ICU 정보보호 석/박사 과정을 위한 교과과정 연구

A Study on Curriculum of Graduate Courses in Information Security at ICU

천정희, 김광조, 이철수

한국정보통신대학교 공학부 정보보호 그룹

Jung Hee Cheon, Kwangjo Kim, Chulsoo Lee

Information Security Group
Information and Communications University

요 약

최근 정보통신 분야의 기술이 발전함에 따라 정보보호의 필요성이 커지고 있으나, 정보보호 인력양성을 위한 교육과정에 관한 충분한 연구가 이루어지지 않아 정보보호 인력 양성에 어려움이 있다. 본 고에서는 현재 한국정보통신대학교(ICU) 석/박사 과정에서 이루어지는 교과과정을 중심으로 정보보호 교과과정을 제시하고 정보보호 고급 인력 양성을 위해 ICU에서 제공하고 있는 사이버 강의, 해외 전문가 초청 세미나 및 국제 공동 연구 프로그램 등을 소개하려 한다. 본 고에서 논의되는 정보보호 교과과정 및 프로그램들이 바람직한 정보보호 교육 방향을 수립하는데 기여하기를 기대한다.

1. 서 론

정보보호에 관한 연구는 고대의 시저암호 이래로 2000년 이상 연구되어 왔다고 할 수 있으나 주로 군사나 외교 등 제한된 분야에서 사용되었으며, 공개적으로 연구된 것은 DES(Data Encryption Standard)나 Diffie와 Hellman의 공개키 개념이 제안된 70년대 중반으로 볼 수 있다. 정보보호는 초기에 주로 수학자나 전자공학자에 의해 연구되었으며 컴퓨터의 발전과 더불어 최근에는 전산과 접목된 보안의 연구가 활발히 이루어지고 있다. 이에 따라 초기에는 수학이나 전산 및 전자 공학에서 일부 응용으로 소개되던 정보보호 이론들이 최근에는 학제간 전공분야를 망라하는 독자적인 과목으로 형성되고 있고 대학교나 대학원에서 독자적인 정보보호학과 혹은 정보보호전공을 제공하는 학교들도 늘어나고 있다. 이에 따라 정보보호 교육을 위한 교재 및 교과과정 개발의 필요성이 증가하고 있으나 이에 따른 충분한 연구가 이루어지지 않고 있어 효율적인 정보보호 교육에 어려움이 되고 있다.

최근 그 필요성이 날로 증가하고 있는 정보, 전자, 통신 등 IT 분야의 전문 인력 양성을 위하여 설립된 한국정보통신대학교(ICU) 에서는 정보보호 인력 양성을 위하여 대학원에 정보보호 트랙을 가지고 독자적인 정보보호 교육과정을 제공하고 있다. 본 고에서는 현재 ICU의 석/박사 과정에서 이루어지는 교과과정을 중심으로 정보보호 교과과정을 제시하고 정보보호 고급 인력 양성을 위해 ICU에서 제공하고 있는 사이버 강의, 해외 전문가 초청 세미나 및 국제 공동 연구 프로그램 등을 소개하려 한다. 본 고에서 논의되는 정보보호 교과과정 및 프로그램들이 바람직한 정보보호 교육 방향을 수립하는데 기여하기를 기대한다.

2. 정보보호 트랙

가) 개요

정보 통신망의 발전에 따라 정보의 불법적인 감청, 위장, 개조 등과 같은 정보화의 역기능이 빠르게 증가하고 있으며, 이러한 사이버 공간상의 불법적인 행위를 방지하기 위하여 다양한 암호 기술 및 서비스가 개발되어 왔다. 정보보호 트랙의 교과과정은 국내외 정보보호 산업 현장에서 즉시 활용이 가능하고 영어를 자유롭게 구사하여 국제적인 감각을 가진 차세대 암호론 및 정보보호 이론을 선도할 수 있는 전문가의 양성을 목표로 한다.
본 트랙에서는 비밀키 암호(블록 및 스트림 암호), 공개키 암호, 전자 서명, 해쉬 함수, 암호 프로토콜, 난수 생성기 등 기초 이론을 바탕으로 기밀성, 무결성, 인증성, 부인 방지, 접근 제어성을 제공하는 네트웍 보안, 컴퓨터보안, 무선 보안, 전자 상거래 보안, 정보전 등 다양한 정보보호 응용 서비스를 제공하는 연구를 수행한다. 이를 위해 수학, 전산, 전자에 걸친 다양한 기본 과목들을 제공하고 있다.

나) 전공별 이수과목

정보보호 트랙은 암호전공과 정보보호 전공 두 가지로 나누어진다. 두 전공 모두 의무과목인 알고리즘과 계산이론 및 전산수학은 필수로 이수하여야 하며 공학도들의 경영 마인드 고취를 위해 경영 과목 3과목도 필수로 이수하여야 한다. 정보보호를 전공하기 위해 수학과 전산이 필수적이므로 본 교과과정에서는 기반과목으로 수학과목인 전산수학, 고급암호수학, 부호이론과 더불어 기본 전산 과목인 알고리즘, 운영체제, 컴퓨터 구조 등의 수강의 권장하고 있다. 이러한 기반과목과 병행하여 암호 전공과 정보보안 전공의 공통 과목으로 현대 암호학, 컴퓨터 보안, 네트워크 보안등을 개설하고 있고 각 전공별 이수 과목은 다음 표와 같다.

구분	암호전공	정보보안전공	석사	박사
의무과목	o 전산수학, 알고리즘와 계산이론 o 경영 과목 3개 과목			
기반과목	알고리즘, 운영체계, 컴퓨터 구조, 전산수학, 고급 암호 수학(518), 부호이론(519)			
기초과목	컴퓨터 네트워크, DB, 분산시스템, 차세대인터넷, 현대 암호학(605), 네트워크 보안(615), 정보시스템 보안관리론(673)			
전공과목 (600~700)	암호 프로토콜(671) 전자상거래보안(719) 타원곡선암호(721)	컴퓨터 보안 (672) 시스템보안(705) 데이터베이스보안(706) 스마트카드보안(797)		
전공심화과목 (700~800)	암호학 특강 I(829) 암호학 특강 II(830)	정보보안 특강 I(831) 정보보안 특강 II(832)		

다) 교과목 해설

위에서 제시한 각 교과목의 내용은 다음과 같다.

1. 고급암호 수학 (Advanced Mathematics for Cryptography)

이 과목에서는 현대 암호학 연구에 기본이 되는 수학적인 도구인 정수론, 유한체론, 복잡도 이론, 확률론, 타원곡선 이론에 대하여 소개하며, 이를 통하여 현대 암호학을 심도있게 이해할 수 있도록 함을 목표로 한다. 정수론에서는 군론, 오일러 함수, 소인수분해, 유클리드 알고리즘, 중국인의 나머지 정리 등을 다루며, 유한체론에서는 다항식 기저, 정규 기저, 최적 정규 기저, 다항식 분해와 유한체 연산 등을 다룬다. 이 이외에도 암호학 연구에 필요한 수학적 기반 지식들이 필요에 따라 추가될 수 있다.

2. 부호 이론 (Coding Theory)

정보이론의 기초가 되는 엔트로피, 상호 정보량, 채널 용량, 잡음 부호화 정리 등을 소개한 후, 블록 부호, Reed-Muller, BCH, Reed-Soloman, Golay 부호 등 기본적인 부호들을 공부한다. 기초 이론으로 부호화, 복호화, 생성 매트리스, 오류 검출 및 정정, 최소 거리, 선형 부호 등도 다루며, 부호론과 암호론의 관련 부분도 검토한다. (선수과목: 고급 암호 수학)

3. 현대 암호학 (Modern Cryptography)

이 과목에서는 정보 통신망의 발전에 따라 발생하는 정보의 불법적인 감청, 개조 등과 같은 역기능을 효과적으로 해소하기 위한 이론과 기법을 연구한다. 주요 내용으로는 고전 암호를 비롯하여, 블록 및 스트림 암호로 불리는 비밀키 암호시스템, RSA, Diffie-Hellman 등의 공개키 암호시스템, 디지털 서명, 해쉬함수, 인증기법, 영지식 증명법 등이 있으며 이에 필요한 기초 지식들도 다루도록 한다.

4. 네트워크 보안 (Network Security)

컴퓨터와 네트워크 상에 존재하는 각종 위협 요소들을 분석하고 정보의 기밀성 제공을 위한 암호 시스템을 간단히 소개하고 정보의 무결성과 인증성 보장을 위한 디지털 서명 방식과 해쉬 함수를 이용하여 암호 프로토콜의 구성과 각종 응용 프로토콜 기술을 익히도록 한다. 또한, 컴퓨터와 네트워크 상에서 사용자의 접근 제어 기술, 인증 서버 구축 기술, S/MIME과 PGP와 같은 안전한 전자 우편 기술, Web 보안 기술, firewall 구축 기술 등을 습득하여 실제 컴퓨터 및 네트워크의 보안 기술을 응용할 수 있는 능력을 배양한다. (선수과목: 현대 암호학)

5. 정보시스템 보안 관리론 (Security Management)

정보시스템 보안 기술에 관한 추세와 표준화 동향을 파악하고 정보 시스템 운영에 필요한 관리적, 운영적 요소들을 파악한다. 위험분석 등 의 정보시스템 위험요소 분석 기법을 이해하여, 정보시스템에 대한 보안 기획/계획 능력을 배양한다. 수강자에게 정보시스템 감사, 정보보호 정책 등을 고려한 정보시스템 보안에 대한 consulting 능력을 갖출 수 있도록 한다.

6. 암호 프로토콜 (Cryptographic Protocols)

본 과목에서는 안전성 증명 가능한 암호 및 서명, 인증, 개인 식별 방식, 대화형/비대화형 영지식 증명에 대하여 공부한다. 증명 가능 안전성은 어의적 안전성, 비유연성, 구별 불가능성, 평문 숙지성의 개념을 포함하며, Blum-Goldwasser, Cramer-Shoup, OAEP 등의 증명가능한 암호 프로토콜과 증명가능한 키 관리 프로토콜도 연구한다. 응용 사례로 전자 현금, 전자 투표, 전자 입찰 등의 설계 기법도 다루어진다. (선수과목: 현대 암호학)

7. 전자 상거래 보안 (E-Commerce Security)

네트워크상에서 전자적인 지불 시스템의 요소 기술을 다룬다. 현금의 특징을 비롯하여 블록 및 공개키 암호 시스템과 해쉬함수를 이용한 디지털 서명 방식을 포함한 정보보호의 기본적인 지식을 습득하고, SET과 SSL 등의 전자 지불 프로토콜에 응용, 소액 전자 지불 시스템, 전자 현금, 스마트 카드 기술, 전자은행 등을 다룬다. 이 과정을 통하여 안전한 전자지불시스템을 이해하고 이의 의미 및 위험요소를 분석하고 안전한 전자 상거래를 구축할 수 있는 기술을 비교 평가해본다.

8. 타원 곡선 암호(Elliptic Curve Cryptography)

본 과정에서는 타원곡선의 기본적인 성질을 공부하고 이를 바탕으로 타원곡선에 기반한 암호, 서명, 인증 등 여러가지 암호 프로토콜을 배운다. 또한 안전한 타원곡선 암호의 설계 및 구현 방법을 습득하여 직접 타원곡선 암호를 설계, 구현할 수 있는 능력을 배양한다. (선수과목: 현대 암호학, 고급 암호 수학)

9. 컴퓨터 보안 (Computer Security)

안전한 컴퓨터 시스템을 구축/유지하기 위한 기술적 수단을 다루고, 컴퓨터 시스템의 일반적 보안문제와 보안 요구 사항을 파악 정의한다. 해킹 기법이나 바이러스 유형을 분석 분류하고 이해한 후, 컴퓨터 시스템의 구성요소 - H/W, S/W (OS. DB, System utility, Network s/w, user program) PC등의 침해기술과 대응 기술을 취급한다. 수강 후 컴퓨터 시스템 보안 제품의 분석, 평가 및 기술 개발의 능력을 부여한다. (선수과목: 현대 암호학)

10. 시스템 보안(System Security)

인터넷을 중심으로 한 정보시스템 환경의 변화 추세와 그에 따른 정보보호 이슈를 이해한다. 토탈 시스템으로서의 정보보호를 위한 방법론, 정보보호 모델을 연구하고 안전한 운영체제, 안전한 데이터 베이스, 다단계 정보보호 개념을 이해한다. 나아가 정보보호의 확장된 개념인 정보보증에 대한 개념, 접근 방법, 관련 기술 요소 등을 취급함으로서 시스템적인 정보보호 능력을 수강학생에게 부여한다. (선수과목: 네트웍 보안, 컴퓨터 보안)

11. 데이터베이스 보안 (Database Security)

데이터베이스보안 문제의 여러 가지 측면과 분산 데이터베이스에서의 동시성 제어와 관련된 주제를 취급한다. 특히, 분산 데이터베이스에서 동시성 제어와 불일치 복구 문제에 관한 문제를 토의한다. 또한, 이러한 보안 모델과 보안요구사항 간의

상호 작용을 연구한다. 접근 제어 방책이 관계형 및 목적형 데이터베이스의 적용 기법도 연구한다.

12. 스마트카드 보안 (Smart Card Security)
Tamper proof device 로서 스마트 카드의 물리적 및 전자적인 특성을 살펴보고 스마트 카드의 안전한 운용에 필요한 암호학적 지식을 습득한다. 스마트 카드의 운용 체계를 습득하여 응용 프로그램의 제작 방법을 실습한다. 스마트 카드의 안전성을 평가하는 수단으로 Simple Power Analysis, Differential Power Analysis 등의 기법을 살펴보고, 카드의 응용 분야 중 하나인 전자 상거래 시스템에의 응용과 Java 카드, PC/SC, MULATTO 등 최신 기술도 연구한다.

13. 암호학 특강 I (Advanced Topics I in Cryptography)
본 과목에서는 블록 암호 및 스트림 암호에 관한 최근 이슈들을 다루도록 한다. 블록 암호에 관하여는 Feistel 구조 및 확장 Feistel 구조, SP 네트워크, 부울 함수, 비 선형성, 전파 특성, S-box 등의 개념 및 이를 이용한 안전한 블록 암호 설계 방법 등의 주제가 있으며 차분 공격법과 선형 공격법 및 기타 유사 해독 방법도 다룰 수 있다. 스트림 암호에 관하여 LFSR, 선형 복잡도, 상관 면역 함수, 상관 공격 등에 관한 지식을 습득하며 다양한 스트림 암호 설계 기법도 다룬다. (선수과목: 고급암호수학)

14. 암호학 특강 II (Advanced Topics II in Cryptography)
본 과목에서는 공개키 암호에 관한 최근 이슈들을 다루도록 한다. 최근의 공개키 암호 방식으로는 타원곡선 암호, 격자 암호, 땋임 암호 등이 있으며 확률적 암호화 기법, 증명가능한 프로토콜 설계 기법, 고속 연산 기법 등도 활발히 연구되는 주제이다. 안전성의 평가 척도로서 소인수 분해 알고리즘과 유한체 및 타원곡선 상에서의 이산 대수 알고리즘, 격자 문제의 해법인 LLL 알고리즘 등을 연구한다. (선수과목: 고급암호수학)

15. 정보보안 특강 I (Advanced Topics I in Information Security)
본 과목은 정보 보안의 최근 연구 주제로서 정보은닉, 지적 재산권 보호, 자바 보안, 안전성이 보장되는 장치 등에 대하여 연구 및 실습한다.

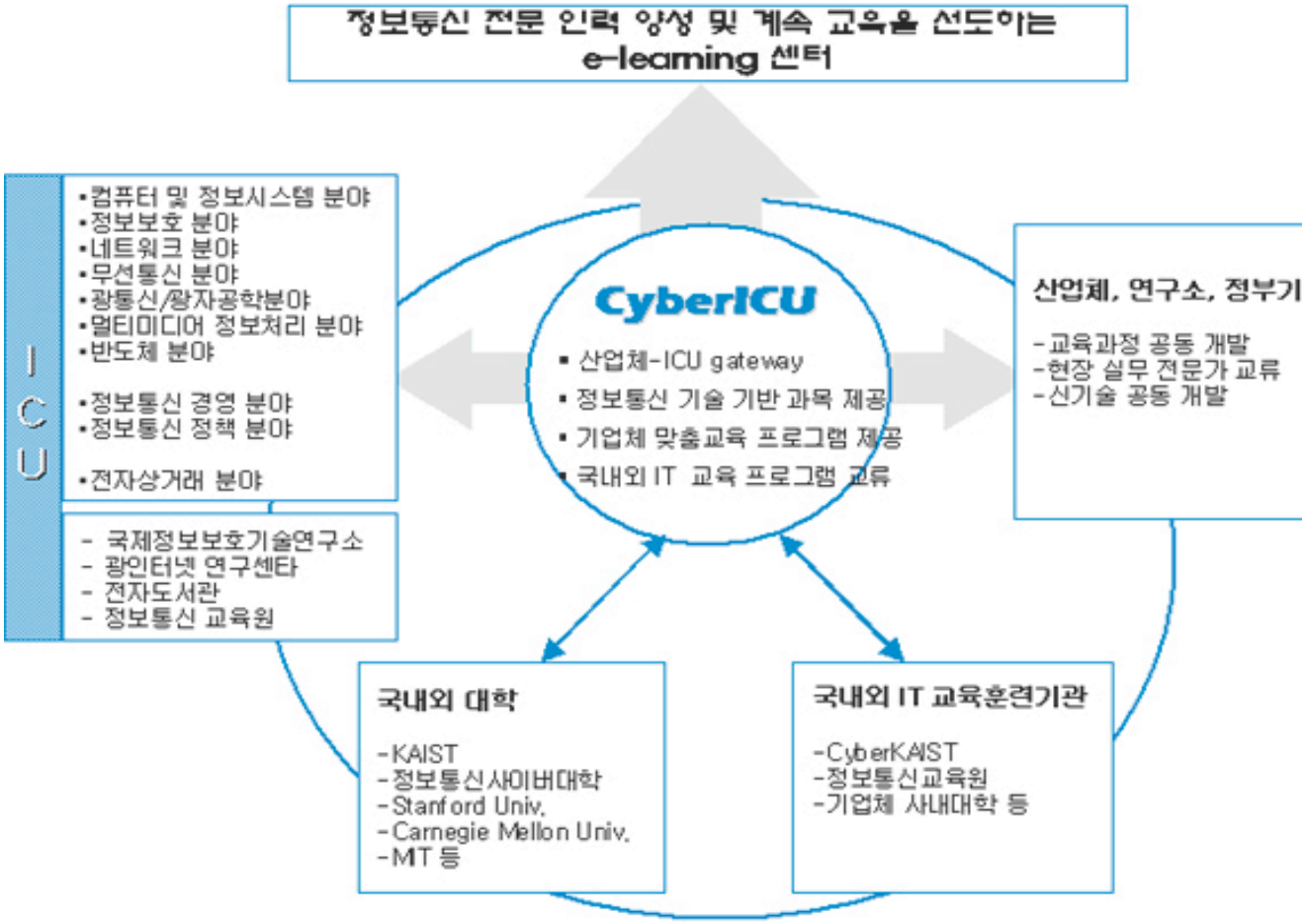
16. 정보보안 특강 II (Advanced Topics II in Information Security)

본과목은 전자 시장에서 정보보안 기술의 기본 구조와 응용 기술을 습득한다. 전자 지불, 전자 현금, SET, 금융 암호 및 PKI, 디지털 티켓, 우표 등에 관한 기술을 연구한다.

3. 보조 프로그램

가) 사이버 ICU

사이버 ICU는 기술혁신과 발전을 주도할 능력있는 석.박사급 고급 전문인력 양성 차원에서 첨단 정보통신기술을 활용한 사이버 교육시스템을 통해 IT 분야의 인력 수요를 충족시킬 수 있는 Learning Resource 센터 역할을 수행하여 ICU의 특화된 전문 교육 프로그램을 제공하는 사이버 교육 프로그램이다. 인터넷을 통하여 실시간으로 제공된 강의는 on-demand로도 제공되어 수강생의 학습 속도에 맞추어 진도관리를 할 수 있고 수강생이 필요한 부분을 선택하여 반복적으로 학습함으로써 학습효과를 높일 수 있다.



정보보호 그룹에서 제공하는 정규강의의 일부분이 사이버 ICU를 통하여도 서비스 되어지고 있는데 올해의 경우 현대 암호학, 정보보호와 전자지불 등이 사이버 강좌로 제공된 바 있다. 이와 더불어 사이버 ICU에서는 매학기 수요조사를 통해 정기적으로 산업 및 연구현장의 교육요구를 파악하여 수요자 중심의 특화된 단기강좌를 제공하고 있는데 올해의 경우 1월과 4월에 Network Security and Internet Security라는 단기 강좌를 개설하였다.

나) 해외 전문가 초청 세미나

정보보호 그룹에서는 정보보호 교육의 세계적 흐름에 맞추어 나가기 위해 매년 해외 정보보호분야의 저명교수 및 전문가를 초빙하여 단기 강좌 및 인터넷 화상 강의를 제공하고 있다. 현재까지 미국, 일본, 영국, 프랑스 등 정보보호 선진국들의 세계적인 교수 및 전문가들의 연구 분야 및 최신 이슈에 대한 국내 단기 강좌를 개설한 바 있으며, 2002년 7월에는 호주 QUT의 Colin Boyd교수에 의한 암호프로토콜 강좌가 개최될 것이며, 추후에 뉴질란드 Otago 대학의 Henry Wolfe 교수에 의한 Computer Forensic에 대한 강좌도 예정되어 있다.

1) 1차 단기강좌

- 강사 : Florida State University의 Yvo Desmedt 교수
- 기간 : 2001. 2 .16 ~ 2. 17
- 제목 : Zero-knowledge, interactive proofs, and their applications in cryptography.
- 수강인원 : 30명

2) 2차 단기강좌

- 강사 : Dr. Gail-Joon Ahn, Univ. of North Carolina at Charlotte
- 기간 : 2001. 5. 28
- 제목 : Cyberspace security II
- 수강인원 : 45명

3) 3차 단기강좌

- 강사 : Chan Yeob Yeun, Toshiba Telecommunication Research Laboratory, England
- 기간 : 2001. 7. 14
- 제목 : Security for M-Commerce

- 수강인원 : 30명 (인터넷으로 중계)

4) 4차 단기강좌

- 강사 : Colin Boyd, QUT, Austrailia
- 기간 : 2002. 7. 9 ~ 7. 11
- 제목 : Cryptographic Protocols

다) 국제 공동 연구 프로그램

정보보호 그룹에서는 국제 공동 연구를 위하여 국제정보보호기술연구소(International Research center for Information Security)를 중심으로 다음과 같은 역할을 수행하고 있다. (상세한 내용는 http://www.iris.re.kr을 참조)

- 해위 유학생 및 post-doctoral 유치
- ICU 학생의 해외(NTT) 인턴쉽 실시
- 해외 대학 및 연구소 국제 공동 연구 체결
  . 미국 (UNCC, Univ. of North Carolina at Charlotte),
  . 호주 (QUT, Monach Univ.)
  . 일본 (동경대, NTT)
  . 프랑스 (ENS)
- PKC2001, IWAP2001, ICISC2001 등 국제 학술 대회 개최 및 Asiacrypt2004 국내 유치

또한, 2002년 FIFA 월드컵을 한일 공동 개최를 기념하여 한일의 암호 전문가들이
힘을 합쳐서 인터넷을 통한 최우수 선수와 골 키퍼를 전자 투표로 선출하는 국제 공동연구(일명 “보토피아”)도 수행하고 있다. http://mvp.worldcup2002.or.kr에 접속하여 누구든지 소정의 등록을 거치면 전자 투표를 할 수 있도록 하였으며, 공개키 암호 기법을 전자 투표에 적용하여 대규모 시험은 본 계획이 세계 최초이다.

보토피아에 참여하고 있는 한국 기업은 IRIS를 비롯하여, KISTI, KSIGN, SECUi.COM, STI, Vocotech 이며 일본 측은 동경대와 NTT가 참여하고 있으며, ORACLE, SUN 사에서는 자사의 제품을 기증하는 등 산학연의 국제 공동 연구로

서 한국과 일본의 IT 기술을 전세계에 홍보하고 PKI의 Killer application으로 전자 투표의 가능성을 점검하고 국내 PKI 산업의 시장 창출 효과를 기대할 수 있다.

5. 결론

이상에서 ICU 석/박사 과정에서 이루어지는 교과과정을 중심으로 정보보호 교과과정을 제시하고 정보보호 고급 인력 양성을 위해 ICU에서 제공하고 있는 사이버 강의, 해외 전문가 초청 세미나 및 국제 공동 연구 프로그램 등을 소개하였다. 현재 제시된 교과과정은 암호학과 정보보호 분야의 이론의 발전과 기술 진전에 따라 새로운 과목이 추가하여 제공된다는 점을 첨언한다. 본 고에서 논의되는 정보보호 교과과정 및 프로그램들이 바람직한 정보보호 교육 방향을 수립하는데 기여하기를 기대한다.