlama sistemleri hala çoğunlukla yüksek-komuta iletişiminde ve diplomatik iletişimde kullanılıyordu. Birleşik Devletleri'nin Signal Corps şifreleme sistemi gibi özel bazı şifreleme sistemlerine rağmen, üst rütbelerin iletişimlerinin sağlanması amacıyla geliştirilmiş bazı şifreleme sistemleri savaşın sonuna dek kullanıldı. Bunların en ünlüsü Alman ADFGVX fraksiyonel şifresiydi. 1920'lerde telgraf ve radyo ile birlikte sağlanan ileri mekanik ve elektromekanik teknolojisi, kriptoygıt ve şifre makine rotorlarının gelişiminde devrim getirmiştir. 1921 ve sonraki on yılda Amerikalı mekanik şifre sistemleri tasarımcısı Edward Hebern ABD'nin kullandığı, giderek gelişen bir rotor serisi tasarladı. Bu çalışma şüphesiz ki ABD'ye ikinci dünya savaşında kriptolojide önemli bir yer sağladı. Hollandalı Hugo Koch ve Alman Arthur Scherbius gibi Avrupalılar, İkinci Dünya Savaşı'nda kullanılan Alman Enigma makinesi gibi en ünlü tarihi ilklerden bağımsız olarak bir rotor kavramı ortaya koyup tasarladılar. Bu makineler İngilizler tarafından İkinci Dünya Savaşı sırasında kullanılan TYPEX için de öncü oldular (Pell, 2006).

2.8. ENİGMA

Bu 1919'da Alman Hugo Koch tarafından tasarlanıp geliştirilen bir şifreleme makinesinin kod adıdır. Güvenilirliği istatistiksel analize dayanıyordu. Alman hükümeti modern askeri kuvvetlerinin yeni ihtiyaçlarını karşılarken güvenliğine bu makineyi de uyarlamıştı. Bu, Almanya'nın askeri servislerinin, haber alma örgütlerinin ve sivil polisin, standart şifre makinesi olmuştu. İleri uç birliklerinin taktik komutasından başka, tek tek uçaklar, tanklar ve gemiler için de kullanılıyordu. Makine düz metin harflerini şifre metin harfleri ile değiştirmek için her biri bir harfe karşılık gelen 26 dişli, üç rotorlu bir sistem üzerine kuruluydu. Rotorlar birbirleri etrafında hızla dönebilirlerdi, böylece Sezar Şifresi'nde olduğu gibi çok sayıda harf değişimi olabilirdi.



Şekil 9: Enigma Makinesi

Rotorlar birleşme yerlerinden birbirlerini döndürürdü, böylece her yerdeğiştirmede $26 \cdot 26 \cdot 26 = 17576$ farklı seçenek oluşurdu. Alıcının mesajı deşifrelemesi için ilk rotor ayarlarını bilmesi gerekirdi, sonra düz metni bulabilmek için şifre metin makineye verilirdi. Birleşik Devletler İkinci Dünya Savaşı sırasında M-134-C (SIGABA) şifre makinesini yaptı. İkinci Dünya Savaşı'nın Japon şifre makinesi Hebern ve Enigma makinesi ile ilginç bir şekilde benzerliğe sahipti.

İkinci Dünya Savaşı sırasında kriptanalizin en büyük başarıları Polonyalı ve Britanyalı şifre kırıcıların Enigma şifresini ve Amerikalı kriptanalizcilerin Japonların KIRMIZI, TURUNCU ve MOR şifrelerini kırmasıdır (Kahn, 1996 ve Pell, 2006)

2.9. MODERN ÇAĞDA KRİPTOGRAFİ

İkinci Dünya Savaşı'ndan sonra gelişen radar teknolojisi kript makinelerine adapte edildi. İlk elektrikli kriptomakinesi rotor makinelerinin yerini alan elektronik yapısı sayesinde daha küçüktü. Bu elektronik makinelerin tek avantajı işlem hızlarıydı. Hala mekanik rotor makinelerinin zayıf yanlarına sahiptiler. Bilgisayar ve elektronik çağı, şifre tasarımcılarına yazım hatalarından veya elektromekanik şifre makineleri gibi pahalı aletlerden uzak anlamda çok büyük bir tasarım özgürlüğü sağlayacaktı. Blok şifrelemenin asıl gelişimi öncüsü DES (Data Encryption Standart) olan LUCIFER projesi ile başlıyordu.

1960'lardaki bilgisayarların ve iletişim sistemlerinin gelişimi ile digital ortamlardaki gizli bilginin güvenliğini sağlama ihtiyacı ortaya çıkmıştır. IBM'de 1970'lerin başında Feistel çalışmasının başlamasıyla ve 1977'de ABD Ulusal Bilgi İşlem Standartları'nın bilgi şifrelemede DES veri şifreleme standardını (Data Encryption Standard) onaylaması ile tarihteki bilinen en iyi kriptografik işlem metodu kullanıma açıldı. Bu dünyadaki birçok finans kuruluşu için elektronik haberleşmede güvenliğin sağlanması demektir. Kriptografinin tarihteki en dikkat çekici gelişimi 1976'da Diffie ve Hellman'ın yayınladığı 'Kriptografide Yeni Yönler' çalışması ile oldu. Bu yayın açık-anahtarlı kriptografide devrim getirmişti ve anahtar değişim konusunda da güvenliği zor bir algoritma problemine dayanan yeni bir metod geliştirilmişti. Her ne kadar, yazarlar açık-anahtarlı bir şifreleme için uygulama vermemişlerse de düşünce açıktır ve bu kriptografik iletişimde oldukça yararlı sonuçlar vaad etmiştir. 1978'de Rivest, Shamir ve Adleman şimdi RSA olarak bilinen ilk uygulanabilir açık-anahtarlı şifreleme ve imza tasarımını keşfettiler. RSA projesi çok büyük sayıların çarpanlarına ayrılması ile ilgili olan başka bir zor matematik problemi üzerine kuruluydu. Kriptografiye bu güç matematik probleminin uygulanması daha iyi çarpanlara ayırma metodlarının bulunması çalışmalarının canlanmasını sağladı. 1980'lerde bilgi güvenliğindeki tek gelişim RSA değildi. Açık-anahtarlı şifreleme projelerinin güçlü ve pratik başka bir sınıfı ElGamal tarafından 1985'te bulundu. Bu da bir logaritma probleminin çözümüne dayanmaktaydı (Pell, 2006).

Kriptografi, yıllar sonra, birkaç bilgi güvenliği tekniğinin gelişmesi ile birlikte adeta etkin bir sanat haline gelmiştir. Geçen yirmi yüzyıl boyunca bu disiplin bir bilim sanatı olmuştur. Şimdi yalnız kriptografi ile ilgili birkaç uluslararası bilimsel konferans yapılmakta ve uluslararası bir bilimsel kuruluş; Uluslararası Kripto-lojik Araştırmalar Kurumu (IACR), bu alandaki araştırmaları desteklemektedir (Pell, 2006).

2.10. KRİPTOGRAFİNİN UYGULANDIĞI ALANLAR

Tipik bir kriptografik uygulama, temel teknikler kullanılarak kurulan bir sistemdir. Bu sistemler, kullanım amacına göre basit ya da karmaşık olabilir. Güvenli iletişim, kimlik belirleme ve kimlik denetimi gibi uygulamalar daha basit yapılar gerektirir.

1. **Elektronik ticaret**(e-ticaret): güvenli elektronik posta, sertifika dağıtımı, güvenli bilgisayar erişimi gibi uygulamalar ise daha karmaşık yapılar gerektirir.
2. **Güvenli iletişim:** Güvenli iletişim, iki tarafın birbirine gönderdiği mesajları şifrelemesi yoluyla, mesajları, istenmeyen üçüncü kişilerin okumasını engellemesidir. Herhangi biri mesajı elde edebilse dahi, şifreyi çözemez. Güvenli iletişim yüzyıllardır varolsa da, anahtar yönetimi sorunu, yaygınlaşmasını engellemiştir. Günümüzde açık anahtarlı kriptografi algoritmaları sayesinde bu sorunun üstesinden gelinmiştir.
3. **Kimlik belirleme ve kimlik denetimi:** Kimlik belirleme ve kimlik denetimi kriptografinin en yaygın kullanım alanlarından birisidir. Kimlik belirleme, birinin ya da bir şeyin kimliğinin doğrulanmasıdır. Örneğin bir bankadan para çekerken, hesap sahibinin kimliğinin doğrulanması için geçerli bir kimlik (örneğin, sürücü belgesi) gösterilmesi istenir. Aynı süreç, kriptografi kullanılarak elektronik olarak da gerçekleştirilebilir. Her ATM kartının, kartı sahibiyle, dolayısıyla hesapla ilişkilendiren bir PIN (Personal Identification Number) numarası vardır. Eğer doğru PIN numarası girilirse, makine kart kullanıcıını yasal kullanıcı olarak kabul eder ve kullanım hakkı tanır. Kriptografinin başka bir önemli uygulaması da kimlik denetimidir. Kimlik denetimi de kişilerin kaynaklara erişimini sağlaması bakımından kimlik belirlemeye benzer. Ancak kimlik denetiminde asıl yapılan ilgili kişinin ilgili işlemi yapmaya yetkisi olup olmadığının tespitidir.

4. Elektronik Ticaret: Son bir kaç yılda internet üzerinden yürütülen işler büyük ölçüde arttı. İnternet üzerinden yürütülen işlere elektronik ticaret veya e-ticaret denir. E-ticaret çevrimiçi (online) bankacılık, internet üzerinden alışveriş, gibi başlıkları içerir. Ancak internet üzerinden kredi kartı numarasını göndermek gibi bir işlem, kişiyi dolandırılmaya açık hale getirir. Bu soruna kriptografik bir çözüm, çevrimiçi girildiği durumlarda kredi kartı numarasını (veya diğer gizli bilgileri) şifrelemektir veya sadece kredi kartı numarasını şifrelemek yerine tüm oturum güvenli hale getirilebilir. Bir bilgisayar bilgiyi şifreleyip internet üzerinden gönderdiği zaman, şifreli bilgi, onu elde eden üçüncü kişilere anlamsız gelir. Sunucu (internet üzerindeki alışveriş merkezi), şifreli bilgiyi alarak şifreyi çözer ve kredi kartı numarasının başkalarının eline geçmiş olabileceği konusunda kaygı duymadan satışa devam eder. İnternet üzerinden iş yapmak yaygınlaştıkça, sahtekârlıklara karşı korunma ihtiyacı da artmaktadır.

5. Sertifika dağıtımı: Kriptografinin diğer bir uygulaması sertifika dağıtımıdır. Sertifika dağıtımı, sertifika hizmet sağlayıcıları gibi güvenilir kurumlar tarafından, kişilere elektronik ortamlarda kimliklerini doğrulama amaçlı kimlik dağıtımını sağlayan bir yapıdır.

6. Uzaktan erişim: Güvenli uzaktan erişim de kriptografinin önemli uygulamalarından biridir. Temel “anahtar kelime” (şifre sorma) sistemleri belli bir seviyede güvenlik sağlar, ancak bazı durumlarda yeterli olmayabilir (Olympos, 2007)

2.11. YAPILAN ÇALIŞMALAR

Myerscough ve diğerleri (1996) şifreleme aktiviteleri ile ilgili bir çalışma yapmışlardır. 1967’de David Kahn tarafından yazılan, şifrelemenin tarihi adlı eserdeki sıralamayı göz önüne almışlardır.

Şifreleme mesajları kodlama ve deşifre etme bilimidir. Kurum sırlarını korumak, bankalarda; hesap bilgilerini, kişisel güvenlikte; bireyleri korumak gibi iş sahasında önemli rol oynar. Bu aktivitede, lise sınıflarında matematik işlemi yapma konusunda şifreleme sanatını tanıtıyoruz. İlk etapta orijinal mesajdaki harflerin sağına ve soluna oynatarak değişikliğe gidildiği Sezar şifresini tanıtıyoruz. Daha sonrada modül 12 ve

26'daki saat ve modüler aritmetiği göreceğiz. Bu şifreleme sanatıyla bağlantılı olan modüler aritmetiğin kullanımını göstermek için gereklidir. Son olarak ta, daha zor aktiviteler için modüler aritmetikteki lineer dönüşümleri tanıtacağız. Bu aktiviteler birçok sahadaki öğrenciler için elverişli ve farklı öğrenim öğrenme tekniklerine kolaylıkla uyarlanabilir. (Myerscough ve diğerleri, 1996)

Myerscough ve diğerleri (1996) şifreleme aktiviteleri ile ilgili yaptıkları çalışmada öğrencilerde merak uyandırarak şifreyi çözmelerini sağlamışlardır. Öğrencilerin şifreyi çözmede zorlandıkları anlarda ipucu vererek onları yönlendirmişlerdir. Yapılan çalışmada araştırmacılar bazı sınıfların şifreyi çözmede zorlandıklarını, bazılarının öğretmen ipucu vermeden şifre hakkında yorum yapmadıklarını fakat birçoğunun şifreyi çözmede inatçı ve başarılı olduğunu söylüyorlar.

Görünüşte matematiğin öğrenciler için zor olduğu matematiği şifreleyerek de matematiğin daha da zor hale geldiği düşünülebilir. Yapılan çalışma matematiğin günlük hayatta nasıl kullanıldığını göstermektedir. Nasıl ki gazetelerdeki şifreli bulmacalar ilgi ile takip ediliyorsa, şifrelenen bir bilgiyi çözmekte öğrenciler tarafından ilgi ile takip edilir.

BÖLÜM III: YÖNTEM

Bu bölümde sırasıyla araştırmanın modeli, uygulama süreci ve verilerin çözümü ile ilgili bilgiler yer almaktadır.

3.1 ARAŞTIRMA MODELİ

Bu çalışmada araştırma modeli olarak “ ön test-son test kontrol gruplu model ” uygulanmıştır.

3.2 VERİ TOPLAMA ARAÇLARI

3.2.1. Matematik Başarı Testi

Bu çalışmada testin geçerliliğini sağlamak için uzman görüşü bağlamında, “ O.K.S., D.Y.P. ve Askeri Liseler Sınavı “dan 3 uzman öğretim üyesi ve öğretim elemanı ve en az 10 yıllık tecrübesi olan 3 öğretmen tarafından seçilen 25 sorudan oluşan matematik testi uygulanmıştır. Testin güvenirliği ise S.P.S.S. 15.00 istatistik programı Cronbach α Testi ile yapıldıktan sonra ($\alpha=0,72$) olarak bulunmuştur. Matematik başarı testi; ön test, son test ve hatırlama testi olarak öğrencilere uygulanmıştır. Ön test, çalışma öncesinde; son test, çalışma bitiminde, hatırlama testi ise çalışma bitiminden altı hafta sonra uygulanmıştır.

3.2.2. Tutum Ölçeği

Araştırmada kullanılan "İlköğretim Matematik Öğretmenleri İçin Kısaltılmış Matematik Tutum Ölçeği", Erol (1989) tarafından geliştirilen matematik tutum Ölçeğinin kısaltılmış biçimidir. Bu tutum ölçeğinde, "matematiğin önemi", "algılanan matematik başarı düzeyi" ve "matematik derslerine olan ilgi" olmak üzere üç boyutla ilgili, olumlu ve olumsuz yargı bildiren 20 cümle bulunmaktadır. 5'li likert tipindedir ve alfa güvenirlik katsayısı 0,74 olarak bulunmuştur (Nazlıcıçek ve Erkin, 2001).

Araştırmada uygulanan tutum ölçeğinden elde edilen alfa güvenirlik katsayısı ise 0,71 olarak bulunmuştur.

Tutum ölçeği uygulamanın başında ve uygulama bittikten sonra, deney ve kontrol gruplarına uygulanmış ve yapılan uygulamanın öğrencinin tutumuna bir etkisinin olup olmadığı ve deneklerin tutumlarının başarılarına etkisinin olup olmadığı araştırılmıştır.

3.2.3. Kişisel Bilgiler Anketi

Araştırmaya katılan öğrencilerin kişisel özelliklerini, ailelerinin sosyo-ekonomik düzeylerini, anne ve babalarının eğitim düzeylerini belirlemek amacıyla oluşturulan ankettir.

3.3. Deneklerin Seçimi

Araştırmaya katılacak olan denekleri belirleme sürecinde, 8/A, B, C, D şubelerinde okuyan 145 öğrenciye “Matematik Başarı Testi (Ön Test)” uygulanmıştır.

8-A sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 32,917, 8-B sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 32,222 bulunmuştur. 8-C sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 25,341. 8-D sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 24,251’dir.

Buna göre;

Oluşturulacak deney ve kontrol grupları için “Matematik Başarı Testinden (Ön Test)” alınan puan ortalamaları birbirine en yakın sınıflardan 8-B uygulamanın yapılacağı deney grubu, 8-A ise kontrol grubu olarak belirlenmiştir.

Uygulama okulunda belirlenen iki gruptan, kontrol grubuna Geleneksel Öğretim Metodu uygulanırken, deney grubuna Şifreleme Aktiviteleri uygulanmıştır. Araştırma sonunda

uygulanacak son testle iki gruba ait başarı farkları karşılaştırılmıştır. Matematik dersine tutum değişikliği gözlemlemek üzere tekrar “ Tutum Ölçeği ” uygulanmıştır.

3.4. Uygulama Süreci

Araştırmanın uygulama aşamasında, Matematik Sistemleri ünitesinin Saat aritmetiği, modül ve verilen bir modüle göre toplama ve çarpma işlemleri konularının öğretiminde kullanılmak üzere, her bir konu için, etkileşim ünitesine dayalı olarak öğretim materyali geliştirilmiştir. Matematik Sistemleri Ünitesi öğretim materyalinin geliştirilmesi aşamasında, ilköğretim okullarında izlenen matematik ders kitapları, eğitim fakültelerinde öğrencilere kaynak olarak önerilen matematik öğretimi kitapları ile Matematik Sistemleri ünitesinin matematik öğretiminde etkililiğini araştıran yerli ve yabancı araştırmalardan yararlanılmıştır.

Tablo 3.1.
Deney Grubunun Çalışma Programı

Hafta	Ders	Materyal	Ödev
1	1	Sezar Şifresi	
	2	Sezar Şifresi	Ek-4'teki 4-5-6. sayfalar
	3	Saat Aritmetiği	
	4	Saat Aritmetiği	Ek-5'teki 4-5-6. sayfalar
2	1	Frekans Analizi	Ek-6'daki 2-3. sayfalar
	2	Çarpan Ağacı	Ek-7'deki 3-4-5. sayfalar
	3	Modüler Aritmetik	
	4	Modüler Aritmetik	Ek-8'daki 3. sayfa
3	1	Asal Sayılar	Ek-9'daki 3. sayfa
	2	Rail Fence / Mors Alfabesi	Ek-10 ve Ek-11'deki 2.sayfa
	3	Pigpen-Polybius Şifresi / Poster	Ek-12
	4	Poster / Tekrar	Ek-13

Birinci Hafta

Birinci haftanın birinci dersinde, Sezar Şifresi tanıtılmıştır. Bilinen en eski şifreleme yönteminin Sezar Şifresi olduğu, komutanlarına göndereceği mesajların düşmanları tarafından okunmasını istemeyen İmparatorun, mesajlarında nasıl "harf atlama" yöntemini kullandığından bahsedilmiştir.

İkinci derste, Şifre Disklerinden bahsedilmiştir. Şifre Diskleri'nde ise bir metnin nasıl kolayca şifrelenebileceği ve yine aynı kolaylıkla şifreli metnin nasıl çözülebileceği anlatılmıştır.

Üçüncü derste ise, saat aritmetiği konusu işlenmiş ve aşağıdaki sorulara cevap aranmıştır.

1. Dört işlemde başka işlemler var mıdır?
2. Neden saat 12 ye bölünmüştür.?
3. Saat üzerinde yaptığımız toplama işlemini başka nerelerde yaparız?
4. 12.30 ile yarım aynı şey midir?
5. Saat 1,5 demiyoruz da neden 13.30 diyoruz?
6. Saat üzerinde akrep ve yelkovan ne işe yarar?
7. Saat olmasaydı zamanı nasıl bilirdik?
8. Eski zamanlarda yaşayan insanlar saat yerine ne kullanıyorlardı?
9. Zaman gösteren saati ilk kez kimler bulmuştur?
10. Onluk sistemden başka sayı sistemlerine neden gereksinim vardır?

Dördüncü derste, Saat Aritmetiği etkinliğinin 1-2 ve 3. Sayfaları öğrencilerle birlikte derste yapılmıştır. 4-5 ve 6. Sayfalar ise öğrencilere ev ödevi olarak verilmiştir.

İkinci Hafta

Birinci Derste, Frekans analizinin ilk kim tarafından ve nasıl bulunduğu hakkında bilgi verildi. Frekans analizinin Sezar şifresini çözmede nasıl kolaylık sağladığından bahsedildi. Son olarak öğrenciler Ek-6'daki metinlerden birini seçerek frekans tablosunu doldurmaya başladılar. Ek-6'daki diğer sayfalar öğrencilere ev ödevi olarak verildi.

İkinci derste, çarpan ağacı ve asal çarpanlar algoritmasının nasıl oluşturulduğundan bahsedildi. Ek-7'deki 1. ve 2. Sayfalar öğrencilerle birlikte yapıldı. 3-4 ve 5. Sayfalar ev ödevi olarak verildi.

Üçüncü derste, Öğrencilere takvim yardımıyla hangi gün doğdukları, bir hemşire veya bir askerin nöbet gülerini buldurma ve bir sayının modunu bulma gibi alıştırmalar yaptırıldı.

Dördüncü derste, Ek-8'deki 1 ve 2. Sayfa öğrencilerle birlikte yapıldı. 3. Sayfa ise ev ödevi olarak verildi.

Üçüncü Hafta

Birinci derste, Asal sayıların tanımından ve günlük hayattaki kullanımından bahsedildi. Ek-9'da yer alan Eratosthenes Kalburu yardımıyla nasıl asal sayıların bulunduğu açıklanır ve 50'ye kadar olan asal sayılar bulduruldu.

İkinci derste, Ek-10 ve Ek-11'deki Rail Fence ve Mors Alfabeti hakkında bilgi verildi.

Üçüncü derste, Ek-12'deki Pigpen-Polybius Şifresi etkinliği yapıldı.

Dördüncü derste, Saat Posterinin nasıl hazırlanabileceği hakkında bilgi verildi. Öğrenciler kendi saat posterlerini tasarladılar.

3.4.2. Verilerin Çözümü:

Bilgi testlerinde her doğru cevaba 1 puan verilmiş ve ön test-son test 100 puan üzerinden değerlendirilmiştir.

Tutum Ölçeği 5'li likert tipinde olup, olumsuz yargıdan olumlu yargıya doğru 1'den 5'e kadar numaralandırılmış ve ölçek toplam 100 puan üzerinden değerlendirilmiştir.

Araştırmada, deney kontrol grubu öğrencilerinin ön test, son test ve matematik tutumları puanlarının ortalamalarına, yüzde ve frekans dağılımlarına bakılmıştır. Verilerin normal dağılım gösterip göstermediklerini incelemek için Kolmogrov-Smirnov Testi kullanılmıştır.

Deney ve kontrol gruplarının homojenliklerinin tespiti için, analizi yapılacak verilerin aritmetik ortalamaları karşılaştırılmış, ayrıca Paired-Samples t Testi kullanılarak verilerin homojenliği kontrol edilmiştir.

Araştırmaya katılan deney ve kontrol grubu öğrencilerinin, Kişisel Bilgiler Anketi sorularına verdikleri cevaplardan elde edilen veriler yüzde ve frekans dağılımları ve uygulanan diğer testlerden elde edilen veriler tablolar halinde verilmiş, oluşturulan bu tablolar üzerinde yorumlar yapılmıştır.

İlişkisiz verilerin bir faktöre göre farklılaşması üzerine yapılan istatistik için veriler normal dağılım gösterdiklerinden dolayı, iki birimli örneklemelerin analizinde Independent Samples t Test, ikiden fazla birimli örneklemelerin analizinde Tek Faktörlü Varyans Analizi (One-Way Anova) kullanılmıştır. İlişkili örneklemelerin farklılaşması üzerine yapılan istatistikleri için ise verilere Paired Samples t Test uygulanmıştır.

BÖLÜM IV: BULGULAR VE YORUMLAR

Bu bölümde bulgular üç ana başlık altında yorumlanmıştır. Birinci başlık altında, Şifreleme Aktivitelerinin uygulanmasının başarıya etkisini araştırmaya yönelik uygulama öncesi elde edilen veriler analiz edilmiştir. İkinci başlık altında, araştırmaya katılan deney grubu öğrencilerinin Kişisel bilgiler anketi sorularına verdikleri cevaplara göre elde edilen veriler analiz edilmiştir. Üçüncü başlık altında, Şifreleme Aktivitelerinin uygulanmasının Başarıya Etkisini test eden hipotezler incelenmiş ve bulgular analiz edilmiştir.

Bu bölümde önce; Başarı Testi (ön test) ve ön tutum ölçeği testinden elde edilen verilerin normal dağılıma uygunluğu incelenmiştir.

4.1. Normal Dağılıma Uygunluk Analizi

Grupların verilerine t testi uygulanabilmesi için, t testi ön koşulu olarak verilerin normal dağılım göstermesi gerekmektedir.

4.1.1. Ön Test Verilerinin Normalliği

Aşağıdaki Tablo 4.1 'de, deney grubuna ait Ön Test verilerinin normal dağılım gösterip göstermediğin test etmek amacıyla uygulanan One Sample Kolmogorov-Smirnov testi sonuçlarına yer verilmektedir.

Tablo 4.1
Deney ve Kontrol Grubuna Ait Ön Test Kolmogorov-Smirnov Testi Sonuçları

Gruplar	N	Ortalama	Standart Sapma	Kolmogorov-Smirnov Z	P
Deney Grubu	36	32,222	10,450	0,661	0,774
Kontrol Grubu	36	32,917	10,027	0,687	0,733

Tablo 4.1'e göre, Deney grubuna ait one Sample Kolmogorov-Smirnov testi sonucunda bulunan p değeri 0,774 ve Kontrol grubuna ait one Sample Kolmogorov-Smirnov testi sonucunda bulunan p değeri 0,733 olduğundan deney ve kontrol grubuna ait ön test verileri normal dağılım gösterir.

4.1.2. Ön Tutum Ölçeği Verilerinin Normalliği

Aşağıdaki Tablo 4.2 'de, deney ve kontrol grubuna ait Ön Tutum ölçeği verilerinin normal dağılım gösterip göstermediğini test etmek amacıyla uygulanan One Sample Kolmogorov-Smirnov testi sonuçlarına yer verilmektedir.

Tablo 4.2

Deney ve Kontrol Grubuna Ait Ön Tutum Ölçeği Kolmogorov-Smirnov Testi Sonuçları

Gruplar	N	Ortalama	Standart Sapma	Kolmogorov-Smirnov Z	P
Deney Grubu	36	47,962	11,987	0,674	0,754
Kontrol Grubu	36	53,890	14,712	0,697	0,717

Tablo 4.2'ye göre, deney grubuna ait one Sample Kolmogorov-Smirnov testi sonucunda bulunan p değeri 0,754 olup ve Kontrol grubuna ait one Sample Kolmogorov-Smirnov testi sonucunda bulunan p değeri 0,717 olduğundan deney ve kontrol grubuna ait ön tutum verilerinin normal dağılım gösterdiği söylenebilir.

4.1.3. Deneklerin Seçimi

Araştırmaya katılacak olan denekleri belirleme sürecinde, 8/A, B, C, D şubelerinde okuyan 137 öğrenciye “Matematik Başarı Testi (Ön Test)” uygulanmıştır.

Oluşturulacak deney ve kontrol grupları için “Matematik Başarı Testinden (Ön Test)” alınan puan ortalamaları birbirine en yakın sınıflardan 8-B uygulamanın yapılacağı deney grubu, 8-A ise kontrol grubu olarak belirlenmiştir. Aşağıdaki Tablo 4.3’de deney ve kontrol gruplarını belirlemek amacıyla yapılan Ön Test sonucunda sınıfların aldıkları puanların aritmetik ortalamalarına yer verilmektedir.

Tablo 4.3
Ön Test Sonuçlarına Göre Aritmetik Ortalamalarının Karşılaştırılması

Gruplar	N	Art. Ort.
8-A (Kontrol Grubu)	36	32,917
8-B (Deney Grubu)	36	32,222
8-C	35	25,341
8-D	30	24,251

Tablo 4.3, araştırmaya katılacak öğrencilerinin sayısını ve Ön Test’ten aldıkları puanların aritmetik ortalamasını vermektedir. Tablodan da anlaşılacağı üzere, 8-A sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 32,917; 8-B sınıfındaki öğrencilerin Ön Test’ten aldıkları puanların aritmetik ortalaması 32,222 bulunmuştur. Buradan deney grubu olarak 32,222’lük ortalama ile 8-B sınıfı, kontrol grubu olarak ise 32,917’lik ortalama ile 8-A sınıfı belirlenmiştir.

4.1.4. Grupların Homojenliği

Tablo 4.4’de, grupların homojenliğini test etmek için yapılmış Eşlenik Çift t-testi sonuçları yer almaktadır.

Tablo 4.4
Paired-Sample t testine Göre Çalışma Gruplarının Homojenliği

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu	36	32,222	10,450	16,132	0,258	0,798
Kontrol Grubu	36	32, 917	10,027			

Tablo 4.4'e göre, $p=0,798$ olup bulunan bu değer 0,05 değerinden büyük olduğu için deney ve kontrol grupları arasında istatistiki anlamda bir farklılık bulunmadığı söylenebilir. Bu sonuç, araştırmaya alınan deney ve kontrol gruplarının homojen olduğunu göstermektedir.

4.1.5. Deneklerin Matematik Tutumları

Tablo 4.5'de, gruplara uygulanan Matematik Ön Tutum Ölçeği'nden elde edilen veriler yer almaktadır.

Tablo 4.5
Deney ve Kontrol Grubu Matematik Ön Tutum Ölçeği Verileri

Gruplar	N	Art. Ort.	ss	Mak. Puan	Min. Puan
Deney Grubu	36	47,962	11,987	67	21
Kontrol Grubu	36	53,890	14,712	85	26

Tablo 4.5'den deney grubunun Matematik Ön Tutum Ölçeği puanlarının aritmetik ortalamasının 47,962 ve kontrol grubunun Matematik Ön Tutum Ölçeği puanlarının aritmetik ortalamasının 53,890 olduğu görülmektedir.

4.1.6. Deney ve Kontrol Grubuna Uygulanan Kişisel Bilgiler Anket Sorularından Elde Edilen Bulgular ve Yorumlar

Bu bölümde deney ve kontrol grubu öğrencilerinin Kişisel Bilgiler Anket Sorularına verdikleri cevaplardan elde edilen yüzde (%) ve frekans (f) verilerine değinilmiştir.

Tablo 4.6

Deney ve Kontrol Grubu Öğrencilerinin Cinsiyetlerine Göre Dağılımları

	Cinsiyet	F	%
Deney Grubu	Kız	21	58,33
	Erkek	15	41,66
	Toplam	36	100
Kontrol Grubu	Kız	17	47,22
	Erkek	19	52,77
	Toplam	36	100
Toplam	Kız	38	52,77
	Erkek	34	47,22
	Toplam	72	100

Tablo 4.6 incelendiğinde deney grubunun % 58,33'ü ve kontrol grubunun %47,22'si kızlardan oluşurken; deney grubunun %41,66'i ve kontrol grubunun %52,77'si erkektir.

Tablo 4.7'de deney grubu öğrencilerine yapılan öğretim sonrası başarılarının cinsiyetlerine göre farklılaşma durumu ile ilgili t-testi sonuçlarına yer verilmiştir.

Tablo 4.7
Deney Grubu Öğrencilerinin Öğretim Sonrası Başarılarının Cinsiyetlerine Göre Farklılaşmasına İlişkin t-testi Sonuçları

Cinsiyet	N	X	ss	sd	t	P
Kız	21	60,000	18,231	17	0,050	0,960
Erkek	15	59,687	18,208			

Tablo 4.7’de t-testi sonucu bulunan p değeri 0,05’ten büyük bir değerdir. Bu sonuçtan, Öğretiminde Şifreleme Aktiviteleriyle yapılan öğretim sonrası öğrenci başarılarının cinsiyetlerine göre farklılaşmadığı söylenebilir.

Tablo 4.8’de deney ve kontrol grubu öğrencilerinin annelerinin eğitim düzeyine göre dağılımlarına yer verilmiştir.

Tablo 4.8
Deney ve Kontrol Grubu Öğrencilerin Annelerinin Eğitim Düzeyine Göre Dağılımları

	Deney Grubu		Kontrol Grubu		Toplam	
	N	%	N	%	N	%
İlkokul Mezunu	14	41,17	11	30,55	25	35,71
Ortaokul Mezunu	5	14,7	7	19,44	12	17,14
Lise veya Dengi Okul Mezunu	3	8,82	3	8,33	6	8,57
Üniversite ve/veya üstü Mezunu	1	2,94	2	5,55	3	4,28
Okuma Yazma Bilmiyor	11	32,35	13	36,11	24	34,28
Toplam	34	100	36	100	70	100

Tablo 4.8’de deney grubu öğrencilerinin annelerinin 11’inin okuma yazmasının olmadığı, 14’ünün ilkokul mezunu olduğu, 5’inin ortaokul mezunu olduğu, 3’ünün lise ve 1’inin üniversite mezunu olduğu görülmektedir.

Deney ve kontrol grubu öğrencilerinin annelerinin toplamda 24'ünün okuma yazmasının olmadığı, 25'inin ilkokul mezunu olduğu, 12'sinin ortaokul mezunu olduğu, 6'sının lise ve 3'ünün üniversite mezunu olduğu görülmektedir.

Hem deney hem de kontrol grubu öğrencilerinde ve toplamda denek annelerinin eğitim seviyeleri frekanslarına göre sıralandığında önceliği ilkokul mezunu annelerin aldığı görülmektedir. Daha sonra sırasıyla okuma yazma bilmeyenler, ortaokul mezunları, lise mezunları ve üniversite mezunu anneler gelmektedir.

Tablo 4.9'da deney ve kontrol grubu öğrencilerinin babalarının eğitim düzeyine göre dağılımlarına yer verilmiştir.

Tablo 4.9
Deney ve Kontrol Grubu Öğrencilerin Babalarının Eğitim Düzeyine Göre Dağılımları

	Deney Grubu		Kontrol Grubu		Toplam	
	N	%	N	%	N	%
İlkokul Mezunu	13	38,23	10	27,77	23	32,85
Ortaokul Mezunu	10	29,41	7	19,44	17	24,28
Lise veya Dengi Okul Mezunu	6	17,64	9	25	15	21,42
Üniversite ve/veya üstü Mezunu	2	5,88	5	13,88	7	10
Okuma Yazma Bilmiyor	3	8,82	5	13,88	8	11,42
Toplam	34	100	36	100	70	100

Tablo 4.9'da deney grubu öğrencilerinin babalarının 3'ünün okuma yazmasının olmadığı, 13'ünün ilkokul mezunu olduğu, 10'unun ortaokul mezunu olduğu, 6'sının lise ve 2'sinin üniversite mezunu olduğu görülmektedir.

Deney ve kontrol grubu öğrencilerinin babalarının toplamda 8'inin okuma yazmasının olmadığı, 23'ünün ilkokul mezunu olduğu, 17'sinin ortaokul mezunu olduğu, 15'inin lise ve 7'sinin üniversite mezunu olduğu görülmektedir.

Hem deney hem de kontrol grubu öğrencilerinde ve toplamda denek babaların eğitim seviyeleri frekanslarına göre sıralandığında önceliği ilkokul mezunu babaların aldığı görülmektedir. Daha sonra sırasıyla ortaokul mezunları, lise mezunları ve üniversite mezunu babalar gelmektedir.

Tablo 4.10’da deney ve kontrol grubu öğrencilerinin aile gelir düzeylerine göre dağılımlarına yer verilmiştir.

Tablo 4.10
Deney ve Kontrol Grubu Öğrencilerinin Ailelerinin Aylık Ortalama Gelir Seviyelerine Göre Dağılımları

	Deney Grubu		Kontrol Grubu		Toplam	
	N	%	N	%	N	%
0-250 YTL	3	8,82	2	5,55	5	7,14
251-499 YTL	7	20,58	8	22,22	15	21,42
500-749 YTL	11	32,35	9	25	20	28,57
750-999 YTL	9	26,47	11	30,55	20	28,57
1000 ve üzeri	4	11,76	6	16,66	10	14,28
Toplam	34	100	36	100	70	100

Tablo 4.10’da deney grubu öğrencilerinin aile gelir düzeylerinin 3’ünün 0-250 YTL arasında, 7’sinin 251-499 YTL arasında, 11’inin 500-749 YTL arasında, 9’unun 750-999 YTL arasında ve 4’ünü 1000 YTL ve üzeri olduğu görülmektedir.

Deney ve kontrol grubu öğrencilerinin ailelerinin toplamda 5’inin 0-250 YTL arasında, 15’inin 251-499 YTL arasında, 20’sinin 500-749 YTL arasında, 20’sinin 750-999 YTL arasında ve 10’unun 1000 YTL ve üzeri olduğu görülmektedir.

Deney grubu öğrencilerinde denek ailelerinin seviyeleri frekanslarına göre sıralandığında önceliği 500-749 YTL düzeyindeki ailelerin, kontrol grubu öğrencilerinde 750-999 YTL arası ailelerin ve toplamda hem deney hem de kontrol grubunda 500-749 YTL ve 750-999 YTL ailelerin gelir düzeylerinin eşit olduğu görülmektedir.

4.2. Modüler Aritmetik Konusunun Öğretiminde Şifreleme Aktivitelerinin Başarıya Etkisini Test Eden Hipotezler, Bulgu ve Yorumları

Bu bölümde mevcut 8 hipotezin doğruluklarını araştırmak amacıyla her bir hipotez için sıfır ve alternatif hipotezler oluşturulmuş, hipotezlerin test istatistiği $\alpha = 0,05$ Önem seviyesinde hesaplanmış ve sonuçlar yorumlanmıştır.

4.2.1. Birinci Hipotez

Birinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Kontrol grubu öğrencilerinin uygulama öncesi ve sonrası başarıları arasında anlamlı bir fark yoktur

H_1 = Kontrol grubu öğrencilerinin uygulama öncesi ve sonrası başarıları arasında anlamlı bir fark vardır.

Tablo 4.11 kontrol grubu öğrencilerinin son test puanlarının normalliğini incelemek için yapılan Kolmogorov-Smirnov testi sonuçlarını göstermektedir.

Tablo 4.11
Kontrol Grubunun Son Test Puanlarına ait Kolmogorov-Smirnov Testi Sonuçları

N	36
Ortalama	51,667
Standart Sapma	19,346
Kolmogorov-Smirnov Z	0,667
P	0,766

Tablo 4.11'ye göre, kontrol grubu son test puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,766 olup, bu değer 0,05 önem seviyesi değerinden büyük olduğu için kontrol grubu öğrencilerinin son test puanları normal dağılım göstermektedir.

Tablo 4.11'den elde edilen sonuçlara göre kontrol grubunun ön test verilerinin de normal dağılım gösterdiği için, birinci hipotezin test istatistiğinde eşlenik çift t-testi kullanılabilir.

Tablo 4.12'te, kontrol grubu öğrencilerinin ön test ve son test puanlarına ilişkin Eşlenik Çift t-testi sonuçlarına yer verilmiştir.

Tablo 4.12
Kontrol Grubunun Ön Test ve Son Test Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Kontrol Grubu Ön Test	36	32,916	10,027	35	0,172	0,865
Kontrol Grubu Son Test	36	33,055	12,205			

Tablo 4.12'de deney grubu öğrencilerinin ön test ve son test puanlarına ilişkin eşlenik çift t-testi sonuçlarına göre [$t=0,172$, $p=0,865>0,05$] anlamlılık değeri 0,865 olup 0,05 değerinden büyük olduğu için H_0 hipotezi kabul edilir. Böylece kontrol grubunun ön test ve son test puanları arasında anlamlı bir fark olmadığı söylenebilir.

4.2.2. İkinci Hipotez

İkinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Deney grubu öğrencilerinin ön test puanları ile son test puanları arasında anlamlı bir fark yoktur.

H_1 = Deney grubu öğrencilerinin ön test puanları ile son test puanları arasında anlamlı bir fark vardır.

Tablo 4.13 deney grubu öğrencilerinin son test puanlarının normallliğini incelemek için yapılan Kolmogorov-Smirnov testi sonuçlarını göstermektedir.

Tablo 4.13
Deney Grubunun Son Test Puanlarına ait Kolmogorov-Smirnov Testi Sonuçları

N	36
Ortalama	59,583
Standart Sapma	17,500
Kolmogorov-Smirnov Z	0,610
P	0,851

Tablo 4.13'ye göre, deney grubu son test puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,851 olup, bu değer 0,05 önem seviyesi değerinden büyük olduğu için deney grubu öğrencilerinin son test puanları normal dağılım göstermektedir.

Tablo 4.13'den elde edilen sonuçlara göre deney grubunun son test verilerinin de normal dağılım gösterdiği için, ikinci hipotezin test istatistiğinde eşlenik çift t-testi kullanılabilir.

Tablo 4.14'te, kontrol grubu öğrencilerinin ön test ve son test puanlarına ilişkin eşlenik çift t-testi sonuçlarına yer verilmiştir.

Tablo 4.14

Deney Grubunun Ön Test ve Son Test Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu Ön Test	36	32,222	10,450			
Deney Grubu Son Test	36	59,583	17,500	35	9,357	0,000

Tablo 4.14'te deney grubu öğrencilerinin ön test ve son test puanlarına ilişkin eşlenik çift t-testi sonuçlarına göre [$t=9,357$, $p=0,000<0,05$] anlamlılık değeri 0,000 olup 0,05 değerinden küçük olduğu için H_0 hipotezi reddedilir. H_1 hipotezi kabul edilir. Böylece deney grubunun ön test ve son test puanları arasında anlamlı bir fark olduğu söylenebilir. Anlamlılık Deney Grubu yönündedir. Sonuç olarak bu değerler, deney grubu öğrencilerinin başarılarında olumlu yönde bir artış olduğunu göstermektedir.

4.2.3. Üçüncü Hipotez

Üçüncü hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Kontrol grubu öğrencileri ile deney grubu öğrencilerinin öğretim sonrası başarıları arasında anlamlı bir fark yoktur.

H_1 = Kontrol grubu öğrencileri ile deney grubu öğrencilerinin öğretim sonrası başarıları arasında anlamlı bir fark vardır.

Tablo 4.15 kontrol grubu öğrencileri ile deney grubu öğrencilerinin son test puanlarında anlamlı bir fark olup olmadığını araştırmak için yapılan ilişkisiz t-testi sonuçlarına yer verilmiştir.

Tablo 4.15
Kontrol ve Deney Grubunun Son Test Puanlarına İlişkin İlişkisiz t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu	36	59,583	17,500			
Son Test Kontrol Grubu	36	33,056	12,205	35	7,080	0,000
Son Test						

Tablo 4.15’de kontrol ve deney grubu öğrencilerinin son test puanlarına ilişkin t-testi sonuçlarına göre [$t=7,080$, $p=0,000<0,05$] anlamlılık değeri 0,000 olup 0,05 değerinden küçük olduğu için H_0 hipotezi reddedilir. H_1 hipotezi kabul edilir. Bu değerler kontrol grubu öğrencileri ile deney grubu öğrencilerin öğretim sonrası başarıları arasında anlamlı bir farkın olduğunu gösterir. Kontrol grubu öğrencilerinin son test puan ortalamaları 33,0556 iken deney grubu öğrencilerinin son test puanları aritmetik ortalaması 59,5833 olduğu görülmektedir. Ortalamalar deney grubu öğrencileri lehine olduğu için, t-testi sonucu bulunan anlamlı farkın deney grubu öğrencileri lehine olduğu sonucuna varılmıştır.

4.2.4. Dördüncü Hipotez

Dördüncü hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Deney grubu öğrencilerinin öğretim öncesi ve öğretim sonrası matematik tutumları arasında anlamlı bir fark yoktur.

H_1 = Deney grubu öğrencilerinin öğretim öncesi ve öğretim sonrası matematik tutumları arasında anlamlı bir fark vardır.

Tablo 4.16’de deney ve kontrol grubu öğrencilerinin öğretim sonrası matematik tutum puanlarının normalliğini incelemek için yapılan Kolmogorov-Smirnov test sonuçlarına yer verilmektedir.

Tablo 4.16

Deney Grubunun Öğretim Sonrası Matematik Tutum Puanlarının Normalliğine İlişkin Kolmogorov-Smirnov Testi Sonuçları

GRUP	DENEY
N	36
Ortalama	60,971
Standart Sapma	11,466
Kolmogorov-Smirnov Z	0,611
P	0,850

Tablo 4.16’ye göre, deney grubu öğrencilerinin öğretim sonrası matematik tutum puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,850 olup, bu değer 0,05 önem seviyesinden büyük olduğu için deney grubu öğrencilerinin son tutum ölçeği puanları normal dağılım göstermektedir. Tablo 4.2’den elde edilen sonuçlara göre deney grubunun ön tutum verileri de normal dağılım gösterdiği için, dördüncü hipotezin istatistiğinde t-testi kullanılabilir.

Tablo 4.17’de, deney grubu öğrencilerinin uygulama öncesi ve sonrası matematik tutum puanları arasındaki fark olup oluşmadığını araştırmak için yapılan eşlenik çift t-testi sonuçlarına yer verilmiştir.

Tablo 4.17

Deney Grubunun Uygulama Öncesi ve Sonrası Matematik Tutumlarının Farklılaşmasına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu	36	47,962	11,986			
Ön Tutum				35	5,461	0,000
Deney Grubu	36	60,972	11,465			
Son Tutum						

Tablo 4.17'deki deney grubu öğrencilerinin uygulama öncesi ve sonrası matematik tutumları farklılaşmasına ilişkin eşlenik çift t-testi sonuçlarına göre [$t=5,461$, $p=0,000<0,05$] anlamlılık değeri 0,000 olup 0,05 değerinden küçük olduğu için H_1 hipotezi kabul edilir, H_0 hipotezi reddedilir. Bu değerler deney grubu öğrencilerinin uygulama öncesi ve sonrası matematik tutumları arasında anlamlı bir farkın olduğunu gösterir. Buna göre deney grubu öğrencilerinin uygulama öncesi ve sonrası matematik tutumları puanlarında oluşan ortalamalarına bakıldığında; uygulama öncesi puan ortalamaları 47,962 iken uygulama sonrası puan ortalamalarının 60,972 olduğu görülmektedir. Yani, deney grubu öğrencilerinin ön ve son matematik tutumları arasında olumlu yönde anlamlı bir farklılık vardır. Anlamlılık Deney Grubu son tutum yönündedir.

4.2.5. Beşinci Hipotez

Beşinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Kontrol grubu öğrencilerinin öğretim öncesi ve öğretim sonrası matematik tutumları arasında anlamlı bir fark yoktur.

H_1 = Kontrol grubu öğrencilerinin öğretim öncesi ve öğretim sonrası matematik tutumları arasında anlamlı bir fark vardır.

Tablo 4.18’da kontrol grubu öğrencilerinin öğretim sonrası matematik tutum puanlarının normalliğini incelemek için yapılan Kolmogorov-Smirnov test sonuçlarına yer verilmektedir.

Tablo 4.18

Kontrol Grubu Öğretim Sonrası Matematik Tutum Puanlarının Normalliğine İlişkin Kolmogorov-Smirnov Testi Sonuçları

GRUP	KONTROL
N	36
Ortalama	51,680
Standart Sapma	12,371
Kolmogorov-Smirnov Z	0,445
P	0,989

Tablo 4.18’a göre, kontrol grubu öğrencilerinin öğretim sonrası matematik tutum puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,989 olup, bu değer 0,05 önem seviyesinden büyük olduğu için kontrol grubu öğrencilerinin son tutum ölçeği puanları normal dağılım göstermektedir. Tablo 4.2’den elde edilen sonuçlara göre kontrol grubunun ön tutum verileri de normal dağılım gösterdiği için normal dağılım gösterdiği için, dördüncü hipotezin istatistiğinde t-testi kullanılabilir.

Tablo 4.19’da, kontrol grubu öğrencilerinin son tutum puanlarında anlamlı bir fark olup olmadığını araştırmak için yapılan eşlenik çift t-testi sonuçlarına yer verilmiştir.

Tablo 4.19

Kontrol Grubu Öğrencilerinin Öğretim Sonrası Tutum Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Kontrol Grubu	36	53,890	14,721			
Ön Tutum Kontrol Grubu	36	51,680	12,371	35	3,059	,004
Son Tutum						

Tablo 4.19'daki kontrol grubu öğrencilerinin uygulama öncesi ve sonrası matematik tutumları farklılaşmasına ilişkin eşlenik çift t-testi sonuçlarına göre [$t=3,059$, $p=0,004<0,05$] anlamlılık değeri 0,004 olup 0,05 değerinden küçük olduğu için H_1 hipotezi kabul edilir, H_0 hipotezi reddedilir. Bu değerler kontrol grubu öğrencilerinin ortalamalarına bakıldığında uygulama öncesi ve sonrası matematik tutumları arasında anlamlı bir farkın olduğunu gösterir. Geleneksel öğretim yöntemi ile yapılan öğretimin matematik dersine karşı tutumlarında bir gelişme göstermediği söylenebilir.

4.2.6. Altıncı Hipotez

Altıncı hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Kontrol ve deney grubu öğrencilerinin uygulama öncesi ve sonrası tutumları arasında anlamlı bir fark yoktur.

H_1 = Kontrol ve deney grubu öğrencilerinin uygulama öncesi ve sonrası tutumları arasında anlamlı bir fark yoktur.

Tablo 4.20'de deney ve kontrol grubu öğrencilerinin ön tutum puanlarının karşılaştırılması verilmiştir.

Tablo 4.20

Deney ve Kontrol Gruplarının Tutum Ölçeği Ön Testi İçin Yapılan İlişkisiz Grup t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu	36	47,962	11,986	35	-1,560	0,128
Kontrol Grubu	36	53,890	14,712			

Deney ve kontrol gruplarının tutum ölçeği ön testi için yapılan ilişkisiz grup t-Testi sonucunda 35 serbestlik derecesinde anlamlılık seviyesi 0,128 olarak bulunmuştur. Anlamlılık değeri araştırmada istatistiksel anlamlılık olarak kabul edilen 0,05'ten büyük olduğundan 0,05 önem seviyesinde karşılaştırılan deney ve kontrol gruplarının matematik dersine karşı tutumlarında çalışma öncesinde fark olmadığı anlaşılmaktadır.

Tablo 4.21'de deney ve kontrol grubu öğrencilerinin son tutum puanlarının karşılaştırılması verilmiştir.

Tablo 4.21

Deney ve Kontrol Gruplarının Tutum Ölçeği Son Testi İçin Yapılan İlişkisiz Grup t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu	36	60,971	11,465	35	3,284	0,002
Kontrol Grubu	36	51,680	12,371			

Deney ve kontrol gruplarının tutum ölçeği son testi için yapılan ilişkisiz grup t-testi sonucunda 35 serbestlik derecesinde anlamlılık seviyesi 0,002 olarak bulunmuştur. Bu değer 0,05'ten küçük olduğu için H_1 hipotezi kabul edilir, H_0 hipotezi reddedilir. Anlamlılık değeri araştırmada istatistiksel anlamlılık olarak kabul edilen 0,05'ten küçük olduğundan 0,05 önem seviyesinde karşılaştırılan deney ve kontrol gruplarının

matematik dersine karşı tutumlarında çalışma sonrasında anlamlı bir fark olduğu anlaşılmaktadır. Bu fark için ortalamalara bakıldığında farkın deney grubu lehine olduğu anlaşılmaktadır. Bu da şifreleme aktiviteleriyle yapılan öğretimin öğrencinin matematik dersine olan tutumunun olumlu yönde değiştiğini gösterir.

4.2.7. Yedinci Hipotez

Yedinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Kontrol grubu öğrencilerinin hatırlamalarında farklılaşma yoktur.

H_1 = Kontrol grubu öğrencilerinin hatırlamalarında farklılaşma vardır.

Tablo 4.22’de, kontrol grubu öğrencilerinin hatırlama testi puanlarının normalliğini incelemek için yapılan Kolmogorov-Smirnov test sonuçlarına yer verilmektedir.

Tablo 4.22

Kontrol Grubu Öğrencilerinin Hatırlama Testi Puanlarına Ait Kolmogorov-Smirnov Testi Sonuçları

N	36
Ortalama	43,194
Standart Sapma	15,545
Kolmogorov-Smirnov Z	0,682
P	0,741

Tablo 4.22’de göre, kontrol grubu öğrencilerinin hatırlama testi puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,741 olup, bu değer 0,05 önem seviyesinden büyük olduğu için kontrol grubu öğrencilerinin hatırlama testi puanları normal dağılım göstermektedir. Tablo 4.1’den elde edilen sonuçlara göre kontrol grubunun son test verilerinin de normal dağılım gösterdiği için, altıncı hipotezin istatistiğinde t-testi kullanılabilir.

Tablo 4.23'te, kontrol grubu öğrencilerinin son test ve hatırlama testi puanlarına ilişkin eşlenik çift t-testi sonuçlarına yer verilmiştir.

Tablo 4.23

Kontrol Grubu Öğrencilerinin Son Test ve Hatırlama Testi Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Kontrol Grubu Son Test	36	51,667	19,346			
Kontrol Grubu Hatırlama Testi	36	43,194	15,545	35	5,642	0,000

Tablo 4.23'te kontrol grubu öğrencilerinin son test ve hatırlama testi puanlarına ilişkin eşlenik çift t-testi sonuçlarına bakılmış [$t=5,642$, $p=0,000<0,05$] anlamlılık değeri 0,000 olup 0,05 değerinden küçük olduğu için H_1 hipotezi kabul edilmiş, H_0 hipotezi reddedilmiştir. Böylece kontrol grubunun son test ve hatırlama testi puanları arasında anlamlı bir fark olduğu söylenebilir.

Bu sonuca göre; ortalamalara bakıldığında kontrol grubu öğrencilerinin modüler aritmetik konusunda klasik anlatım metodunun uygulanmasının, öğrencilerin hatırlamalarını olumsuz etkilediği düşünülebilir. Bu da geleneksel yöntem ile yapılan öğretimde öğrencinin öğrendiği bilgilerde hatırlamanın az olduğu söylenebilir.

4.2.8. Sekizinci Hipotez

Sekizinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Deney grubu öğrencilerinin hatırlamalarında farklılaşma yoktur.

H_1 = Deney grubu öğrencilerinin hatırlamalarında farklılaşma vardır.

Tablo 4.24'te, deney grubu öğrencilerinin hatırlama testi puanlarının normalliğini incelemek için yapılan Kolmogorov-Smirnov test sonuçlarına yer verilmektedir.

Tablo 4.24

Deney Grubu Öğrencilerinin Hatırlama Testi Puanlarına Ait Kolmogorov-Smirnov Testi Sonuçları

N	36
Ortalama	56,667
Standart Sapma	16,647
Kolmogorov-Smirnov Z	0,603
P	0,860

Tablo 4.24'e göre, deney grubu öğrencilerinin hatırlama testi puanlarının normalliğini araştırmak için yapılan Kolmogorov-Smirnov testi sonucunda p değeri 0,860 olup, bu değer 0,05 önem seviyesinden büyük olduğu için deney grubu öğrencilerinin hatırlama testi puanları normal dağılım göstermektedir. Tablo 4.1'den elde edilen sonuçlara göre deney grubunun son test verilerinin de normal dağılım gösterdiği için, altıncı hipotezin istatistiğinde t-testi kullanılabilir.

Tabl 4.25'da, deney grubu öğrencilerinin son test ve hatırlama testi puanlarına ilişkin t-testi sonuçlarına yer verilmiştir.

Tablo 4.25

Deney Grubu Öğrencilerinin Son Test ve Hatırlama Testi Puanlarına İlişkin Eşlenik Çift t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu Son Test	36	59,583	17,500			
Deney Grubu Hatırlama Testi	36	56,667	16,647	35	3,167	0,003

Tablo 4.25’da deney grubu öğrencilerinin son test ve hatırlama testi puanlarına ilişkin eşlenik çift t-testi sonuçlarına bakılmış [$t=3,167$, $p=0,003<0,05$] anlamlılık değeri 0,003 olup 0,05 değerinden küçük olduğu için H_1 hipotezi kabul edilmiş, H_0 hipotezi reddedilmiştir. Böylece deney grubunun son test ve hatırlama testi puanları arasında anlamlı bir fark olduğu söylenebilir. Ortalamalara bakıldığında Şifreleme Yöntemi ile yapılan öğretimde öğrencinin öğrendiği bilgilerde hatırlamanın az olduğu söylenebilir.

4.2.9. Dokuzuncu Hipotez

Sekizinci hipotez için sıfır ve alternatif hipotezler aşağıdaki şekilde oluşmuştur:

H_0 = Deney ve Kontrol grubu öğrencilerinin hatırlamalarında farklılaşma yoktur.

H_1 = Deney ve Kontrol grubu öğrencilerinin hatırlamalarında farklılaşma vardır.

Tablo 4.26’de, deney ve kontrol grubu öğrencilerinin hatırlama testi puanlarına ilişkin t-testi sonuçlarına yer verilmektedir.

Tablo 4.26

Deney ve Kontrol Grubu Öğrencilerinin Hatırlama Testi Puanları Arasındaki Farka İlişkin İlişkisiz t-testi Sonuçları

Gruplar	N	Art. Ort.	ss	sd	t	P
Deney Grubu Hatırlama Testi	36	56,667	15,545			
Kontrol Grubu Hatırlama Testi	36	43,195	16,647	35	-3,461	0,001

Tablo 4.26’da deney ve kontrol grubu öğrencilerinin hatırlama testi puanlarına ilişkin t-testi sonuçlarına bakılmış [$t=-3,461$, $p=0,001<0,05$] anlamlılık değeri 0,001 olup 0,05 değerinden küçük olduğu için H_1 hipotezi kabul edilmiştir. Böylece deney ve kontrol gruplarının hatırlama testi puanları arasında anlamlı bir fark olduğuna karar verilmiştir. Deney grubu öğrencilerinin hatırlama testi puan ortalaması 56,667 iken, kontrol grubu öğrencilerinin hatırlama testi puan ortalaması 43,195’tir. Böylece deney grubu lehine anlamlı bir fark olduğu görülmüştür.

Öğrencilerin öğrendiği bilgilerde hem Şifreleme Aktiviteleri ile hem de geleneksel öğretim yöntemiyle yapılan öğretim sonucunda unutma meydana gelmektedir. Ancak Şifreleme Aktiviteleri ile yapılan öğretimde unutmanın, geleneksel öğretim yöntemiyle yapılan öğretimdeki unutmaya göre çok daha az olduğu anlaşılmaktadır.

Buradan modüler aritmetik konusunun şifreleme aktiviteleri ile öğretim yapılmasının bu öğrencilerin hatırlamalarına etkisinin, klasik anlatım metodundan daha etkili olduğu söylenebilir.

BÖLÜM V: SONUÇLAR VE ÖNERİLER

5.1. SONUÇLAR

Yapılan bu çalışmanın amacı, ilköğretim 8. sınıflarda Modüler aritmetik konusunun öğretiminde Şifreleme aktivitelerinin kullanılmasının öğrencilerin matematik dersi başarısına etkisinin olup olmadığını araştırmaktır. Bu amaç doğrultusunda Ağrı ili, Doğubayazıt ilçesinde bulunan Ş.Ö.Gürhan Yardım İlköğretim Okulu'nda, ilköğretim ikinci kademe 8.sınıf matematik dersi müfredatında bulunan matematik sistemleri ünitesinin Saat aritmetiği, modül ve verilen bir modüle göre toplama ve çarpma işlemleri konularının öğretimi üzerine 12 ders saati süreyle, uygulamacının hazırladığı ders materyalleriyle bir uygulama çalışması yapılmıştır. Bu bölümde çalışmadan elde edilen sonuçlar hakkında bilgi verilmiştir.

- İlköğretim 8.sınıf matematik öğretiminde Şifreleme aktiviteleriyle işlenen matematik dersi ile düz anlatım yöntemiyle işlenen arasında, şifreleme aktiviteleriyle işlenen lehine anlamlı bir farklılık vardır.
- Şifreleme aktivitelerinin uygulandığı deney grubu ile düz anlatım yönteminin uygulandığı kontrol grubu öğrencilerinin hatırlama düzeyleri arasında yapılan t-testi sonuçlarında deney grubu lehine anlamlı bir fark olduğu belirlenmiştir. Şifreleme Aktiviteleri 8. Sınıf matematik dersinde öğrenilenleri hatırlamayı kolaylaştırmaktadır.
- İlköğretim okulları 8.sınıf matematik dersi müfredatında bulunan “Modüler Aritmetik” konusunun öğretiminde, Şifreleme Aktiviteleriyle yapılan öğretim sonucu, öğrencilerin matematik tutumları pozitif yönde farklılaşmıştır.

5.2. ÖNERİLER

Araştırmadan elde edilen sonuçlar ışığında aşağıdaki öneriler getirilebilir.

- Matematik derslerinde öğrenci başarıları değerlendirilmeleri genel yazılılarla sınırlı kalmamalı, işlenen konulara ait hedeflere ulaşım seviyesini ölçen sınavlar da yapılmalıdır.
- Öğretmenler öğrencilere yol göstermeli, öğrencilerin eksik konularında gerekli materyal ve kaynaklara ulaşmaları için çalışmalı ve bazı materyaller öğrencinin kendisine yaptırılarak psiko-motor gelişimi sağlanmalıdır.
- Öğretmenler, öğrencilerin farklı ilgi ve yeteneklere sahip olacağı gerçeğini göz önüne alarak, buna göre değerlendirme ölçekleri hazırlamalıdır.
- Bu çalışma ilköğretim okullarının 8.sınıf matematik konularından olan “Matematik Sistemleri” ünitesiyle sınırlandırılmıştır. Matematik müfredat programında yer alan diğer konular ve üniteler üzerinde de Şifreleme Aktiviteleri ile yapılan öğretimin etkinliği üzerine araştırmalar yapılmalıdır.
- Şifreleme Aktiviteleri ile yapılan eğitim matematik başarıları üzerinde daha etkili bulunduğu için, bu metotla ilgili olarak öğretmenler, öğrenciler, okul yöneticileri ve veliler bilgilendirilmelidir.
- Şifreleme Aktiviteleriyle öğretim yapılabilmesi için öğretmenlere yardımcı kitaplar hazırlanmalı, kitaplarda öğrencilerin ilgi ve yeteneklerine göre hazırladıkları etkinliklere ve uygulamalara yer verilmelidir.
- Orta öğretim okulları matematik konularının Şifreleme Aktiviteleri kullanılarak öğretimlerinin başarıya etkisi araştırılmalıdır.
- Benzer çalışma daha uzun süre ve örneklemeler üzerinde yapılmalıdır.

KAYNAKÇA

- Altun, M.(2000). *Matematik Öğretimi*. (10. Baskı) Bursa: Alfa Yayınları.
- Alpözen, Y. *Rsa Şifreleme Algoritması*,
<http://www.msakademik.net> Web adresinden 10 Temmuz 2007 tarihinde edinilmiştir.
- Alpözen, Y. *RSA Anahtar Dağıtımı ve RSA ile Dijital İmza Oluşturma*,
http://www.msakademik.net/makaleler_detay.aspx?id=513 Web adresinden 10 Temmuz 2007 tarihinde edinilmiştir.
- Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. United States of Amerika: Wiley.
- Baki, A. Bilgisayar Destekli Matematik, Ceren Yayın. (1. Baskı) İstanbul: Ceren Yayın.
- Beissingir, J.(2006). *The Cryptoclub: Using Mathematics to Make and Break Secret Codes*. United States of Amerika: AK Peters, Ltd.
- Bilallar, Ş. (2005). Osmanlı'da Gizli Yazı,
<http://arsiv.sabah.com.tr/2005/05/09/gnd106.html>, Web adresinden 5 Eylül 2005 tarihinde edinilmiştir.
- Bolt, B., Hobbs, D. (1990). 101 Mathematicall Projects. (2.Basım), New York: Cambridge.
- Bruner, J. S. (1983). Intuitive and analytic thinking. M. Donaldson, R. Grieve ve C. Pratt. (Eds). Early childhood development and education: Readings in psychology. Oxford: Basil Blackwell
- Burnett, S. Paine, S. *RSA Security's Official Guide to Cryptography*, March 29, 2001.
- Candiker, A. Kriptoloji: harflerin ve sayıların gizli buluşması,
http://ahmetcandiker.blogspot.com/2007_03_01_archive.html, Adresinden 3 Nisan 2007 tarihinde edinilmiştir.
- Coşkun, H. *Şifreleme ve Asal sayılar*, Matematik Dünyası, Kış 2006. 65-67
- Codes & Ciphers Maths Resources for Teachers, <http://www.bletchleypark.org.uk> Web adresinden 11 Şubat 2007 tarihinde edinilmiştir.
- Churchhouse, R. (2002). *Codes and Ciphers; Julius Caesar, the Enigma, and the Internet*. (1. Baskı) Cambridge: Cambridge University.

- Dede, M. (2007) Sezar Bile Şifreli Haberleşiyordu, Ya Siz?,
<http://www.netpano.com/makale/?makale=29> adresinden 3 Ağustos 2007 tarihinde edinilmiştir.
- Dossey, J. (1992). The nature of mathematics: Its role and its influence. In D. Grouws (Ed.), *Handbook of research on mathematics teaching and learning* (pp. 39-48). New York: MacMillan Publishing Company.
- EREN A.M (2005). *Açık Anahtarlı Kriptografi*. <http://edergi.linux.org.tr> Web adresinden 3 Ağustos 2007 tarihinde edinilmiştir.
- Eskici, A. *Polybius Şifresi*, Matematik Dünyası, Yaz 2004. 72-73.
- Eskici, A. Kriptografi,
<http://www.alieskici.com/kisisel/math/akademik/kriptografi.zip>. Web adresinden 2 Ocak 2007 tarihinde edinilmiştir.
- Gardner, H. (1983). *Frames of mind: The theory of multiple intelligences*. New York: Basic Books, Inc.
- Hill, Raymond. *A first Course in Coding Theory* (1. Baskı), New York: Oxford.
- Ifrah, Georges. *Bir Gölgenin Peşinde* (9. Baskı), Ankara: Tubitak
- Ifrah, Georges. *Çakıl Taşlarından Babil Kulesine* (8. Baskı), Ankara: Tubitak
- <http://math.cankaya.edu.tr/index/hedef0203fallcigdem5.doc> Web adresinden 14 Aralık 2006 tarihinde edinilmiştir.
- Kahn, D. (1996). *Seizing the Enigma*, Arrow Books.
- Kallis, A.S. *Codes & Ciphers*. <http://www.otr.com/ciphers.shtml>. Web adresinden 4 Şubat 2007 tarihinde edinilmiştir.
- Karadağ, N. *Asallar ve Şifreleme*, Bilim Teknik Dergisi, 449, 84.
- Karayılanoğlu, E. *Bir zamanlar Ben Söylemekteydim*,
<http://www.ilknokta.com/V2/Pg/MetaDetail/Number/15836.htm>. Web adresinden 10 Haziran 2007 tarihinde edinilmiştir.
- Kimpton, D. *Çıldır Tan Şifreler*. (1.Baskı) İstanbul: Timaş.
- Koblitz, N. *The following is a slightly shortened version of my article in Cryptologia*, Vol. 21, No. 4 (1997).

<http://www.math.washington.edu/~koblitz/crlogia.html> Web adresinden 2 Ağustos 2007 tarihinde edinilmiştir.

Kodaz, H. RSA Şifreleme Algoritmasının Uygulaması, <http://ab.org.tr/ab03/sunum/90.doc> Web adresinden 17 Haziran 2007 tarihinde edinilmiştir.

Leary, T. Cryptology in the 16th and 17th Centuries. <http://home.att.net/~tleary/cryptolo.htm>. Web adresinden 3 Şubat 2007 tarihinde edinilmiştir.

Lines, M. Bir Sayı Tut. (4. Baskı), Ankara: Tubitak

Matematik 6-8. Sınıflar Programı, <http://ttkb.meb.gov.tr> Web adresinden 11 Ekim 2005 tarihinde edinilmiştir.

Menezes, A., Ooscot, P., Vanstone, S. *Handbook of Applied Cryptography*, October 16, 1996

Myerscough, D. Cryptography: Cracking codes, <http://proquest.umi.com/pqdweb?did=10505874&sid=3&Fmt=3&clientId=43845&RQT=309&VName=PQD>. Web adresinden 10 Mayıs 2007 tarihinde edinilmiştir.

Mors Kodu, <http://www.mors.gen.tr/mors/content/tarihce> , Web adresinden 16 Mayıs 2007 tarihinde edinilmiştir.

Nesin, Ali. Asal Sayılar. www.alinesin.org/popular_math/K_6_asal_sayilar.doc Web adresinden 23 Nisan 2007 tarihinde edinilmiştir.

Oktar, A. Türkçe Üzerine Bir Matematik Modelleme, <http://www.ucnokta.com/modules.php?name=bilgi&file=print&id=220> Web adresinden 6 Eylül 2006 tarihinde edinilmiştir.

ORAL, H. *Phi Tarihinden Günümüze: Ebced ve Şifreleme*, Matematik Dünyası, Yaz 2003. 54-57.

ORAL, H. *Phi Tarihinden Günümüze: İlk Şifreleme Kitapları*, Matematik Dünyası, Kış 2003. 59-60.

Örencik, B. Matematiksel Kriptanaliz, <http://www3.itu.edu.tr/~orencik/> adresinden 6 Eylül 2006 tarihinde edinilmiştir.

Özaygen, A. *Şifreleme*. Bilim Teknik Dergisi, 360, 104.

- Özdemir, A.Ş. *Çözümlü Sayılar Teorisi Problemleri*, İstanbul: Salan Kitap.
- Özdemir, A.Ş, ve Güler, E. (2007). *Using “e” in Cryptology*, ICMOSPS’07. Durban, Güney Afrika.
- Pell, O. *Cryptology*. http://www.ridex.co.uk/cryptology/#_Toc439908861. Web adresinden 28 Ocak 2007 tarihinde edinilmiştir.
- Sevim, Ç. *Public-Key Cryptosystems Based On The Discrete Logarithm*.
- Schneier, B. *Applied Cryptography*, John Wiley and Sons, 1996.
- Siap, İ. Ve Abualrub, T. (2007). *Quaternary Quasi Cyclic Codes of Even Length* , ICMOSPS’07. Durban, Güney Afrika.
- Singh S. (1999). *Code Book; The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. (1. Baskı) . United States of Amerika: Anchor
- Spaht, C., Link, C.W., ve Martin, R. (2002). *Using Cryptology to Stimulate the Student’s Interest in Mathematics Through Application of Functions and Their Inverses*, United States of Amerika: The University of Louisiana at Lafayette.
- Türkiye Kriptografi sayfaları, *Kriptografiye Küçük bir Giriş*, <http://gsu.linux.org.tr/kripto-tr/index.html>. Web adresinden 15 Mayıs 2005 tarihinde edinilmiştir.
- Tattersall, J. *Elementary number theory in nine chapters* (1.Baskı), New York: Cambridge.
- <http://www.nsa.gov/teachers/es/data59.pdf>
- <http://www.puzz.com/cryptos.html>
- http://www.cerias.purdue.edu/education/k12/teaching_resources/lessons_presentations/cryptology.html
- <http://www.madglibs.com/games/madciphers.php?cid=194>
- <http://www.nsa.gov/kids/home.cfm>
- <http://web.csustan.edu/math/Coughlin/SMC06.pdf>
- <http://www.sciencemuseum.org.uk/pdfs/4.2.3%20Make%20a%20code%20wheel%20405KB.pdf>
- <http://www.pbs.org/wgbh/nova/decoding>

<http://www.scienceyear.com/outthere/index.html?page=/outthere/spy/index.html>

<http://www.scouting.org.za/codes>

<http://www.otr.com/ciphers.shtml>

<http://morsecode.scphillips.com>

<http://library.thinkquest.org/28005/flashed/index2.shtml>

http://www.tki.org.nz/r/wick_ed/maths/interactives_code.php

<http://cryptoclub.math.uic.edu/indexmain.html>

http://www.10ticks.co.uk/s_codebreaker.asp

www.mff.org/mmc/mmc.taf?page=code

<http://www.olympus.org/index.php/article/articleview/265/1/2>

http://www.geocities.com/enes_guler/crypto.html

EK 1: Matematik Başarı Testi (Ön Test- Son Test- Kalıcılık Testi)

$1 + \frac{1}{5 + \frac{1}{5 + \frac{1}{5}}}$ işleminin sonucu kaçtır?

- A) $\frac{161}{135}$ B) $\frac{225}{36}$ C) $\frac{126}{25}$ D) $\frac{1}{5}$

6 tane 5'in çarpımının, 5 tane 5'in toplamına bölümü kaçtır?

- A) 6^4 B) 5^4 C) 5 D) $\frac{6}{5}$

$\sqrt{5 + \sqrt{64 \sqrt{\frac{1}{16}}}}$ işleminin sonucu kaçtır?

- A) 9 B) 3 C) $\sqrt{5}$ D) $\sqrt{6}$

★ işlemi, $a \star b = a^b + \sqrt{2ab} + b^a$ şeklinde tanımlanıyor. $2 \star 4$ işleminin sonucu kaçtır?

- A) 20 B) 24 C) 32 D) 36

$x = -2$ ve $y = -1$ için, $x^2y^3 + 2xy^2 - 3x^2y - x + y^2$ ifadesinin değeri kaçtır?

- A) -10 B) -6 C) 3 D) 7

$3x+1 \equiv 2 \pmod{5}$ denkleğinde x yerine yazılabilecek doğal sayıların en küçüğü kaç olur?

- A) 1 B) 2 C) 3 D) 4

$5 \square 2 = 12$

$6 \square 3 = 21$

$7 \square 4 = 32$

Yukarıda örnekleri verilen $\square$ işlemine göre, $3 \square 6$ işleminin sonucu kaçtır?

- A) 19 B) 21 C) 24 D) 27

10 günde bir nöbet tutan bir hemşire ilk nöbetini pazartesi günü tutuyor. Hemşire, sekizinci nöbetini hangi gün tutar?

- A) Pazartesi B) Çarşamba
C) Perşembe D) Cuma

a, b ve c ardışık çift doğal sayılardır. $a < b < c$ ise,

$\frac{(a-b)-(b-c)}{a-c}$ ifadesinin değeri kaçtır?

- A) -1 B) 0 C) 2 D) 4

$(3 \oplus 4) \oplus 3^3 \equiv x \pmod{5}$ denkleğinde, x yerine aşağıdakilerden hangisi gelebilir?

- A) 1 B) 2 C) 3 D) 4

Birinci gün cumartesi ise, 120 nci gün hangi gün olur?

- A) Pazar B) Pazartesi
C) Cuma D) Cumartesi

17 yıl 11 ay 23 gün
- 16 yıl 9 ay 20 gün

Verilen çıkarma işleminin sonucu hangisidir?
(1 ay 30 gün alınacaktır.)

- A) 1 yıl 5 ay 7 gün B) 1 yıl 5 ay 23 gün
C) 1 yıl 2 ay 3 gün D) 5 ay 7 gün

İşe gitmek için sabah saat 7.15 te evden çıkan bir baba, akşam evine geldiğinde saat 8.45 i göstermektedir. Baba, kaç saat sonra evine geri dönmüştür?

- A) 8,5 B) 12 C) 13 D) 13,5

1. işlem : $48 - 4 = 44$

2. işlem : $44 \times \frac{3}{4} = 33$

Verilen işlemlerle aşağıdaki problemlerden hangisinin çözümü yapılmıştır?

- A) 48 in 4 eksiğinin üçte biri kaçtır?
B) Hangi sayının $\frac{3}{4}$ ünün 4 eksiği 48 dir?
C) 48 tane karpuzun 4 ü yenildi. Geriye kalanların $\frac{3}{4}$ ü satıldı. Satılan karpuz sayısı kaçtır?
D) 48 metre kumaşın önce 4 metresi, sonra $\frac{3}{4}$ ü satıldı. Geriye kaç metre kumaş kaldı?

Ahmet, defterine bir sayı yazıyor. Sayıyı aşağıdaki şekilde tanımlıyor.

- Asal sayıdır.
- Basamaklarındaki rakamlar yer değiştirdiğinde çift sayı oluyor.
- Rakamların sayı değerleri toplamı iki basamaklıdır.
- 10^2 nin yarısından büyüktür.

Buna göre, Ahmet'in yazdığı sayı aşağıdakilerden hangisidir?

- A) 101 B) 79 C) 67 D) 47

a	1	2	3	4
b	2	1	$\frac{2}{3}$	$\frac{1}{2}$

a ile b arasındaki değişim yukarıdaki tabloda gösterilmiştir. Buna göre, a ile b arasında nasıl bir ilişki vardır?

- A) $a = \frac{b}{2}$ B) $a = \frac{1}{b}$ C) $a = \frac{2b}{9}$ D) $a = \frac{2}{b}$

I	II	III	IV
(5;10)	(4;8)	(4;9)	(?;?)

Tablodaki geometrik şekiller ile altlarındaki ikililer arasında bir ilişki vardır. Buna göre, IV nolu şeklin altına yazılacak olan ikili hangisidir?

- A) (4;6) B) (4;7) C) (3;6) D) (3;7)

Bir sporcu 4 gün antrenman yapıp 1 gün dinlenmektedir. İkinci dinlenmeyi pazar günü yaptığına göre, onbeşinci dinlenmeyi hangi gün yapar?

- A) Çarşamba B) Salı
C) Pazartesi D) Pazar

Bugün günlerden Pazar olduğuna göre, 37 gün önce günlerden hangisiydi?

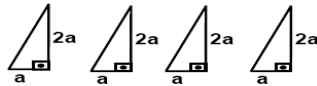
- A) Çarşamba B) Perşembe C) Cuma
D) Cumartesi E) Pazar

Ürün Adı	I. Kalite Fiyatı (Milyon TL)	II. Kalite Fiyatı (Milyon TL)
Sehpa	45	35
Tava	20	15
Çaydanlık	35	25
Tencere	30	20

Bir mağazada satılan bazı ürünlerin kalitelerine göre fiyatları tabloda verilmiştir. Bir müşteri, her üründen yalnız bir tane alarak toplam 100 milyon TL ödüyor.

Müşteri, aldığı ürünlerin seçimini nasıl yapmıştır?

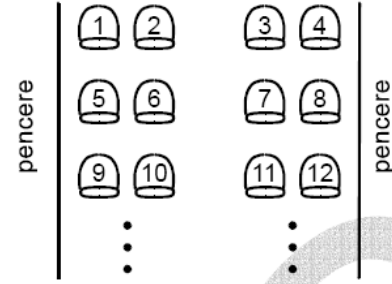
- A) Hepsini II. kalite seçmiştir.
B) İkisini I.kalite, ikisini II. kalite seçmiştir.
C) Üç tanesini II. kalite, bir tanesini I. kalite seçmiştir.
D) Üç tanesini I. kalite, bir tanesini II. kalite seçmiştir.



Yukarıdaki şekiller kullanılarak aşağıdakilerden hangisi olusturulamaz?

- A) B)
C) D)

Bir trendeki koltuklar, 1 den başlayarak ve soldan sağa doğru artarak aşağıda verilen şekildeki gibi numaralandırılıyor.



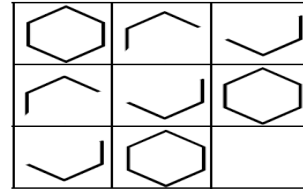
Buna göre, aşağıdaki koltuk numaralarından hangisi pencere kenarındadır?

- A) 73 B) 75 C) 78 D) 82 E) 83

Bir hasta üç değişik ilacı 6, 9 ve 10 saatte bir almaktadır.

Bu hasta, ilaçların üçünü bir arada kaç saatte bir alır?

- A) 30 B) 45 C) 90 D) 120 E) 150



Yukarıdaki tabloda satırlardaki ve sütunlardaki karelerin içine bir kurala göre şekiller yerleştirilmiştir. Buna göre, tabloda boş bırakılan yerde, aşağıda verilen şekillerden hangisi bulunmalıdır ?

- A) B)
C) D)

Beşinci, altıncı ve yedinci terimleri sırasıyla 11, 18 ve 29 olan sayı dizisinin her bir terimi kendinden önceki iki terimin toplamına eşittir.

Buna göre, bu dizinin üçüncü terimi kaçtır?

- A) 2 B) 3 C) 4 D) 5 E) 6

EK 2: Matematik Tutum Ölçeği

Aşağıdaki maddeleri dikkatlice okuyunuz. Her madde sizin matematikle ilgili görüşünüzü almaya yöneliktir. Lütfen bu maddelerdeki durumların sizin için ne kadar geçerli olduğunu belirtiniz.

		Asla	Nadiren	Bazen	Sık Sık	Her Zaman
1	Matematik dersleri zevkli geçer.					
2	Matematik dersinde canım sıkılıyor.					
3	Matematiğim kuvvetlidir.					
4	İleride matematik öğretmeni olmak istiyorum.					
5	Matematik dersinde başka şeylerle ilgilenirim.					
6	Matematik dersinde konuları anlayamıyorum.					
7	Matematik bilgisi gerektiren konularda başarılıyım.					
8	Matematik dersi benim için keyifli bir oyun saati gibidir.					
9	Matematik dersi yerine ilgilendiğim başka bir derse girmeyi tercih ederim.					
10	Matematik bilmek ileride işime yarayacak.					
11	Belli temel bilgilerin dışında matematik bilmek gereksizdir.					
12	Matematik ödevlerimden nefret ederim.					
13	Matematik başarılı olduğum bir derstir.					
14	İleride matematikle ilgili bir alanda çalışırsam başarılı olabilirim.					
15	Matematiği neden okumak zorunda olduğumuzu anlayamıyorum.					
16	Matematik insanı daha iyi düşünmeye zorlar.					
17	Matematik dersi beni bunaltıyor.					
18	Matematik bilgisi iyi olan bir kişi diğer bilimleri rahatça anlar.					
19	Çalışırsam matematikten iyi notlar alabilirim.					
20	Matematik öğretmenleri çalışkandır.					

EK 3: Bilgi Formu Anket Soruları

BİLGİ FORMU ANKET SORULARI

1. Adınız Soyadınız

.....

2. Cinsiyetiniz? () Kız () Erkek

3. Okulunuzun Adı

4. Anne ve babanızın öğrenim durumu nedir?

	Anne	Baba
İlkokul Mezunu	()	()
Ortaokul Mezunu	()	()
Lise ve dengi okul mezunu	()	()
Yüksek okul mezunu	()	()
Diğer (.....)	()	()

5. Babanızın mesleği nedir?

Memur () İşçi () Ticaret () Diğer
(.....)

6. Annenizin mesleği nedir?

Memur () İşçi () Ev Hanımı () Diğer
(.....)

7. Babanız çalışıyorsa ortalama aylık geliri? (.....)

8. Anneniz çalışıyorsa ortalama aylık geliri? (.....)

9. Ailenizin oturduğu konut tipi nedir?

Müstakil Ev () Apartman Dairesi () Gecekondu ()
Diğer (.....)

10. Oturduğunuz evdeki oda sayısı?

Bir () İki () Üç () Üçten fazla (.....)

11. Çalışma odanız var mı? Evet () Hayır ()

12. Çalışma odanızı (kendiniz hariç) kaç kişiyle paylaşıyorsunuz?

Bir () İki () Üç () Üçten fazla (.....)

13. Okula gitmediğiniz zamanlar bir işte çalışıyor musunuz?

Evet () Hayır ()

14. Dershaneye gidiyor musunuz?

Evet () Hayır ()

15. Özel ders alıyor musunuz?

Evet () Hayır ()

16. Evde derslerinize daha çok kim yardımcı oluyor?

Hiç kimse yardımcı olmuyor () Annem ()

Babam ()

Ablam/ağabeyim () Diğer ()

17. Derslerinize yardım eden kişi ne kadar sıklıkla yardım ediyor?

Her Zaman () Sık sık () Bazen () Nadiren ()

Hiç ()

18. İlköğretim 1. Kademe (4. ve 5. Sınıf öğretmeni) öğretmeninizin ismi nedir?

(.....)

19. Bu sene matematik dersinize giren öğretmeninizin ismi nedir?

(.....)

20. I. Dönem karnenizde matematik ders notunuz kaçtır?

1 () 2 () 3 () 4 () 5 ()

[illegible]

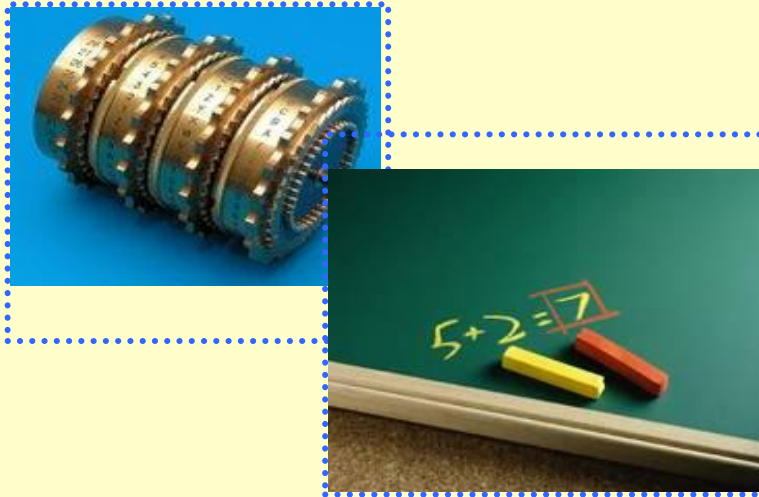
Sezar Şifresi-2

a.) **BİLMECE:** Yeni doğan zenci bir bebeğin dişleri ne renktir?

CEVABI:

Düz Metin

Şifreli Metin Ğ M V Ö H U M C S O Y Z U



b.) BİLMECE: 2 adam 5 kere satranç oynamış, her biri aynı sayıda oyun kazanmış fakat hiç bir oyun berabere bitmemiş. Bu nasıl olur

CEVABI:

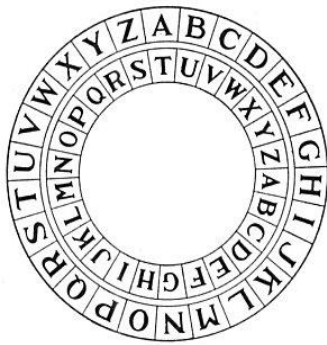
[illegible]

S	C	R	D	P	L	C	S	U	P	Z	V

Sezar Şifresi-3

Şifre Diskleri:

İlk şifre makinesi, Leon Alberti tarafından icat edilmiştir. Alberti'nin şifre diski iki bakır diskten oluşuyordu. Bu disklerden biri büyük, diğeri küçüktü. Merkezlerinden bağlanan 2 diskten küçük olan disk dönebiliyordu. Büyük diskin kenarında normal alfabe, küçük diskin üzerinde de şifreli alfabe bulunuyordu.



4. a.) "Özel Bilgi" cümlesini Şifre Diskini kullanarak şifreleyiniz. (Saatin tersi yönünde 5 kaydırarak.)

	Düz Metin	ö	z	e	l	b	i	l	g	i
	Şifreli Metin									

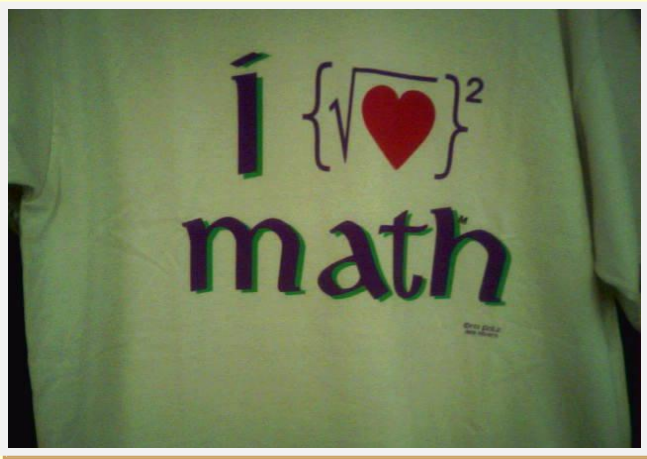
- b.) Okulunuzun adını Şifre Diskini kullanarak şifreleyiniz. (8 kaydırarak.)

[illegible]

Sezar Şifresi-4

5.) Kendi bilmecenizi yazın ve şifreleyiniz. Sonra sınıftaki arkadaşlarınıza sorunuz.

BİLMECE: _____

[illegible]

Sezar Şifresi-5

Sayılarla Mesaj Gönderme.

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

1.)Şifreleme Şeridini kullanarak harfleri sayılarla değiştir.

Düz Metin b e n i m l e s i n e m a d a b u l u ş

Şifreli Metin

2.)3 kaydırılmış Şifreleme Şeridini kullanarak harfleri sayılarla değiştir.

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	0	1	2

Düz Metin b e n i m l e s i n e m a d a b u l u ş

Şifreli
Metin

3.) 1. Sorunun cevabından 2.sorunun cevabına geçilirken hangi matematiksel işlem kullanılmıştır? Açıklayınız.

a.)4 kaydır

Düz Metin	a	s	u
Sayı			
Kaydırılan Sayı			

b.) 5 kaydır

Düz Metin	t	e	l	g	r	a	f
Şifreli Metin							
Kaydırılan Sayı							

Sezar Şifresi-6

c.) 8 kaydır. (S'nin şifrelenmesinde farklı olan nedir?)

Düz Metin	m	o	r	s		k	o	d	u
Sayı									
Kaydırılan Sayı									

SAAT ARTİMETİĐİ



Mekanik saat (16. yy)

1577'de dakikayı gösteren ilk saat yapılmış. Jost Burgi'nin amacı, astronomların kullanacağı bir yardımcı üretmekmiş. 1656'da sarkaç icat edilmiş, bu da saatleri daha güvenilir hale getirmiş. Koluna saat takan ilk kişi ise Fransız matematikçi ve filozof Blaise Pascal. Yıllardan 1660. Saat kavramını standartlarına oturtan ise 1878'de Sir Sanford Fleming olmuş.



2.) Ayşe'nin cumartesi saat 11.00'de tiyatro kursu vardır. Tiyatro kursu 3 saat sürdüğüne göre, Ayşe'nin kursu ne zaman biter?

3.) Murat Erzurum'dan İstanbul'a gidecektir. Yolculuk tam 13 saat sürmektedir. Murat sabah 8'de yola çıktığına göre saat kaçta Erzurum'da olur?

4.) Dedesi'ni ziyarete gidecek olan Cemal arabasıyla 13 saatlik bir yolculuk yapmıştır. Bir otelde 8 saat dinlenen Cemal yolculuğuna devam etmiştir. 13 saat sonra dedesinin yanına ulaşmıştır. Cumartesi sabahı 10'da yola çıkan Cemal, dedesinin yanında kaçta olmuştur?

1.) Aşağıdaki işlemleri saat aritmetiđini kullanarak yapınız?

a.) $5+10=$

b.) $8+11=$

c.) $7+3=$

d.) $9+8+8=$

SAAT ARTİMETİĞİ-2

7.) Öğlen 2'de kamp yerinde olacak Beyza, 5 saat önce evden yola çıkmıştır. Beyza yola çıktığında saat kaçtı?

8.) Problemde saati ters yönde ilerlettik. Saat aritmetiğinde çıkarma işlemi böyledir. Aşağıdaki işlemleri saati kullanarak yapınız?

a.) $3-7=$ _____

b.) $2-3=$ _____

c.) $5-6=$ _____

d.) $5-10=$ _____

5.) Aşağıdaki ifadeleri 24 saatlik sisteme çeviriniz?

a.) 3 (Öğleden sonra) _____

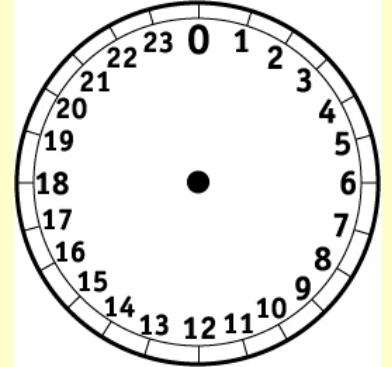
b.) 9 (Öğleden önce) _____

c.) 11:15 (Öğleden sonra) _____

d.) 4:30 (Öğleden önce) _____

e.) 6:45 (Öğleden sonra) _____

f.) 8:30 (Öğleden sonra) _____



6.) Aşağıdaki ifadeleri 12 saatlik sisteme çeviriniz?

a.) 13:00 _____

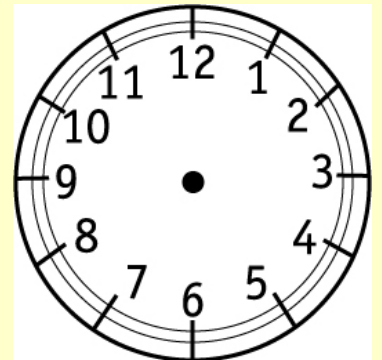
b.) 5:00 _____

c.) 19:15 _____

d.) 21:00 _____

e.) 11:45 _____

f.) 15:30 _____



SAAT ARİTİMETİĞİ-3

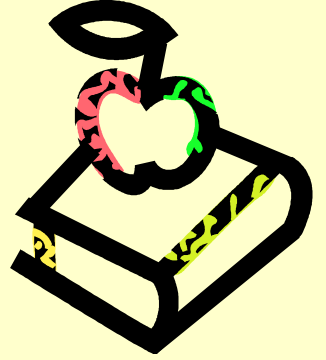
9.) Aşağıdaki işlemleri saat aritmetiğini kullanarak yapınız? (24 saatlik sisteme göre.)

a.) $20+6=$ _____

b.) $11+17=$ _____

c.) $22-8=$ _____

d.) $8-12=$ _____



10.) Aşağıdaki işlemleri 10'luk saate göre yapınız?

a.) $8+4=$ _____

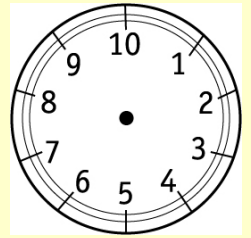
e.) $6-8=$ _____

b.) $5+8=$ _____

f.) $3+5=$ _____

c.) $7+7=$ _____

d.) $10+15=$ _____



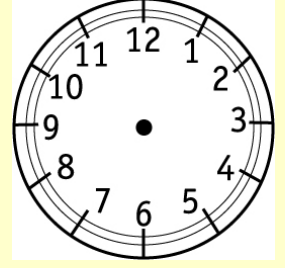
11.) $2+2$ 'nin 4 olmadığı bir saat bulunuz?

SAAT ARTİMETİĞİ-4

1.) Her sayıya 3 sayı denkliği listeleyiniz.

a.) $6 \bmod 12$ _____

b.) $9 \bmod 12$ _____

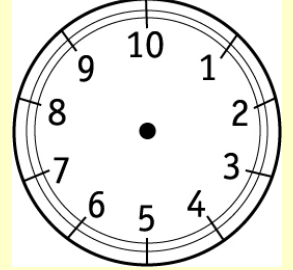


2.) Her sayıya 3 sayı denkliği listeleyiniz.

a.) $2 \bmod 10$ _____

b.) $9 \bmod 10$ _____

c.) $0 \bmod 10$ _____

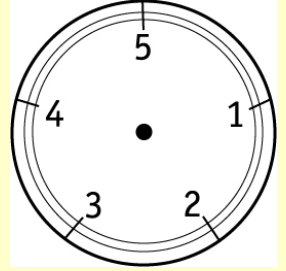


3.) Her sayıya 3 sayı denkliği listeleyiniz.

a.) $1 \bmod 5$ _____

b.) $3 \bmod 5$ _____

c.) $2 \bmod 5$ _____



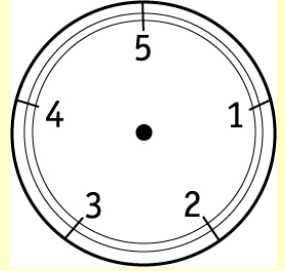
4.) Her sayıyı küçültün.

a.) $8 \bmod 5 =$ _____

b.) $13 \bmod 5 =$ _____

c.) $6 \bmod 5 =$ _____

d.) $4 \bmod 5 =$ _____



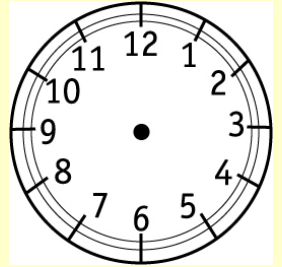
5.) Her sayıyı küçültün.

a.) $18 \bmod 12 =$ _____

b.) $26 \bmod 12 =$ _____

c.) $36 \bmod 12 =$ _____

d.) $8 \bmod 12 =$ _____



SAAT ARTİMETİĞİ-5

6.) Her sayıyı küçültün.

a.) $8 \bmod 3 =$ _____

b.) $13 \bmod 6 =$ _____

c.) $16 \bmod 11 =$ _____

d.) $22 \bmod 7 =$ _____

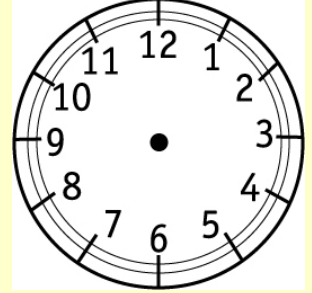
7.) Her sayıyı küçültün.

a.) $-4 \bmod 12 =$ _____

b.) $-1 \bmod 12 =$ _____

c.) $-6 \bmod 12 =$ _____

d.) $-2 \bmod 12 =$ _____



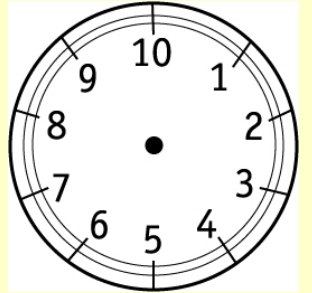
8.) Her sayıyı küçültün.

a.) $-4 \bmod 10 =$ _____

b.) $-1 \bmod 10 =$ _____

c.) $-6 \bmod 10 =$ _____

d.) $-2 \bmod 10 =$ _____



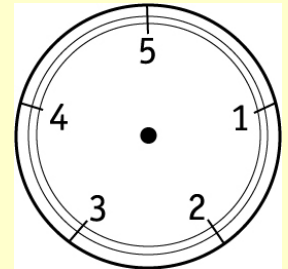
9.) Her sayıyı küçültün.

e.) $-3 \bmod 5 =$ _____

f.) $-1 \bmod 5 =$ _____

g.) $8 \bmod 5 =$ _____

h.) $7 \bmod 5 =$ _____



10.)Her sayıyı küçültün.

a.) $-2 \bmod 24 =$ _____

b.) $23 \bmod 20 =$ _____

b.) $16 \bmod 11 =$ _____

d.) $-3 \bmod 20 =$ _____

Frekans Analizi

El-Kindi, bir filozof, matematikçi, fizikçi, astronom, hekim, coğrafyacı ve hatta müzikte bir uzman idi. Onun bu alanların tamamına özgün katkılar yapmış olması şaşırtıcıdır. Eserlerinden dolayı, Arapların Filozofu olarak bilinir.

Matematikte, sayı sistemi üzerine dört kitap yazmıştır ve modern aritmetiğin büyük bir bölümünün kuruluşunu hazırlamıştır. Arap sayılar sisteminin büyük ölçüde el-Harizmi tarafından geliştirilmiş olduğundan şüphe yoktur, ancak El-Kindi de bu konu üzerine zengin katkılarda bulunmuştur. Aynı zamanda, astronomi ile ilgili çalışmalarında yardım etmesi için küresel geometriye de katkıda bulunmuştur.

El-Kindi'nin en büyük araştırması, Kriptografik Mesajların Deşifre Edilmesi Üzerine bir Yazı, İstanbul'da 1987 yılında kamuoyuna açılan Süleymaniye Osmanlı Arşivinde ortaya çıkarılmıştır. Arapça söz dizimi, ses bilimi ve istatistik hakkında oldukça ayrıntılı tartışmaları içermektedir.

Aşağıdaki metinlerden istediğiniz birini seçip 2. Sayfadaki frekans analizi tablosunu doldurunuz?

I.

Eflatun'a sormuşlar;

İnsanoğlunun sizi en çok şaşırtan iki davranışı nedir?

Eflatun tek tek sıralamış, Çocukluktan sıkılırlar ve büyümek için acele ederler. Ne var ki çocukluklarını özlerler. Para kazanmak için sağlıklarını yitirirler. Ama sağlıklarını geri almak için de para öderler. Yarınlarından endişe ederken bugünü unuturlar. Sonuçta, ne bugünü, ne de yarını yaşarlar. Hiç ölmeyecek gibi yaşarlar. Ancak hiç yaşamamış gibi ölürlər.



II.

İki parmağının ucunun iki gözüne koy...

Bir şey görebilir misin dünyadan?

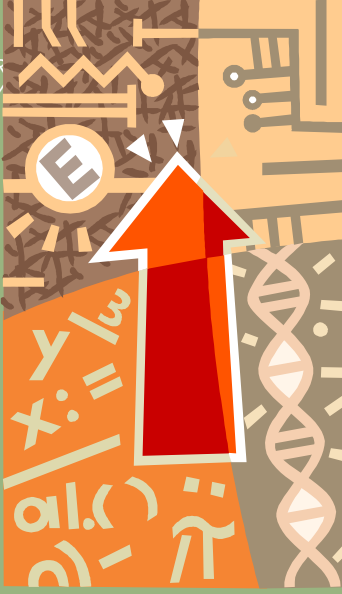
Görememek ayıbı, gösterememek kusuru uğursuz nefsin parmağına ait işte...

Parmağını gözünden kaldırdı ilkin, sonra gör dilediğini böyle...

İnsan gözden ibarettir aslında, geri kalan cesettir.

Göz ise ancak Sevgiliyi görene denir.

Mevlana Celaleddin Rumi



Frekans	Kesir	Ondalık Kesir (3 basamak)	Yüzde(%)
A			
B			
C			
Ç			
D			
E			
F			
G			
Ğ			
H			
I			
İ			
J			
K			
L			
M			
N			
O			
Ö			
P			
R			
S			
Ş			
T			
U			
Ü			
V			
Y			
Z			
Toplam			

- I. Metinde T harfi kaç tanedir? _____
- II. Metin 100 harften oluşsaydı T harfi kaç adet olurdu? % _____
- III. Metinde E harfi kaç tanedir? _____
- IV. Metin 1000 harften oluşsaydı E harfi kaç adet olurdu? _____

V. Metindeki harfleri çok kullanılanıdan az kullanılanı doğru sıralayınız?

[illegible]

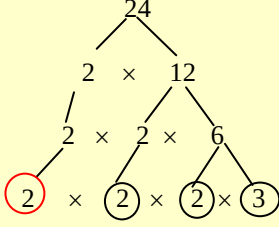
VI. Sağ tarafta Türkçede kullanılan harfler ve yüzdelikleri verilmiştir. Sizde sol taraftaki sütuna metinde geçen harfleri ve yüzdeliklerini yazınız ve sonra her iki sütunu karşılaştırınız?

A	26.323
E	16.308
K	13.542
İ	13.384
M	11.263
L	10.496
T	9.669
R	8.698
N	8.206
S	7.929
I	7.579
U	4.952
D	4.532
Ü	4.526
Y	3.773
B	3.703
O	3.635
H	3.577
Z	3.083
Ş	2.851
P	2.379
C	2.300
F	2.251
V	2.236
Ç	2.104
G	2.042
Ğ	1.214
Ö	916
J	125

Çarpan Ağacı

Bir doğal sayı seçilir, bu sayının asal sayıların çarpımı şeklinde yazılıp yazılamayacağı araştırılır. Asal çarpanlara ayırmada aşağıdaki gibi yöntemler kullanılarak asal sayıların 1 ve kendisinden başka çarpanları olmadığı buldurulur.

1. Çarpan ağacı



$$24 = 2 \times 2 \times 2 \times 3$$

$$= 2^3 \times 3$$

2. Asal çarpanlar algoritması

24	2	
12	2	
6	2	
3	3	
1		

$$24 = 2 \times 2 \times 2 \times 3$$

$$= 2^3 \times 3$$

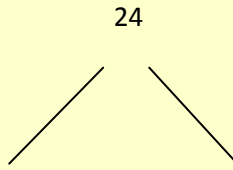
1. Aşağıdaki sayıların çarpanlarını bulunuz?

- a.) 15 _____
- b.) 24 _____
- c.) 36 _____
- d.) 60 _____
- e.) 23 _____

2. 30'dan küçük bütün asal sayıları yazınız?

3. Aşağıdaki sayıları çarpan ağacı kullanarak çarpanlarına ayırınız?

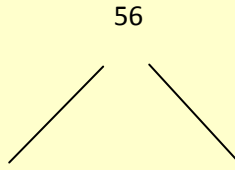
a.)



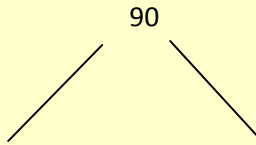
a. 24= _____

ÇARPAN AĞACI-2

b.)



c.)



a. $56 =$ _____

b. $90 =$ _____

1. Aşağıdaki sayılardan hangileri 2 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

a.) 284

b.) 181

c.) 70

d.) 5456

2. Aşağıdaki sayılardan hangileri 3 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

a.) 585

ÇARPAN AĞACI-3

b.) 181

c.) 70

d.) 6249

3. Aşağıdaki sayılardan hangileri 4 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

a.) 348

b.) 236

c.) 621

d.) 8480

4. Aşağıdaki sayılardan hangileri 5 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

a.) 80

b.) 995

c.) 232

d.) 444

5. Aşağıdaki sayılardan hangileri 6 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

a.) 96

b.) 367

c.) 642

d.) 842

ÇARPAN AĞACI-4

6. Aşağıdaki sayılardan hangileri 9 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

e.) 333

f.) 108

g.) 348

h.) 1125

7. Aşağıdaki sayılardan hangileri 10 ile bölünebilir? Bunu işlem yapmadan nasıl anlarız?

i.) 240

j.) 1005

k.) 60

l.) 9900

8. Sayıların ortak çarpanlarını yazınız?

a.) 10 ve 25

Ortak Çarpanlar: _____

b.) 12 ve 18

Ortak Çarpanlar: _____

c.) 45 ve 60

Ortak Çarpanlar: _____

9. Aşağıdaki sayıların en büyük ortak bölenlerini bulunuz?

a.) 12 ve 20

E.B.O.B: _____

b.) 50 ve 75

E.B.O.B: _____

c.) 30 ve 45

E.B.O.B: _____

ÇARPAN AĞACI-5

10. Aşağıdaki sayıları önce çarpanlarına ayırınız, sonra ortak çarpanlarını bulunuz?

a.) 14= _____

22= _____

10= _____

Ortak Çarpan: _____

b.) 66= _____

210= _____

180= _____

Ortak Çarpan: _____

c.) 30= _____

90= _____

210= _____

Ortak Çarpan: _____

Modüler Aritmetik

1. Mod 28'e göre aşağıdaki işlemleri yapınız?

a.) $29 = \underline{\hspace{2cm}} \text{ mod } 28$

e.) $33 = \underline{\hspace{2cm}} \text{ mod } 28$

b.) $12 = \underline{\hspace{2cm}} \text{ mod } 28$

f.) $40 = \underline{\hspace{2cm}} \text{ mod } 28$

c.) $-4 = \underline{\hspace{2cm}} \text{ mod } 28$

g.) $52 = \underline{\hspace{2cm}} \text{ mod } 28$

d.) $-10 = \underline{\hspace{2cm}} \text{ mod } 28$

h.) $-7 = \underline{\hspace{2cm}} \text{ mod } 28$

2. "Kriptoloji" kelimesini aşağıdaki formu kullanarak şifreleyiniz?

	K	R	i	P	T	O	L	O	J	i
Harfleri Sayıya Çevir	13	20								
3 ile Çarp	39	60								
mod 28	11	4								
Sayıyı Harfe Çevir	i	D								

3. Aşağıdaki işlemleri yapınız?

a.) $175 \text{ mod } 28 = \underline{\hspace{2cm}}$

b.) $106 \text{ mod } 28 = \underline{\hspace{2cm}}$

c.) $78 \text{ mod } 28 = \underline{\hspace{2cm}}$

d.) $150 \text{ mod } 28 = \underline{\hspace{2cm}}$

4. Aşağıdaki işlemleri yapınız? (İpucu: $10 \times 28 = 280$)

a.) $586 \text{ mod } 28 = \underline{\hspace{2cm}}$

b.) $792 \text{ mod } 28 = \underline{\hspace{2cm}}$

c.) $541 \text{ mod } 28 = \underline{\hspace{2cm}}$

d.) $364 \text{ mod } 28 = \underline{\hspace{2cm}}$

5. Hesap makinesi kullanarak aşağıdaki işlemleri yapınız?

a.) $254 \text{ mod } 24 = \underline{\hspace{2cm}}$

b.) $827 \text{ mod } 26 = \underline{\hspace{2cm}}$

c.) $700 \text{ mod } 9 = \underline{\hspace{2cm}}$

d.) $500 \text{ mod } 5 = \underline{\hspace{2cm}}$

e.) $1500 \text{ mod } 26 = \underline{\hspace{2cm}}$

f.) $120 \text{ mod } 11 = \underline{\hspace{2cm}}$

6. Aşağıdaki işlemleri yapınız?

a.) $500 \text{ mod } 7 = \underline{\hspace{2cm}}$

b.) $25,000 \text{ mod } 5280 = \underline{\hspace{2cm}}$

c.) $1000 \bmod 24 =$

d.) $10,000 \bmod 365 =$

7. Problem 5'ten bir soru seçip arkadaşınıza nasıl yaptığınızı açıklayınız?

8. Sezar'ın “geldim, gördüm, yendim” anlamındaki sözünü forumu kullanarak şifreleyiniz?

	w	e	n	i	w	i	d	i	w	i	c	i
Harfleri Sayıya Çevir												
11 ile Çarp												
mod 28												
Sayıyı Harfe Çevir												

9. Astronotlar bir görev için Pazar günü uzayda kaldılar. Hangi gün dönerler?

a.) 4 gün uzayda kaldılar? _____

b.) 15 gün uzayda kaldılar? _____

c.) 100 gün uzayda kaldılar? _____

d.) 1000 gün uzayda kaldılar? _____

10. Bugün günlerden Çarşamba ise,

a.) 3 gün sonra hangi gündür?

b.) 75 gün sonra hangi gündür?

c.) 300 gün sonra hangi gündür?

11. Eğer yıl 400'e tam bölünüyorsa yıl, artık yıldır. Eğer yıl 4'e tam bölünebiliyor, 100'e tam bölünemiyorsa, artık yıldır.

1900 artık yıl değil, 2004 artık yıldır.

- a.) 2004 yılından sonraki iki artık yılı yazınız? _____
- b.) Hangi yıllar artık yıldır? (1996, 1776, 1890) _____

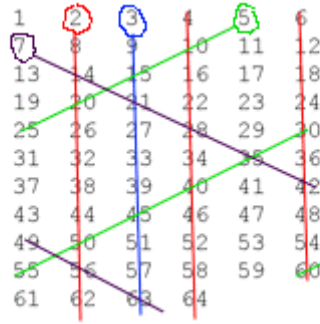
12. Bu yıl 4 temmuz Salıdır. Seneye 4 temmuz hangi gündür? Bu sorunun nasıl çözülebileceğini açıklayınız?

13.) a. Bugün haftanın hangi günüdür? _____

b. Seneye bugün haftanın hangi günü olur? Bu sorunun nasıl çözülebileceğini bulunuz?

14.) Seneye doğum günün hangi gün olacaktır? (Takvim kullanabilirsin.)

15.) 21. Doğum günün hangi gündür? (Artık yılları hesaba katmayı unutma!) Nasıl bulabileceğini açıklayınız?



1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	100

ASAL SAYILAR

Eratosthenes tarafından M.Ö. 3 yy da geliştirildi. 1 ile 100 arasındaki asal sayıları bulmak istediğimizi farz edelim. Bu sayılardan oluşan bir tablo yapın ve şu şekilde devam edin. En küçük asal iki olduğundan, 2 nin bütün katlarının üzerlerini çiziniz. Sonraki çizilmeyen sayı 3 olduğundan 3 ü çember içine alıp katlarının üzerlerini çiziniz. Sonraki 5 sayısı için de aynısını yapın ve böyle devam edin. Sayılar çoğaldığında bu işlem uzayacak ve nerede son bulacağını bilmek gerekecektir. Bir teoreme göre, bir sayının asallığını araştırmak için en son, onun kareköküne en yakın asal incelenirse yetecektir. 100 ün karekökü 10 olduğundan 7 nin katlarını silmek yetecektir. Sonuçta kalan sayılar (çizilmeyenler) aradığımız asal sayılardır. .

ASAL SAYILAR

1. Aşağıdaki sayıların asal olup olmadığını bulunuz? Nasıl bulduğunuzu açıklayınız.

a.) 343 _____

b.) 1019 _____

c.) 1369 _____

d.) 2417 _____

e.) 2573 _____

f.) 1007 _____

- 2.) Eratosthenes (Eratosten) kalburu:

1'den 100'e kadar olan sayılar yazılır. 2, yuvarlak içine alınır. 2'nin bütün katları boyanır veya üzerine çarpı koyulur. Aynı işlem 3 için yapılır. 4, 2'nin katı olduğu için işleme 5 ile devam edilir. İşlem, benzer şekilde tamamlanır. 100'den küçük bütün asal sayılar ortaya çıkartılır.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

- g.) 50'ye kadar olan asal sayılar:

—

Etkinlik: Asal sayıların elde edilmesi (*Eratosthenes Kalburu*)

Grup: İki kişi

Materyal: 100 lük sayı tablosu, renkli kalem

İşlemler: “1 hariç, 1 ve kendisinden başka bir doğal sayıya tam olarak bölünemeyen sayılara **asal** sayı denir.”

- 2 asaldır, çünkü 1 ve 2’den başka doğal sayı böleni yoktur. Bir sayı asal ise, onun hiçbir katı asal olamaz.
- Aşağıdaki işlemleri yaparak 100’e kadar olan asal sayıları elde ediniz.
- 1 sayısı asal değildir, çünkü tanımda hariç tutulmuştur, onun için 1 sayısının üzerini çizin
- 2 sayısını yuvarlak içerisine alınız, 2 asaldır. 2’nin tüm katlarını renkli bir kalemle çizin, çünkü onlar asal değildir.
- 3 sayısı asaldır, yuvarlak içerisine alınız. 3’ün tüm katlarını başka bir renkli kalemle çizin.
- 4 ve 4’ün tüm katları çizilidir. (*Neden?*)
- 5’i yuvarlak içerisine alınız, çünkü 5 asaldır ve 5’in tüm katlarını çizin. (*Daha önce çizilmemiş ve şimdi çizilen ilk sayı kaçtır?*)
- 6’yı çizmeniz gerekmemektedir, *neden?*
- 7’yi yuvarlak içerisine alınız ve 7’nin tüm katlarını çizin.
- 8, 9 ve 10 için sayı çizmeniz gerekmemektedir, *neden?*
- 11 için aynı işlemi yapınız.

Bu işlemlerin sonunda tabloda hiç çizilmeden kalan sayıların bir listesini yapınız. Bu sayılar 100’e kadar olan **asal** sayılardır. Asal sayılar, sayılar büyüdükçe seyrelmektedir.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

 Rail fence

ASLAN KRAL!

A L N R L
 \ S / \ A / \ K / \ A / \ !

ALNRLSAKA!

Düz Metin:

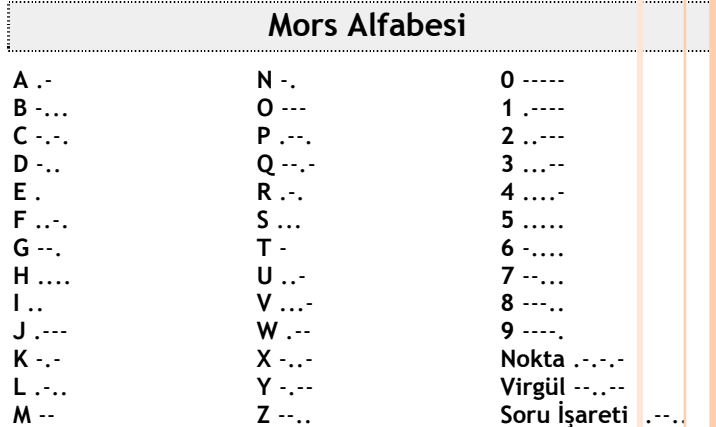
Biz yarın geleceğiz!

B		Z		A		I		G		L		C		Ğ		Z	
	İ		Y		R		N		E		E		E		İ		!

Şifreli Metin:

Düz Metin: Bu Adam Casus

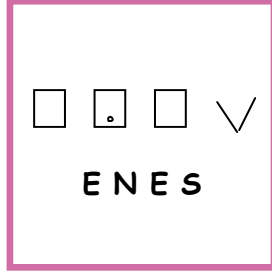
Şifreli Metin:



Orijinal mors kodu kısa ve uzun sinyallerin kombinasyonunun bir sayıya karşılık gelmesinden oluşmuştu. Her sayı da bir harfe karşılık geliyordu.

Pigpen-Polybius Şifresi

On sekizinci yüzyılda, farmasonlar adında gizli bir örgüt, Amerikan iç savaşında Konfederasyon askerleri ve müşterilerinin okumalarını istemedikleri bilgileri mallan üzerine yazmak isteyen bazı tüccarlar tarafından da kullanılmıştır.



➤ Pigpen Şifresi'ni kullanarak isminizi şifreleyiniz?

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

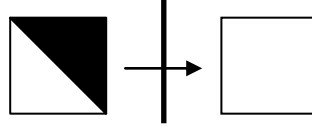
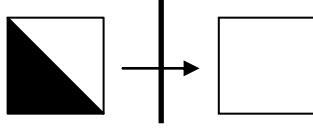
Bir diyagrama dayalı olarak kullanılan başka bir şifrede binlerce yıl önce Polybius adında bir Yunanlı tarafından keşfedilmiştir.

➤ Polybius Şifresi'ni kullanarak isminizi şifreleyiniz?

➤ “ 2432355215331145153311452431 ” Polybius şifresiyle şifrelenmiş cümleyi bulunuz?

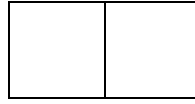
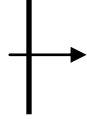
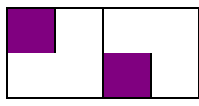
BİR SAAT SANAT POSTERİ HAZIRLAYIN

1. İlk olarak: Dikey ya da yatay şekilde yansıtılan desenleri çiziniz. Sonra dikey çizgileri karşı tarafına yansıttıklarını çiziniz.



Her taraf, bir "ayna yansıması" olmalı eğer dikey çizgisinde kâğıdınızı katlasanız, resimlerin renkli üçgen bölümü aynen eşleşmeli.

- a.) Dikey çizginin karşı tarafında iki desenin yansıttığını çizin.



← Desenleri yansıtınız.

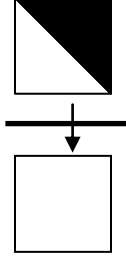
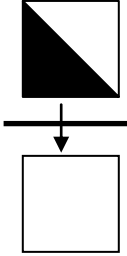
← Desenleri yansıtınız.

Konum 1 2

2 1

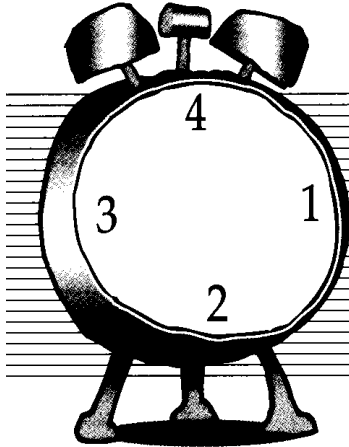
- b.) Yatay satırların karşı tarafında desenlerin yansıttıklarını çizin:

Yatay satırlar katlandıklarında karşı tarafla eşleşmeli.



Desenler ve konumları yansıtınız.

2. SAAT ARİTMATİĞİ



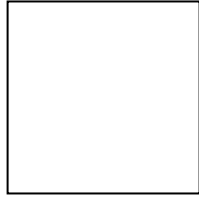
+	1	2	3	4
1				
2				
3				
4				

3. RENKLİ KODLAR: 4'lük saat için basit dizaynlar oluřturunuz?

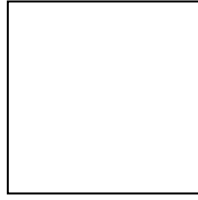
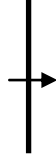
1	2	3	4

4. Tasarımlarınızın her birini dikey ve yatay řekilde yansıtmak:

Dikey Hatlar'ını karşı tarafında yatay yansımalar.



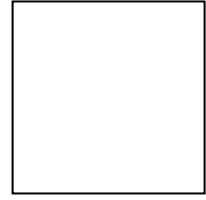
Dizayn 1



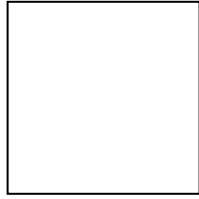
Dizayn 1'i yansıt



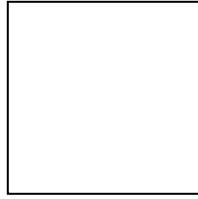
Dizayn 2



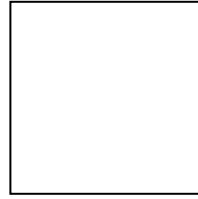
Dizayn 2'yi yansıt



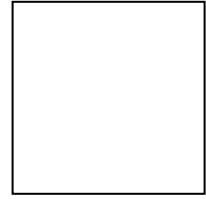
Dizayn 3



Dizayn 3'ü yansıt



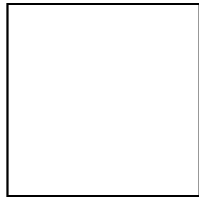
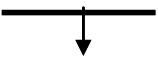
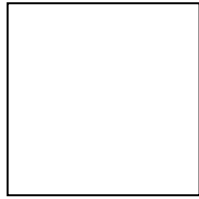
Dizayn 4



Dizayn 4'ü yansıt

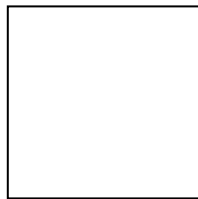
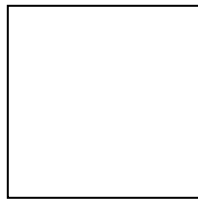
Yatay Hatlar'ını karşı tarafında dikey yansımalar.

Dizayn 1



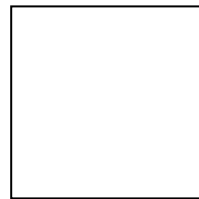
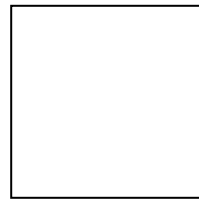
Dizayn 1'i yansıt

Dizayn 2



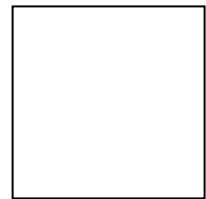
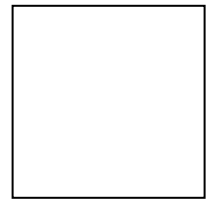
Dizayn 2'yi yansıt

Dizayn 3



Dizayn 3'ü yansıt

Dizayn 4



Dizayn 4'ü yansıt

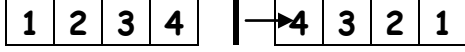
2. Tasarımları aktarınız.

Dört 4 x 4 kılavuzlarında renklendirmek için tasarımlarınızı kullanınız.

Klavuz 1: Orjinal

Klavuz 2: Klavuz 1'i düşey olarak karşı tarafa yansıtın.

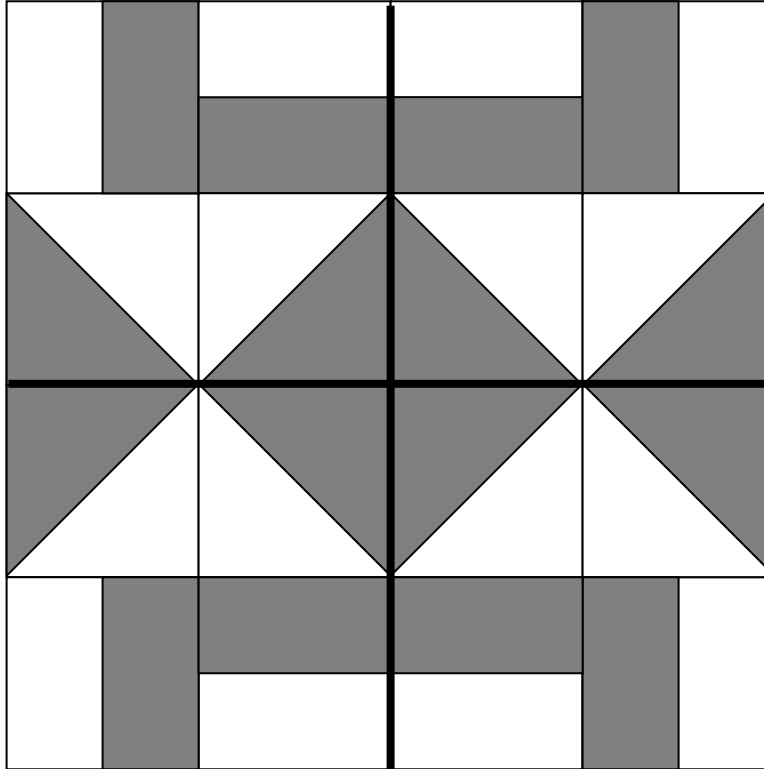
Desenler ve konumları yansıtınız.



Klavuz 3 & 4: Bir Yatay Çizgi boyunca Klavuz 1 ve 2 'yi karşı tarafa yansıt.

Yansıma Yerleşim örneği: Desenler ve konumları yansıtın.

Orjinal. Tablo.	→	Dikey. Yansıtın.
Yatay. Yansıtın.	↓	Yatay. Yansıtın.

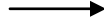


Bunlar karanlık satırlar, sadece gösteri amaçları içindir. Onlar, tamamlanan posterinde olmayacaklar.

Bir saat sanat posterini yapın: 4 saat saat yansıması.

1.Kısım

Desenler ve
konumları
yansıtınız.



2. Kısım

Desenler ve
konumları yansıtınız.

Desenler ve
konumları yansıtınız.

3. Kısım

4.Kısım

