2022년도 정보보호 전문가를 위한
암호교육

| 기 간 | 2022년 3월 23일(수)~25일(금)

| 장 소 | 온라인 교육

| 주 최 | 한국암호포럼, 한국정보보호학회

| 주 관 | 한국암호포럼

프로그램 위원장		곽 진 교수(아주대학교)
프로그램 위 원		홍득조 교수(전북대) 장남수 교수(세종사이버대) 김종성 교수(국민대) 서석충 교수(국민대) 김희석 교수(고려대) 서화정 교수(한성대) 김기문 팀장(KISA) 김준섭 책임(KISA)
등 록 안 내		

교육비

구 분	교 육 비
학 생 / 일 반	20 만원 / 30 만원

온라인 등록

● 사전등록	:	2022년 03월 21일(월)까지
● 기타사항	:	1) 교육 증명서 발급 2) 온라인 접속 링크 등록자 개별 공지
● 등록방법	:	학회홈페이지(https://www.kiisc.or.kr) → 학회행사 → 사전등록바로가기
● 결 재 방 법	:	등록정보 작성 후 결재방법 선택 및 결재

사전 등록 송금처

● 예 금 주	:	한국정보보호학회
● 계좌번호	:	국민은행 754201-04-135596 (예금주: 한국정보보호학회)
● 안내사항	:	1) 사전등록시 등록비는 위의 구좌로 송금하시고, 입금자가 대리일 경우 연락바람 2) 신용카드 결재시 세금계산서 발급 불가 (부가가치세법 시행령 제 57조)

문의처 : 한국정보보호학회

- 전 화 : 02-564-9333~4 (내선번호 5)
- 전자우편 : kiisc@kiisc.or.kr

교육 일정

날 짜	시 간	강 의 제 목	강 사
3월 23일 (수)	09:00 ~ 10:00	블록암호 개요	홍득조 교수 (전북대)
	10:00 ~ 11:00	정보보안과 암호기술	
	11:00 ~ 12:00	블록암호의 알고리즘 구조	
	12:00 ~ 13:00	DES에 대한 차분구조	
	13:00 ~ 14:00	공개키 암호 개요	장남수 교수 (세종사이버대)
	14:00 ~ 15:00	인수분해 기반 암호	
	15:00 ~ 16:00	이산대수 기반 암호	
	16:00 ~ 17:00	타원곡선 이산대수 기반 암호	
3월 24일 (목)	09:00 ~ 10:00	해시함수	김종성 교수 (국민대)
	10:00 ~ 11:00	전용 해시함수	
	11:00 ~ 12:00	블록암호 기반 해시함수	
	12:00 ~ 13:00	메시지인증코드와 암호화 인증	
	13:00 ~ 14:00	난수발생기 개요	서석충 교수 (국민대)
	14:00 ~ 15:00	난수발생기 표준 및 구조	
	15:00 ~ 16:00	검증대상 난수발생기	
	16:00 ~ 17:00	난수발생기 구현적합성 검증 방법 및 잡음원 엔트로피 평가방법 소개	
3월 25일 (금)	09:00 ~ 10:00	부채널 분석 개념과 종류	김희석 교수 (고려대)
	10:00 ~ 11:00	부채널 분석 평가방법 및 기준	
	11:00 ~ 12:00	전력 분석 방법 및 대응기술	
	12:00 ~ 13:00	부채널 분석 연구 현황 및 사례	
	13:00 ~ 14:00	암호구현 개요	서화정 교수 (한성대)
	14:00 ~ 15:00	소프트웨어/하드웨어 암호 구현	
	15:00 ~ 16:00	블록암호/공개키 암호 구현	
	16:00 ~ 17:00	양자컴퓨터/양자내성 암호 구현	

교 육 개 요

○ 03월 23일(수)

제 목	블록암호	강 사	홍득조 교수 (전북대학교)
약 력	2006년 고려대학교 공학박사 2006년 ~ 2007년 고려대학교 정보보호기술연구센터 연구교수 2007년 ~ 2015년 국가보안기술연구소 선임연구원 2015년 ~ 전북대학교 IT정보공학과 부교수		
E-mail	deukjo.hong@jbnu.ac.kr		
내 용	1. 블록암호 소개 - 블록암호 알고리즘 개요 - 국내외 표준 블록암호 2. 블록암호의 운영 모드 - 암호화 운영 모드 - 인증 암호화 모드 3. 블록암호 알고리즘의 구조 - DES, AES, 경량 블록암호 4. DES에 대한 차분 공격		

제 목	공개키 암호	강 사	장남수 교수 (세종사이버대)
약 력	2004년 고려대학교 공학석사 2010년 고려대학교 공학박사 2010년 ~ 세종사이버대학교 부교수		
E-mail	nschang@sjcu.ac.kr		
내 용	1. 공개키 암호 개요 -공개키 암호 시스템 -대칭키 암호와 비대칭키 암호 2. 인수분해기반 암호 - 공개키 암호 : RSAES - 전자서명 : RSA-PSS 3. 이산대수기반 암호 - 키 공유 : DH - 전자서명 : DSA 4. 타원곡선 이산대수 기반 암호 - 타원곡선 연산 - 타원곡선 암호		

○ 03월 24일(목)

제 목	해시함수	강 사	김종성 교수 (국민대)
약 력	2006년 벨기에 루벤대학교 COSIC 암호학 공학박사 2007년 ~ 2008년 고려대학교 정보보호대학원 Post Doc. 2009년 ~ 2012년 경남대학교 e-비즈니스학과 조교수 2013년 ~ 국민대학교 정보보안암호수학과/금융정보보안학과 교수		
E-mail	jskim@kookmin.ac.kr		
내 용	1. 해시함수 -정의 및 사용 -안전성 2. 전용해시함수 - SHA-1 - SHA series 안전성 동향 3. 블록암호기반 해시함수 4. 메시지인증코드와 암호화 인증		

제 목	암호학적 난수발생기	강 사	서석충 교수 (국민대학교)
약 력	2011년 고려대학교 공학박사 2011년 ~ 2014년 삼성전자 2014년 ~ 2019년 국가보안기술연구소 2019년 ~ 국민대학교 정보보안암호수학과 부교수		
E-mail	scseo@kookmin.ac.kr		
내 용	1. 난수발생기 개요 2. 난수발생기 표준 및 구조 3. 검증대상 난수발생기 - 블록암호 기반 CTR_DRBG 동작 원리 - 해시함수 기반 HASH_DRBG 동작 원리 - HMAC 기반 HMAC_DRBG 동작 원리 4. 검증대상 난수발생기 구현적합성 검증 방법 5. 난수발생기 잡음원 엔트로피 평가 방법 소개		

○ 03월 25일 (금)

제 목	부채널 분석	강 사	김희석 교수(고려대)
약 력	2011년 고려대학교 공학박사 2011년 ~ 2012년 영국 Bristol 대학교 Post Doc. 2013년 ~ 2016년 한국과학기술정보연구원 선임연구원 2016년 ~ 고려대학교 인공지능사이버보안학과 교수		
E-mail	80khs@kroea.ac.kr		
내 용	1. 부채널 분석이란 -부채널 분석 개념 -부채널 분석의 중요성 2. 부채널 분석의 종류 - 부채널 분석에 활용 가능한 부채널 정보 - 분석 대상 및 공격 기법 3. 부채널 분석 평가 방법 및 기준 - 부채널 분석 평가 방법 및 기준 - 부채널 분석 관련 주요 연구 및 평가 기관 4. 전력 분석 방법 - 전력 분석이란 - 상관계수 전력 분석 5. 전력 분석 대응 기술 - 대칭키 암호 대응 기술 - 공개키 암호 대응 기술 6. 부채널 분석 연구 현황 - 대칭키 암호에 대한 부채널 분석 연구 현황 - 공개키 암호에 대한 부채널 분석 연구 현황 7. 부채널 분석 실제 사례		

제 목	암호구현	강 사	서화정 교수 (한성대)
약 력	2016년 부산대학교 공학박사 2015년 ~ 2015년 싱가포르 난양공대 인턴 2016년 ~ 2017년 싱가포르 과학기술청 연구원 2017년 ~ 한성대학교 사이버보안학과 교수		
E-mail	hwajeong84@gmail.com		
내 용	1. 암호구현 개요 -암호구현의 목적과 방법 2. 소프트웨어 암호구현 - 소프트웨어 암호 구현 요구 사항 및 특징 3. 하드웨어 암호구현 - 하드웨어 암호 구현 요구 사항 및 특징 4. 블록 암호구현 5. 공개키 암호구현 6. 양자컴퓨터 구현 7. 양자내성 암호구현		