

2022년 국가 암호기술 전문인력 양성과정(8기) 모집 안내

한국암호포럼/국가보안기술연구소는 실용암호 연구 분야의
우수 암호인력을 발굴하고 육성하기 위하여
2022년 국가 암호기술 전문인력 양성과정(8기)을
운영합니다.

국가 암호기술 전문인력 양성과정(8기)

- ☐ 기간: 2022. 4. ~ 2022. 10.
- ☐ 과정 구성
 - 주제: 암호 응용 및 융합기술
 - 세부 과정: 암호 분석 기술, 암호 모듈의 안전성, IoT 무선 취약점과 암호, 디지털 포렌식과 암호 등
 - * 교육과정(안) 참조
- ☐ 모집인원: 15명 내외
- ☐ 3주~4주당 1회 교육 실시
 - * 교육 장소: 서울 및 대전
 - * 실습 등 포함
- ☐ 교육 주제별 과제 부여

주최 및 후원

- ☐ 주최: 한국암호포럼
국가보안기술연구소
- ☐ 후원: 국가정보원

모집 방법

- ☐ 지원자격
 - 암호 또는 정보보호 관련 학과에 재학중인 대학원생
 - SW 프로그래밍 기능자(C, Python 등)
- ☐ 제출물: 지원서
 - * 지원서 양식은 한국암호포럼 홈페이지에서 다운로드 (www.kcryptoforum.or.kr) 후 이메일로 제출
- ☐ 접수기한: 2022. 3. 23(수)
- ☐ 선정결과 공지: 2022. 3. 31(목)
 - * 개별 이메일로 결과 통보 예정
- ☐ 이메일 접수처 및 문의처:
kcryptoexpert@gmail.com

우수자 혜택

- ☐ 과제 수행 결과 평가를 통해 우수자를 선정하여 포상(상장 및 포상)
 - * 포상 규모는 추후 결정

□ 교육과정(안)

회차	날짜	교육 내용
1	4.20 (수)	○ 암호모듈의 안전성 및 검증 - 검증대상 암호알고리즘 및 구현적합성 검증방법 - 안전한 키 생성 및 관리 방안 - 검증대상 암호알고리즘 개발 실습 - 암호모듈 주요 요구사항 개발 실습 - 과제: Simple 암호모듈 구현
2	5.25 (수)	○ 암호 HW 분석 기술 - HW 분석기술 개요 - 펌웨어 덤프 및 역분석 실습 - 과제: 메모리 펌웨어 덤프 실습
3	6.15 (수)	○ 부채널 분석기술 - 부채널 분석 이론 - 부채널 분석 실습 (실험 환경 구축) - 과제: 암호모듈 부채널 취약성 분석
4	7.6 (수)	○ 네트워크 보안 제품과 관리 기술 - 네트워크 보안 제품 개요 - 네트워크 보안 제품 동작 원리 및 설계 - 암호키 관리 기술 및 응용 - 네트워크 보안 제품 구현 실습 - 과제: 네트워크 보안제품 개발 및 트래픽 분석
5	8.3 (수)	○ IoT 무선취약점과 암호 - 비표준 IoT 무선 취약점 사례 - 드론 보안 취약점 및 대응 방안 - SDR & USRP 소개 - FM 라디오 및 차량 스마트키 신호 복조 실습 - 과제: USRP를 활용한 FM 라디오 수신
6	8.31 (수)	○ 디지털 포렌식과 암호 - 저장매체 기반 암호화 방식 - USB 보안 저장매체 포렌식 - FDE, TPM, DRM 등 안티포렌식 대응 - 과제: FDE 기반 취약점 실습
7	9.28 (수)	현장 견학
		○ 양자컴퓨터와 양자암호 - 양자컴퓨터를 이용한 공개키암호 공격 - 양자 키분배 장치 소개

* 교육 일정 및 내용은 COVID-19 상황 등으로 조정될 수 있음

* 위 교육 외에, 발대식, 수료식, 통합워크샵 및 간담회 등이 별도 일정으로 진행될 수 있음