

2021년 암호모듈검증

전문교육 심화과정 (온라인 교육)

한국인터넷진흥원(KISA)에서는 암호모듈 개발 시 활용할 수 있도록 암호모듈 구현 관점에서의 암호수학, 검증대상 암호알고리즘, 및 암호모듈검증 기준 해석 등의 전문교육을 개최하오니 많은 관심과 참여 부탁드립니다.



신청 기간

10. 11(월) ~ 10. 29(금)

접수방법

※ 우측 QR코드를 통해
교육신청 접수
※ 암호이용활성화 누리집
(seed.kisa.or.kr) 공지
통해 상세 내용 확인 가능



교육기간

11. 8(월) ~ 11. 12(금) (20시간/5일)

※ 세부 일정표는 차후 공지

교육방법

실시간 온라인 교육 (ZOOM)

교육대상

암호 및 암호모듈검증에 관심 있는
누구나 (200 명 대상)

※ 관련 선수 지식은 공지사항 참고

교육확정 안내

11. 3(수) 18시 개별 안내

문의처

(주)한국정보보호교육센터

02-921-1466 / edu@kisec.com

교육 커리큘럼

암호수학 (6시간)

1일차	RSA 구현 시 필요한 효율적 연산법, 소수판정법 등	한국정보보호교육센터 서광석 원장
2일차 (오전)	유한체 K, 타원곡선 E(K)에서의 효율적 연산 등	

검증대상 암호알고리즘 (6시간)

2일차 (오후)	검증대상 암호알고리즘 구현 (블록암호와 운영모드, 해시함수 등)	세종사이버대학교 장남수 교수
3일차	검증대상 암호알고리즘 구현 (공개키 암호, 전자서명 등)	

암호모듈검증 기준 해석 (8시간)

4일차	암호모듈검증 기준 설명 심화 암호모듈 구현 안내	국가보안기술연구소 이성하 김하은 연구원
5일차	엔트로피 검증 신기준 설명 HW 암호모듈 검증 방법 설명	

EVENT

01

교육 과정에 성실히
참여하고 (참석률 80% 이상),
설문조사 (2 회)에
참여하신 모든 분께
커피쿠폰을 드립니다!

02

교육 과정에 성실히
참여하고(참석률 80% 이상),
설문조사 (2 회)에 참여하신 분 중
3분을 추첨하여
애플워치를 드립니다!!