[UCI]I804:24011-200000256919

2012년 2월

교육학석사(수학교육)학위논문

중등 수학교육과정에서 유도 가능한 암호이론에 대한 연구

조선대학교 교육대학원

수학교육전공

오 인 성

중등 수학교육과정에서 유도 가능한 암호이론에 대한 연구

Research of cryptology derived by mathematical curriculum in secondary school

2012년 2월

조선대학교 교육대학원

수학교육전공

오 인 성

중등 수학교육과정에서 유도 가능한 암호이론에 대한 연구

지도교수 박 순 철

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2011년 10월

조선대학교 교육대학원

수학교육전공

오 인 성

오인성의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 안 영 준 인

심 사 위 원 조선대학교 교수 한 승 국 인

심 사 위 원 조선대학교 교수 박 순 철 인

2011년 12월

조선대학교 교육대학원

목　　차

Abstract

Ⅰ. 서 론 1

1. 연구의 필요성 및 목적 1
2. 연구 문제 2
3. 용어의 정의 2
4. 연구의 제한점 3

Ⅱ. 이론적 배경 4

1. 암호의 역사적 배경 4
2. 암호 체계의 소개 7
3. 암호이론의 요약 13

Ⅲ. 암호이론의 기초가 되는 수학이론 18

1. 정수의 기본 성질 18
2. 약수와 배수 19
3. 약수의 개수와 약수의 합 20
4. 최대공약수와 최소공배수 21
5. 소　수 24
6. 소인수분해 26
7. 특수한 유형의 소수 27
8. 소수 판정 27
9. 합 동 28
10. Fermat 정리와 Euler 정리 29

Ⅳ. 중 ·고등학교에서 활용할 수 있는 암호체계 31
1. Ceasar 암호 32
2. Affine 암호 32
3. Vigenère 암호 33
4. Hill 암호 34

Ⅴ. 설문지 결과 비교분석 39
1. 암호학 수업 전 39
2. 암호학 수업 후 40
3. 설문지 결과 분석 41

Ⅵ. 결론 및 제언 44
참고문헌 45
부록1 교수-학습지도안 46
부록2. 설 문 지 50

표목차

<표 Ⅱ-1 전이암호 표의 예> ····· 7
<표 Ⅱ-2 각 문자 빈도> ····· 8
<표 Ⅱ-3 빈도에 따른 문자 분류표> ····· 9
<표 Ⅱ-4 동음이의 암호표의 예> ····· 10
<표 Ⅱ-5 플레이페어 암호의 키> ····· 12
<표 Ⅳ-1 암호체계와 관련된 중등수학 내용> ····· 31
<표 Ⅳ-2 Affine 암호화> ····· 33
<표 Ⅳ-3 비게네르 암호> ····· 34
<표 Ⅳ-4 Hill 암호(영문)> ····· 36
<표 Ⅳ-5 Hill 암호(한글)> ····· 37
<표 Ⅴ-1 암호학 수업 전 설문지 결과> ····· 40
<표 Ⅴ-2 암호학 수업 후 설문지 결과> ····· 41

ABSTRACT

Research of cryptology derived by mathematical curriculum in secondary school

In Seong Oh
Advisor : Prof. Park, Soon Cheol
Major in Mathematics Education
Graduate School of Education, Chosun University

This research aims to understand the mathematical theory which is related to the cryptology and the cryptosystem which can be applied to the secondary school curriculum. Secondly, this research aims to figure out the development of learners' mathematical interest after learning the cryptology. Therefore, the following subjects for inquiry are selected for the purpose of this study.

1. What is the mathematical theory which is related to the cryptology and what is the cryptosystem which can be applied in the secondary school curriculum?
2. How is the development of learners' mathematical interest after learning the cryptology which is applied to the secondary school curriculum?

To solve the problems above, this study refers to the literature of mathematical theories which is related to the cryptology, and summarizes the cryptosystem which can be applied to the secondary school curriculum. Based on these research materials, this study investigates learners's mathematical interest after learning Ceasar cryptosystem in the optional course by conduction a survey.

The research has shown the results as follows.

First, Ceasar and Affine cryptosystem can be applied to the sections of numbers and operations, the character and expression, and the functions in middle school. Hill's cryptosystem can be applied to the matrix in "Math Ⅰ" and to the transformation of matrix in 'Geometry and Vectors'. ADFGVX

cryptosystem encrypts plain texts through the several processes using concepts of functions in middle school and matrix in "Math Ⅰ". And for decoding process, students should be taught reverse thinking process because they can not use the inverse function in the middle school curriculum.

Second, students who didn't learn the cryptology tend to regard mathematics a theoretical subject. After the cryptology class, however, students understand that the cryptology is related to mathematics closely and mathematics is also available. Therefore, the cryptology classes is able to induce the interest of mathematics and can be a practical math education in the modern society.

Ⅰ. 서 론

1. 연구의 필요성 및 목적

현재의 우리는 개인용 컴퓨터와 인터넷의 발전과 사용의 증가에 따라 정보의 양이 증가하였고, 정보 교류에 있어서는 거리의 개념이 거의 없어진 정보화 사회에 살고 있다. 모든 사회 활동과 인간 생활에서의 정보 자체가 주요한 원천이 되었다. 그러나 정보를 관리하고 운영하는 과정에서 오는 취약성 때문에 정보를 관리하는 시스템과 운영체제에서는 정보를 훼손하거나 통신망 등의 불법적인 침입, 바이러스 등으로 인해 정보의 보호가 절실하게 거론이 되고 있다. 정보화 사회에서는 자신이 원하는 정보를 쉽게 구할 수 있지만 자신도 모르는 사이에 침해받을 수 있으며 보호되지 못하는 정보로 인해 막대한 물질적·정신적 피해를 볼 수도 있다. 급격한 IT환경 변화 속에서 사이버 위협에 대한 우려도 급증하고 있다. 특히 사업자 관리소홀로 인한 쇼핑몰, 통신사, 정유사 등에서의 대형 고객정보 유출사고가 잇따라 발생하여, 개인정보/프라이버시 침해 사고를 경험하는 일이 다반사이다. 뿐만 아니라, 기업의 정보시스템 및 정보보호 자원의 안전성에 대한 자체적인 평가도 하락한 것으로 나타나, 사회 전반에 보안 위협에 대한 우려가 확산되고 있다. 이로 인해 정보화 사회에서 정보를 보호하는 것이 정보의 공개만큼이나 중요한 일이 되었다. 이러한 정보 보호기술 중의 하나가 암호화 기법이다. 이는 제 3자가 정보를 획득하더라도 그 의미를 분석할 수 없도록 하는 것으로서 수학적 지식에 기반을 두고 있다.

일반적으로, 수학교육 관련 전문가들은 수학교육의 목적으로 정신도야성, 실용성, 문화적 가치 및 심미성을 강조하고, 이러한 목적들이 학생들에게 실감 있게 느껴질 수 있도록 학교 수학교육의 목표 및 내용, 방법 등을 정선하는 일이 중요하다고 지적하고 있다.

우리는 흔히 수학의 실용성과 관련하여 “수학이 다른 과학의 기초가 되고 문명이 발달하는 초석이 되기 때문에 공부해야 한다”는 관점을 표명하기도 하는데, 이는 보편적인 설득력을 지니지 못한다(황혜정외 5인, 2008). 지금까지의 수학교육은 수학의 실용적 측면과의 연관성을 무시하고 교과서 중심으로 이루어졌다. 이로 인해 수학교사는 ‘수학의 실용성을 알고 있으면서도 설명할 수 없다’는 딜레마에 빠지게 되었다. 수학의 실용성은 컴퓨터와 첨단과학기술의 발달로 수학 교과를 가르치는 첫 번째 이유가 되었다. 수학은 컴퓨터의 출현으로 인해 가속화되고 있는 현대사회의 발달 속에서 그 중요성은 더욱 더 증가되고 있다.

이에 7차 교육과정에서 방과 후 학교, 특기적성교육이나 창의적 재량활동, 교과 심화학습 등을 통해서 교과서 이외의 내용이 다양하게 도입되고 있는 추세이므로

이런 시간을 통해 암호학을 활용해 보는 것도 학습동기와 흥미를 유발하고 학습결과를 실생활에 응용할 수 있다는 점에서 의미 있는 일이다. 실제로 암호학을 주제로 수학수업을 실시하여 분석한 결과 암호학과 수학이 밀접한 관계에 있고 암호학 내용에 흥미가 있으며 수학도 실용적인 과목으로 인식하는 것으로 나타났다. 그리고, 수학과목에 대한 흥미와 관심도 향상된 것으로 나타났다(이선영, 2002).

본 논문에서는 현재 주목받고 있는 암호론과 관련된 수학 이론은 무엇이 있으며, 2007년 고시한 중 · 고등학교 교육과정에서 도입할 수 있는 암호체계는 무엇이 있는지를 알아보고자 한다. 그리고 수학이 논리적 사고를 바탕으로 하는 학문의 기본수단 정도로만 인식하는 고정관념을 깨고 우리 생활 가까이에서 활용되고 있으며, 특히 21세기의 과학과 정보사회를 이끌어 내어 실생활에 많은 영향을 미치고 있음을 강조하여 수학에 대한 흥미를 유발하고자 한다.

2. 연구 문제

본 연구는 암호학과 관련된 수학 이론은 무엇이며, 중·고등학교 교육과정에서 도입할 수 있는 암호체계는 무엇이 있는지 알아보고자 한다. 그리고 중학교 재량활동시간을 이용하여 학생들의 수학에 대한 흥미도가 어떻게 변하였는지 알아보고자 한다.

본 연구의 목적을 위하여 다음과 같은 연구문제를 선정하였다.

1. 암호학과 관련된 수학 이론은 무엇이며 중 · 고등학교 교육과정에 도입할 수 있는 암호체계는 어떠한 것이 있는가?

2. 암호학을 도입한 수업 결과, 학생들의 수학에 대한 흥미도는 어떠한 변화가 있는가?

3. 용어의 정의

암호학에서 주로 사용하는 용어는 다음과 같다.

1) 송신자 (sender)
   - 정보를 안전하게 보내기를 원하는 사람이나 주체
2) 수신자 (receiver)
   - 정보를 받는 사람이나 주체
3) 공격자 (attacker)
   - 암호 방식의 정당한 참여자가 아닌 자로 암호문으로부터 평문을 해독하려는 제 3자, 특히, 송 · 수신자 사이의 암호 통신에 직접 관여하지 않고 네트워크

상의 정보를 관찰함으로써 공격을 수행하는 공격자를 도청자(eavesdropper)라 한다.

4) 평문(Plain text, Clean text)
   - 일반일들이 알아볼 수 있는 보통의 문장
5) 암호문 (Cipher text)
   - 평문을 암호화 알고리즘과 암호키를 이용하여 변환시킨 문서
6) 암호화 (Encryption, Encoding)
   - 평문을 암호키를 이용하여 암호문으로 변환시키는 과정
7) 복호화(Decryption, Decoding)
   - 암호문을 원래의 평문으로 변환시키는 과정
8) 키 (Key)
   - 평문을 암호문으로 암호화 하는데 사용하고, 암호문을 복호화하여 원래의 평문을 얻을 수 있는 열쇠
9) 암호 해독 (Cryptanalysis)
   - 암호문에 대한 정보를 전혀 알지도 못하고 키도 없이 암호문을 평문으로 복원하려는 것
10) 암호 알고리즘(cryptographic algorithm)
   - 암호화와 복호화에 사용되는 수학적인 함수이며, 암호화에 사용되는 암호화 알고리즘과 복호화에 사용되는 복호화 알고리즘이 있다.
11) 인증 (Authentication)
   - 수신자가 받은 정보가 원래의 송신자로부터 온 것임을 확인하는 것으로서 도청자를 송신자나 수신자로부터 구별하기 위한 과정(한국정보보호학회, 2002)

4. 연구의 제한점

본 연구는 다음과 같은 제한점이 있다.

1. 본 연구의 대상은 연구자가 근무하고 있는 중학교에 다니는 중학생들로 한정되어있기 때문에 연구 결과를 일반화 하는데 한계가 있고, 연구 결과를 해석하는데 제한점이 있다.
2. 본 연구는 Ceasar 암호만을 도입하여 수업을 진행하였으므로, 연구 결과를 다른 암호체계로 일반화하는 데에 제한점이 있다.

Ⅱ. 이론적 배경

1. 암호의 역사적 배경

암호(暗號: cryptography, cipher)란 보통의 기호나 문자와는 달리 그 의미를 바로 알 수 없는 기호나 문자열을 말한다. 암호란 그리스어로 숨겨진 비밀이라는 뜻의 crypt와 글자라는 의미의 graph가 합쳐진 것으로, 암호라는 단어가 생긴 것에서 알 수 있듯이 암호는 비밀을 유지하기 위해 발명되었다. 그리고 cipher라는 단어는 원래 아라비아어로 숫자 0을 의미한다. 이것이 암호의 의미로 사용된 것은 아라비아 숫자가 유럽으로 전해진 역사와 관계가 있다. 0은 무언가를 숨기고 있는 비밀의 부호로 생각해 암호의 어원으로 자리 잡았다.(장은성, 1999)

암호는 자신과 밀접한 관계가 없는 사람들은 알아듣지 못하도록 하기 위해 사용되는 모든 언어라 할 수 있다. 의사소통이 쉽게 이루어지고 정보를 모두가 공유하게 됨으로써 아무런 차별이 생기지 않게 되어 우리와 남을 차별하기 위해 암호가 등장한다. 이처럼 암호의 목적은 자신들만이 알고 있는 정보를 보호하기 위하여 탄생된 것이다. 그런 욕구는 문명이 발달할수록 더욱 커져서 다양한 암호기법이 발달해 왔다.

1) 고대 암호

약 4000년 전 고대 이집트에서는 민중문자를 신성문자로 바꿔 썼으며, 2300년 경 페르시아의 볼모로 잡혀갔던 히스티아이오스왕은 노예의 머리에 문신을 새겨서 노예를 통해 비밀 통신을 하였다.

우리가 알고 있는 가장 오래된 암호 방식은 기원전 440년경 고대 희랍인들이 사용한 scytale 암호라고 불리는 정치 암호이다. 이 암호의 방식은 전달하려는 평문을 재배열하는 방식을 곤봉에 종이(papyrus)를 감아 평문을 횡으로 쓴 다음 종이를 풀면 평문의 각 문자는 재배치되어 평문의 내용을 인식할 수 없게 하는 것이다. 이 때 암호문 수신자는 송신자가 사용한 곤봉과 직경이 같은 곤봉에 암호문이 적혀 있는 종이를 감고 횡으로 읽으면 평문을 얻을 수 있는 것이다.

최초의 환자(換字) 암호는 로마 시대의 Julius Caesar가 사용한 시저(caesar) 암호이다. 이 암호 방식은 평문의 각 문자를 우측으로 3문자씩 이동시켜 그 위치에 대응하는 다른 문자로 치환함으로써 평문을 암호문으로 변환하는 암호 방식이다. 즉,

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
↓ ↓
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

으로 평문을 암호문으로 치환하는 방식이다. 이 암호문에서 평문으로 복호화하는 방법은 암호화의 역처리를 하는데, 암호문 문자를 좌측으로 3문자씩 이동시키는 것이다.

고전암호계에서 암호화하는 방법은 크게 세 가지 방법으로 분류할 수 있다.

(1) 암호화하는 문자들의 개수의 적당한 약수를 택하여 문자를 나열한 뒤에 행과 열을 바꾸어 쓰고 순서대로 문자들을 나열하는 방법인 **전치암호(transpose cipher)**이다.

(2) 문자들의 개수의 적당한 약수를 택하여 문자들을 나열한 뒤에 문자들의 순서를 적당히 바꾸어 나열하는 **치환암호(permutation cipher)**이다.

(3) 문자들의 집합의 각 원소를 다른 문자로 변화하는 **대입암호(substitution cipher)**이다.

고전 암호는 암호화과정과 해독과정을 복잡하게 하기 위하여 이들 세 가지 암호화 방법을 적절하게 혼합한 곱암호(product cipher)를 설계하면서 발전하여 왔고 현대암호 또한 이러한 원리로부터 설계된다.

2) 중세 암호

중세에는 특별히 암호 기술의 진전이 없이 고대의 암호 기술을 그대로 사용하였다. 이 시대의 특징은 이제까지의 군사작전의 짧은 암호문이 아니라 정치적인 목적을 가진 기다란 암호문이 쓰이기 시작했다는 것이다. 또한 14, 15세기 외교와 상업이 활발해지면서 암호에 대한 수요가 생기기 시작했으며, 가장 먼저 상업 활동이 시작된 이탈리아에서 최초의 완전 암호인 베네치아 암호가 고안되었다. 15세기 중엽 이탈리아의 건축가 레온 바티스타 알베르티(Leon Battista Alberti, 1404~1472)는 원판암호를 만들었다. 이 암호 방식은 큰 원판은 고정되어 있고 작은 원판은 자유롭게 회전할 수 있으며, 작은 원판의 알파벳이 원자이고 큰 원판에 무작위로 나열된 알파벳은 암자로 암호화하고자 하는 문자를 작은 원판에서 찾아 큰 원판에 대응하는 문자로 바꾸기만 하면 된다.

3) 근대 암호

17세기 근대 수학의 발전과 더불어 고급 암호가 발전하기 시작하였지만, 본격적인 근대수학을 도입한 과학적인 근대암호는 20세기에 들어와서 시작되었다고 할 수 있다. Vigenere가 고안한 암호방식, Playfair가 만든 2문자 조합 암호, Fleissner의 그릴(grill)암호 이후, 두 차례의 세계 대전을 거치면서 암호 방식 설계와 해독에 관한 연구가 아주 활발히 추진되었다.

근대 암호의 기초가 된 것은 1920년 Freidman이 발표한 "일차 반복률과 암호 응용", C.E.Shannon이 발표한 "비밀 시스템의 통신이론"이다. Friedman은 제2차 세계대전 중 독일 군이 사용했던 ENIGMA 암호와 일본군이 사용하던 무라사끼 암호(97식 암호)를 해독한 사람으로 유명하지만, 유전자 구조 해석의 길을 개척한 선각자로도 잘 알려져 있다. Shannon은 확률론을 기초로 한 정보 이론을 창시한 사람으로 원리적으로 해독 불가능한 암호 방식을 제안하고 안전성을 평균 정보량을 이용하여 수리적으로 증명하였다.

우리가 알고 있는 근대 암호학의 연구를 촉진시킨 것은 두 차례의 세계대전이 계기가 되었다. 하지만, 기술적으로는 전신 기술의 발달과 세계대전 후의 전자계산기의 출현으로 암호화, 복호화 및 암호 해독의 속도가 향상됨으로써 암호 실용화 연구가 활발하게 되었다.

4) 현대 암호

현대 암호라는 것은 1970년대 후반 Stanford 대학과 MIT대학에서 시작되었다.

종래의 관용 암호 방식(대칭키 암호 방식)은 암호화키와 복호화키로 동일한 키(비밀키)를 사용하기 때문에 송신자와 수신자가 비밀 통신을 하기 전에 키를 분배하여 보관하고 있어야 한다. 반면에 공개키 암호 방식은 암호화키와 복호화키를 분리하여 암호화키는 공개하고 복호화키는 비밀리에 보관하도록 되어 있다. 공개키 암호 방식은 관용 암호 방식과는 달리 암호화키를 사전에 전송할 필요가 없어 불특정 다수 비밀 통신 가입자 사이에 암호 통신망 구축이 용이하다. 대표적인 공개키 암호 방식은 RAS 암호 방식을 비롯해 수학적 문제에 기반을 둔 여러 방식들이 개발되고 소개되었다.

1977년 미국 상무성 표준국은 전자계산기 데이터 보호를 위한 암호 알고리즘을 공개 모집하였고 IBM사가 제안한 과용 암호 방식을 데이터 암호 규격(DES: Data Encryption Standard)으로 채택하여 상업용으로 사용하기 시작했다. 이 DES의 출현으로 컴퓨터 통신망을 이용한 문서 전송, 전자상거래등이 활성화되면서 안전성 확보를 위한 방안으로 암호 이용이 불가피하게 되었다고 할 수 있다(김희원, 2005).

고대, 근대 암호 방식은 키뿐만 아니라, 암호 알고리즘을 비밀로 하였으나, 현대 암호 방식은 공개키 암호방식의 암호화키와 암호 알고리즘을 공개하고 있다. 공개적으로 암호방식의 안전성을 검토하게 하여 안전성을 확인하도록 하고 있는 것이다. 이렇게 함으로써 암호학은 수리 과학으로 발전하기 시작하였다.

2. 암호 체계의 소개

1) 전이암호

전이암호(transposition cipher)란 평문의 문자를 재배열하는 알고리즘이다. 평문을 n개의 문자단위로 나누고, n개의 문자에 재배치를 생각한다.

$Z_d = \{1, 2, 3, \cdots, d\}$라 하고 $f : Z_d \rightarrow Z_n$은 Z_n위에서의 일대일 대응함수라 할 때 전이암호를 위한 키는 $K = (d, f)$이다.

즉 평문

$$M = m_1 \cdots m_d m_{d+1} \cdots m_{2d} \cdots$$

을 암호화하면 암호문은

$$C = m_{f(1)} \cdots m_{f(d)} m_{f(1)} \cdots m_{f(d)} \cdots$$

가 된다.

[보기 1] 키 $K = (d, f)$가 $d = 4,\ f(1) = 2,\ f(2) = 1,\ f(3) = 4,\ f(4) = 3$을 이용하여 평문 UNIVERSITY를 암호화해 보자.

<표 Ⅱ-1 전이암호 표의 예>

	1	2	3	4	5	6	7	8	9	10
평 문	U	N	I	V	E	R	S	I	T	Y
암호문	N	U	V	I	R	E	I	S	Y	T

참고로 전이암호에서는 평문의 각 문자 빈도가 암호문에서도 같아서 전이암호를 사용한 사실을 암호해독자가 쉽게 알아 낼 수 있고, <표Ⅱ-B-2>에 의해서 복호화가 가능하다는 것을 알 수 있다.

<표 Ⅱ-2 각 문자 빈도>

문자	P	문자	P	문자	P
A	0.0856	J	0.0013	S	0.0607
B	0.0139	K	0.0042	T	0.0249
C	0.0279	L	0.0339	U	0.0092
D	0.0378	M	0.0249	V	0.0149
E	0.1304	N	0.0707	W	0.0017
F	0.0289	O	0.0797	X	0.0199
G	0.0199	P	0.0199	Y	0.0008
H	0.0528	Q	0.0012	Z	
I	0.0627	R	0.0677		

2) 대치암호

대치암호(substitution cipher)의 종류에는 단순 대치암호, 동음이의 대치암호, 다표식 대치암호, 쌍자 대치암호와 같이 네 종류로 나눌 수 있다.

(1) 단순 대치암호(simple substitution cipher)

단수 대치암호는 평문과 암호문의 각 문자가 일대일로 대응하는 암호시스템이다. 평문의 각 문자를 대응되는 문자로 바꾸는 것으로 만일 A를 26개의 영문 알파벳의 집합이라고 하고 A 위에서의 일대일 대응함수를 $f: A \rightarrow A$라 하면 f는 단순 대치암호의 키다 된다. 이 때 평문을

$$M = m_1 m_2 \cdots$$

이라 할 때, 키 f에 의하여 암호화된 암호문 C는 다음과 같다.

$$C = f(m_1) f(m_2) \cdots$$

[보기2] 일대일 대응 함수 f가 다음과 같이 주어졌다고 하자.

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

그러면 평문 M = I LOVE YOU에 해당하는 암호문 C는 다음과 같다.

C = A DGZP VGY

시저가 사용했던 시저 암호는 영문자 알파벳에 순서를 두어 키만큼 해당 문자의 위치를 옮기는 암호로서 다음과 같은 수식으로 표현된다.

$$f(a) \equiv a + k \pmod{26}$$

여기서 a는 영어 문자에 대응되는 정수, 즉
$A=0, B=1, C=2, \cdots X=23, Y=24, Z=25$이고, k는 키에 해당하는 정수이다.

[보기 3] 시저 암호에서 $k=4$인 경우, 평문

M = I LOVE YOU

은 다음과 같이 암호화 된다.

C = M PSZY CSY

수학적인 용어로 표현하면 아핀변환(affine transformation)에 의한 암호화는 다음과 같은 수식으로 표현된다.

$$f(a) \equiv ak_1 + k_0 \pmod{26}$$

위와 같은 방법으로 평문을 암호화하더라도 조금만 관심을 갖고 보면 평문에서 사용한 단문자 빈도를 이용하여 암호문만을 가지고 키를 알아내는 방법인 암호문 공격방식(ciphertext-only attack)에 의하여 쉽게 해독할 수 있다. 평문에서 나타난 각 문자의 빈도는 대치된 암호문의 문자빈도와 일치하기 때문에 주어진 암호문에서 사용한 각 문자의 빈도와 이미 조사된 평문의 각 문자의 빈도를 비교하면 암호문을 해독할 수 있다.

<표 Ⅱ-3 빈도에 따른 문자 분류표>

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

[보기 4] 시저 암호를 이용한 암호문에서 P라는 영문자 빈도가 두 번째로 높으면 암호 해독자는 P를 T에 대응하는 암호문이라고 판단할 수 있다. 그러나 각 문자의 빈도는 평문에 따라 약간의 차이가 있다.

(2) 동음이의 대치암호(homophonic substitution cipher)

동음이의 대치암호란 평문의 각 문자에 여러 개의 문자가 대응하는 암호로써 평문 각 문자의 빈도 분포가 대치된 암호문의 빈도 분포와 동일하게 되는 단순대치 암호의 단점을 보완한 것이다. 즉 하나의 평문에 대응하는 암호문이 여러 개가 나올 수 있다.

[보기 5] 26개의 영문자를 0부터 99까지의 정수로 다음과 같이 배정하여 암호화

하는 경우를 생각해 보자. A~Z까지의 문자 중 필요한 일부분의 대치표이다. 이때 영문자 각각에 할당된 정수 개수는 각 문자의 빈도에 비례하며 모든 정수는 하나의 영문자에만 할당되도록 한다.

<표 Ⅱ-4 동음이의 암호표의 예>

영문자	할당된 정수								
A	19	34	17	56	67	60	41	83	
B	07	22							
C	53	65	88	09					
D	43	21	15	18	04				
E	01	13	23	35	42	66	80	54	76
F	27	02	44	92					
G	36	82	05						
H	19	71	11	08	99	48			
I	00	14	52	65	49	57	81		
J	85								
⋮									

위의 대치암호표에 의하면 평문

M : FIFACHIEF

을 다음과 같이 암호화할 수 있다.

C : 025227348819573544

위와 같이 암호문에서는 평문의 각 문자에 대한 빈도가 같지 않으며, 암호문의 각 빈도차는 줄어든다. 그러나 diagram, trigram 등과 같은 통계적 특성이 여전히 암호문에서도 나타나게 되어 해독이 가능하다(통계학적 전문지식이 필요함).

(3) 다표식 대치암호

다표식 대치암호는 평문과 암호문 사이의 여러 개의 대응함수가 있는 암호이다. 단순대치 암호는 평문 각 문자가 다른 문자로 하나씩 대치되는 암호이기 때문에 평문의 단문자 분포가 대응되는 문자의 빈도와 같다. 동음이의 대치암호는 평문의 diagram, trigram 등과 같은 통계적 특성을 배제할 수 없다. 그래서 단순 대치암호와 동음이의 대치암호의 문제점을 보완하기 위하여 다표식 대치암호를 앨버트(L.B.Albert)가 개발하였다. 대부분 다표식 대치암호는 주기가 d인 주기적 대치암호이다.

주기 d에 대하여 각 대치암호 함수 $f_i\,(i=1,2,\cdots,d)$는 영어 알파벳 집합 A에서 A로의 대치암호를 나타낸다.

$$\begin{array}{lcccccc} \text{평 문 :} & m_1 & \cdots & m_d & m_{d+1} & \cdots & m_{2d} \\ \text{암호문 :} & f_1(m_1) & \cdots & f_d(m_d) & f_1(m_{d+1}) & \cdots & f_d(m_{2d}) \end{array}$$

이 때 $d=1$인 경우는 단순 대치암호와 같다. 다표식 대치암호의 종류에는 Vigenere 암호, Beaufort 암호, Running key 암호, Rotor and Hageline machine, Vernam 암호, One-time pad 등이 있다.

(4) 쌍자 대치암호(polygram substitution cipher)

앞에서 설명한 암호의 대부분은 평문을 각 문자 단위로 암호화하는 방법이지만, 쌍자 대치암호는 한 번에 여러 개의 암호를 암호화함으로써 각 문자에 대한 빈도를 암호문에서 무의미하게 하여 암호 해독을 어렵게 하는 암호를 말한다.

쌍자 대치암호로는 Playfair 암호와 Hill 암호가 있다.

① Playfair 암호

영국인 플레이페어(L.Playfair)의 이름을 따서 명명된 두 문자 대치암호로 휘트스톤(C.Wheatstone)이 개발하여, 제 1차 세계대전 당시 상용된 암호이다. 키는 [표]와 같이 5×5문자 행렬로 주어지는데, J와 I는 동일시하며 평문 m_1m_2는 다음과 같이 암호화한다.

ⓐ m_1과 m_2가 같은 행에 있으면 c_1과 c_2는 m_1과 m_2의 오른쪽의 문자로 대치하며, 이 때 첫 번째 열은 마지막 열의 오른쪽 문자로 한다.c_1과

ⓑ m_1과 m_2가 같은 열에 있으면 c_1과 c_2는 m_1과 m_2로 대치하며, 첫 번째 행은 마지막 행의 밑의 문자로 간주한다.

ⓒ m_1과 m_2의 열과 행이 모두 다를 경우, c_1과 c_2는 m_1과 m_2를 포함하는 사각형의 모퉁이의 문자로 하되, c_1과 c_2과 같은 행에 c_2는 m_2와 같은 행의 문자로 한다.

ⓓ $m_1=m_2$이면 m_1과 m_2사이에 dummy 문자 X를 넣는다.

ⓔ 만일 문자의 수가 홀수이면, 평문의 끝에 dummy 문자 X를 채운다.

<표 Ⅱ-5 플레이페어 암호의 키>

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

[보기 6] 평문 ATTACKEDFANCE를 암호화해 보자

M = AT TA CK DE FA NC EX

C = PN NP DF IK NC WF GV

이와 같이 플레이페어 암호의 경우 평문 단문자의 통계적 특성이 암호문에서 전혀 나타나지 않지만, 평문의 diagram 등의 특성은 암호문에서도 여전히 나타나므로 해독할 수 있다.

② Hill 암호

Hill 암호는 d문자 평문을 d문자 암호문으로 바꾸는 일차변환을 말한다. d가 2일 경우 평문 $M = m_1 m_2$은 다음과 같이 암호화한다.

$$c_1 \equiv k_{11} m_1 + k_{12} m_2 \pmod{n}$$
$$c_2 \equiv k_{21} m_1 + k_{22} m_2 \pmod{n}$$

여기서 $k_{11}, k_{12}, k_{21}, k_{22}$는 n과 서로 소이다. 이러한 형태의 암호문의 키 K는 다음과 같이 행렬 형태로 나타낼 수 있다.

$$K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

그러므로 암호문 $C = KM$, 즉

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$$

이다.

일반적인 Hill 암호는 평문의 d 문자를 암호의 d문자로 대응시키는 일차 변환이므로 암호문에 대응하는 평문을 d개 이상으로 알고 있다면 이러한 암호 시스템은 해독할 수 있다.

[보기 7] Hill 암호체계를 이용하여 평문 LOVE를 암호화하여라.

정방행렬 $K = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$을 키로 사용하여 암호화하기 위하여 알파벳

ABCDEFGHIJKLMNOPQRSTUVWXYZ

을 정수

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

에 대응시키고 LOVE를 $LO=\begin{pmatrix}11\\14\end{pmatrix}$와 $VE=\begin{pmatrix}21\\4\end{pmatrix}$로 나누어 행렬 K와 곱하면 암호문을 얻는다.

$$\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}11\\14\end{pmatrix}=\begin{pmatrix}3\cdot 11+2\cdot 14\\4\cdot 11+3\cdot 14\end{pmatrix}=\begin{pmatrix}61\\86\end{pmatrix}\quad\begin{pmatrix}\text{26이상의 정수는 26으로}\\\text{나누어 그 나머지로 한다.}\end{pmatrix}$$
$$=\begin{pmatrix}26\cdot 2+9\\26\cdot 3+8\end{pmatrix}\equiv\begin{pmatrix}9\\8\end{pmatrix}=JI$$

$$\begin{pmatrix}3&2\\4&3\end{pmatrix}\begin{pmatrix}21\\4\end{pmatrix}=\begin{pmatrix}3\cdot 21+2\cdot 4\\4\cdot 21+3\cdot 4\end{pmatrix}=\begin{pmatrix}71\\96\end{pmatrix}\quad\begin{pmatrix}\text{26이상의 정수는 26으로}\\\text{나누어 그 나머지로 한다.}\end{pmatrix}$$
$$=\begin{pmatrix}26\cdot 2+19\\26\cdot 3+18\end{pmatrix}\equiv\begin{pmatrix}19\\18\end{pmatrix}=TS$$

그러므로 평문 LOVE는 암호문 JITS가 된다.

이렇게 암호화된 문장은 키 행렬 K의 역행렬을 구하여 원문으로 해독할 수 있다. 즉

$$\begin{pmatrix}3&2\\4&3\end{pmatrix}^{-1}=\begin{pmatrix}3&-2\\-4&3\end{pmatrix}\equiv\begin{pmatrix}3&24\\22&3\end{pmatrix}$$

이므로

$$\begin{pmatrix}3&24\\22&3\end{pmatrix}\begin{pmatrix}9\\8\end{pmatrix}=\begin{pmatrix}3\cdot 9+24\cdot 8\\22\cdot 9+3\cdot 8\end{pmatrix}=\begin{pmatrix}219\\222\end{pmatrix}$$
$$=\begin{pmatrix}26\cdot 8+11\\26\cdot 8+14\end{pmatrix}\equiv\begin{pmatrix}11\\14\end{pmatrix}=LO$$

$$\begin{pmatrix}3&24\\22&3\end{pmatrix}\begin{pmatrix}19\\18\end{pmatrix}=\begin{pmatrix}3\cdot 19+24\cdot 18\\22\cdot 19+3\cdot 18\end{pmatrix}=\begin{pmatrix}489\\472\end{pmatrix}$$
$$=\begin{pmatrix}26\cdot 18+21\\26\cdot 18+4\end{pmatrix}\equiv\begin{pmatrix}21\\4\end{pmatrix}=VE$$

그러므로 이 암호 시스템을 이용하는 경우, 암호를 보내는 측과 받는 측에서는 모두 행렬 K를 간직해야 하고, 이 때 행렬 K가 이 암호시스템의 암호해독 열쇠이다.

3. 암호이론의 요약

암호는 크게 두 가지 용도로 쓰인다. 첫째는 자료의 보안성을 유지하기 위하여 도청을 방지할 수 있도록 암호가 사용되는 경우이고, 둘째는 자료가 송신 도중 제삼자의 개입으로 인한 교란을 방지하기 위한 확증성에 사용된다.

이러한 암호는 초창기에는 군사나 외교와 같은 한정된 부분에 사용되었기 때문에 그 역사에 비해 일반인들에게 알려진 시기는 늦은 편이다. 초창기 암호 제작 기술은 크게 대입(substitution)과 치환(transpositon)방식으로 나눌 수 있다. 대입방식

은 앞에서 밝혔듯이 한 문자를 다른 문자로 교체하는 방식으로 제 1차 세계대전 때 플레이페어라는 암호 시스템이 사용되었다.

치환방식은 평문의 문서 순서를 일정한 규칙에 따라 바꾸는 것으로 평문에 있던 문자가 그 개수만큼만 암호문에 나타난다. 예를 들면 I LOVE YOU를 $A=1, B=2, \cdots, Z=26$으로 대응시켜 9 12 15 22 5 25 15 21로 바꾸어 생각한 뒤 3을 더해 12 15 18 25 8 28(2) 18 24로 변경하면 그 뜻은 알기 힘든 L ORYH BRX로 바뀐다. 만일 메시지를 수신한 사람에게 3을 더했다는 사실을 알려 준다면 수신자는 전송된 암호메시지에서 3을 뺌으로써 원래의 메시지를 읽을 수 있다. 이 과정을 좀더 구체적으로 이야기 하면

① 원래의 메시지를 평문(plaintwxt)이라고 한다. : I LOVE YOU

② 암호화하여 바뀐 메시지를 암호문이라고 한다. : L ORYH BRX

③ 평문을 암호문으로 바꾸는 과정을 암호화(encryption)라 한다. 위의 경우 암호화 방식은 평문에 3을 더한다.

④ 암호문을 평문으로 바꾸는 과정을 복호화(decryption)라 한다.

⑤ 암호화와 복호화 과정에서 알고리즘과 함께 키가 사용된다.

현대 암호시스템의 경우 암호화 및 복호화 알고리즘은 공개하고 키를 공개하지 않음으로써 암호의 안전성에 있다. 따라서 현대 암호시스템이 제공하는 안전성은 키의 보관에 큰 비중이 있다. 대표적인 비밀 키 방식으로 전 세계적으로 사용하고 있는 DES(data encryption standard)방식을 들 수 있는데 1970년대에 들어서면서 상용컴퓨터가 널리 보급되고 기업들은 정부에서 보증하는 믿을 수 있는 민간용 암호를 요구하게 되었다. 이렇게 해서 나온 것이 Unix Password 확인 시에 지금도 사용되고 있는 DES이다. DES는 기밀이 아닌 정보를 보호할 목적으로 설계된 블록 단위 암호시스템이다.

암호가 급속한 발전과 더불어 일반인 사이에서 연구된 시기는 컴퓨터의 발전과 함께 공개 키 개념이 처음으로 선보인 1970년대이다. 이후로 현대 암호시스템의 양대 산맥인 공개 키 방식과 비밀 키 방식이 서로 장단점을 보완하며 발전하였다.

1) 공개키 방식 암호

1970년대에 키가 공개된 암호 체계가 새로 나왔다. 암호화 방법을 알고 있더라도 해독하는 방법을 알지 못한다면 암호화 방법을 공개해도 큰 피해가 없을 것이기 때문이다. 이 방식에서는 각 사용자는 다른 사용자에게 공개할 공개키와 자신이 보관할 비밀키를 각자 선택한다. 만약 비밀키의 안전성만 제공되면 공개키로 생성된 암호문을 통신상에서 얻었다고 해도 해독하기 어렵다. 왜냐하면 해독에는 공개키에 해당하는 비밀키를 알아야만 가능하도록 알고리즘이 설계되어

있기 때문이다.

공개 키 개념은 1976년 디피(Diffie)와 헬먼(Hellman)이 처음으로 제안하였으며 암호론은 수학적으로는 복잡성이론(complexity Theory)와 기본 가설인 One Way Function의 존재를 가정하고 있다. n개의 Bit를 변수 X로써 입력하였을 때 함수의 값 $f(X)$를 얻는 데 필요한 최소한의 연산의 개수가 n을 변수로 하는 다항식이지만, Y가 주어졌을 때 $f(X)=Y$를 만족하는 X를 찾는 데 필요한 최소한의 연산의 개수가 n을 변수로 하는 어떤 차수의 다항식보다 많은 것을 One Way Function이라고 정의한다. 다시 말해, 두 유한집합 A,B사이의 일대일 대응인 함수 $f: A \rightarrow B$에 대하여, 각 원소 $a \in A$의 함숫값 $f(a)$는 쉽게 계산해 낼 수 있으나 f의 역함수$f^{-1}: B \rightarrow A$를 구하기 상당히 어려울 때, 즉, 각 원소 $b \in B$에 대하여 $f(a)=b$인 $a \in A$를 구하기 어려울 때, 함수 f를 일방향 함수(One Way Function)라고 한다. 즉 암호문으로 만드는 과정은 간단하지만 적군이 암호문을 해독하는 것은 어렵다는 것이다. 그리고 추가적인 정보(덫문)를 가지고 있는 경우에만 일방향 함수 f의 역함수를 쉽게 구할 수 있을 때 함수 f를 덫문 일방향 함수(trapdoor one-way function)라고 한다.

예를 들어, 서로 다른 두 홀수인 素數 p, q에 대하여 곱 $m=pq$를 계산하는 일은 대단히 쉽다. 그러나 양의 정수 m이 적당한 두 素數 p, q의 곱이라는 사실만을 알고 합당한 시간 안에 m의 두 소인수를 구하는 일은 대단히 어렵다. 한편, m의 값과 $\varphi(m)$의 값을 알면 p, q를 알아낼 수 있다. 즉, $\varphi(m)$의 값과 같은 추가적인 정보가 바로 덫문이다.

공개 키 체계를 구축하는 데에는 덫문 일방향 함수(trapdoor one-way function)가 이용된다. 1980년대에 정수론을 이용하여 제안된 많은 공개 키 암호는 소인수분해 등의 문제가 One Way Function이라는 가정하에 나오게 되었다. 공개열쇠라는 용어는 함수 f와 y를 공개해도 $f(x)=y$인 x를 찾기가 어렵다는 의미이다. 소인수분해에 기초한 공개 키 암호는 제안자 세 사람의 이름 첫 글자를 따서 RSA 암호라고 부른다. 이들이 만든 회사 RSA Inc.는 얼마 전에 일억 달러 정도에 팔렸다. 요즘에 인기 있는 Netscape나 전자화폐, 전자주민등록증 등도 대개는 RSA 암호를 사용한다.

전 세계적으로 사용되는 대표적인 공개 키 시스템으로는 큰 수의 소인수분해의 어려움에 안전성의 기반을 두고 설계된 RSA가 있다. RSA는 DES에 비해 높은 안전성을 제공하고 있다. RSA와 같은 공개 키 시스템은 메시지와 키 값을 증가시킬 수 있도록 설계되어 있기 때문에 항상 일정한 안전성을 제공한다.

이와 같이 암호에 기본적인 이론을 제공하는 수학이 정수론이다. 이런 의미를 수학적으로 말하면 암호화 과정은 하나의 함수이고 암호해독 과정은 그 함수의

역함수를 찾는 작업이다. 따라서 역함수를 구하기 어려운 함수가 무궁무진하듯이 해독이 거의 불가능한 암호도 많은 것이다. 암호에 쓰이는 계산방법은 보통의 산수 계산이 아니고 진법계산, 즉 정수론에서 법 계산과 같은 것이다.
이러한 계산은 사칙연산이 가능하다. 이러한 계산과 관련된 "페르마의 작은 정리"라는 것이 있다. x가 소수일 때 a의 x제곱은 x를 법으로 하는 a와 같다는 것이다. 즉

$$a^x \equiv a \pmod{x}$$

RSA 암호체계는 페르마의 작은 정리와 함정함수를 이용했다. 암호화에 사용되는 법과 암호화 열쇠는 공개하지만 암호문을 가로챈 제삼자는 해독 열쇠가 없기 때문에 암호를 읽을 수 없도록 만든 것이다.

2) 비밀 키 방식

비밀 키 시스템은 공개 키 방식과 비교해 전자서명이라는 기능을 제공한다. 앞에서 본 암호화 시스템에서는 수신자의 공개 키로 임의의 사람이 메시지에 암호를 보내면 수신자 B가 자신의 비밀 키로 메시지를 복호화 하였는데, 전자서명 방식에서는 송신자가 자신의 비밀 키를 이용해 메시지를 복호화 알고리즘에 돌린 결과를 메시지와 함께 전송한다. 이 때 수신자 B는 송신자 A의 공개 키를 이용해 사인된 메시지를 암호화 알고리즘에 돌려 함께 전송되어 온 메시지와의 관계로 사인의 진실 여부를 확인해 볼 수 있다.

한편 인증 기능의 구조를 서명 등의 [본인 확인]의 경우를 보면

① 수비기능에서는 복호의 역할을 다한 비밀 키를 작용하여 서명문을 작성한다.

② 그 서명문을 받은 사람은 서명인이 공개하고 있는 공개 키를 작용하여서 서명이 진짜인가 어떤가를 확인한다.

공개 키를 작용함로써 만약 암호가 풀린다면 그 공개 키에 대응한 비밀 키로 서명되었기 때문에 그 비밀 키는 서명자만의 비밀이기 때문에 본인 확인이 끝난 것으로 된다는 이론이다.

3) PGP의 태동과 활용

E-Mail 메시지를 암호화함으로써 메시지를 누군가가 중간에서 빼간다 하더라도 그 내용을 알아볼 수 없게 만들고 해쉬함수(hash function)를 사용하여 메시지의 변경 여부도 알아 낼 수 있다. 이러한 개념으로 만들어진 것이 바로 PGP(pretty good privacy)이다. PGP는 1991년에 필립 짐머만(Philip Zimmermann)이 만들었다. 그러나 PGP가 처음 나왔을 때 문제가 발생했다. 사

용하는 프로그램 중에 공개 키 알고리즘으로 사용한 RSA 알고리즘이 이미 특허 등록된 상태였기 때문에 이를 사용한 PGP를 공개 버전으로 만들 수 없었다. 그래서 필은 RSA의 개념을 그대로 사용하여 C언어를 사용한 프로그램을 자신이 직접 구현하여 PGP 안에 삽입했다(박형빈, 2002).

Ⅲ. 암호이론의 기초가 되는 수학이론

암호학의 기초가 되는 이론들은 대부분 정수론을 기반으로 하고 있으며 함수 및 통계 단원과도 관련이 깊다. 특히, 고전 암호 방식의 기본인 법연산이나 알고리즘의 일반화, RSA 암호 방식의 기본인 소수, 유클리드 호제법, 오일러의 정리, 페르마의 정리 등의 내용이다.

1. 정수의 기본 성질

1) 나눗셈 알고리즘(Division Algorithm)

두 정수 $a, b(b \neq 0)$에 대하여

$$a = bq + r, \quad 0 \leq r < |b|$$

인 두 정수 q, r가 유일하게 존재한다.

이와 같은 두 정수 q, r를 각각 a를 b로 나누었을 때의 몫(quotient), 나머지(remainder)라고 한다.

나눗셈 알고리즘은 몫과 나머지를 계산하는 절차를 제공해 주지 못하므로 진정한 의미의 알고리즘은 아니다.

2) 정수 분류의 정리

고정된 양의 정수 m에 대하여 임의의 정수 n을

$$n = mk + r \qquad (k\text{는 정수, } 0 \leq r < m)$$

와 같은 꼴로 나타낼 수 있고, 따라서 정수를 m으로 나누었을 때의 나머지는 $0, 1, \cdots, m-1$중의 하나이다.

예를 들어, 모든 정수 n은

$$2k \text{ 또는 } 2k+1 \qquad (k\text{는 정수})$$

의 꼴로 나타낼 수 있다. 적당한 정수 $k(k = 0, \pm 1, \pm 2, \cdots)$에 대하여 $n = 2k$일 때 n을 짝수(even number)라 하고 또 $n = 2k+1$일 때 n을 홀수(odd number)라고 한다. 예를 들어, $-4, -2, 0, 2, 4, 6$은 짝수이고, $-3, -1, 1, 3$은 홀수이다.

마찬가지로, 모든 정수는

$$4k, 4k+1, 4k+2, 4k+3 \qquad (k\text{는 정수})$$

의 꼴로 나타낼 수 있다.

[정리1] 임의의 정수는 양의 정수 k로 나눈 나머지에 의해

$$kn, kn+1, kn+2, \cdots, kn+(k-1) \qquad (\text{단, } n\text{는 정수})$$

로 분류되며, 임의의 정수는 이 중 어느 하나의 꼴로 나타낼 수 있다.

B. 약수와 배수

정수 전체의 집합 $\mathbb{Z}$위는 나눗셈이 정의되지 않으나 두 정수 사이의 곱셈에 관한 성질을 이용하여 약수와 배수를 정의한다.

두 정수 a, b에 대하여

$$b = ac$$

인 정수 c가 존재할 때, a를 b의 약수(約數, divisor) 또는 인수(因數, factor)라 하고, b를 a의 배수(倍數, multiple)라고 하며 이 사실을 $a|b$로 나타낸다. 또 이 때

'a는 b를 나눈다(나누어 떨어뜨린다).' 'b는 a로 나누어 떨어진다.'

고 말한다. 한편, $a|b$가 아닐 때, 이 사실을 $a \nmid b$로 나타낸다.

정의에 따라 $a \neq 0$인 경우에 $a|b$는 b를 a로 나누었을 때의 나머지가 0임을 뜻한다. 그리고, 모든 정수 a에 대하여 $0 = a \cdot 0$이므로 $a|0$이다.

[정리1] 정수 a, b, c에 대하여

(1) $1|a, a|a, a|0$

(2) $a|b$이면, $a|(-b), (-a)|b, (-a)|(-b)$이다.

(3) $a|b, b|c$이면 $a|c$이다.

[증명] (1) 분명히 $a = a \cdot 1$, $0 = a \cdot 0$이므로 (1)이 성립한다.

(2) $a|b$이면, 적당한 정수 c에 대하여 $b = ac$이고 이 때

$$-b = a(-c),\ \ b = (-a)(-c),\ \ -b = (-a)c$$

이므로 $a|(-b), (-a)|b, (-a)|(-b)$이다.

(3) $a|b$, $b|c$이면, 적당한 정수 d, e에 대하여 $b = ad$, $c = be$이고 이 때, $c = be = (ad)e = a(de)$이므로 $a|c$이다.

[정리2] 정수 a, b, c에 대하여 $a|b, a|c$일 때, 임의의 정수 x, y에 대하여 $a|(bx + cy)$이다. 특히, $a|b, a|c$일 때, $a|(b+c), a|(b-c)$이다.

[증명] $a|b, a|c$이면, 적당한 정수 d, e에 대하여 $b = ad, c = ae$이고, 이 때, 임의의 정수 x, y에 대하여

$$bx + cy = adx + aey = a(dx + ey)$$

이므로 $a|(bx + cy)$이다.

i) $x = 1, y = 1$일 때, $a|(b+c)$ ii) $x = 1, y = -1$일 때, $a|(b-c)$

정수 a의 배수 전체의 집합을 $a\mathbb{Z}$로 나타낸다. 즉,

$$a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$$
$$1\mathbb{Z} = \mathbb{Z}, \quad 0\mathbb{Z} = \{0\}$$

실수 x에 대하여, x보다 작거나 같은 정수 중에서 가장 큰 정수를 x의 정수부분(integral part)이라 하고 이것을 $[x]$로 나타낸다. 또 실수 $x-[x]$를 x의 소수부분(decimal part)이라 하고 이것을 $\{x\}$로 나타낸다. 즉,

$$x = [x] + \{x\}, \quad [x] \in \mathbb{Z}, \quad 0 \le \{x\} < 1$$

흔히 $[x]$를 $\lfloor x \rfloor$로 나타내고 이것을 x의 최저한도(floor)라 하고,

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = [x]$$

를 최대 정수 함수(greatest integer function) 또는 Gauss 함수라고 한다.

그리고, x보다 크거나 같은 정수 중에서 가장 작은 정수를 $\lceil x \rceil$로 나타내고 이것을 x의 최고한도(ceiling)라고 한다.

예를 들어, $[7] = 7$, $[2.6] = 2$, $[\frac{100}{9}] = 11$, $[-4.8] = -5$

$$\lceil 7 \rceil = 7, \ \lceil 2.6 \rceil = 3, \ \left\lceil \frac{100}{9} \right\rceil = 12, \ \lceil -4.8 \rceil = -4$$

이다.

[정리3] 두 양의 정수 a, b에 대하여 $1, 2, \cdots, a$중에서 b의 배수인 것의 개수는 $[\frac{a}{b}]$이고, a를 b로 나누었을 때의 몫은 $[\frac{a}{b}]$이다.

[증명] 먼저 $a = bq + r, \quad 0 \le r < b$라고 하면,

$$bq \le a < b(q+1), \quad \frac{a}{b} = q + \frac{r}{b}, \quad 0 \le \frac{r}{b} < 1$$

이고 따라서 $1, 2, \cdots, a$중에서 b의 배수인 것은 모두 q개 있으며 또한 $q = [\frac{a}{b}]$이다.

3. 약수의 개수와 약수의 합

각 양의 정수 n에 대하여 $\tau(n)$과 $\sigma(n)$의 값을 다음과 같이 정하자.

$\tau(n)$=(n의 양의 약수 전체의 갯수)

$\sigma(n)$=(n의 양의 약수 전체의 합)

위에서 정한 두 함수 τ, σ와 같이, 자연수(양의 정수)전체의 집합 $\mathbb{N}$에서 실수 전체의 집합 $\mathbb{R}$로의 함수를 정수론적 함수(number-rheoretic function) 또는 산술적 함수(arithmetic function)라고 한다.

4. 최대공약수와 최소공배수

두 정수 a, b에 대하여

$$e|a, \quad e|b$$

인 정수 e를 a와 b의 공약수(common divisor)라고 한다.
또, 다음 세 조건을 만족시키는 정수 d를 a, b의 최대공약수(greatest common divisor)라 하고, 이것을 (a, b)또는 $GCD\{a, b\}$로 나타낸다.

(i) $d \geq 0$
(ii) $d|a$, $d|b$, 즉 d는 a와 b의 공약수이다.
(iii) 정수 e에 대하여 $e|a$, $e|b$이면 $e|d$이다.
즉, a와 b의 공약수는 모두 d의 약수이다.

두 정수 a, b에 대하여

$$a|c, b|c$$

인 정수 c를 a와 b의 공배수(common multiple)라고 한다.
또 다음 세 조건을 만족시키는 정수 l을 a, b의 최소공배수(least common multiple)라 하고, 이것을 $[a, b]$또는 $LCM\{a, b\}$로 나타낸다.

(i) $l \geq 0$
(ii) $a|l$, $b|l$, 즉 l는 a와 b의 공배수이다.
(iii) 정수 c에 대하여 $a|c$, $b|c$이면 $l|c$이다.
즉, a와 b의 공배수는 모두 l의 배수이다.

특히 $a > 0$, $b > 0$인 경우에 최대공약수 (a, b)는 a, b의 양의 공약수 중에서 가장 크고, 또 최소공배수 $[a, b]$는 a, b의 양의 공배수 중에서 가장 작다.

[정리1] 두 정수 a, b에 대하여 a와 b의 최대공약수 $d = (a, b)$는 단 하나 존재한다. 그리고 $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$라고 하면,

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

이고, $d = as + bt$인 s, t가 존재한다.[1)]

[증명] $S = a\mathbb{Z} + b\mathbb{Z}$라고 하자. 임의의 두 정수 x, y에 대하여

$$ax = ax + b \cdot 0 \in S, \qquad by = a \cdot 0 + by \in S$$

이므로 $a\mathbb{Z} \subset S$, $b\mathbb{Z} \subset S$이고 $S \neq \varnothing$이다. 그리고, 임의의 정수 x, y, u, v에 대하여

$$(ax + by) \pm (au + bv) = a(x \pm u) + b(y \pm v) \in S$$

1) 두 정수 a와 b의 최대공약수가 1일 때, 즉 $(a, b) = 1$일 때, 두 정수 a, b는 서로 소(relatively prime)라고 한다.

이므로, S는 덧셈과 뺄셈에 관하여 닫혀 있으므로, $S = d\mathbb{Z}$, $d \geq 0$인 정수 d가 존재한다.

한편, $a \in a\mathbb{Z} \subseteq S = d\mathbb{Z}$, $b \in b\mathbb{Z} \subseteq S = d\mathbb{Z}$이므로 $d \mid a$, $d \mid b$이다. 또, $d \in d\mathbb{Z} = S$이므로 $d = as + bt$인 두 정수 s, t가 존재한다. 따라서, $e \mid a$, $e \mid b$이면 $e \mid d$이다. 그러므로 d는 a, b의 최대공약수이다.

다음에, d, d'을 a, b의 최대공약수라고 하면, 정의의 조건에 의하여 $d \mid d'$, $d' \mid d$, $d \geq 0$, $d' \geq 0$이므로 $d = d'$이다.

[정리2] 두 정수 a, b에 대하여 a와 b의 최소공배수 $l = [a, b]$는 단 하나 존재하고 또 $a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$이다.

[증명] 먼저 $ab \in a\mathbb{Z} \cap b\mathbb{Z}$이므로 $a\mathbb{Z} \cap b\mathbb{Z} \neq \varnothing$이다. 그리고 분명히 $a\mathbb{Z} \cap b\mathbb{Z}$는 덧셈과 뺄셈에 대하여 닫혀 있으므로,

$$ab \in a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}, \quad l \geq 0$$

인 정수 l이 존재한다. 한편, $l \in l\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$이므로 $a \mid l$, $b \mid l$이다.

그리고 $a \mid c, b \mid c$이면, $c \in a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$이므로 $l \mid c$이다. 따라서 l은 a, b의 최소공배수이다.

다음에 l, l'을 a, b의 최소공배수라고 하면, 정의에 의하여 $l \mid l'$, $l' \mid l$이고 또 $l \geq 0, l' \geq 0$이므로 $l = l'$이다.

[정리3] 유클리드의 알고리즘(Euclidean algorithm) 두 정수 a, b에 대하여 $r_0 = a$, $r_1 = b$라 할 때, 다음이 성립한다고 하자.

$$\begin{array}{lll}
r_0 = a_0 r_1 + r_2, & 0 < r_2 < r_1 & a_0 \\
r_1 = a_1 r_2 + r_3, & 0 < r_3 < r_2 & \\
r_2 = a_2 r_3 + r_4, & 0 < r_4 < r_3 & \\
\quad \vdots & \quad \vdots & a_{n-1} \\
r_{n-1} = a_{n-1} r_n + r_{n+1}, & 0 < r_{n+1} < r_n & \\
r_n = a_n r_{n+1} & &
\end{array}
\qquad
\begin{array}{c|c|c}
r_0 & r_1 & a_1 \\
a_0 r_1 & a_1 r_2 & \\
\hline
\vdots & \vdots & \\
r_{n-1} & r_n & a_n \\
a_{n-1} r_n & a_n r_{n+1} & \\
\hline
r_{n+1} & 0 &
\end{array}$$

이 때, $(a, b) = r_{n+1}$이다. 그리고

$$\begin{array}{l}
s_0 = 1, \quad s_1 = 0, \quad s_i = s_{i-2} - a_{i-2} s_{i-1} \\
t_0 = 0, \quad t_1 = 1, \quad t_i = t_{i-2} - a_{i-2} t_{i-1}
\end{array} \qquad (2 \leq i \leq n+1)$$

이라고 하면 다음이 성립한다.

$r_i = as_i + bt_i\,, \quad (0 \le i \le n+1)$

i	0	1	2	$\cdots$	$n-1$	n	$n+1$
a_i	a_0	a_1	a_2	$\cdots$	a_{n-1}		
s_i	1	0	s_2	$\cdots$	s_{n-1}	s_n	s_{n+1}
t_i	0	1	t_2	$\cdots$	t_{n-1}	t_n	t_{n+1}

특히, $(a,b) = r_{n+1} = a\,s_{n+1} + b\,t_{n+1}$

[증명] 나눗셈 알고리즘에 의하여 정수 $a_0, a_1, \cdots, a_n$과 $r_0, r_1, \cdots, r_{n+1}$이 존재하고, $(a,b) = (b, r_2) = (r_2, r_3) = \cdots = (r_n, r_{n+1}) = r_{n+1}$이 성립한다.

다음에 $i=0$, $i=1$인 경우에 다음 등식이 성립한다.

$$r_0 = a = 1 \cdot a + 0 \cdot b = a\,s_0 + b\,t_0$$

$$r_1 = b = 0 \cdot a + 1 \cdot b = a\,s_1 + b\,t_1$$

이제 $1 \le k \le n$일 때, $i = 0, 1, \cdots, k$에 대하여 등식

$$r_i = a\,s_i + b\,t_i$$

가 성립한다고 가정하면 다음이 성립한다.

$$\begin{aligned} r_{k+1} &= r_{k-1} - a_{k-1} r_k \\ &= a\,s_{k-1} + b\,t_{k-1} - a_{k-1}(a\,s_k + b\,t_k) \\ &= a(s_{k-1} - a_{k-1} s_k) + b(t_{k-1} - a_{k-1} t_k) \\ &= a\,s_{k+1} + b\,t_{k+1} \end{aligned}$$

따라서 $i = 0, 1, \cdots, n+1$에 대하여 $r_i = a\,s_i + b\,t_i$이다(박승안외1인, 2002)

유클리드 알고리즘이 실생활 문제를 푸는데 어떻게 활용될 수 있는지 살펴보자.

이번 주말에 실시하는 봉사 활동에 참여하는 학생 수가 남학생 5460명, 여학생 3234명이다. 각 조에 속하는 남학생과 여학생 각각의 인원수가 같도록 여러 개의 조로 나누어 봉사 활동을 실시할 때, 될수록 많은 조로 나누는 방법을 알아보자. 각 조에 속하는 남학생과 여학생 각각의 인원수가 같아야 하고, 될수록 많은 조로 나누어야 하므로, 구하는 조의 수가 5460과 3234의 최대공약수이다. 5460과 3234의 최대공약수는

$$\begin{array}{l} 5460 = 2 \times 2 \times 3 \times 5 \times 7 \qquad\quad \times 13 \\ 3234 = 2 \qquad \times 3 \qquad \times 7 \times 7 \times 11 \\ \hline \qquad\quad 2 \qquad \times 3 \qquad \times 7 = 42 \end{array}$$

이므로, 42개의 조로 나누면 된다. 그런데 5460, 3234처럼 작은 수가 아니고 10자리 이상의 큰 수가 나오면 소인수 분해 자체가 어렵기 때문에 위와 같은 방법으로 최대공약수를 구하는 것은 무리이다. 따라서 유클리드 알고리즘을 이용하여야만 구할 수 있다. 그러면 여기서 유클리드 알고리즘으로 구하는 방법에 대해서 살펴보자.

우선 유클리드 알고리즘에 의해 다음의 식을 구할 수 있다.

$$5460=3234\times1+2226$$
$$3234=2226\times1+1008$$
$$2226=1008\times1+210$$
$$1008=210\times4+168$$
$$210=168\times1+42$$
$$168=42\times4+0$$

위의 등식에 의해 우리는 42가 최대공약수라는 것을 알 수 있다.

주어진 두 수의 최대공약수를 구하기 위해 현행 중학교 교과서에서 제시된 방법은, 두 수를 소인수분해하여 공통으로 존재하는 소수들을 곱함으로써 최대공약수를 구할 수 있다는 것이다. 이러한 방법과 비교하여 유클리드 알고리즘을 분석해 보면, 주어진 수의 크기가 작을 때는 유클리드 알고리즘의 유용성이 적다고 보여 질 수 있지만, 조금만 더 수가 커지면 중학교 교과서에 있는 것처럼 소인수 분해를 해서 최대공약수를 구한다는 것은 너무도 힘들 것이다. 이때에 유클리드 알고리즘의 유용성이 빛을 발할 것이다(김영미, 2003).

5. 소 수[2)]

소수는 자연수에서 어떤 의미를 지니는지 생각해 보면 1을 한 번 더하면1, 두 번 더하면 2, 세 번 더하면 3, …, 이와 같이 1과 덧셈만 있으면 모든 자연수를 만들어 낼 수 있다.

이번에는 곱셈으로 자연수를 만들어 보자. 1을 한 번 곱하면 1, 두 번 곱해도 1, 세 번 곱해도 1이다. 1은 아무리 여러 번 곱해도 항상 1이므로 1과 곱셈만으로는 자연수를 모두 만들어 낼 수 없다. 그러면 2를 여러 번 곱하면 모든 자연수를 다 만들어 낼 수 있을까? 2를 두 번 곱하면 4, 세 번 곱하면 8, …. 2를 몇 번 곱하면 6, 15를 만들 수 있을까? 이 수들은 2를 아무리 여러 번 곱해도 만들 수 없고, 3 또는 5가 필요하다. 그러면 곱셈으로 121을 만들기 위해서는 어떤 수가 필요할까? 이와 같이 하면 2, 3, 5, 7, 11,…등과 같은 소수가 모두 필요하게 된다. 이 때, 아주 중요한 성질을 하나 발견할 수 있다. 8은 2를 세 번 곱해서 만들어지는 수이므로 8의 성질은 2의 성질을 알면 추측할 수 있다. 또, 45는 3을 두 번, 5를 한 번 곱해서 만들어지는 수이므로 45는 3과 5의 공통적인 성질을 갖게 된다. 이런 이유

2) 양의 정수 p가 1보다 크고 p의 약수는 $1, -1, p, -p$뿐일 때, p를 소수(prime number, prime)라고 한다. 한편, 1보다 큰 정수 a가 소수가 아닐 때, 즉

$$a = de, \qquad 1 < d < a, \quad 1 < e < a$$

인 정수 d, e가 존재할 때, a를 합성수(composite number)라고 한다.

로 수학자들은 소수에 관심을 가지게 되고, 자연수에 대하여 연구할 때도 소수에 대해서만 집중적으로 연구하면 되는 것이다.

그러면 소수는 현실적으로 어떤 쓰임새가 있을까?

은행에 가서 통장을 만들어 본 사람은 반드시 비밀 번호를 써 넣었을 것이다. 이 비밀 번호는 다른 사람으로부터 자신의 통장 정보를 보호하는 역할을 한다. 잔액이 얼마인지 알려고 할 때나 돈을 찾으려고 할 때는 이 비밀 번호를 알아야 한다. 일종의 암호인 것이다. 또, 어떤 회사의 지사에서 본사로 비밀을 요하는 서류를 통신으로 보낼 때도 다른 회사에서 풀 수 없는 암호를 써야 할 것이다. 이런 암호는 기업 활동이나 전쟁 등과 같이 비밀을 요하는 일에 필수적이다. 전에는 숫자나 글자를 적당히 섞어서 암호를 만들었으나 암호 해독율이 높아지면서 풀기 어려운 암호를 만드는 것이 매우 중요한 일이 되었다(김영미, 2003).

이렇게 중요한 역할을 하는 소수에 대해서 좀 더 살펴보자.

[정리1] 소수 p와 임의의 정수 a에 대하여 $(a,\ p)=1$이거나 $(a, p)=p$이고 또 다음이 성립한다.

(1) $(a, p)=1 \Leftrightarrow p \nmid a$ (2) $(a, p)=p \Leftrightarrow p \mid a$

[정리2] (유클리드) 소수 p와 정수 a, b에 대하여 다음이 성립하다.

$$p \mid ab \quad \Rightarrow \quad p \mid a \text{ 또는 } p \mid b$$

[정리3] 정수 a가 $a \geq 2$이면, a의 소인수 즉 소수인 인수가 적어도 하나 존재한다.

[증명] 정수 a의 약수 중에서 1보다 큰 약수 전체의 집합을 S라고 하자. 이 때, $a \mid a,\ a \geq 2$이므로 $a \in S$이고 따라서 $S \neq \varnothing$이다. 그러므로 정수의 정렬성(整列性)에 의하여 S에는 최소원 p가 존재한다.

한편, d를 p의 1보다 큰 약수라고 하면, $d \mid p, d \mid a$이므로 $d \mid a$이고 따라서 p의 최소성에 의하여 $d=p$이다. 그러므로 p는 소수이다.

[정리4](유클리드) 소수는 무한히 많다.

[증명] 유한개의 소수만이 존재한다고 가정하고 이들 서로 다른 소수를 $p_1, p_2, \cdots, p_n$이라고 하자. 이 때,

$$N = p_1 p_2 \cdots p_n + 1$$

이라고 하면, $N \geq 2$이므로 N의 소인수 p가 존재한다. 한편, 소수는 $p_1, p_2, \cdots, p_n$ 뿐이므로, p는 이들 중 어느 하나와 일치한다.

따라서, $p \mid N, p \mid p_1 p_2 \cdots p_n$이므로

$$p \mid (N - p_1 p_2 \cdots p_n)$$

즉, $p \mid 1$을 얻게 되어 모순이 생긴다. 이것은 유한 개의 소수만이 존재한다는 가정이 옳지 않음을 뜻하므로 소수는 무한히 많다.

6. 소인수분해[3)]

[정리1] (유일인수분해정리, Unique Factorization Theorem)

(ⅰ) 정수 $n\,(n \geq 2)$은 유한 개의 소수 $p_1, \cdots, p_k$의 곱 $n = p_1 \cdots p_k$로 소인수분해된다.

(ⅱ) 정수 $n\,(n \geq 2)$의 소인수분해는 본질적으로 단 한 가지뿐이다. 즉,

$$n = p_1 \cdots p_s \qquad\qquad n = q_1 \cdots q_t$$

를 n의 소인수분해라고 하면, $s = t$이고 또 N의 소인수 $p_1, \cdots, p_s$와 $q_1, \cdots, q_t$는 그 순서만이 다르다.

양의 정수 $n\,(n \geq 2)$의 서로 다른 소인수가 $p_1, \cdots, p_r$뿐일 때, n은 단 한 가지 방법으로 다음과 같이 소인수분해된다.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \qquad (e_1 \geq 1, e_2 \geq 1, \cdots, e_r \geq 1)$$

위와 같은 꼴로 나타낸 것을 n의 표준분해(standard decomposition)라고 한다.

[정리2] 두 양의 정수 a, b가 주어져 있을 때, 이 두 양의 정수를

$$a = p_1^{k_1} p_2^{k2} \cdots p_t^{k_t}, \qquad b = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t}$$

$$(p_1, p_2, \cdots, p_t \text{는 서로 다른 소수이고 } k_i \geq 0,\ l_i \geq 0)$$

이 때, 각 $i\ (1 \leq i \leq t)$에 대하여 $m_i = \min\{k_i, l_i\}$, $n_i = \max\{k_i, l_i\}$라고 하면

(1) $(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}, \qquad [a, b] = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$

(2) $(a, b)[a, b] = ab, \qquad (a, b) = 1 \Leftrightarrow [a, b] = ab$

두 양의 정수의 표준분해를 알고 있을 때에는, 위의 정리를 이용하여 그 최대공약수를 구할 수 있다. 그러나, 상당히 큰 정수를 소인수분해하는 일은 대단히 어려우며 이러한 특성이 암호학(暗號學, Cryptology)에 이용된다.

---

3) 양의 정수 $n\ (n \geq 2)$은 유한 개의 소수 $p_1, \cdots, pk$의 곱

(*) $\qquad n = p_1 \cdots p_k$

으로 나타내어진다. 이 때, 양의 정수 n은 소인수분해(素因數分解)된다고 말하고 또 (*)를 n의 소인수분해(prime factorization)라고 한다.

소수를 구하는 알고리즘과 정수를 인수분해하는 알고리즘은 여러 가지가 개발되어 있으며, 이러한 알고리즘의 계산 과정에는 최대공약수를 구하는 알고리즘이 사용된다.

7. 특수한 유형의 소수

1) Fermat 소수

다음과 같은 꼴의 양의 정수를 페르마 수(Fermat number)라고 한다.

$$F_n = 2^{2^n} + 1 \qquad (n \geq 0)$$

특히, F_n이 소수일 때 F_n을 페르마 소수(Fermat prime)라고 한다.

실제로, 현재 Fermat 수 중에서 소수로 알려진 것은

$$F_0 = 2^1 + 1 = 3, \quad F_1 = 2^2 + 1 = 5, \quad F_2 = 2^4 + 1 = 17$$
$$F_3 = 2^8 + 1 = 257, \quad F_4 = 2^{16} + 1 = 65537$$

뿐이다. 사실 Fermat 소수는 눈금 없는 자와 컴퍼스만을 이용하여 주어진 원에 내접하는 정 n각형을 작도하는 문제와 밀접한 관계가 있다. 실제로, 이러한 정 n각형이 작도 가능한 경우는 n이 다음과 같은 꼴의 정수 일 때뿐이다.

(ⅰ) $n = 2^m \ (m \geq 2)$ 또는,

(ⅱ) $n = 2^k p_1 \cdots p_r \qquad (k \geq 0,\ p_1, \cdots, p_r$는 Fermat 소수)

2) Mersenne 소수

양의 정수 $M_m = 2^m - 1 \quad (m \geq 1)$을 메르센 수(Mersenne number)라고 한다. 특히,

$$M_p = 2^p - 1 \qquad (p\text{는 소수})$$

가 소수일 때, M_p를 메르센 소수(Mersenne prime)라고 한다.

예를 들어, 다음 정수는 Mersenne 소수이다.

$$M_2 = 2^2 - 1 = 3, \qquad M_3 = 2^3 - 1 = 7$$
$$M_5 = 2^5 - 1 = 31, \qquad M_7 = 2^7 - 1 = 127$$

Mersenne 소수가 무한히 많은지는 아직까지 알려져 있지 않다. 현재까지 알려진 Mersenne 소수는 47개이다(박승안외 1인, 2002).

8. 소수 판정

양의 정수가 소수인지를 판정하는 문제는 암호학, 부호 이론, 정보 이론 등의 통신 이론에서는 대단히 중요한 문제이다. 주어진 수가 소수인지 아닌지를 알아내려

는 노력은 기원전부터 시작되었다. 무한히 많은 자연수 중 소수는 몇 개일까? 또 가려내는 방법은 없을까? 많은 수학자들이 이것을 해결하려고 노력하였으나 큰 성과를 거두지 못하였다.

자연수 중에서 소수를 찾는 방법 중 하나는 에라토스테네스((Eratosthenes)가 발견한 것으로 마치 체(sieve)를 이용하여 소수를 골라내는 것 같아서 에라토스테네스의 체라고 불린다. 이것은 수학에서 중요하고 아주 흥미있는 결과라고 할 수 있는데 지금부터 구체적으로 에라토스테네스와 그가 고안한 체에 대해서 살펴보자. 에라토스테네스의 체를 구체적으로 살펴보면 소수가 1과 자기 자신만을 약수로 갖는다는 사실을 이용하여 각 자연수의 배수들을 하나씩 제거해 나가면 원하는 수까지의 소수를 찾을 수 있도록 고안하였다. 예를 들어, 50이하의 수에 대해서 에라토스테네스의 체에 의한 방법으로 소수를 가려보면 먼저 1부터 50까지의 자연수를 쓰고 우선 1은 소수에서 제외되므로 지우고, 다음에 나타나는 2를 남기고, 2의 배수들을 사선으로 그어 지워 나간다. 이어서 2 다음 수인 3을 남기고, 3의 배수들을 역시 지워 나간다. 그러면 6이나 12 같은 수들은 2번 사선이 그어지게 된다. 이와 같은 방법으로 5, 7, 11,13,…등의 소수를 구하고, 그것의 배수들을 지워 나갈 때 남은 수가 50이하의 소수이다.

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

에라토스테네스의 방법 이외에 다수의 소수 판정법이 개발되었으나, 주어진 아주 큰 수의 소수 성질을 구체적으로 판정할 수 있는 방법은 현재까지도 알려지지 않고 있다(김영미,2003).

9. 합 동[4)]

4) 고정된 양의 정수 m에 대하여, 두 정수 a, b의 차가 m의 배수일 때, 즉, $m \mid (a-b)$일 때, a와 b는 法 (modulus) m에 관하여 합동(合同)이라 하고(a is congruent to b modulo m) 또 이 사실을

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

으로 나타낸다. 즉, $a \equiv b \pmod{m} \iff m \mid (a-b)$

합동 기호 $\equiv$가 들어 있는 식을 합동식(合同式)이라고 한다. 또, $a \equiv b \pmod{m}$가 아닐 때,

合同 개념은 독일의 대수학자 가우스(Carl Friedrich Gauss)가 19세기 초에 도입한 개념이다.

합동 개념은 일상생활에서 자주 대하는 개념이다. 예를 들어, 시계의 시간을 가리키는 바늘은 12 또는 24를 법으로 하여 같은 시간을 나타내고 달력에서는 제한된 범위에서 7을 법으로 하여 같은 요일이 되풀이된다.

양의 정수 m에 대하여, 정수 전체의 집합 $\mathbb{Z}$위에 정의된 합동관계 $a \equiv b \pmod{m}$는 동치관계이다. 즉,

C1. $a \equiv a \pmod{m}$

C2. $a \equiv b \pmod{m} \quad \Rightarrow \; b \equiv a \pmod{m}$

C3. $a \equiv b \pmod{m}, \; b \equiv c \pmod{m} \quad \Rightarrow \; a \equiv c \pmod{m}$

정수 전체의 집합 $\mathbb{Z}$위에서의 합동관계 $a \equiv b \pmod{m}$에 의하여 결정되는 동치류를 법 m에 관한 잉여류(residue class)라고 한다. 여기서 a를 포함하는 법 m에 관한 잉여류는 $\overline{a}$는 다음과 같다.

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\} = \{a + mk \mid k \in \mathbb{Z}\}$$

[정리1] 중국인의 나머지 정리(Chinese Remainder Theorem) 양의 정수 $m_1, m_2, \cdots, m_n \;\; (n \geq 2)$이 쌍마다 서로 소일 때 $M = m_1 m_2 \cdots m_n$이라고 하면 다음이 성립한다.

(1) 임의의 정수 u를 $m_1, m_2, \cdots, m_n$으로 나누었을 때의 나머지를 각각 $r_1, r_2, \cdots, r_n$이라고 하면

$$u \equiv r_i \pmod{m_i} \quad (1 \leq i \leq n)\text{이다.}$$

(2) 임의의 정수 $c_1, c_2, \cdots, c_n$에 대하여 연립일차합동식

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv c_n \pmod{m_n} \end{cases}$$

은 법 M에 관하여 단 한 개의 해 $x \equiv u \pmod{M}$을 가진다.

10. Fermat 정리와 Euler 정리

[정리1] 페르마의 정리(Fermat's Theorem)

소수 p에 대하여

이 사실을 $a \not\equiv b \pmod{m}$로 나타낸다.

(1) 모든 정수 a에 대하여 $a^p \equiv a \pmod{p}$이다.

(2) $(a, p) = 1$인 정수 a에 대하여 $a^{p-1} \equiv 1 \pmod{p}$이다.

[정리2] 오일러의 정리(Euler's Theorem)

1) 오일러의 함수

양의 정수 m에 대하여, $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$이라 하고

$$\mathbb{Z}_m^* = \{r \in \mathbb{Z}_m \mid (r, m) = 1\}$$

이라고 하자. 또 정수 $0, 1, \cdots, m-1$ 중에서 m과 서로 소인 정수 전체의 개수를 $\varphi(m)$으로 나타낸다.

즉, $\varphi(m) = |\mathbb{Z}_m^*|$이고, 이와 같이 정의된 정수론적 함수 φ를 오일러의 φ함수(Euler φ-function)라고 한다.

2) 오일러의 정리

양의 정수 m과 $(a, m) = 1$인 정수 a에 대하여 다음이 성립한다.

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

특히, p가 소수일 때 $a^{p-1} \equiv a^{\varphi(p)} \equiv 1 \pmod{p}$이다(박승안외1인, 2002).

Ⅳ. 중 ·고등학교에서 활용할 수 있는 암호체계

다음 표는 암호이론과 관련된 2007년 7차 개정 교육과정에서의 중등수학 내용을 정리한 것이다.

<표 Ⅳ-1 암호체계와 관련된 중등수학 내용>

과정	내용	암호학 관련 분야
중학교 1학년~3학년	◦ 수와 연산 : Ceasar 암호의 계산(사칙연산 이외의 연산까지 확장) ◦ 문자와 식 : Ceasar 암호를 식으로 표현하기 ◦ 함수 : Ceasar 암호를 함수로 표현하기 ◦ 확률과 통계 : 최빈값을 이용한 암호체계 ◦ 기하	Ceasar 암호 체계 ※ 최빈값을 이용한 암호체계
고등학교 1학년	◦ 수와 연산 : 일반화된 Ceasar 암호의 계산 ◦ 문자와 식 : 일반화된 Ceasar 암호를 식으로 표현하기 ◦ 함수 : Ceasar 암호를 함수로 표현하기, ◦ 확률과 통계 ◦ 기하	Ceasar 암호 체계의 일반화(초등 암호학)
수학 Ⅰ	◦ 행렬과 그래프 : Hill 암호 체계 ◦ 지수함수와 로그함수 ◦ 수열 ◦ 수열의 극한	Hill 암호체계
수학 Ⅱ	◦ 방정식 ◦ 부등식 ◦ 삼각함수 ◦ 함수의 극한과 연속 ◦ 미분법	
미적분과 통계 기본	◦ 함수의 극한과 연속 ◦ 다항함수의 미분법 ◦ 다항함수의 적분법 ◦ 확률 ◦ 통계	
적분과 통계	◦ 적분법 ◦ 순열과 조합 ◦ 확률 ◦ 통계	
기하와 벡터	◦ 일차변환과 행렬 : Hill 암호 체계와 ◦ 이차곡선 : 최근 타원곡선을 이용한 암호체계 발견 ◦ 공간도형과 공간좌표 ◦ 벡터	Hill 암호 체계 ※ 최근 이차곡선을 이용한 암호체계 발견

1. Ceasar 암호

시저(Ceasar)가 사용하여 유명해진 시저암호는 영문자 알파벳 각각을 세 자리 뒤의 다른 알파벳으로 대치하는 것이다. 즉 평문의 A는 D로 B는 E로, …,X는 A로 대치하는 것이다. 이것은 다음과 같이 표현될 수 있다.

① 각 알파벳 문자를 0부터 25까지의 정수로 표현한다. ② 이 정수에 3을 더한 후 26으로 나눈 나머지를 구한다. ③ 구한 값을 규칙 ①에 의해 다시 문자로 바꾼다.

따라서 각 문자를 0부터 25까지의 정수로 대응시켰을 때 시저암호는
$f: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$를 다음과 같이 정의한 함수로 표현될 수 있다.

$$f(x) \equiv x+3 \pmod{26}$$

즉, $f(0)=3, f(24)=1$이므로 f는 $f(A)=D, f(Y)=B$와 같이 생각할 수 있다.

[예제] 시저암호에 의해 평문 M은 다음과 같이 암호문 C로 암호화된다.

M = RENAISSANCE
C = UHQDLVVDQFH

함수 단원에서 Ceasar 암호를 함수로 표현하게 함으로써 적용할 수 있다. 하지만 중학교 1학년에서는 $y=ax$꼴의 함수만 배우고 중학교 2학년에 와서야 $y=ax+b$꼴의 함수를 배우므로 시저암호의 함수 $y=x+3$는 중학교 2학년에서 지도해야 하며, 중학교 1학년에서는 함수로 도입하지 않고 알파벳 각각을 세 자리 뒤의 다른 알파벳으로 대치하는 것으로 가르친다. 또한 시저 암호에 대해 설명을 해주고 이것을 식으로 표현하게 함으로써 문자와 식 단원에 적용할 수 있다. 복호화 과정에서는 교과과정상 중학교에서는 역함수를 사용할 수 없으므로 자연스러운 역사고 과정을 통해 지도하고 고등학교 1학년에 가서 역함수를 사용하여 지도한다.

2. Affine 암호

시저암호의 규칙 $f(x) \equiv x+3 \pmod{26}$에서 3대신 다른 수를 사용할 수 있으며, 시저 암호의 표현 방식을 따르면 주어진 정수 k를 키로 생각할 수 있다.

이것을 확장하여 함수를 아핀변환(affine transformation)을 사용할 수도 있다. 즉, x는 각 영문자에 대응하는 0과 25 사이의 정수일 때, k_0과 k_1은 키로서 0과 25사이

의 정수로 $(k_1, 26)=1$을 만족하게 선택하면 영문자는 다음과 같은 아핀변환에 의해 암호화될 수 있다.

$$f(x) \equiv k_1 x + k_0 \pmod{26}$$

[예제] 아핀 암호를 사용하기 위해서 26과 서로소인 수 3을 택하여 비밀키를 $k_1=3$, $k_0=1$로 하자. 암호화 함수는 $f(x) \equiv 3x+1 \pmod{26}$이 되고 다음 표와 같이 암호화 된다.

<표 Ⅳ-2 Affine 암호화>

평문	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
x	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
암호문	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y
$3x+1$	01	04	07	10	13	16	19	22	25	02	05	08	11	14	17	20	23	00	03	06	09	12	15	18	21	24

평문 M이 다음과 같다고 할 때 위의 표를 따라 암호화하면 다음과 같은 암호문 C를 얻을 수 있다.

M = A BARKING DOG NEVER BITES

C = B EBAFZOT KRT ONMNA EZGND

복호화할 때는 암호문을 $f(x) \equiv 3^{-1}(x-1) \equiv 9(x-1) \pmod{26}$에 대입하여 계산하면 평문을 얻을 수 있다.

함수 단원에서 아핀 암호를 함수로 표현하게 할 때 아핀 변환 $f(x)=k_1x+k_0$에서 k_0가 0인 경우 중학교 1학년 학생에게 적용가능하고 $k_0 \neq 0$이면 중학교 2학년에서 적용 가능하다. 시저 암호와 마찬가지로 아핀암호에 대해 설명하고 이것을 식으로 표현하게 함으로써 문자와 식 단원에 적용할 수 있고, 복호화 과정에서 역함수 사용은 고등학교 1학년에서 가능하다.

3. Vigenère 암호

비게네르(Vigenère) 암호는 시저암호를 이용한 주기적 대치 암호이다. 평문에 길이가 d인 비밀키를 계속 이어 더하여 암호화하는 암호법이며, 따라서 평문의 같은 문자가 암호문에서는 여러 가지 문자로 대응된다. 즉, 키 수열이 $K=k_1k_2\cdots k_d$(각 k_i는 0과 25사이의 정수)이고 x가 영문자에 대응하는 0과 25사이의 정수라 할 때, 키 수열 K에 의하여 다음과 같이 표현된다.

$$f_i(x) \equiv x + k_i \pmod{26}$$

[예제] 평문 M이 다음과 같고 암호키를 LOVE라 할 때 비게네르 암호방식으로 암호화해 보자.

M = TALK TO THE WALL

먼저 평문과 비밀키를 숫자로 변환해 놓고 평문 숫자에 비밀키 숫자를 연이어 mod 26에 관해 더하여 다음 표와 같은 암호문 숫자를 생성한 다음 숫자를 문자로 다시 변환을 하면 암호문을 얻을 수 있다.

<표 Ⅳ-3 비게네르 암호>

평문	T	A	L	K	T	O	T	H	E	W	A	L	L
평문 숫자	19	00	11	10	19	14	19	07	04	22	00	11	11
비밀키	L	O	V	E	L	O	V	E	L	O	V	E	L
비밀키 숫자	11	14	21	04	11	14	21	04	11	14	21	04	11
암호문	E	O	G	O	E	C	O	L	P	K	V	P	W
암호문 숫자	04	14	06	14	04	02	14	11	15	10	21	15	22

위 표에서 보면 암호문 C는 다음과 같다.

C = EOGO EC OLP KVPW

복호화는 암호문에서 LOVE(11 14 21 04)를 차례로 빼나가면 평문을 얻을 수 있다.

함수 단원에서 일차함수 $y=x+b$를 배울 때 변수 x에 더해지는 b는 고정된 숫자이다. 비게네르 암호 함수 $f_i(x)=x+k_i$에서는 변수 x의 평문에서의 위치에 따라 더해지는 숫자 k_i가 반복적으로 바뀐다. 이것은 일차함수에 대한 사고력을 확장시켜 준다.

4. Hill 암호

Hill 암호법은 평문을 2문자씩 몇 개의 블록으로 나눈 다음 각 문자를 숫자로 변환하여 행벡터 $M=(m_1\ m_2)$로 나타낸 후 2×2 가역행렬(암호키) $K\in M_{2\times 2}(\mathbb{Z}_{26})$를 곱하여 암호문 C를 얻는 암호법이다.

$$C\equiv MK\equiv (m_1\ m_2)\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \pmod{26}$$

한편 암호문 C에 역행렬 K^{-1}을 곱하여 평문 M을 구한다.

$$CK^{-1}\equiv MKK^{-1}\equiv M \pmod{26}$$

[예제] 암호키가 $K=\begin{pmatrix}1&2\\0&3\end{pmatrix}$일 때 다음 평문을 Hill 암호를 이용하여 암호화를 해 보자.

M = SEEING IS BELIEVING

이 평문을 숫자로 변환을 하면 다음과 같다. 이 때 숫자 2개가 한 블록이 된다. (마지막 23은 블록의 문자의 수를 맞추기 위하여 임의로 선택하여 삽입한 것이다.)

18 4, 4 8, 13 6, 8 18, 1 4, 11 8, 4 21, 8 13, 6 23

위의 숫자쌍을 1×2 행벡터로 나타낸 후 암호키 K를 곱하면 다음과 같은 암호문을 얻는다.

$$(18\ \ 4)\begin{pmatrix}1&2\\0&3\end{pmatrix}\equiv(18\ \ 22)\pmod{26},\ \cdots\ ,(6\ \ 23)\begin{pmatrix}1&2\\0&3\end{pmatrix}\equiv(6\ \ 3)\pmod{26}$$

18 22, 4 6, 13 18, 8 18, 1 14, 11 20, 4 19, 8 3, 6 3

이것을 영문으로 나타내면 다음과 같다.

C = SWEGNS IS BOLUETIDG D

복호화할 때는 역행렬 $K^{-1}\equiv\begin{pmatrix}1&8\\0&9\end{pmatrix}\pmod{26}$을 암호문의 오른쪽에 곱하여 평문을 얻을 수 있다.

Hill 암호체계는 수학 I 의 행렬과 그래프에서 행렬과 직접적인 관계가 있다. 1×2 행렬과 2×2행렬을 이용해서 암호화하는 과정은 행렬의 곱셈 연산을 학습하는데 도움을 주고, 복호화하는 과정에서는 역행렬을 이용함으로써 역행렬과 역행렬의 존재성 여부 등을 학습하는데 도움을 준다(송정은, 2005).

행렬 B가 행렬 A의 역행렬일 때, 행렬 A를 이용하여 암호문을 만들고 행렬 B를 이용하여 그것을 해독하는 것으로 두 행렬 A, B를 모르면 이 암호문을 해독할 수 없으므로 숫자화하는 표는 알려지더라도 누설될 염려가 없다. 따라서, 두 행렬 A, B를 주기적으로 바꾸어 주면 통신 내용의 보안이 효과적으로 유지될 수 있는 방법이다.

1) 영문을 암호화하는 경우

두 행렬 A, B를 $A=\begin{pmatrix}3&1\\2&1\end{pmatrix}$, $B=\begin{pmatrix}1&-1\\-2&3\end{pmatrix}$이라 하고, 알파벳과 기호 $*$(단어 사이를 띄는 기호로 사용)를 다음과 같이 숫자화 한다.

<표 Ⅳ-4 Hill 암호(영문)>

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	*	
15	16	17	18	19	20	21	22	23	24	25	26	27	

다음은 'I LOVE YOU'란 문장을 숫자화하여 행렬로 만들면 아래와 같이 된다.

I	*	L	O	V	E	*	Y	O	U
9	27	12	15	22	5	27	25	15	21

$$M = \begin{pmatrix} 9 & 27 & 12 & 15 & 22 \\ 5 & 27 & 25 & 15 & 21 \end{pmatrix}$$

그리고 이것을 암호화하기 위해 M의 왼쪽에 A를 곱하여 N을 만든다.

$$\begin{aligned} N = AM &= \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 9 & 27 & 12 & 15 & 22 \\ 5 & 27 & 25 & 15 & 21 \end{pmatrix} \\ &= \begin{pmatrix} 32 & 108 & 61 & 60 & 87 \\ 23 & 81 & 49 & 45 & 65 \end{pmatrix} \end{aligned}$$

이다. 그런데 A가 2×2행렬이므로 이것을 다음과 같은 두 행렬을 가지는 행렬 N으로 만든다. 이 때, 숫자의 개수가 홀수이면 행렬곱 AM이 정의되도록 M의 마지막에 $*$에 해당되는 숫자 27을 첨가한다.

이 N으로부터 숫자화된 암호문

32, 108, 61, 60, 87, 23, 81, 49, 45, 65

을 만든다. 이후 이 암호문을 전송하며, 이것을 받은 상대방은 이 N으로부터 원문 M을 찾아낼 수 있다.

상대방과 미리 약속을 하여 A가 무엇인지 알고 있다면 암호문을 받은 측은 A의 역행렬 B를 이용하여 해독이 가능하다.

$$BN = B(AM) = A^{-1}(AM) = M$$

따라서 암호문을 두 행을 가지고 행렬로 만들고, 이것의 왼쪽에 B를 곱하면 해독할 수 있다.

$$\begin{aligned} BN &= \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 32 & 108 & 61 & 60 & 87 \\ 23 & 81 & 49 & 45 & 65 \end{pmatrix} \\ &= \begin{pmatrix} 9 & 27 & 12 & 15 & 22 \\ 5 & 27 & 25 & 15 & 21 \end{pmatrix} \end{aligned}$$

이므로 다음 문자을 얻는다.

9	27	12	15	22	5	27	25	15	21
I	*	L	O	V	E	*	Y	O	U

2) 한글을 암호화하는 경우

영문으로 된 문장을 암호화하는 것처럼, 한글로 된 문장도 암호화 할 수 있다. 이런 일을 위해 해야할 첫 번째 작업은 한글로 된 문장(평문)을 수학적 모델링하는 것이다.

두 행렬 A, B를 다음과 같이 정의하고

$$A=\begin{pmatrix}1&0&1\\3&3&4\\2&2&3\end{pmatrix},\ B=\begin{pmatrix}1&2&-3\\-1&1&-1\\0&-2&3\end{pmatrix}$$

한글 자음과 모음, 기호를 다음 표와 같이 숫자화하여 보자.

<표 Ⅳ-5 Hill 암호(한글)>

ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅊ
1	2	3	4	5	6	7	8	9	10
ㅋ	ㅌ	ㅍ	ㅎ	ㅏ	ㅑ	ㅓ	ㅕ	ㅗ	ㅛ
11	12	13	14	15	16	17	18	19	20
ㅜ	ㅠ	ㅡ	ㅣ	ㅐ	ㅒ	ㅔ	ㅖ	*	?
21	22	23	24	25	26	27	28	29	30

다음 문장 ‘즐거운 수학’을 암호화하기 위해 먼저 숫자화하면 아래와 같이 된다.

ㅈ	ㅡ	ㄹ	ㄱ	ㅓ	ㅇ	ㅜ	ㄴ	ㅅ	ㅜ	ㅎ	ㅏ	ㄱ
9	23	4	1	17	8	21	2	7	21	14	15	1

그런데 A가 3×3 행렬이므로 이것을 다음과 같은 3개의 행을 갖는 행렬 M으로 만든다. 숫자의 개수가 3의 배수가 아니면 마지막에 *에 해당하는 29를 계속 첨가한다.

$$M=\begin{pmatrix}9&23&4&1&17\\8&21&2&7&21\\14&5&1&29&29\end{pmatrix}$$

앞에서와 같은 방법으로 다음과 같이 숫자화된 암호문을 만들 수 있다.

$$N = AM = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix} \begin{pmatrix} 9 & 23 & 4 & 1 & 17 \\ 8 & 21 & 2 & 7 & 21 \\ 14 & 5 & 1 & 29 & 29 \end{pmatrix}$$
$$= \begin{pmatrix} 23 & 28 & 5 & 30 & 46 \\ 107 & 152 & 22 & 140 & 230 \\ 76 & 103 & 15 & 103 & 163 \end{pmatrix}$$

이므로 숫자화된 암호문은 다음과 같다.

23, 28, 5, 30, 46, 107, 152, 22, 140, 230, 76, 103, 15, 103, 163

그러면 $B = A^{-1}$를 이용하여 암호문을 해독하여 보자. 즉, $B = A^{-1}$이므로

$$BN = \begin{pmatrix} 1 & 2 & -3 \\ -1 & 1 & -1 \\ 0 & -2 & 3 \end{pmatrix} \begin{pmatrix} 23 & 28 & 5 & 30 & 46 \\ 107 & 152 & 22 & 140 & 230 \\ 76 & 103 & 15 & 103 & 163 \end{pmatrix}$$
$$= \begin{pmatrix} 9 & 23 & 4 & 1 & 17 \\ 8 & 21 & 2 & 7 & 21 \\ 14 & 5 & 1 & 29 & 29 \end{pmatrix}$$

이므로 다음 문장을 얻는다.

9	23	4	1	17	8	21	2	7	21	14	15	1
ㅈ	ㅡ	ㄹ	ㄱ	ㅓ	ㅇ	ㅜ	ㄴ	ㅅ	ㅜ	ㅎ	ㅏ	ㄱ

간단한 행렬 이론을 배우게 되는 고등학교 2학년 수학 과정에서, 위 암호 이론을 소개하는 것은 그다지 어려운 일은 아니라고 생각되며, 이와 같은 심화 학습은 수학에 대한 호기심과 매력을 학생들에게 보여주기에 아주 좋은 자료라고 보여진다(김영미, 2003).

Ⅴ. 설문지 결과 비교분석

전라남도 곡성군에 위치한 중학교 2학년 학생 29명을 대상으로 설문을 진행하였다. 학생들은 중학교 2학년 수학 삼각형의 성질까지 학습하였다. 2011년 10월 14일 암호학 수업 전 부록2의 A문항을 통하여 사전조사를 실시하였고, 15일 2차시에 걸쳐 부록1의 교수학습계획서에 따라 수업을 진행한 후 부록2의 B문항으로 다시 설문조사를 하여 그 결과를 비교분석 하였다. 본 연구의 대상은 연구자가 근무하고 있는 중학교에 다니는 중학생들로 한정 되어있기 때문에 연구 결과를 일반화하는데 한계가 있고, 연구 결과를 해석하는데 제한점이 있다. 또, Ceasar 암호만을 도입하여 수업을 진행하였으므로, 연구 결과를 다른 암호체계로 일반화하는 데에 제한점이 있다.

1. 암호학 수업 전

암호학 수업 전 수학과목에 대해서 흥미도를 조사한 결과 55.18%의 학생이 흥미가 없다고 답하였으며(문항1) 수학과목에 대해서 48.27%의 학생이 실용적인 학문이 아니라고 답하였다(문항2). 또한 수학 과목에서 실용적인 내용을 배우게 되면 흥미가 생길 것이라고 답한 학생이 보통이다라는 답을 포함하여 72.41%였고(문항3) 암호학에 대해 알고 있는가에 대해서는 거의 대부분의 학생들이 보통 이하의 답을 하였다(문항4).

암호학과 수학의 관련성에 대해서 24.14%의 학생만이 긍정적은 답을 하였고(문항5), 암호학이 흥미로운가에 대해서는 보통이다라는 답을 포함하여 58.62 %의 학생이 흥미롭다고 답하였으며(문항6), 암호학이 실용적인가에 대해서는 96.55%의 학생이 긍정적인 답을 하였다(문항7). 암호학을 배우면 수학공부에 도움이 될 것인가에 대해서는 보통이다라는 답을 포함하여 24.14%만이 긍정적으로 답하였고(문항8), 암호학에 대해 잘 알게 되면 수학공부가 더 흥미로울 것인가에 대해서는 보통이다라는 답을 포함하여 41.38%가 긍정적으로 답하였다(문항 9). 암호학내용을 수학교육과정에 소개해야 하는가에 대하여 보통이다라는 답을 포함하여 10.34%만이 긍정적으로 답하였다(문항 10).

<표 Ⅴ-1 암호학 수업 전 설문지 결과> 명 (%)

답문항 / 질문문항	①	②	③	④	⑤	계
1	0 (0)	3 (10.34)	10 (34.48)	14 (48.28)	2 (6.90)	29 (100)
2	0 (0)	2 (6.90)	13 (44.83)	9 (31.03)	5 (17.24)	29 (100)
3	0 (0)	8 (27.59)	12 (41.38)	7 (24.14)	2 (6.90)	29 (100)
4	0 (0)	0 (0)	1 (3.45)	17 (58.62)	11 (37.93)	29 (100)
5	1 (3.45)	6 (20.69)	15 (51.72)	6 (20.69)	1 (3.45)	29 (100)
6	0 (0)	4 (13.79)	13 (44.83)	10 (34.48)	2 (6.90)	29 (100)
7	3 (10.34)	15 (51.72)	10 (34.48)	1 (3.45)	0 (0)	29 (100)
8	0 (0)	1 (3.45)	6 (20.69)	19 (65.52)	3 (10.34)	29 (100)
9	0 (0)	4 (13.79)	8 (27.59)	15 (51.72)	2 (6.90)	29 (100)
10	0 (0)	1 (3.45)	2 (6.90)	20 (68.97)	6 (20.69)	29 (100)

2. 암호학 수업 후

암호학 수업 후 수학과목에 흥미가 있다고 답한 학생은 보통이라는 답을 포함하여 58.62%로서 암호학 수업 전의 44.83%와 비교할 때 흥미가 더 늘어난 것을 볼 수 있다(문항 1). 수학이 실용적인가에 대해서는 24.14%만이 그렇지 않다고 답하였고(문항 2), 암호학과 수학이 관련 있는가에 대하여 보통이라는 답을 포한하여 96.56%가 긍정적으로 답하였으며(문항 3), 암호학 내용에 흥미가 있는가에 대하여는 보통이라는 답을 포함 72.41%가 긍정적으로 답하였다(문항 4). 암호학 내용에 실용적인가에 대해서는 보통이라는 답을 포함하여 96.55%가 그렇다고 답하였고(문항 5), 암호학을 통하여 수학공부에 흥미를 가지게 되었는가에 대해서는 보통이라는 답을 포함하여 65.52%가 그렇다고 답하였으며(문항 6), 암호학 내용이 실제 수학수업을 하는데 있어 도움이 된다고 답한 학생은 보통이다 포함하여 82.76%나

차지했다(문항 8). 정보화 시대에 암호학이 필요한가에 대해서는 보통이다라는 답을 포함하여 93.10%가 긍정적으로 답하였다(문항 7). 수학교육과정에 암호학 내용을 포함하는 것은 정보화 시대에 부응하는 것인가에 대해서는 보통이다라는 답을 포함하여 82.76%가 긍정적으로 답하였다(문항 10).

<표 Ⅴ-2 암호학 수업 후 설문지 결과> 명 (%)

답문항 / 질문문항	①	②	③	④	⑤	계
1	0 (0)	5 (17.27)	12 (41.38)	11 (37.93)	1 (3.45)	29 (100)
2	1 (3.45)	5 (17.24)	16 (55.17)	7 (24.14)	0 (0)	29 (100)
3	8 (27.59)	17 (58.62)	3 (10.34)	1 (3.45)	0 (0)	29 (100)
4	1 (3.45)	6 (20.69)	14 (48.28)	7 (24.14)	1 (3.45)	29 (100)
5	5 (17.24)	19 (65.52)	4 (13.79)	1 (3.45)	0 (0)	29 (100)
6	1 (3.45)	6 (20.69)	12 (41.38)	8 (27.59)	2 (6.90)	29 (100)
7	5 (17.24)	10 (34.48)	12 (41.38)	2 (6.90)	0 (0)	29 (100)
8	1 (3.45)	9 (31.03)	14 (48.28)	4 (13.79)	1 (3.45)	29 (100)
9	0 (0)	3 (10.34)	6 (20.69)	15 (51.72)	5 (17.24)	29 (100)
10	2 (6.90)	10 (34.48)	12 (41.38)	3 (10.34)	2 (6.90)	29 (100)

3. 설문지 결과 분석

암호학 수업을 듣기 전과 암호학 수업을 들은 후 설문지를 조사하여 비교분석 해보면 다음과 같다.

먼저 수학과목에 대한 흥미도를 조사한 결과 수학과목에 흥미가 있다고 답한 학생은 보통이라는 답을 포함하여 암호학 수업을 듣기 전에는 44.83%, 암호학 수업을 들은 후에는 58.62%로, 근소한 변화지만 암호학 수업을 통하여 수학과목에 흥미가 유발되었고 수학과목에 대해 긍정적인 변화가 있었음을 알 수 있다.

수학의 실용성에 대한 인식을 조사한 결과 암호학 수업 전에는 6.90%, 암호학 수

업 후에는 20.69%의 학생이 실용적이라고 답하여 암호학 수업 후 수학의 실용성에 대한 인식이 변화하였음을 알 수 있다. 또한 보통이다라는 답을 포함하여 비교했을 경우 암호학 수업 후에는 75.86%의 학생이 수학이 실용적이라고 답하여 암호학 수업 전의 51.72%보다 훨씬 증가했다. 이는 암호학 수업 후 학생들에게 수학이 실용적이라는 인식이 강해졌음을 보여준다.

수학에서 실용적인 내용을 배우게 되면 흥미가 생길 것인가에 대해서는 보통이다라는 답을 포함하여 68.97%의 학생들이 그렇다고 답하여 수학교육이 실용적인 내용을 포함할 필요가 있음을 보여준다.

암호학 수업을 하기 전 암호에 대해 알고 있는 학생은 3.45%로서 암호학에 거의 대부분의 학생이 무지하다는 것을 알 수 있다.

암호학과 수학의 관련성에 관한 조사에서 암호학 수업 전에는 24.14%의 학생이, 암호학 수업 후에는 82.76%의 학생이 관련있다고 대답한 점으로 미루어 보아 암호학과 수학의 연관성에 관해서도 학생들이 잘 모르고 있었음을 알 수 있다.

암호학의 흥미성에 관한 조사에서 암호학 수업 전에는 13.79%의 학생이, 암호학 수업 후에는 24.14%의 학생이 암호학에 흥미가 있다고 답하였다. 암호학 수업을 하기 전 암호학에 대해 알고 있는 학생이 없는 가운데 조사한 것이므로 암호학 수업 전 13.79%의 학생이 암호학이 흥미롭다고 대답한 내용은 정확한 것이 아닐 수 있으나 암호 분야로 그 범위를 넓혀 결과를 이해한다면 암호학 분야에 관한 흥미도가 증가했다고 볼 수 있다. 또한 비록 많은 변화는 아니지만 수업 후 암호학에 대한 흥미도가 높아졌다는 것은 암호학 수업의 효과가 긍정적이라는 면을 반영하고 있다고 볼 수 있다.

암호학의 실용성에 관한 조사에서 암호학 수업 전에는 62.07%, 암호학 수업 후에는 82.76%로 수업 전이나 후나 전반적으로 암호학이 실용적이라고 생각하고 있었고 수업 후 좀 더 수치가 상승했음을 알 수 있다.

암호학을 배우면 수학공부에 도움이 될 것인가에 대해 수업 전에는 3.45%, 수업 후에는 34.48%의 학생이 도움이 된다고 생각했다. 이는 암호학 내용이 수학내용과 실제적으로 많은 관련성이 있고 또 암호학을 배움으로써 수학공부를 하는데 도움이 된다고 볼 수 있다.

암호학 수업 전 암호학에 대해 잘 알게 되면 수학공부가 흥미로울 것인가에 대해 보통이다라는 답을 포함하여 24.14%의 학생이 그렇다고 답하여 암호학을 통하여 수학과목에 대한 흥미 진전을 도모할 수 있는 가능성을 보여주었다.

암호학 수업 후 암호학을 통하여 수학공부에 흥미를 가지게 되었는가에 대해 10.34%의 학생이 그렇다고 답하였고 보통이다라는 답을 포함해서는 31.03%가 긍정적으로 답을 하였다. 이는 암호학을 통하여 수학공부에 흥미를 가지게 되었다는

점에서 중요한 결과라 할 수 있다.

암호학 수업 후 정보화 시대에 암호학이 필요한가에 대해 51.72%의 학생이 그렇다고 답해 암호학이 정보화 시대에 적합하며 시대에 맞는 교과서 내용이 이루어져야 함을 간접적으로 시시한 것이라 할 수 있다.

암호학 내용이 수학교육과정에 소개된다면 수학공부에 흥미가 있을까라는 조사에서는 암호학 수업전에는 13.79%만이, 암호학 수업 후에는 10.34%만의 학생이 긍정적으로 답하여 암호학이 수학교육과정에 소개되어도 수학과목에 대한 흥미도가 증가함을 뚜렷이 볼 수는 없었다.

본 설문지 조사 결과 암호학 수업을 듣기 전에는 암호학에 대해서는 잘 알지 못하고 수학과목은 실용적이지 못하며 흥미가 없다고 생각하는 경향이 강했으나 암호학 수업을 들은 후에는 암호학과 수학이 밀접한 관계에 있고 암호학 내용이 흥미가 있으며 또한 수학도 실용적인 과목이라는 인식의 변화를 가져왔다. 또한 암호학 수업을 듣기 전 암호학에 대해 잘 모르는 관계로 암호학 내용이 수학교육과정에 소개되는데 대해서 그다지 관심이 없었으나 암호학 수업을 들은 후에는 현대 정보화 사회에 맞는 실용적인 내용인 암호학이 수학교육과정에 소개되는 데 긍정적으로 생각하는 학생들이 늘었다. 따라서 암호학 내용을 재량활동 시간등을 이용하여 소개시켜 수학공부의 흥미를 유발시키고 변화하는 현대 사회에 맞는 실용적인 수학교육의 밑거름이 되게 할 수 있다는 가능성을 보게 되었다.

Ⅵ. 결론 및 제언

본 논문에서는 비교적 초보적인 수학지식으로 쉽게 이해가 가능한 암호이론을 역사적 배경과 기초적인 수학 이론으로 학생들의 흥미를 유발시켜 암호이론의 중요성과 필요성을 말하고 있으며 암호에서 사용되는 수학 이론을 바탕으로 중등수학 교육과정과 관련된 내용을 파악하였다.

첫째, 중등학교 학생들이 암호학 분야를 접해봄으로써 수학이 얼마나 우리 생활과 밀접한가를 체험할 수 있을 것이다. 또한 정보화 시대에 정보보호의 중요성에 대한 인식을 심어주고 수학 과목에 대한 흥미를 유발시킬 수 있다는 점에서 수학교육에서 암호학 내용의 도입은 의미있다고 생각된다.

둘째. Ceasar 암호 체계와 아핀 암호 체계는 평문작성에 사용되는 문자 전체의 집합이 적당한 정수 m에 대하여 $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$과 일대일 대응되는 것으로써 교과 과정 중에서는 중학교 수학의 수와 연산, 문자와 식, 함수 단원에 적용이 될 수 있다. Hill 암호체계는 암호화하는 과정에서의 행렬의 곱, 역행렬의 존재성 여부파악, 역행렬 구하기 등은 교육과정 중 '수학Ⅰ'과 '기하와벡터'의 일차변환과 행렬에 적용될 수 있다. 그리고 복호화 과정에서는, 중학교 학생들에게는 교과과정 상 역함수를 사용할 수 없으므로 자연스러운 역사고 과정을 통해 지도해야 할 것이다.

셋째, 수학의 다른 분야와 마찬가지로, 암호학 또한 여러 분야의 아이디어를 모아놓은 집합체이다. 암호는 앞에서 살펴 보았듯이 수학 이론 기반 위에서 개발되고 있다. 이러한 암호학을 중등수학에 도입하기 위해서는, 암호학의 내용을 초등화하고 적당한 도입시기를 결정하는 교사의 노력이 필요하다 하겠다.

넷째, 암호체계는 보다 알아보기 어렵고 효과적으로 메시지를 변형하는 방법, 즉 암호화하는 방법을 연구하는 부분(cyptography)과 주어진 한정된 정보 아래서 킷값을 모른 채 암호문을 복호화하는 부분(cryptanlysis)으로 구성되어 하나의 학문인 암호학(cryptology)을 이루고 있다. 현대의 암호이론은 수준 높은 수학의 전반적인 이론을 이용하기 때문에 수학을 깊게 공부하지 않은 사람은 이해하기 어렵다.

인지적 자극은 흥미를 갖게 하고 동기유발을 할 수 있게 한다. 또한 동기유발은 학습효과를 상승시킨다. 이에 암호체계를 창의적 재량활동이나 교과 심화학습에 활용해 봄으로써 학생들의 수학 학습에 대한 인식을 개선하고 흥미와 실생활에 필요성을 느끼며 동기 유발이 되었음을 알 수 있었다. 이에 더 나아가 미래 사회를 준비하는 학생들이 문제해결 능력을 기를 수 있기를 바란다.

참고문헌

[1] 김미정. “중등수학에서의 암호학 지도법 연구” 교육학 석사학위논문, 전남대학교, 2002.
[2] 김영미. “중고등 교육과정에서의 정수이론과 현실에의 응용” 교육학 석사학위논문, 한남대학교, 2003.
[3] 김희원. “암호학에 관한 연구” 교육학 석사학위논문, 신라대학교, 2005.
[4] 노은영. “중고등학생을 위한 교재 개발 연구” 교육학 석사학위논문, 고려대학교, 2003.
[5] 박승안·김응태. 『정수론』5판, 경문사, 2002.
[6] 박형빈. 『수학은 생활이다』, 경문사, 2002.
[7] 송정은. “이차곡선을 이용한 암호체계”, 교육학 석사학위논문, 성균관대학교, 2005.
[8] 유동환. “중등수학교육과정에서의 암호학과 부호이론 교육에 대한 연구” 교육학 석사학위논문, 단국대학교, 2006.
[9] 이명구. “중등학교 수학교과에서 암호학 도입을 위한 교재 구성방안 모색” 교육학 석사학위논문, 건국대학교, 2000.
[10] 이선영. “고등학교 수학교육과정에의 암호학의 도입가능성에 관한 연구 -RSA알고리즘을 중심으로-” 교육학 석사학위논문, 대전대학교, 2003.
[11] 이현민. “중등교육과정에서의 암호이론 적용” 교육학 석사학위논문, 부산외국어대학교, 2010.
[12] 장은성. 『네트워크 사회의 에티켓 암호학』, 전파과학사, 1999.
[13] 정효정. “정수에 관한 기본개념과 정리를 활용한 암호체계” 교육학 석사학위논문, 동국대학교, 2007.
[14] 황혜정 외 5인. 『수학교육학신론』,문음사, 2002.

부록1 교수-학습지도안

단원	Ceasar 암호			차시	1/2
수업목표	· 평문을 암호문으로 바꿀 수 있다.				
단계	수업내용	교수·학습 활동		시간(분)	자료 및 지도상의 유의점
		교사	학생		
도입	◈인사 ◈출석확인	◈인사 ◈학생의 이름을 호명하여 출석여부를 확인한다.	◈인사 ◈선생님이 호명하면 손을 들면서 크게 대답한다.	1분	◈학생과 선생이 함께 동시에 인사한다.
	◈수업목표 제시	◈수업목표를 제시한다.	◈수업목표를 다같이 읽는다.	1분	
전개	◈암호이론의 배경설명	◈암호이론에 대한 소개를 한다.	◈설명을 듣는다.	8분	
	◈조별활동	◈ "I am a student"와 암호문을 제시한다. ◈ "Dreams come true"를 암호문으로 고친다.	◈제시된 암호화의 원리를 추측하고 이를 적용하여 "Dreams come true"를 암호화 한다.	10분	◈ 학생 스스로 하도록 유도한다.
	◈토론 및 발표	◈암호문을 보고 각 조별로 토론한다.	◈조원과 암호문을 보고 얘기한다. ◈조원과 토론한 내용을 각 조의 조장이 발표한다.	5분	
	◈개념정리	◈평문을 암호문으로 바꾸는 원리에 대한 내용을 ppt화면으로 보여준다. ◈조별활동 내용과 연관하여 설명한다.	◈질문에 대답하면서 암호화 원리에 대한 개념을 이해한다.	10분	◈중간에 학생들에게 간단히 질문을 던져 주의를 환기시킨다.
	◈문제 풀이	◈문제 1 "Good luck to you"를 암호문으	◈문제 1번을 풀어본 후에 한 명이 나와서 발표를 하고 나머지 학생들은	7분	◈ 학생들이 문제를 풀 때 지나다

		로 바꾸어라. ◈문제 2 “Boys be ambitious”를 암호문으로 바꾸어라.	경청한다. ◈문제 2번을 풀어본 후에 한 명이 나와서 발표를 하고 나머지 학생들은 경정한다.		니면서 모르는 학생은 개별적으로 지도한다. ◈한 명의 학생이 나와서 발표할 때 나머지 학생들이 경청할 수 있도록 한다.
정리	◈수업 총 정리	◈평문을 암호문으로 바꾸는 방법을 총 정리한다.		1분	◈파워포인트 자료제시
	◈다음 학습 내용 소개	◈암호문을 평문으로 바꾸는 방법		1분	◈너무 장황한 설명이 되지 않도록 주의한다.
	◈정리, 인사	◈인사를 하고 수업을 마친다.	◈인사를 한다.	1분	

단원	Ceasar 암호			차시	2/2
수업목표	· 암호문을 평문으로 바꿀 수 있다.				
단계	수업내용	교수·학습 활동		시간(분)	자료 및 지도상의 유의점
		교사	학생		
도입	◈인사 ◈출석확인	◈인사 ◈학생의 이름을 호명하여 출석여부를 확인한다.	◈인사 ◈선생님이 호명하면 손을 들면서 크게 대답한다.	1분	◈학생과 선생이 함께 동시에 인사한다.
	◈수업목표제시	◈수업목표를 제시한다.	◈수업목표를 다같이 읽는다.	1분	
	◈전시학습 복습	◈ "I am a student"를 암호문으로 바꾸어라.	◈질문에 대한 답을 한다.	1분	◈파워포인트 자료 제시
전개	◈조별활동	◈"ldpdvwxghq"가 무엇을 의미하는지 평문으로 바꾸어 본다. ◈“guhdvfrphwuxh"가 무엇을 의미하는지 평문으로 바꾸어 본다.	◈복호화 원리를 추측하고 이를 적용하여 해석한다.	10분	◈ 학생 스스로 하도록 유도한다.
	◈토론 및 발표	◈암호문을 보고 각 조별로 토론한다.	◈조원과 평문을 보고 얘기한다. ◈조원과 토론한 내용을 각 조의 조장이 발표한다.	5분	
	◈개념정리	◈평문을 암호문으로 바꾸는 원리에 대한 내용을 ppt화면으로 보여준다. ◈조별활동 내용과 연관하여 설명한다.	◈질문에 대답하면서 복호화 원리에 대한 개념을 이해한다.	10분	◈중간에 학생들에게 간단히 질문을 던져 주의를 환기시킨다.
	◈문제 풀이	◈문제 1	◈문제 1번을 풀어본 후	7분	◈학생들이

		“jrrgoxfnwrbrx”를 평문으로 바꾸어라. ◈문제 2 “erbvehdoelwlrxv”를 평문으로 바꾸어라.	에 한 명이 나와서 발표를 하고 나머지 학생들은 경청한다. ◈문제 2번을 풀어본 후에 한 명이 나와서 발표를 하고 나머지 학생들은 경정한다.		문제를 풀 때 지나다니면서 모르는 학생은 개별적으로 지도한다. ◈한 명의 학생이 나와서 발표할 때 나머지 학생들이 경청할 수 있도록 한다.
	◈수학적 표현	◈암호화 및 복호화 과정을 함수와 관련하여 설명한다.	◈질문에 대한 답을 하며 경청한다.	7분	
정리	◈수업 총 정리	◈평문을 암호문으로 바꾸는 방법을 총정리한다.		1분	◈ 파워포인트 자료 제시
	◈다음 학습 내용 소개	◈암호문을 평문으로 바꾸는 방법		1분	◈너무 장황한 설명이 되지 않도록 주의한다.
	◈정리, 인사	◈인사를 하고 수업을 마친다.	◈인사를 한다.	1분	

부록2. 설 문 지

A. 암호학 수업을 듣기 전

1. 수학과목에 흥미가 있는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

2. 수학이 실용적인 학문이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

3. 수학에서 실용적인 내용을 배우게 된다면 흥미가 더 생길 것 같은가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

4. 암호에 대해 알고 있는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

5. 암호학과 수학이 관련 있다고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

6. 암호학은 흥미로운 내용이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

7. 암호학은 실용적이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

8. 암호학을 배우면 수학공부에 도움이 될 것이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

9. 암호학에 대해 잘 알게 되면 수학공부가 더 흥미로울 것이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

10. 암호학 내용을 수학교육과정에 소개해야 한다고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

B. 암호학 수업을 들은 후

1. 수학과목에 흥미가 있는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

2. 수학이 실용적인 학문이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

3. 암호학과 수학이 관련있다고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

4. 암호학 내용에 흥미가 있는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

5. 암호학 내용이 실용적이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

6. 암호학을 통하여 수학공부에 흥미를 가지게 되었는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

7. 정보화 시대에 암호학은 필요하다고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

8. 암호학 내용이 실제 수학수업을 하는데 있어 도움이 되는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

9. 암호학 내용이 수학교육과정에 소개된다면 수학공부를 하는데 흥미가 더 있을까?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다

10. 수학교육과정에 암호학 내용을 포함하는 것은 정보화 시대에 부응하는 것이라고 생각하는가?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 그렇지 않다 ⑤ 매우 그렇지 않다