**[크립토랩 소개]**

크립토랩은 동형암호 원천기술 포함 다양한 특허를 보유하고 있고, 동형암호 기반의 서비스를 개발하고 있는 차세대 데이터 보호기업 입니다.

동형암호는 전세계적으로 활발한 투자가 이루어지고 있는 분야 입니다. Microsoft, Intel, IBM, Facebook 등 대기업에서 연구 중임은 물론, `20년 Duality Technologies, Inpher 를 포함한 다수의 동형암호 스타트업 들이 US$ 10M 이상의 투자 유치에 성공한 것을 볼때 향후 전망도 좋습니다.

크립토랩은 보유한 원천기술 기반으로 금융, 의료, 제어, 그리고 마케팅 등 사회 각 분야의 민감한 데이터를 안전하게 보호하면서 데이터를 분석하는 동형통계 분석도구와 암호화된 데이터의 머신러닝, 딥러닝 등 다양한 AI기술을 접목하여 4차산업혁명 시대를 선도해 나갈 것입니다. 이를 통해 최고의 데이터 동형암호 스타트업으로 성장할 것입니다.

크립토랩에 대한 보다 자세한 정보는 홈페이지(https://www.cryptolab.co.kr) 를 참고하세요.

**1. 양자내성암호 (PQC) 알고리즘 및 전환기술 연구개발**

* 기간: 2개월 (협의 후 기간 추가 가능)
* 처우: 월 200만원.

본 인턴쉽을 성공적으로 완료한 분은 우선 채용함은 물론 최신형 아이패드프로를 드립니다.

**[주차별 교육 내용]**

* 1주차: PQC 교육
* 2주차: PQC 응용분야 및 현재 공개키 암호를 PQC로 전환하기 위해 필요한 PQC Transition 을 위해 필요한 항목 교육
* 3주차: PQC 알고리즘 개발 및 적용 - 1
* 4주차: PQC 알고리즘 개발 및 적용 - 2
* 5주차: PQC Transition 기술 개발 - 1
* 6주차: PQC Transition 기술 개발 - 2
* 7주차: PQC Transition 기술 개발 - 3
* 8주차: Demo & 개발된 프로그램이 향후 적용 가능한 분야 소개

**[필요 직무능력]**

2달동안 본 실습을 완료하기 위한 직무능력은 아래와 같습니다.

* 암호 기초 지식 - 공개키, 대칭키 암호. (동형암호 기술까지 이해할 필요는 없습니다. 회사에서 실습기간중에 교육합니다.)
* C/C++ 사용 암호라이브러리 개발 및 C/C++ 기반 암호라이브러리 활용 경험 (OpenSSL, BoringSSL, mbedTLS 와 같은 오픈소스)

그리고 아래 경험이 있다면 더욱 좋습니다.

. PQC 알고리즘 연구/개발 경험.

. 암호키 발급 포함 기존 오픈소스 (예: OpenSSL, BoringSSL, mbedTLS) 를 활용한 key lifecycle management 개발 경험.

**[실습종료 후 학생 습득 가능 역량 기술]**

실습을 성공적으로 완료할 경우 PQC 에 대해 현업에서 필요로 하는 아래 역량을 키울 수 있을 것입니다.

* 공개키 암호와 PQC 암호의 차이 및 장단점.
* PQC 알고리즘 활용 방안 실습
* PQC Transition 의 필요성 이해 및 대응을 위한 기술 연구개발

**2. 동형암호 교육 및 WebAssembly를 사용한 동형암호 라이브러리 개발**

* 기간: 2개월 (협의 후 기간 추가 가능)
* 처우: 월 200만원.

본 인턴쉽을 성공적으로 완료한 분은 우선 채용함은 물론 최신형 아이패드프로를 드립니다.

**[주차별 교육 내용]**

* 1주차: 동형암호 개념 교육
* 2주차: WebAssembly 학습
* 3주차: WebAssembly로 포팅 할 simple 동형암호 소스코드 학습 및 코드 개발 준비
* 4주차: WebAssembly 기반 동형암호 코드 개발 - 키생성
* 5주차: WebAssembly 기반 동형암호 코드 개발 - 암/복호화
* 6주차: WebAssembly 기반 동형암호 코드 개발 - 동형연산
* 7주차: WebAssembly 기반 동형암호 코드 개발 - Test
* 8주차: Demo & 개발된 프로그램이 향후 적용 가능한 분야 소개

**[필요 직무능력]**

2달동안 본 실습을 완료하기 위한 직무능력은 아래와 같습니다.

* 암호 기초 지식 - 공개키, 대칭키 암호 (동형암호 기술까지 이해할 필요는 없습니다. 회사에서 실습기간중에 교육합니다.)
* C/C++ 사용 암호라이브러리 개발 경험
* C/C++ 기반 암호라이브러리 활용 경험 (OpenSSL, BoringSSL, mbedTLS 와 같은 오픈소스)
* C++ 프로그램 최적화 경험

아래 경험이 있다면 더욱 좋습니다.

* WebAssembly 개발 경험
* 블록체인 개발 경험

**[실습종료 후 학생 습득 가능 역량 기술]**

실습을 성공적으로 완료할 경우 PQC 에 대해 현업에서 필요로 하는 아래 역량을 키울 수 있을 것입니다.

* 공개키 암호와 PQC 암호의 차이 및 장단점 이해
* PQC 알고리즘 활용 방안 실습
* PQC Transition 의 필요성 이해 및 대응을 위한 기술 연구개발

**3. 동형암호 교육 및 동형암호 플랫폼 프론트엔드 개발**

* 기간: 2개월 (협의 후 기간 추가 가능)
* 처우: 월 200만원.

본 인턴쉽을 성공적으로 완료한 분은 우선 채용함은 물론 최신형 아이패드프로를 드립니다.

**[주차별 인턴십 내용]**

* 1주차: 동형암호 개념 및 동형암호 개발 프레임워크 교육
* 2주차: 동형암호 플랫폼 교육 및 프론트엔드 기술 (React) 학습
* 3주차: 동형암호 플랫폼 프론트엔드 개발 - 동형암호 프로젝트 관리 UI
* 4주차: 동형암호 플랫폼 프론트엔드 개발 - 동형암호 프레임웍 기반 프로그래밍 지원 UI
* 5주차: 동형암호 플랫폼 프론트엔드 개발 - 동형암호 프레임웍 기반 프로그래밍 지원 UI
* 6주차: 동형암호 플랫폼 프론트엔드 개발 - 동형암호 리소스 관리 UI
* 7주차: 동형암호 플랫폼 프론트엔드 개발 - Test
* 8주차: Demo & 개발된 프로그램이 향후 적용 가능한 분야 소개

**[필요 직무능력]**

2달동안 본 실습을 완료하기 위한 직무능력은 아래와 같습니다.

* React 기반 프론트엔드 개발 경험
* Jupyter노트북 사용경험
* 암호 기초 지식 - 공개키 암호 작동 방식 이해

아래 경험이 있다면 더욱 좋습니다.

* 파이썬 플라스크, 장고 기반 백엔드 개발 경험
* Docker 활용, 구성 경험
* AWS 등 클라우드 기술 활용 경험

**[실습종료 후 학생 습득 가능 역량 기술]**

실습을 성공적으로 완료할 경우 Privacy Enhancing Computing의 핵심 기술 중 하나인 동형암호 알고리즘을 이해할 수 있을 것으로 예상합니다. 현재 이쪽 분야 전문가는 매우 부족합니다.

**4. 동형암호 교육 및 파이썬 기반 동형암호 프레임워크를 이용한 동형 통계함수 개발**

* 기간: 2개월 (협의 후 기간 추가 가능)
* 처우: 월 200만원.

본 인턴쉽을 성공적으로 완료한 분은 우선 채용함은 물론 최신형 아이패드프로를 드립니다.

**[주차별 인턴십 내용]**

1주차: 동형암호 개념 및 동형암호 플랫폼 교육

2주차: 파이썬 동형암호 프레임워크 학습

3주차: 개발 대상 통계함수(t검정, f검정,z검정, 회귀분석, 기타 통계분석 등) 학습 및 코드 개발 준비

4주차: 동형암호 프레임웍 기반 동형 통계함수1 코드 개발

5주차: 동형암호 프레임웍 기반 동형 통계함수2 코드 개발

6주차: 동형암호 프레임웍 기반 동형 통계함수3 코드 개발

7주차: 동형암호 프레임웍 기반 동형 통계함수 테스트

8주차: Demo & 개발된 프로그램이 향후 적용 가능한 분야 소개

**[필요 직무능력]**

2달동안 본 실습을 완료하기 위한 직무능력은 아래와 같습니다.

* 통계 기초 지식 - 개발 대상이 될 통계함수에 대한 기초 지식 (통계함수 수식을 동형암호 프레임웍으로 구현하는 작업입니다.)
* Python 클래스기반 개발 경험

아래 경험이 있다면 더욱 좋습니다.

* R 기반 데이터 분석 경험 또는

파이썬 통계, ML 패키지(numpy, SciPy, Pandas, anaconda, scikit.learn) 활용 개발 경험

* C/C++ 개발 경험.

**[실습종료 후 학생 습득 가능 역량 기술]**

실습을 성공적으로 완료할 경우 Privacy Enhancing Computing 의 핵심 기술 중 하나인 동형암호 알고리즘을 이해할 수 있을 것으로 예상합니다. 현재 이쪽 분야 전문가는 매우 부족합니다.

그외 아래 역량도 습득할 수 있을 것으로 예상합니다.

* 통계 패키지에서 구현되는 통계함수, 알고리즘 기술 습득