한국학교수학회논문집 제 12 권, 제 3 호
Journal of the Korean School Mathematics Society
Volume 12, Number 3, 231-245, September 2009

상업 정보 계열 고등학교 암호 교육 프로그램 개발 및 적용에 관한 연구*

박중수1) · 정상조2)

본 논문은 암호 및 정보보호와 관련된 내용들을 상업 정보 계열 고등학교 학생들에게 소개하고자 할 때, 사전에 학생들의 정보화 수준 및 암호와 정보보호의 이해에 대한 실태를 파악하고, 제7차 수학과 교육과정과 2007 개정 수학과 교육과정 및 상업 정보 계열 고등학교 전문 교과 교육과정을 검토하여 수학 교과와 전문 교과 사이의 연관성을 파악함으로써, 상업 정보 계열 고등학교에서 수업 시간에 활용할 수 있는 교재를 개발하고 이를 실제 수업에 적용한 결과에 대한 분석이다. 개발된 교재를 사용하여 상업 정보 계열 고등학교 학생들에게 암호 기초 이론을 강의하고 관련 알고리즘을 프로그래밍 언어를 사용하여 프로그래밍하게 한 결과 암호 학습이 수학학습의 동기 유발은 물론이고 수학 교과와 전문 교과 사이의 매개역할을 할 수 있는 것으로 조사되었고, 이러한 결과를 토대로 프로그래밍 실습을 포함한 암호 학습을 제7차 수학과 교육과정의 '실용수학' 또는 2007 개정 수학과 교육과정의 '수학의 활용'에 추가할 것을 제안하였다.

주요용어 : 정보보호, 암호, 수학과 교육과정, 상업 정보 계열 전문 교과 교육과정

I. 서 론

1. 연구의 필요성 및 목적

21세기는 지식 기반 정보화 사회로 특징지워지며, 이에 적합한 교육은 단순 기능인의 양성보다는 자기 주도적으로 지적 가치를 창조할 수 있는 자율적이고, 창의적인 인간의 육성에 그 중점을 두어야 한다(교육인적자원부, 1997). 이에 대비하기 위한 수학과의 역할은 수학의 기본적인 지식과 기능을 습득하고, 수학의 기본적인 개념, 원리, 법칙을 토대로 탐구하고 예측하여 실생활의 여러 가지 문제를 합리적으로 해결하며, 창의적인 문제 해결력을 배양시키는 데에 있다. 2007 개정 수학과 교육과정에서는 문제해결력과 더불어 제반 고등 사고 능력을 포함하는 '수학적 힘(mathematical power)'의 신장을 목표로 하고 있는데, 여기서

* 이 연구는 2005년도 한국학술진흥재단 퓨처코리아 지원 사업에 의한 것임.

1) 우석대학교 (jspark@woosuk.ac.kr)
2) 목원대학교 (math888@paran.com)

수학적 힘이란 창의적 사고력, 논리적 사고력, 비판적 사고력, 문제 해결 능력, 추론 능력, 의사소통 능력, 수학에 대한 자신감과 긍정적인 태도, 수학과 인접 학문과의 관련성 및 수학의 유용성 인식 등을 포함하는 포괄적인 개념이라고 볼 수 있다(교육인적자원부, 2007).

암호 학습은 이러한 21세기 정보화 사회에 대비할 수 있게 정보보호에 대한 안목을 넓혀 주고 수학적 이론과 이를 현실문제에 적용한 실제 문제를 다루게 함으로써 수학적 이론의 중요성을 인식하고, 이론과 실제 문제 사이의 간격을 좁혀 주며, 프로그래밍 활동을 통하여 창의적이고, 논리적이며, 비판적인 사고력과 추론 능력, 수학에 대한 자신감을 배양할 수 있는 장점이 있다. 정보보호의 중요성과 필요성을 인식하는 데 있어서 암호 알고리즘의 이해는 필수적인 것이며, 알고리즘의 구현을 통하여 논리적 사고력의 신장과 문제해결력을 기를 수 있는데 적절할 것이다. 암호 알고리즘의 이해는 학교수학과도 밀접하게 관련이 있는 바, 예를 들어 함수, 치환, 정수론에서 합동, 소수, 소인수분해, 행렬, 확률 등 학교수학의 다양한 분야가 사용됨으로써 학교수학의 의미를 더 발전시킬 수 있다(노은영 2003; 이병구, 2000; 임정현, 2007).

본 연구는 상업 정보 계열 고등학교에서 학생들의 암호에 대한 이해와 암호 알고리즘의 프로그래밍화를 통하여 수학교육의 개선을 꾀하고자 하는 데 목적이 있으며, 이를 위해서 새로운 교재의 개발과 실제 수업 적용에 대한 연구이다.

2. 연구 내용 및 방법

본 연구는 완주군 소재의 한 상업 정보 계열 고등학교에서 '정보화 사회에서 암호의 이해와 활용'이라는 주제를 가지고 주당 2시간씩 2학기(1년) 동안 진행된 것이다. 본 연구는 2005 한국학술진흥재단의 퓨쳐코리아 지원사업의 하나로 선정되어 진행된 것으로 사교육의 사각지대에 있는 읍·면 단위 학생들에게 대학이나 실험실의 첨단 연구 결과들을 소개함으로써 창의적이고 미래 지향적인 인재를 양성하는 데 목적이 있다. 사업에 참여할 지도교사를 선정하고, 그 지도교사가 지도하고 있는 특별활동반인 '사무자동화반'을 대상으로 하였다. 사업 개시 전에 해당 학교를 방문하여 학생들의 특별활동 상황을 점검하였고, 교육과정과 교과목들을 파악하였다. 또 개별 면담을 통하여 정보보호나 암호 및 암호화 알고리즘의 구현에 대한 학생들의 기대와 동기를 청취하였으며, 교재를 집필하기 전에 사전 설문조사와 간단한 기초 수학 능력을 테스트하였다. 사전 설문조사를 통하여 학생들의 정보보호나 암호에 대한 인식도, 암호 알고리즘의 구현을 위한 학생들의 준비도, 암호 이론과 수학 교과 내용, 그리고 전문 교과 내용과의 관련성을 조사하였다.

개발된 교재를 사용하여 매주 두 시간씩(2학점) 두 학기(한 학기 15주), 62시간 동안 암호 학습을 위한 기초 수학과 고전암호, 블록암호, 현대암호의 기본적인 알고리즘을 강의하였으며, 학생들이 암호 알고리즘을 프로그래밍 언어를 사용하여 구현하게 하였다. 사용된 프로그래밍 언어는 자바스크립트를 사용하였으며, 각 개인의 프로그램을 인터넷 상에 공개하고 토론하였다. 62시간의 강의 시간 동안 이론과 실습을 1대 3정도의 비율로 진행하였다. 학생들은 강의를 통하여 정보보호의 필요성과 방법, 암호시스템의 전반적인 이해와 고전암호, 블록암호, 스트림 암호, 현대 암호의 기본적인 알고리즘을 학습하였다.

본 연구는 암호의 원리와 방법을 이해하고 구현하는 것이 상업 정보 계열 학생들의 수학 학습과 동기 유발에 긍정적인 효과를 끼치는지, 상업 정보 계열 교육과정 상에서 수학 교과와 전문 교과목 사이의 연관성을 확보하고 수학 교과뿐만 아니라 전문 교과목의 학습에도

도움이 되는지 살펴보았다.

Ⅱ. 이론적 배경

1. 수학 학습·지도와 컴퓨터 프로그래밍

(1) 수학적 지식과 컴퓨터 프로그래밍

수학적 지식은 개념적 지식과 절차적 지식으로 분류할 수 있는데, 개념적 지식은 해당 주제의 주변 관련성을 풍부하게 함유하고 있는 지식으로, 관련된 지식 사이에 존재하는 관계망 자체에 대한 지식이라고 할 수 있다. 절차적 지식은 수학의 형식적 언어로 표현된 알고리즘, 규칙 등으로 구성되며, 절차적 지식을 소유하였다는 말은 수학의 아이디어를 표현하는 기호 자체와 이 기호 사용의 규칙에 익숙해져 있음을 의미한다. 수학의 학습·지도에서 개념적 지식의 지도가 바람직하다고 볼 수 있으나, 절차적 지식이라 하더라도 각 수학적 과제를 순서적으로 처리하는 동안 주변 지식과 관계를 형성하면서 절차를 수행하면 유의미한 학습이 될 수 있다(Hiebert & Lefevre, 1986). 한편 절차적 지식의 학습이 유의미한 학습이 되기 위해서 강옥기(2006)는 다음과 같은 단계를 제시하고 있다. 첫째 학습의 주제와 목표를 제시하여 학습 의욕을 갖게 하는 도입 단계와 둘째 지도하고자 하는 수학적 기능의 실행 순서를 제시하는 기능 제시 단계, 셋째 지도하고자 하는 기능의 알고리즘을 잘 이해할 수 있도록 사용된 용어들과 기능들에 대한 정확한 설명 단계, 넷째 제시된 알고리즘의 타당성을 확인하는 단계이다. 타당성의 확인에는 설명된 알고리즘의 분석을 통한 연역적 타당성 확인(deductive justification)과 프로그램의 결과를 확인하는 실제적 타당성 확인(pragmatic justification)이 있다. 마지막으로 연습의 단계가 있다. 연습 단계에서는 맹목적이며 기계적인 연습이 되지 않도록 학생들의 활동에 대한 토론과 즉각적인 피드백을 제공하는 것이 바람직하다(강옥기, 2006).

암호이론은 수학 이론과 알고리즘으로 구성되어 있으므로 수학적 지식에서 개념적 지식과 절차적 지식을 모두 포함한다고 볼 수 있다. 학생들은 암호 알고리즘을 프로그래밍하고 결과를 확인하는 활동을 통해서 수학의 절차적 지식을 습득할 뿐만 아니라 배경이 되는 수학의 개념적 지식에 대하여 반성하고 피드백하는 과정을 거치게 됨으로써 수학 학습을 유의미한 학습으로 이끌 수 있다.

(2) 문제해결과 컴퓨터 프로그래밍

하나의 프로그램을 완성하기 위해서는 알고리즘을 이해하고, 목표를 인식하고, 프로그램을 설계하며, 작성하고 실행을 해야 한다. 또 프로그램을 실행한 후에는 결과를 확인하고 오류를 수정하고 보다 효율적인 프로그램이 가능한지 검토해야 한다. 이러한 단계는 Polya가 말하는 문제해결의 단계, 즉 문제의 이해, 계획, 실행, 반성의 단계와 유사하다고 볼 수 있다. 이는 Bloom과 Scheon(1988)의 연구에서도 확인되는 바, 이들은 프로그래밍의 학습 경험이 문제해결에 미치는 영향에 대한 연구에서 프로그래밍을 학습한 학생들은 그렇지 않은 학생들보다 체계적인 시도를 많이 하였으며, 그들은 답을 더 많이 검토하고 잘못된 부분을 교정한 것으로 나타났다(신동선·류희찬(1998), 재인용). 이와 같은 결과가 나타난 이유는 프로그래밍에서 사용했던 과정들이 문제해결로 전이된 것으로 설명되어진다고 볼 수 있다.

학생은 컴퓨터 프로그램을 작성하기 위해서 주어진 문제를 완전히 파악한 후, 순서도를 작성하고, 그에 따라 프로그래밍은 구체적이면서도 논리적으로 구성해야 하되 그 표현 또한 정확해야 하는데, 이러한 과정은 수학적 사고를 요구하며, 문제해결 과정과도 유사하다. Clement(1986)는 프로그래밍 학습의 결과를 평가하는 실험에서, 프로그래밍을 통해 특정 인지 및 메타인지 능력과 창의성의 측면에서 수행능력이 증가함을 확인할 수 있었다. 컴퓨터 프로그래밍을 하는 과정은 문제해결 과정의 모든 면을 연습하는 창조적이고 발명적인 활동이며, 프로그래밍 활동은 문제해결에 대한 실험적 방법을 촉진시키며, 프로그래밍 언어의 사용은 학생들에게 자연적 구조(natural framework)와 기본적인 어휘(standard vocabulary), 수학을 토론하게 하는 개인적 경험들을 제공한다고 주장하였다(류희찬 · 배은희(2000), 재인용).

Shumway(1984)는 특정한 수학 학습내용을 프로그래밍 활동을 통하여 지도하였을 때 얻어지는 잠재적 효과를 컴퓨터 소양(Computer Literacy), 특수한 수학적 개념(Specific Mathematics Concepts), 일반적 수학적 개념(General Mathematics Concepts), 수학적 사고(Mathematical thinking), 문제해결(Problem solving), 논리적 추론(Logical Reanoning)의 여섯 가지로 들고 있다. 즉 프로그래밍 활동을 통해서 문제해결력뿐만 아니라 컴퓨터 하드웨어에 대한 소양을 가질 수 있으며, 수학적 사고와 수학적 개념의 습득은 물론이고 논리적 추론 능력과 같은 고등 사고 능력의 배양도 습득될 수 있다(류희찬 · 배은희(2000), 재인용). 이러한 컴퓨터 프로그램 학습의 효과들은 상업 정보 계열 고등학교에서 전문 교과목의 학습과 연결될 수 있다.

(3) 수학적 태도 개선과 컴퓨터 프로그래밍

수학교육의 목적은 수학적으로 사고하는 능력과 태도를 개발하는 것이라고 볼 할 수 있다(우정호, 2001). 학생들은 학습해야 할 개념들이 포함되어 있거나, 출력에 그러한 개념들이 나오는 프로그램들을 작성하고 실행할 때에 학습이 더 잘 될 수 있고, 프로그래밍 과정에서 특수한 수학적 개념을 학습할 수 있는 것으로 알려져 있다. 또 컴퓨터의 시각적, 조작적 기능은 학생들로 하여금 수학 학습 내용이 구체적인 경험이나 자기 통제 하에 이루어짐으로써 수학에 쉽게 접근할 수 있게 해준다. 학생들은 컴퓨터 프로그램을 통해서 일반화와 추측하기, 오류수정 등 수준 높은 인지과정을 학습할 수 있다. 분석, 단순화, 특수화, 일반화, 정의, 추측, 구조화 등의 과정은 학생들이 효과적인 프로그래밍 활동을 통해 향상될 수 있다. 모든 프로그래밍 언어들은 논리의 기본 개념 위에 기초한다. 프로그래밍 활동은 학생들에게 풍부한 논리적 추론의 경험을 제공하고, 프로그램 언어 안에 있는 고유의 논리적 원리를 가르칠 수 있다.

또 프로그래밍 과정에서 필연적으로 수반되는 오류수정 활동을 통해 수학적 태도를 개선시킬 수 있다. 오류수정은 프로그래밍상의 문제점을 개선해 나아가는 과정으로 오류수정을 하지 않는 프로그래밍 과정은 생각하기 힘들다. 왜냐하면, 한 프로그램이 논리적으로 틀린 점이 없다고 해도 그 보다 개선된 프로그램은 얼마든지 존재할 수 있기 때문이다. 따라서 컴퓨터 문화에서는 완벽한 지식이나 완전히 틀린 지식은 존재하지 않는다. 프로그래밍이 수학교육에 도입되면 학생들의 오류에 대한 부담이 없어지므로 수학에 대한 태도를 개선시킬 수 있다. 학생은 컴퓨터 프로그래밍을 함으로써, 컴퓨터에 대해 매우 강력한 감각이 획득되고, 수학의 사고방식과 매우 친근해진다(신동선 · 류희찬, 1998).

(4) 자바스크립트

자바스크립트(JavaScript)는 객체 기반의 스크립트 프로그래밍 언어이다. 스크립트(Script) 언어란 컴퓨터 프로세서나 컴파일러가 아닌 다른 프로그램에 의해 번역되고 수행되는 명령문의 집합을 말한다. 자바스크립트는 본래 넷스케이프 커뮤니케이션즈사의 브렌단 아이히(Brendan Eich)에 의해 처음에는 모카(Mocha)라는 이름으로, 나중에는 라이브스크립트(LiveScript)라는 이름으로 개발되었으며, 최종적으로 자바스크립트가 되어 1996년 2월에 발매한 월드 와이드 웹 브라우저인 넷스케이프 내비게이터 2.0에 실장되었다. 현재의 자바스크립트는 HTML 문서 내에 '<SCRIPT>'라는 태그 안에 삽입되어 웹브라우저에서 실행된다.

자바스크립트는 썬 마이크로시스템즈의 자바와 구문(syntax)이 유사한 점이 많으나 두 언어는 직접적인 관련은 없다. 자바스크립트는 자바 언어에 비하여 한정적인 객체와 메서드를 가지고 있기 때문에 인터넷 게임과 같은 복잡한 프로그램을 만들기에는 부족하나, 객체가 단순화되어 있고 학습하기 쉽다. 또한 자바스크립트는 다양한 수학적 조작 활동을 수행하는 데 필요한 명령어와 내장 객체를 가지고 있다. 자바스크립트는 별도의 컴파일을 하지 않아도 되므로 빠르게 작성하고 결과를 확인할 수 있다. 예를 들어, 웹상에서 HTML 문서 내에 <SCRIPT>와 </SCRIPT> 태그 사이에 자바스크립트 코드를 삽입하거나, 자바스크립트로 작성된 코드인 '*.js'를 호출하여 사용한다. 자바스크립트는 대화상자를 지원하므로 웹상에서 대화형 프로그램을 작성할 수 있다. 자바스크립트는 각종 제어문을 지원하므로 구조적 프로그래밍이 가능하며, 이는 차후의 프로그래밍 습관을 기르는 데 손색이 없는 구조화된 프로그래밍 언어임을 의미한다. 또 프로그래밍 작성 시 하드웨어에 대한 깊은 지식을 요하지 않고, 일상적으로 사용하는 언어와 유사한 언어로 구성되어 있으며 프로그램의 수정이나 보완이 대단히 용이한 고급 프로그래밍 언어이다. 자바스크립트는 절차적이며 기능단위 언어이다. 절차(procedure)란 일련의 명령어들을 모아 이름을 붙여 만든 것으로, 그 이름이 프로그램 내에서 새로운 명령어로 사용될 수도 있다. 자바스크립트에서 사용된 절차는 또 다른 절차 내에서 사용될 수 있으며, 이러한 절차들을 모아 기능단위(module)로 결합시킬 수 있다. 결론적으로 자바스크립트는 구조적 프로그래밍을 지원하는 객체지향 고급 프로그래밍 언어이다.

2. 상업 정보 계열 고등학교 교육과정

상업 정보 계열 고등학교는 지식 기반 정보화 사회에서 요구되는 자기 주도적 학습 능력과 직업 기초 능력을 기르고, 상업 분야의 실무 능력을 함양하며, 계속적인 전문 교육을 통하여 더 많은 지식과 정보를 습득할 수 있는 기반을 마련하는 데 교육의 중점을 두는 직업 교육 기관이다. 상업 정보 계열 고등학교 교육의 목적은 상업 정보 관련 분야의 기초 지식과 실무 능력을 함양하고, 평생에 걸쳐 전문 교육을 이수하는데 필요한 기초 학습 능력을 배양하는 데 있다. 이러한 목적을 달성하기 위하여 상업 정보 계열 고등학교 교육의 성격은 상업 정보 관련 분야에 취업이나 창업을 하는 데 필요한 기초 지식과 실무 능력을 배양하거나, 상급 학교에 진학하여 전문 교육을 이수함으로써 동일 분야에 기여할 수 있는 전문 인력을 양성하는 데 있다(교육인적자원부a, 1997).

제7차 수학과 교육과정에서 상업 정보 계열 학생들이 선택하는 '실용수학'은 10단계 수학의 도달 여부에 관계없이 학생들이 실생활에 필요한 수학을 학습하기 위하여 선택할 수 있

는 과목으로서, 수학의 기본적인 개념, 원리, 법칙을 활용하여 일상생활에서 일어나는 여러 가지 문제를 수학적으로 사고하고 합리적으로 해결하는 능력과 태도를 기르게 하는데 목적이 있다. '실용수학'의 내용은 수학의 실용적 측면을 강조하여 계산기와 컴퓨터, 경제생활, 생활 통계, 생활 문제 해결 등의 4개 영역으로 하고, 10단계 이하 수준의 수학 내용을 바탕으로 수학의 실용성을 인식할 수 있는 다양한 생활문제를 소재로 하여 쉽고 흥미롭게 학습할 수 있도록 구성되어 있다(교육인적자원부b, 1997).

2007 개정 수학과 교육과정에서 '수학의 활용'은 "국민공통 기본교육 기간인 고등학교 1학년까지의 수학을 학습한 학생이면 선택할 수 있는 과목으로, 실생활에 필요한 수학적 지식과 기능을 습득하도록 하는 데 적합하다. '수학의 활용'의 학습을 통하여 실생활의 여러 가지 문제를 수학의 관점에서 이해하고 합리적으로 해결하는 능력을 신장시키며, 수학에 대한 관심과 흥미를 길러 수학에 대한 긍정적인 태도를 기를 수 있다."로 되어 있다. '수학의 활용'의 내용은 '명제와 논리', '지수와 로그', '수열', '확률과 통계', '도형과 그래프'의 영역으로 구성된다(교육인적자원부b, 2007).

제7차 상업 정보 계열 고등학교 전문교과 교육과정에는 모두 32개의 교과목이 제시되어 있으며, 이들 교과목 중에서 암호 또는 정보보호와 관련된 내용이 언급된 단원을 포함하고 있는 교과는 단 한 개의 교과목인 '전자 계산 실무(상-16)'이며, (바) 컴퓨터 보안과 윤리 단원에서 (1) 이용자의 윤리 (2) 저작권 보호 (3) 컴퓨터 범죄 (4) 컴퓨터 보안 정도로 다루고 있다. 그러나 2007년 개정된 상업 정보 계열 전문 교과 교육과정에서는 다음 <표 1>에서와 같이 7개 교과목에 걸쳐 언급된다. 이는 개정된 교육과정에서 암호 및 정보보호의 중요성이 매우 증대된 결과로 보인다.

<표 1> 암호 또는 정보보호와 관련 단원이 포함되어있는 교과목

과목		단원명	내용
과목 번호	과목명		
상-2	컴퓨터 일반	가. 정보 사회	(1) 정보와 지식 (2) 정보 통신 윤리 (3) 정보 보호 (4) 정보 기기의 활용 전망
상-7	경영 정보 시스템	나. 경영 정보 시스템의 기술 기반	(1) 하드웨어 및 소프트웨어 (2) 네트워크 구성 및 관리 (3) 데이터베이스 관리 (4) 보안
상-20	자료 처리	라. 데이터베이스	(1) 데이터베이스의 구조 (2) 데이터베이스의 관리 (3) 데이터베이스의 보안
상-23	사무 관리 실무	라. 정보 통신	(1) 정보 검색 (2) 정보 교환 (3) 정보 보안

상-28	전자 상거래 일반	마. 전자 상거래 운영 및 관리	(1) 상품 구매 및 판매 관리 (2) 물류 관리 (3) 전자 결제 시스템 (4) 전자 상거래 보안과 전자 인증 (5) 전자 상거래 고객 관리
상-29	인터넷 쇼핑몰 관리	마. 전자 결제 및 보안	(1) 신용 카드 (2) 전자 수표 (3) 전자 화폐 (4) 전자 상거래 보안
상-30	전자 상거래 실무	마. 전자 상거래 관련 기본법과 문제 해결	(1) 전자 거래 기본법 (2) 전자 상거래 등에서의 소비자 보호에 관한 법률 (3) 전자 서명법 (4) 전자 상거래 윤리

Ⅲ. 본론

1. 교육 대상에 대한 기초 조사

교육 대상 학생은 전북 완주군 소재 한 고등학교의 상업 정보 계열 1~3학년 여학생 18명(1학년 10명, 2학년 6명, 3학년 2명)이다. 학생들의 기초수학에 대한 수준을 알아보기 위하여 유리수의 사칙계산과 정수에서 소인수분해, 일차방정식의 해에 대한 간단한 테스트를 실시하였으나(<표 2>) 결과는 매우 미흡하며 기초적인 유리수의 연산 능력도 부족한 것으로 나타났다. 따라서 교재 구성과 수업 진행에서 암호 이론의 기초가 되는 수학을 강의할 필요가 있다.

<표 2> 학생들의 기초수학에 대한 수준

문제	정답율	오답율
$\frac{1}{2}+\frac{1}{3}$를 계산하시오.	38.9%(7명)	61.1%(11명)
$x+5=7$을 푸시오.	77.8%(14명)	22.2%(4명)
24의 약수를 구하시오.	33.3%(6명)	66.7%(12명)
120을 소인수분해하시오.	0.0%(0명)	100.0%(18명)
30보다 작은 소수를 모두 구하시오.	0.0%(0명)	100.0%(18명)

컴퓨터 사용과 프로그래밍에 대한 설문조사에서 학생들은 일주일에 3~4일 하루 2~3시간 정도 컴퓨터를 사용하지만 학습을 위해서라기보다는 주로 인터넷 검색을 위해서 사용하는 것으로 나타났다. 여학생들이어서 컴퓨터 게임 시간은 그리 많지 않다.

프로그래밍 가능 여부에 대한 조사에서는(<표 3>) 2~3학년의 경우프로그래밍 경험이 있지만 자신의 수준을 '하'라고 생각하고 있다. 1학년의 경우 프로그래밍 경험이 없다. 기초적

인 수학 계산과 개념이 부족하고 프로그래밍에 대한 자신감이 없는 경우에 학생들에게 기초적인 수학적 지식과 프로그래밍 언어 교육은 필수적이지만 학생들의 자신감을 키우기 위해서, 또 학생들이 앞으로 구조적 프로그래밍에 익숙해지고 다양한 제어문을 이해하기 위해서도 순서도를 강의하는 것이 효과적이라 생각된다.

<표 3> 프로그래밍 가능 여부에 대한 조사 결과

설문 내용	구분			가중치 평균
학생은 프로그래밍 경험이 있습니까?(18명)	①있다	②없다		0.22*
	11명	7명		
	61%	39%		
프로그래밍 경험이 있다면 자신의 수준을 어느 정도라고 생각하십니까?(11명)	①상	②중	③하	-0.73**
	0명	3명	8명	
	0%	27%	73%	
학생의 사용 가능한 프로그래밍 언어를 쓰시오.	비주얼 베이직			

* 가중치 평균은 {(①의 인원×1)+(②의 인원×(−1))}/18이다.
** 가중치 평균은 {(①의 인원×1)+(②의 인원×0)+(③의 인원×(−1))}/11이다. 가중치 평균 범위는 −1~1이다.

2. 수업진행 및 교재 구성

수업은 전반기(2004년 2학기) 30시간과 후반기(2005년 1학기) 32시간 총 62시간 동안 진행하였다. 전반기의 수업 내용(<표 4>)은 암호와 관련 있는 기초적인 수학 학습과 고전암호의 이해, 그리고 순서도, 자바스크립트 언어의 이해와 구현이다. 후반기의 수업 내용(<표 5>)은 전반기의 수업을 심화하는 내용으로 다양한 암호 기법과 구현을 통하여 암호에서 수학의 필요성을 이해하게 하고, 현대 암호화 알고리즘의 기법을 통하여 암호가 실제 생활과 밀접하게 관련되어 있음을 보이고자 하였다(정상조 · 박중수, 2005). 특히 DES는 현재 금융기관에서 비밀번호 암호화 알고리즘으로 사용되고 있으므로 상업 정보 계열 고등학교 학생들에게 실제적인 경험이 될 것으로 보인다(정상조 · 박중수, 2003). 수업 중에 암호와 관련된 영화 시청이나 과학관 방문 행사도 있었다.

<표 4> 교육 내용(전반기)

시수 (30)	교육 내용(전반기)		교육자료	비고 (교육과정)
	이론	실습		
2	정보화 사회와 암호		파워포인트	
2	암호 용어 해설			
2	암호 시스템 설명			
2	고전 암호에서 시저암호	시저 암호 구현	자바스크립트	순서도
4	기초정수론	기초 정수론 계산 구현		수와 연산
4		소수 판정법 구현		

4	통계적 방법에 의한 고전암호 공격			통계, 확률
4	기타 고전암호			
2	비즈네르 암호			
2		비즈네르 암호 구현	자바스크립트	
2	비즈네르 암호 공격		자바스크립트	

<표 5> 교육 내용(후반기)

시수	교육 내용(후반기)		교육자료	비고
(32)	이론	실습		(교육과정)
2	행렬 암호		파워포인트	수와 연산
2		행렬암호 구현	자바스크립트	행렬
2	일회용 암호		자바스크립트	
2		일회용 암호 구현		
2	DES 암호			함수, 치환
2		DES 암호에서 치환 구현		
4		DES 암호화알고리즘 구현		
2	공개키 암호(키 분배, 키 관리)			
2	RSA 암호			
4		RSA 암호 구현	자바스크립트	수와 연산
2	정보보호 관련 영화 감상			
4	현대 암호(해쉬함수, 전자서명)			
2	총정리			

3. 수업 후 설문조사

수업에 참여한 학생들을 대상으로 수업 후 설문조사를 실시하였으며(<표 6>), 학생들은 수업에 성실하게 임했고, 교육 내용이 상업 정보 계열 학생들에게 매우 유익했다고 답하였다. 암호 학습이 수학 학습에 도움이 되었으며, 전문 교과 학습, 그리고 전문 교과목 중에서도 정보보호 또는 보안 관련 과목을 이수하는데 매우 유익했다고 답하였다. 이로써 암호 학습이 수학 교과와 전문 교과 사이의 매개 역할을 충실히 수행할 수 있을 것으로 보인다.

<표 6> 암호 교육에 대한 설문

설문 내용	①매우 그렇다	②그렇다	③보통이다	④그렇지 않다	⑤매우 그렇지 않다	가중치 평균
학생은 암호 교육에 성실하게 임했습니까?	2명	4명	10명	0명	0명	0.25*
	12.50%	25.00%	62.50%	0.00%	0.00%	
암호 교육 내용의 난이도는	0명	10명	6명	0명	0명	0.31*

적당했습니까?	0.00%	62.50%	37.50%	0.00%	0.00%	
암호 교육이 유익했습니까?	2명	10명	4명	0명	0명	0.44*
	12.50%	75.00%	12.50%	0.00%	0.00%	
암호 교육이 수학학습에 도움이 되었습니까?	1명	10명	5명	0명	0명	0.37*
	6.25%	62.50%	31.25%	0.00%	0.00%	
암호 교육이 전문교과목 학습에 도움이 되었습니까?	1명	9명	6명	0명	0명	0.34*
	6.25%	56.25%	37.50%	0.00%	0.00%	
전문교과목 중 암호나 정보보호 관련 학습에 도움이 되었습니까?	2명	10명	4명	0명	0명	0.44*
	12.50%	75.00%	12.50%	0.00%	0.00%	
전문교과목 중 프로그래밍 관련 학습에 도움이 되었습니까?	2명	9명	5명	0명	0명	0.41*
	12.50%	56.25%	31.25%	0.00%	0.00%	

* 가중치 평균은 {①의 인원×1+②의 인원×0.5+③의 인원×0+④의 인원×(−0.5)+⑤의 인원×(−1)}/16 이다. 가중치 평균 범위는 −1~1이다.

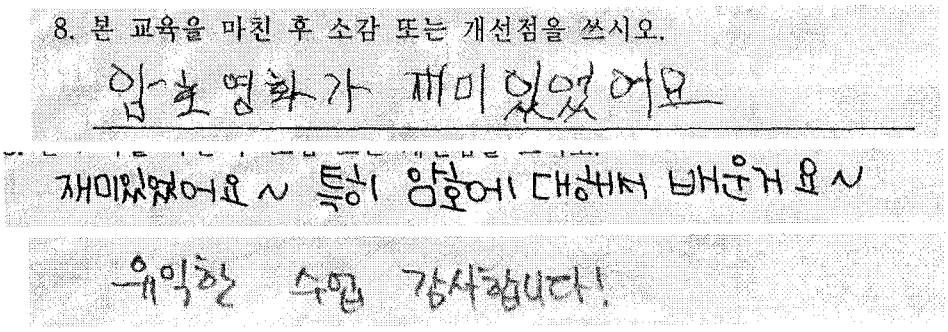
수업을 받은 학생과 받지 않은 학생을 비교하기 위하여 상업 정보 계열 교육 대상 학생(16명)과 상업 정보 계열 비교육 학생(45명) 2개 그룹으로 나누어 설문조사를 실시하였다. 정보보호의 중요성과 필요성에 대하여 설문조사를 실시한 결과 두 그룹 모두에서 정보보호에 대한 중요성은 같은 수준으로 인식하고 있으나 교육을 받은 학생들이 교육 받지 않은 학생들보다 정보보호의 필요성에 대하여 인식도가 높다. 이는 암호 학습에서 암호 실제 사용되는 암호 알고리즘을 학습하고 구현한 결과로 해석된다.

<표 7> 정보보호의 중요성과 필요성

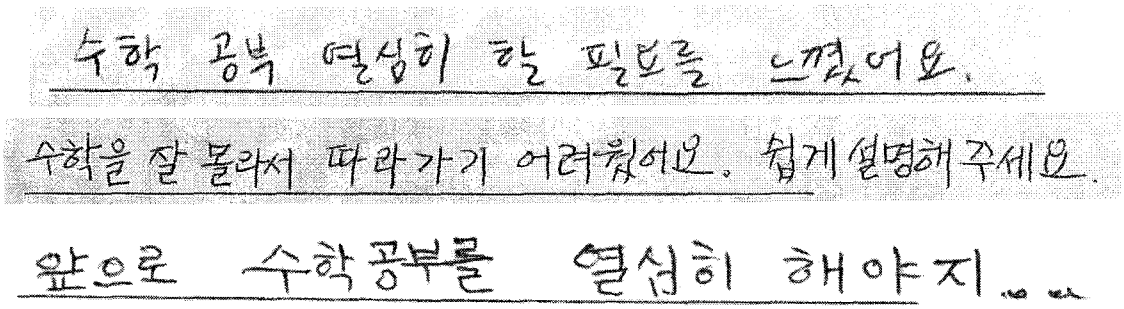
설문 내용	조사그룹	①매우그렇다	②그렇다	③보통이다	④그렇지 않다	⑤매우 그렇지 않다	가중치 평균
학생은 정보보호가 중요하다고 생각합니까?	전문계 교육	8명	6명	2명	0명	0명	0.61*
		50.00%	37.50%	12.50%	0.00%	0.00%	
	전문계 비교육	20명	15명	10명	0명	0명	0.61*
		44.44%	33.33%	22.22%	0.00%	0.00%	
학생은 일상생활에서 정보보호(암호)의 필요성을 느끼는가?	실업계 교육	6명	8명	2명	0명	0명	0.63*
		37.50%	50.00%	12.50%	0.00%	0.00%	
	실업계 비교육	13명	24명	8명	0명	0명	0.56*
		28.89%	53.33%	17.78%	0.00%	0.00%	

* 가중치 평균은 {①의 인원×1+②의 인원×0.5+③의 인원×0+④의 인원×(−0.5)+⑤의 인원×(−1)}/(각 그룹 인원)이다. 가중치 평균 범위는 −1~1이다.

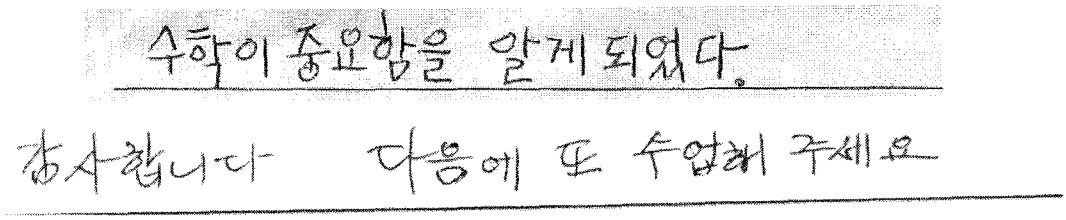
수업을 마친 후 수업에 대한 소감 및 개선점을 쓰도록 하는 설문조사 문항에 대하여 학생들의 응답을 몇 가지로 분류해 볼 수 있었는데, 가장 많은 의견으로 18명의 학생 중 7명의 학생이 암호 수업이 유익하고 재미있었다는 의견이었다.



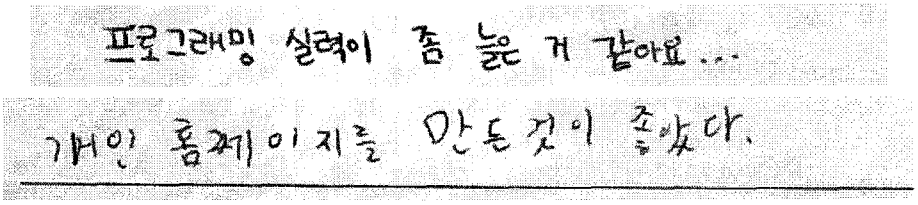
학생들의 이러한 응답은 암호 학습이 수학 학습에 있어서 동기 유발에 충분히 기여할 수 있을 것으로 해석된다. 왜냐하면 암호의 알고리즘을 이해하기 위하여 어쩔 수 없이 기초수학을 학습하여야 하는데 상업 정보 계열 학생들이 암호 학습에 흥미를 가졌다는 사실은 수학 학습에 흥미를 보인 것으로 해석될 수 있기 때문이다. 또 이와 관련하여 소수 의견이기는 하지만 전보다 수학과 친숙해졌다거나 기초수학에 대한 필요를 느꼈다는 응답에서도 확인할 수 있다.



암호 수업을 받은 학생들 중 4명의 학생이 암호를 학습한 후 수학이 실생활에 유용하고 쓸모 있음을 알게 되었다고 응답하였으며, 차후 비슷한 수업이 있다면 좋겠다는 답을 하였다.



18명의 학생 중에서 2명의 학생이 암호 학습에서 프로그래밍 실습을 함으로써 프로그래밍 실력이 향상되었다거나 프로그래밍 실습을 통하여 성취감을 얻었다는 의견이 있었다.



이는 프로그래밍 실습을 통한 암호 학습이 상업 정보 계열 고등학교 교과과정 상에서 수학 교과와 전문 교과 사이의 매개 역할을 충분히 수행할 수 있음을 의미하는 것으로 해석될 수 있을 것이다. 이 밖의 소수 의견으로 논리적 사고력이 향상된 것 같다는 의견이 있었다. 이는 암호 알고리즘의 학습에서 알고리즘의 분석, 프로그래밍 과정에서의 여러 가지 제어문의 사용, 문제해결 등이 논리적 사고력을 촉진한 것으로 추측할 수 있다.

IV. 결론

우리나라의 수학과 교육과정은 해방 이후 교수요목기를 시작으로 현재의 2007 개정에 이르기까지 60여년에 걸쳐 꾸준히 개선되어 왔다. 그러나 비교적 최근에 와서야 수학과 교육과정에서 전문계열 학생들을 위한 수학 선택과목이 신설되었다. 1992년 3월 개정 공포된 제6차 수학과 교육과정에서는 수학의 실생활 적용을 강조한 '실용수학'을 신설하여 실업계 고등학교 학생들의 필요를 충족하도록 하였으며, 제7차 수학과 교육과정에서는 국민 공통 기본 교육과정상에 '수학 10-가'와 '수학 10-나'를 배정하고, '실용수학', '수학 I', '수학 II', '미분과 적분', '확률과 통계', '이산수학' 같은 다양한 선택 과목을 개설하였으며, 전문계열 학생들은 '실용수학'을 선택할 수 있도록 하였다. 마찬가지로 2007 개정 수학과 교육과정에서도 전문계열 학생을 위하여 '수학의 활용'을 신설하였으나 이는 '수학 I'에 가깝다.

수학과 교육과정 상에서 전문계열 학생들을 위한 선택과목이 신설되고 이를 통하여 수학과 실생활 문제를 접목하고 전문 교과목의 학습에 필요한 수학을 지원하려는 노력에도 불구하고 전문계열 학생들의 수학 실력은 크게 향상되지 않고 있다. 이는 제6차 교육과정에서 전문계 고등학교 수학교육 상황을 연구한 결과와 제7차 교육과정에서 전문계 고등학교의 수학과 학습의 문제점을 지적한 연구들에서 밝힌 대로 학생들의 대수적 계산능력 부족과 학습량에 비해 수업 시수 부족, 수학 교과와 전문 교과 사이의 연계성 부족 세 가지로 요약된다 (구제현, 1991; 권경내, 2000; 신해인, 1997; 오춘영, 2004; 윤외한, 1998; 장병현, 1997).

학생들의 대수적 계산 능력 부족은 본 연구의 사전 설문조사에서도 확인되고 있는데 기본적인 계산 능력이 저하된 상황에서 전문 교과의 내용을 이해하기 쉽지 않을 것이다. 그러나 본 암호교육에 참여한 학생들은 1년간의 교육을 통하여 기초적인 수학적 계산 기능의 필요성을 절실하게 느끼며, 수학이 실생활에 매우 유용하며, 수학적 사실들이 현실문제와 밀접하게 관련되어 있음을 인식하게 되었음을 말하고 있다. 또 암호 학습을 통하여 예전보다 수학과 친숙해졌음을 말하고 있다. 이는 아무리 간단한 암호 알고리즘이라 하더라고 학교수학의

기본적인 학습 내용인 함수와 치환, 행렬, 확률 등의 개념이 포함되어 있으므로 은연중에 수학적 개념을 접하게 되었음을 의미한다고 볼 수 있다.

모든 프로그래밍 작업은 알고리즘을 정확히 이해한 후 이를 프로그래밍 언어를 사용하여 구현하고 그 결과를 확인함으로써 완성된다. 프로그래밍 활동은 다양한 인지적 기능을 요구하는바 프로그래밍 언어에 대한 정확한 지식과 알고리즘에 대한 지식이 어우러져서 모든 단계가 논리적인 오류 없이 짜여 져야 하는데, 학생들은 반복적인 프로그래밍 활동을 통하여 문제에 대한 집중력이 향상되고, 문제 해결에 대한 절차를 익히며, 오류의 수정을 통하여 성취감을 맛봄으로써 자신감과 수학적 태도의 향상에 기여할 수 있다. 또 논리적으로 옳은 프로그램이라고 하더라고 더 개선된 제어 구조를 사용한 보다 효과적인 프로그램이 얼마든지 존재할 수 있기 때문에 창의적인 프로그래밍이 가능하다. 학생들은 1년간의 프로그래밍 활동을 통하여 보다 나은 문제 해결력과 논리적 사고력이 향상되었음을 말하고 있다. 또 수학의 개념적 지식과 절차적 지식이 서로 분리되지 않고 연결되어 있음을 알게 되었다고 한다.

전문계열 고등학교의 수학과 교육의 문제점을 지적한 논문들이 대부분 현장에 계신 교사들에 의하여 진행된 연구라는 점을 감안하면 현장의 전문계열 고등학교에서 수학교육 개선에서 필요한 사항으로 계산능력과 기초적인 수학 지식을 포함하는 기초적인 수학능력의 향상과 수학교과와 전문교과 사이의 연계를 강화하는 방향이어야 함을 알 수 있는데 이를 위해서 암호는 좋은 교육 재료가 될 수 있을 것이다. 왜냐하면 암호 이론의 학습과 구현을 위해서 기초 수학과 프로그래밍이 요구되며, 암호 학습이 수학 학습의 필요성을 부각시키고, 프로그래밍 활동을 통하여 수학교과와 전문 교과 사이의 매개 역할을 수행할 수 있기 때문이다. 상업 정보 계열 고등학교 전문교과 교육과정 상에 개설된 32개 교과목 중에서 암호와 정보보호, 보안과 관련된 교과목 수가 7개 과목이다.

최근 관련 연구들을 보면 중등학교 수학에서 암호와 관련된 내용들을 접목시키거나 또는 중등학교 수학에 암호관련 내용을 직접적으로 반영하려는 시도들이 이루어지고 있다(이병구, 2000; 노은영, 2003; 임정현, 2007; 이화여자대학교 수리과학연구소, 1998). 본 연구에서는 정보 상업 계열 학생들의 특별활동 시간을 활용하여 1년 2학기 동안 매주 2시간씩 프로그래밍 실습을 병행한 암호와 알고리즘 및 프로그래밍을 지도한 결과 암호의 학습과 프로그래밍 실습이 학생들로 하여금 정보화 사회에서 정보보호의 중요성을 인식하게 하고 정보보호를 위해서 어떤 일을 해야 하는지 알 수 있게 하였으며, 프로그래밍 언어를 사용하여 알고리즘을 구현함으로써 컴퓨터 언어 구사 능력도 기를 수 있었다. 이러한 결과들을 토대로 본 연구에서는 제7차 수학과 교육과정에서 '실용수학' 또는 2007 개정 수학과 교육과정에서 '수학의 활용' 내에 암호와 그 구현에 관한 내용을 추가할 것을 제안한다. 또는 특별활동 자료로 활용할 것을 제안한다.

참고문헌

강옥기 (2006). 수학과 학습지도와 평가론(제2판). 경문사.

교육인적자원부a (1997). 상업 계열 고등학교 전문교과 교육과정. 교육부 고시 제 1997-15호. 별책 21.

교육인적자원부b (1997). 수학과 교육과정. 교육부 고시 제 1997-15호. 별책 8.

교육인적자원부a (2007). 상업 정보 계열 전문 교과 교육과정. 교육인적자원부 고시 제

2007-79호. 별책 21.
교육인적자원부b (2007). 수학과 교육과정. 교육인적자원부 고시 제 2007-15호. 별책 8.
구제현 (1991). 공업계 고등학교에서 수학교과 학습지도 상의 문제점 분석 및 개선방안 모색 -기계과, 배관과, 금속과를 중심으로. 충남대학교 대학원 석사학위 논문.
권경내 (2000). 실업계 고등학교 수학교육 실태와 수학교과의 관심도에 관한 연구 -상업계 고등학교를 중심으로. 경희대학교 대학원 석사학위 논문.
노은영 (2003). 중고등학생을 위한 암호학 교재 개발 연구. 고려대학교 대학원 석사학위 논문.
류희찬 · 배은희 (2000). LOGO 프로그래밍을 활용한 대수 학습 자료 개발 연구. 대한수학교육학회 논문집. pp. 859~882).
신동선 · 류희찬 (1998). 수학교육과 컴퓨터. 경문사.
신해인 (1997). 공업계 고등학교의 수학교과와 전공교과목의 연계성에 관한 연구 -제6차교육과정을 중심으로. 충북대학교 대학원 석사학위 논문.
오춘영 (2004). 상업계 고등학교 수학교과서의 재구성이 학습자에게 미치는 영향. 한국수학교육학회 시리즈 A <수학교육>. 제 43권, 제 1호. pp. 13~33.
우정호 (2001). 학교수학의 교육적 기초(증보판). 서울대학교출판부.
윤외한 (1998). 공업계 고등학교 교육과정에서 수학교과목과 전공교과목의 관계성에 관한 연구 -기계과, 전기과, 전자과를 중심으로. 경성대학교 대학원 석사학위 논문.
이병구 (2000). 중등학교 수학교과에서 암호학 도입을 위한 교재 구성 방안 모색. 건국대학교 대원 석사학위 논문.
이선영 (2003). 고등학교 수학교육과정에서의 암호학의 도입 가능성에 관한 연구 -RSA 알고리즘을 중심으로. 대전대학교 대학원 석사학위 논문.
이화여자대학교 수리과학연구소 (1998). 정보통신에서 수학의 역할. 이화여자대학교 출판부.
임정현 (2007). 상업계 학생들을 위한 수학 암호론 교재 개발에 대한 연구. 건국대학교 교육대학원 석사학위 논문.
장병현 (1997). 실업계 고등학교에서 수학교육 활성화 방안. 경북대학교 대학원 석사학위 논문.
정상조 · 박중수 (2003). DES를 이용한 암호의 이해와 활용 및 DES에서의 한글 구현, J. Korean School Math. Soc. 6(2), pp. 101~115.
정상조 · 박중수 (2005). 자바스크립트와 암호, 한국학술진흥재단 미래형 인재양성을 위한 Future Korea 지원 사업 '정보화 사회에서 암호의 이해와 활용' 강의노트. http://math88.com.ne.kr/crypto.htm
Hiebert & Lefevre (1986). Conceptual and Procedural Knowledge in Mathematics-an Introductory Analysis, in (ed. J. Hiebert) Conceptual and Procedural Knowledge: the Case of Mathematics, LEA Pub., pp. 6~8.

상업 정보 계열 고등학교 암호 교육 프로그램 개발 및 적용에 관한 연구

A Study on the Development and Application of Cryptography Teaching Program for Vocational High School Mathematics

Park, JoongSoo[3] · Chung, Sang-Cho[4]

Abstract

The purpose of this study is to develop a contents when we are going to introduce cryptography and information security for vocational high school students. For this we do a survey of the students' level for understanding of information security and the 7th curriculum for school mathematics, 2007 revised curriculum for school mathematics, the curriculum for vocational high school, and we search for the material that connects between mathematics subjects and vocational subjects. We develop a text book that introduces information security and cryptography. After we teach vocational high school students by using this developed book, we get the result that learning cryptography with computer programming makes a good motivation of learning mathematics and roles a parameter between mathematics curriculum and vocational curriculum. As a result we propose that the developed contents can be used in 'Practical Mathematics' in the 7th curriculum for school mathematics or 'Application of Mathematics' in 2007 revised curriculum for school mathematics.

Key Words : Information Security, Cryptography, Curriculum for school mathematics, Curriculum for vocational high school.

3) Woosuk University (jspark@woosuk.ac.kr)
4) Mokwon University (math888@paran.com)