# Effects of Cryptographic Activities on Understanding Modular Arithmetic

**Ahmet Şükrü Özdemir**[1]

**Enes Güler**[2]

**Nuh Aydın**[3]

**Abstract**

Students who are actively engaged in learning mathematics understand the subject better. In fact, one of the main problems of mathematics education today is to find ways to motivate and engage students in the classroom. In this quantitative study, cryptographic activities are used as an aid in teaching the topic of modular arithmetic in 8th grade and their effects on students' understanding are examined. The second author taught the topic of modular arithmetic to two groups of students in 8th grade. In the control group the teacher used the traditional method of teaching and in the experimental group he used cryptographic activities and puzzles. The analysis of the data shows that students who learned the subject through cryptographic activities were more successful than students taught traditionally. Attitudes and performances of students in the experimental group are found to be more positively affected by the experience.

**Key Words:** Activity-based learning, modular arithmetic, cryptographic activities

## 1. Introduction

People have always been interested in keeping some information secret from others. The modern subject that is concerned with privacy and confidentiality of communication is called cryptography. Sometimes cryptology is also used synonymously (Hankerson, 2000).

Caesar is one of the first persons known in history to have used secret, encrypted texts. When the messengers were ambushed and his orders were stolen, Caesar found a new way to give his orders. He scrambled the messages that conveyed his commands as if they were meaningless texts. In his method, he substituted every letter of the original text with the previous third letter in the alphabet. This is called encryption. He told his servants that when they receive a text which seems meaningless to them, just replace each letter of the text with the letter preceding it by three positions in the alphabet. When the servants did this, a secret message suddenly emerged like the touch of a magical stick. This is called decryption. For example, the message "HIDE" would be encrypted as "EFAB". This simple scheme is called the Caesar cipher.

[1] Assoc. Prof. Dr. Marmara University, Atatürk Faculty of Education, Elementary Education, *ahmet.ozdemir@marmara.edu.tr*
[2]Doğu Beyazıt Elementary School, *enesguler43@hotmail.com*
[3] Assoc. Prof. Dr. Kenyon College, Gambier OH, *aydinn@kenyon.edu*

The word cryptography comes from the fusion of two Greek words ‘Kryptos’ which means secret and 'logos' which means word. The word cipher comes from the Hebraic word 'saphar' which means giving numbers (Candiker, 2007).

The long-lasting interest in cryptography has become even stronger in the modern age of communication. It is well known how important and decisive cryptography was in the World War II. The breaking of the German encryption machine “Enigma” with “Clossus” developed by the allies shortened the war and saved many lives. One can argue that victory belonged to mathematicians.

With the wide spread of computers and online transactions, more and more applications require confidential communication in modern daily life. While advanced mathematics was not used in designing cryptographic systems in earlier times, it was later realized that many parts of advanced and abstract mathematics can be used in designing cryptographic systems. The most relevant parts of abstract mathematics used in modern systems are number theory and abstract algebra.

Cryptographic systems are divided into two main categories: symmetric-key cryptography and public-key cryptography. In the former method, the encryption and decryption keys are the same, or one is easily obtained from the other. Therefore, both keys must be kept private. Ceaser cipher is an example of this scheme. Public-key cryptography is a more modern notion introduced in 1976 (Diffie & Helman, 1976) where encryption key is made public and decryption key is private. A well-known and widely used example of public-key cryptography is the RSA system (Rivest, Shamir and Adleman, 1978). Modular arithmetic plays an essential role in the design and implementation of the RSA cryptosystem.

The figure below gives a general representation of private communication using cryptography.

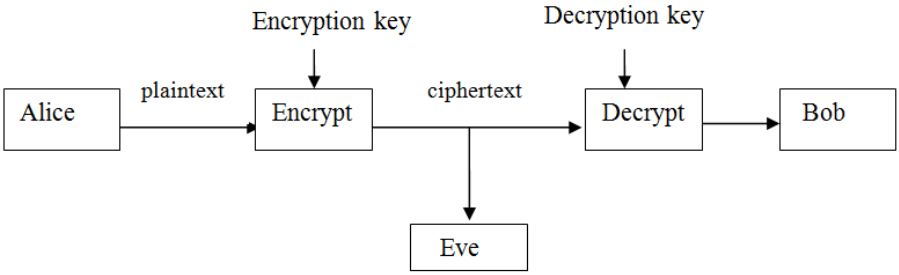


**Figure 1.** A general picture of confidential communication in the presence of adversaries

There are three generic characters in cryptography. Alice wants to send secret messages to Bob and Eve is the eavesdropper. Alice has a message to send to Bob. It is called plaintext. She encrypts the plaintext using the encryption key. The text obtained after encryption is called the ciphertext. Bob uses the decryption key to decrypt the message Alice sent. Only Bob has the decryption key so he is the only one who can decrypt Alice’s messages. Alice and Bob want to design their cryptographic system so that even if Eve intercepts some or all of the messages she cannot read (decrypt) them without getting the decryption key. If they use a public-key system, then Bob publishes his public key so that anyone who wishes to send a secret message to Bob can do so using that key. Intuitively,

encryption can be likened to putting something important into a box and locking it. Decryption is unlocking the box. In public key systems, anyone can lock a box but only the owner of the private key can unlock it.

One of the most exciting applications of mathematics to real life is cryptography and cryptanalysis. Humankind has been interested in cryptography since ancient times. This interest will continue as long as people communicate with each other with information they want to keep secret from unauthorized parties. In fact, with widespread use of computers, electronic devices and online transactions, cryptographic applications are getting even more important and finding more common applications. Many of the cryptosystems are based on number theoretical problems, and modular arithmetic is one of the most fundamental tools in those applications.

Caesar's cipher was a simple substitution cipher. Over time, more and more sophisticated mathematical concepts are used in designing cryptographic systems. During the 2nd World War "non-computer based cryptography" reached the peak point. Alan Turing, who is considered to be the founder of computer science and artificial intelligence, devised a number of techniques to break German ciphers during the 2nd World War that Germans regarded as "undecryptable".

In 1938, a year before the 2nd World War started, Turing was invited to Bletchley Park to join a secret duty. His mission was to decrypt the Nazi military cryptoes. As a result, Turing and his colleagues produced a machine named "Clossus". This instrument shortened the war for two years and saved lots of lives. Glory was of mathematicians. English army managed to turn the war into their favor before the Germans even conceived what was going on. This is an example that shows that a cryptographic application can be a matter of life and dead.

In our technologically developing world the importance of cryptography is increasing everyday thanks to dissemination of application areas. For instance, in mobile phones, internet communication, bank-cards, and televisions and in all parts of our life cryptography is being used even if we may not be aware of it.

### 1.1. Purpose of the Study

The purpose of this study is to investigate the effect of introducing cryptography as a motivating topic in teaching modular arithmetic to $8^{th}$ grade students.

## 2. Method

In this study "the model of pre-test and post-test control group" was applied as a research model.

Mathematics success test was applied to students as pre-test, post-test and retention test. Pre-test was applied before the study, post-test was applied at the end of the study and retention test was applied six weeks after the instruction was completed.

Attitude scale was applied to experiment and control groups at the beginning and at the end of the application. It was investigated whether the application had an effect on students' attitude and whether the experimental subjects' attitude had an effect towards success.

### 2.1. Experimental Group Subjects and Their Selection

There were two criteria for the selection of the subjects for the experimental group. One was a sufficient level of mastery of the operations and skills that are prerequisite for the topic, and the other one was an inadequate mastery of the topic to be taught. The experimental group subjects who fulfilled the selection criteria were selected among $8^{th}$ grade students in Ş. Ö. Gürhan Primary School located in Doğubeyazıt district in the city of Ağrı. To select the students, a 'Mathematics Achievement Test' (pre-test) was administered to the 136 $8^{th}$ grade students. Two classrooms were chosen so that control and experimental group students' prerequisite skills test average scores are close to each other (Experimental Group = 32,22 and Control Group = 32,91 ) and single way Anova was used to test the homogeneity of the groups. Both groups were taught "Mathematical Systems" unit in $8^{th}$ grade mathematics curriculum in 2006-2007 academic year by the same teacher who is the second author of this article. The control group was taught in a traditional way. For the experimental group cryptographic activities were used as a motivation to the topic. The details of the activities for the experimental group are given below, in the "research and application process" subsection.

### 2.2. Data Gathering Instruments

#### 2.2.1. Mathematics Achievement Test

A mathematics test that consists of 25 questions was used in this study. The test was administered as a pre-test before the start of the study. The same test was administered as post-test at the end of the teaching unit. The differences in the test results are used to measure the achievement difference before and after the teaching unit for each group.

To ensure the quality and validity of the test, it was written by a team of three teachers who had at least 10 years of teaching experience, and three faculty members who are experienced in writing standardized examinations of O.K.S.(High School Achievement Examinations), DYP (Scholarship Examinations and Military High School Examinations). The reliability of the test was measured by the Cronbach α Test and it is found to be ($\alpha$ = 0.72).

#### 2.2.2. Attitude Scale

We used an attitude measurement scale called "A Shortened Mathematics Attitude Scale for Primary Mathematics Teachers" which is a shortened version of Mathematics Attitude Scale developed by Erol (1989). In this attitude scale, there are 20 sentences that express positive and negative attitudes towards mathematics concerning three aspects: 'the importance of mathematics', 'perceived mathematics achievement level' and 'the interest in mathematics lessons'. It was a quinary likert scale type and alpha reliability coefficient was

found to be 0.74 ( Nazliçiçek and Ertekin, 2001 ). The alpha reliability coefficient for the attitude scale used in this study is found to be 0.71.

The attitude scale was given to the control and experimental groups before and after the teaching practice. The goal was to determine whether teaching practice had an effect on students' attitude, and also to determine whether the attitudes of students had an effect on their achievements.

The inquiry used in the research was produced in order to define the personal characteristics, socio-economic level of families and educational level of parents.

### 2.3. Application Process

During the application phase of the research, activity based teaching materials were developed for every topic. The topics for the teaching unit, called "Mathematics Systems", included the concept of modular arithmetic, addition and multiplication operations according to a given modulus and clock arithmetic. A number of resources we're used in developing teaching materials for Mathematics Systems unit. These include textbooks for primary schools, teaching mathematics books suggested for prospective teachers, and studies that investigate the effectiveness of this particular topic in teaching mathematics. Examples of resources used are Altun (2002), and Baki (2002). The following table shows the daily coverage of the topics.

**Table 1.** The schedule of the course activities

| Week | Lesson | Topic | Homework |
|---|---|---|---|
| 1 | 1 | Caesar Ciphers | |
| | 2 | Caesar Ciphers | Pages 4-5-6$^{th}$ in appendix-4. |
| | 3 | Clock Arithmetic | |
| | 4 | Clock Arithmetic | Pages 4-5-6$^{th}$ in appendix-5. |
| 2 | 1 | Frequency Analysis | Pages 2-3$^{rd}$ in appendix-6. |
| | 2 | Multiplier Tree | Pages 3-4-5$^{th}$ in appendix-7. |
| | 3 | Modular Arithmetic | |
| | 4 | Modular Arithmetic | Page 3 in appendix 8 |
| 3 | 1 | Prime Numbers | Page 3 in appendix 9 |
| | 2 | Rail Fence / Morse Code | Page 2 in appendices 10 and 11 |
| | 3 | Pigpen-Polypus Cipher / Poster | Appendix - 12 |
| | 4 | Poster / Review | Appendix - 13 |

**First Week**

In the first lesson of the first week, Caesar Ciphers were introduced. Students were told that the oldest known enciphering method is Caesar Cipher in which the emperor used the

method known as 'skipping characters' when he wanted to hide his orders from his enemies.

In the second lesson, Enciphering Disks were taught. Students were taught how a text can easily be encrypted and decrypted with this method.

In the third lesson, Clock arithmetic was introduced and the answers to the following questions were sought:

1. Are there any operations other than the four usual arithmetic operations?
2. Why is the clock divided into 12 parts?
3. Where else do we use the same addition that we use on a clock?
4. Why do we say 13:30 instead of one and half?
5. What are the functions of clock hands?
6. How could we determine the time if we did not have any clocks?
7. What did the ancient people use to determine the time?
8. Who invented the clock?
9. Why do we need number systems other than the decimal system?

In the fourth lesson, the activities on pages 1-3 related to clock arithmetic were carried out with the students in the class. Pages 4-6 were assigned as homework for the students.

**Second Week**

In the first lesson, some information about frequency analysis was given and how it enables us to decrypt Caesar ciphers was taught. Finally students began to fill in frequency tables by choosing one of the texts from appendix-6. The other pages in appendix -6 were given as homework to the students.

In the second lesson, multiplier trees and prime multiplier algorithms are explained. First and second pages in appendix-7 were done with the students in class. Pages 3-5 were given as homework.

In the third lesson, such activities as finding the exact day of students' birthday with the help of a calendar, finding days of a soldiers' guard duty, and finding the values integers in a given modulus were carried out.

In the fourth lesson, first and second pages in appendix-8 were done with the students in class. The third page was given as homework.

**Third Week**

In the first day, the definition of a prime number was introduced and some examples from daily life are given. Sieve of Eratosthenes, a method of finding prime numbers (appendix-9), is explained and students were asked to find all prime numbers up to 50 using this method.

In the second lesson, Rail Fence and Morse Code (appendix -10 and appendix-11) were explained.

In the third lesson Pigpen-Polypus cipher activity was done (appendix-12).

In the fourth lesson, guidance on how to prepare a clock poster was provided. Students designed their own clock posters.

### 2.4. Data Analysis

In the achievement test, 1 point was given for every correct answer, and pre-test and post-test were evaluated out of 100 points.

Attitude scale was a quinary likert scale type and it was scaled from 1 (negative attitude) to 5 (positive attitude). The scale was evaluated over 100 points.

In the analysis of data, control and experimental group students' average scores of pre-tests and post-tests, the average scores of their mathematical attitudes, and their percentages and frequency distributions were examined. Kolmogorov-Simirnov Test was used in order to examine whether the data showed normal distribution. This test was chosen to determine whether a parametric test or a non-parametric test should be employed to analyze the data.

The arithmetic means of the data were compared in order to determine the homogeneity of the control and experimental groups. Moreover, the homogeneity of the data was tested by using one way ANOVA test.

The data gathered from the control and the experimental group students' answers on Personal Information Survey questions is presented as percentages, and frequency distributions. Further, the data gathered from the other tests is given in tables and they are interpreted.

Since the data showed normal distribution for a statistics about unrelated data's differentiation according to a factor, for the analysis of two-digit samples an independent t-test was used. For samples that had more than two digits one-way ANOVA was used. For the statistics about related samples' differentiation, Paired Samples t-test was used.

## 3. Findings

From the results of the Kolmogorov- Smirnov test, it can be concluded that the distribution of the experimental group's pre-test and post-test data is normal (pre-test: $p=0,754 > 0,05=\alpha$ and p post-test: $p=0,851 > \alpha = 0, 05$). By the same test, the distribution of control

group's pre-test and post-test data is normal as well (pre-test: p=0,717>0,05=α and post-test: p=0,766 > α = 0, 05).

According to t-test results (Table 2), there are meaningful differences between pre-test and post-test scores of both the experimental group and the control group. For the direction of the differentiation, if we consider the averages ($\bar{x}$), we see a meaningful increase in the achievement of experimental group.

**Table 2.** The t-test data for experimental and control group students' pre-test and post- test scores.

| Groups | Tests | n | Average | SS | Sd | t | p |
|---|---|---|---|---|---|---|---|
| Control Group | Pre-Test | 36 | 32,916 | 10,027 | 35 | 0,172 | 0,865 |
| | Post-Test | 36 | 33,055 | 12,205 | | | |
| Experimental Group | Pre-Test | 36 | 32,222 | 10,45 | 35 | 9,357 | 0,000 |
| | Post-Test | 36 | 59,583 | 17,5 | | | |

According to t-test results (Table 3) for the control and the experimental group students' post-test scores, there is a meaningful difference between post-test scores of the two groups. For the direction of the differentiation, if we consider the averages, we see that the difference between post- test scores is in favor of the experimental group students.

**Table 3.** The t-test data for experimental and control group students' post-test scores.

| Groups | n | Average | SS | Sd | t | p |
|---|---|---|---|---|---|---|
| Experimental Group | 36 | 59,583 | 17,5 | 35 | 7,08 | 0,000 |
| Control Group | 36 | 33,056 | 12,205 | | | |

According to the Kolmogorov-Smirnov test results on pre-attitude and post-attitude data of students in each group, the distributions of both group's pre-attitude and post-attitude are normal, (experimental group: p pre-attitude: p=0,754> α=0,05 and p post-attitude : p= 0,850> α=0,05; control group: p pre-attitude: p=0,717> α=0,05 and p post-attitude : p= 0,989> α=0,05). Again, Kolmogorov-Smirnov was applied to determine whether a parametric test or a non-parametric test should be employed to analyze the data.

**Table 4.** The t-test results for experimental and control group students' pre-attitude and post-attitude scores.

| Tests | Groups | n | Average | SS | Sd | t | p |
|---|---|---|---|---|---|---|---|
| Pre-Test | Experimental | 36 | 47,962 | 11,986 | 35 | -1,560 | 0,128 |
| | Control | 36 | 53,89 | 14,712 | | | |
| Post-Test | Experimental | 36 | 60,971 | 11,465 | 35 | 3,284 | 0,002 |
| | Control | 36 | 51,68 | 12,371 | | | |

We can make the following conclusions from Table-4 which contains t-test results on the two groups: a) There is not a meaningful difference between the control and the experimental group students' attitudes towards mathematics before the teaching practice application [t= -1,56 ve p=0,128 >α= 0,050], b) There is a meaningful difference between the control and the experimental group students' attitudes towards mathematics after the teaching practice application [t = 3,284 ve p=0,002 < α= 0,050]. Since the value of the meaningfulness is smaller than 0,05 which means statistical meaningfulness, it is concluded that there is a meaningful difference between the control and the experimental groups' attitudes towards mathematics (considering the threshold level of 0,05). When we look at the averages for this difference, it is seen that this difference is in the favor of the experimental group. This shows that teaching with ciphering activities changed the attitudes of the students in this study towards mathematics in a positive way.

## 4. Discussion, Conclusion and Suggestions

In this study, we introduced cryptography to secondary school students as a motivating subject to teach some of the related mathematical concepts and operations. In the first step, we introduced the Caesar encryption method in which we move characters to the right or left by some fixed amount. Later, we taught clock and modular arithmetic in moduli 12 and 16. These activities can easily be adapted to various teaching and learning techniques suitable for students at different levels (Myerscough et al,1996). For example, linear transformations can be used at higher grades to discuss more complicated encryption systems as well as more advanced number theory and abstract algebra at university level (Aydin, 2009).

Myerscough et al (1996) conducted a study where they tried to enable students to decipher encrypted messages by arousing their curiosity. When students have difficulties to decipher, they guide them by giving some clues. The authors tell us that in some classrooms students had difficulties to decipher, some students did not try to break the codes before getting a clue from the teacher but most of them were very successful and decisive to break the codes.

Some might think that introducing encryption and decryption in mathematics classroom could make mathematics even more difficult. However, this can make students more motivated towards mathematics, showing them that mathematics is used in real life. Moreover, some students may become interested in the topic because they enjoy solving puzzles.

According to the results of this study, in teaching mathematics to $8^{th}$ grade students, there is a statistically meaningful difference in students' attitudes towards mathematics between the group of students instructed with ciphering activities and the group of students instructed in a traditional way in favor of the former. We also observed that ciphering activities made it easier to remember the material learned before the $8^{th}$ grade. The attitudes

of the students in this study towards mathematics changed in a positive way as a result of teaching with ciphering activities in 8th grade.

This study shows cryptographic activities can be used to motivate and teach a certain topic in 8th grade mathematics more effectively. It is possible to use similar activities in different grades and at different levels. For example, more advanced and realistic encryption schemes can be implemented on computers, as opposed to doing everything by hand, in a computer programming course or in a mathematics course that uses computers, hence connecting mathematics to computers and reinforcing mathematical topics learned in earlier grades. It is likely that some students who would otherwise not be interested in mathematics might become interested due to such activities.

## References


Altun, M. (2002). *İlköğretim ikinci kademede matematik öğretimi* İstanbul: Delta Yayınları

Aydin N. (2009) Enhancing Undergraduate Curriculum via Coding Theory and Cryptography. *PRIMUS* (19) Issue 3, 296-309.

Baki, A. (2002), *Öğrenenler ve öğretenler için bilgisayar destekli matematik*, İstanbul: Ceren Yayın.

Coşkun, H. (2006). Şifreleme ve Asal Sayılar, *Matematik Dünyası*, Kış 2006. 65-67.

Codes & Ciphers Mathematics Resources for Teachers [Online] http://www.bletchleypark.org.uk

Churchhouse, R. (2002). *Codes and Ciphers; Julius Caesar, the Enigma, and the Internet*. Cambridge: Cambridge University.

Diffie, W & Hellman M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*. IT-22 (6): 644-654.

Eskici, A. (2004). Polybius Şifresi, *Matematik Dünyası*, Yaz, 2004. 72-73.

Hankerson, D. R. et al (2000) Coding Theory and Cryptography: The Essentials: Marcel Dekker, New York, Basel.

Kallis, A.S. Codes & Ciphers. http://www.otr.com/ciphers.shtml.

Myerscough, D. (1996). Cryptography: Cracking codes, *Mathematics Teacher*, 743-750

Oral, H. (2003). Phi tarihinden günümüze: Ebced ve şifreleme, *Matematik Dünyası* Yaz, 2003, 54-57.

Oral, H. (2003). Phi tarihinden günümüze : İlk Türkçe şifreleme kitaplari, *Matematik Dünyası*, Kış, 2003, 59-60.

Özdemir, A. Ş. (2004) *Sayılar teorisi çözümlü problem kitabı*. Salan Yayınevi, İstanbul.

Özdemir, A.Ş, and Güler, E. (2007). Using "e" in Cryptology, *ICMOSPS'07*. Durban, South Africa.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the. ACM* 21(2): 120-126

Singh S. (1999). *Code Book; The Evolution of Secrecy from Mary Queen of Scots to Quantum*, New York: Doubleday