Ch.15

암호화 모듈 원칙

대전대학교 정보보안학과
담당교수 조영복(ybcho@dju.ac.kr)

대전대학교 4차 산업혁신 선도대학

학습목차

암호화 모듈 원칙

학습내용

- 암호화 모듈
- IoT 암호화 모듈

학습목표

- 암호화 모듈을 학습하고 IoT 보안을 위해 적절히 사용될 수 있는 방법을 학습하고 이해한다.
- IoT 암호화 모듈을 학습하고 이해한다.

암호화모듈

암호화
알고리즘

암호화
방식

IoT 보안을 위해서는 **암호화 모듈**이 필요함

모듈

독립된 기능을 하는 함수나 변수들의 집합

모듈 자체가 하나의 프로그램

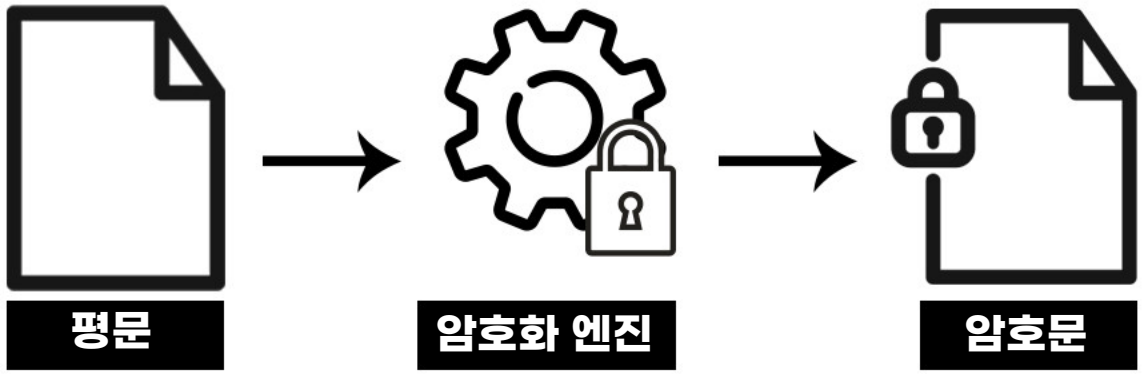
다른 프로그램의 부품으로 사용하여 재사용에 용이함

외장 모듈 : 개발자들이 만든 라이브러리

내장 모듈 : 내장 라이브러리

암호화 모듈

암호(대칭/비대칭), 난수 생성, 소수 판정, 해시, 전자서명, 인증 등 **암호기능**을
소프트웨어, 하드웨어, 펌웨어 또는 이를 조합하는 형태로 구현한 것



암호모듈 검증

(Korea Cryptographic Module. Validation Program:KCMVP)

암호모듈 검증을 통해 암호화 모듈의 안전성 평가

암호모듈 검증 (KCMVP)	
검증 대상	전자정부법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가 · 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도
검증 기준	
검증 기관	

암호모듈 검증

(Korea Cryptographic Module. Validation Program:KCMVP)

암호모듈 검증을 통해 암호화 모듈의 안전성 평가

암호모듈 검증 (KCMVP)	
검증 대상	소프트웨어, 하드웨어, 펌웨어
검증 기준	
검증 기관	

암호모듈 검증

(Korea Cryptographic Module. Validation Program:KCMVP)

암호모듈 검증을 통해 암호화 모듈의 안전성 평가

암호모듈 검증 (KCMVP)	
검증 대상	
검증 기준	KS X ISO, IEC 19790
검증 기관	

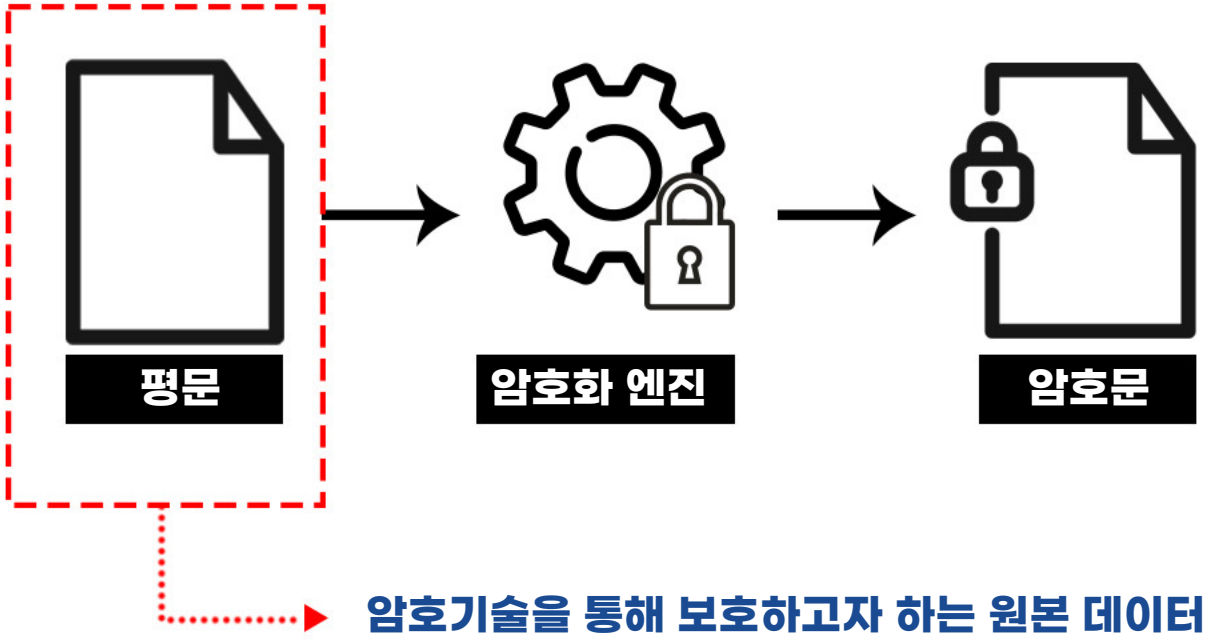
암호모듈 검증
(Korea Cryptographic Module. Validation Program:KCMVP)

암호모듈 검증을 통해 암호화 모듈의 안전성 평가

암호모듈 검증 (KCMVP)	
검증 대상	
검증 기준	
검증 기관	한국인터넷진흥원, 국가보안기술연구소

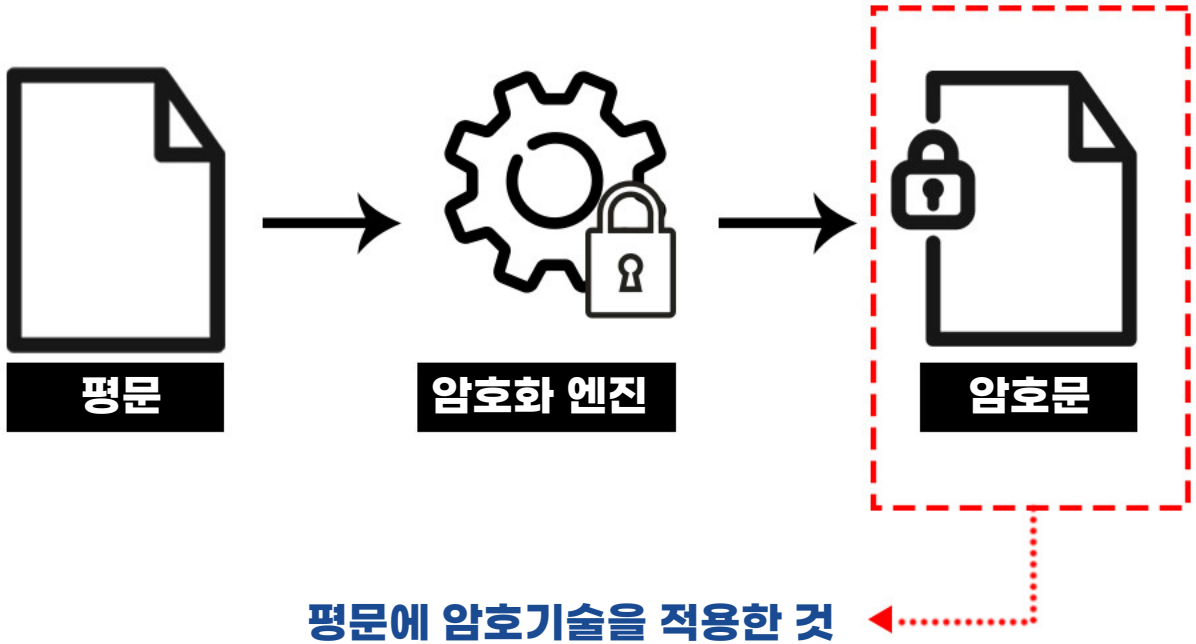
KISA 암호기술의 정의

중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 기술



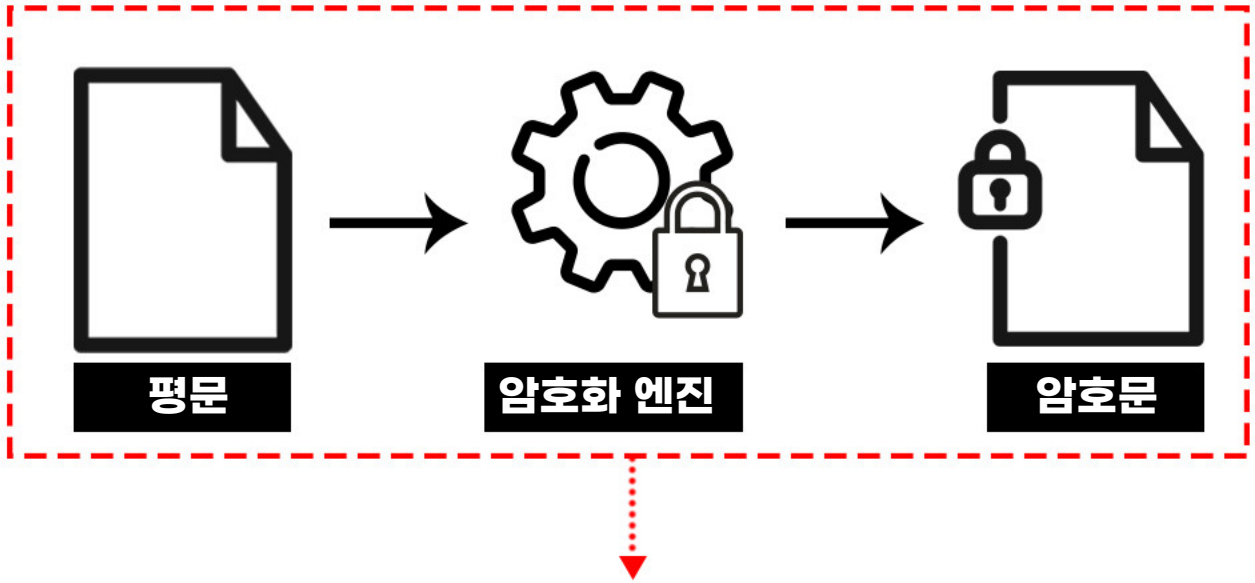
KISA 암호기술의 정의

중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 기술



KISA 암호기술의 정의

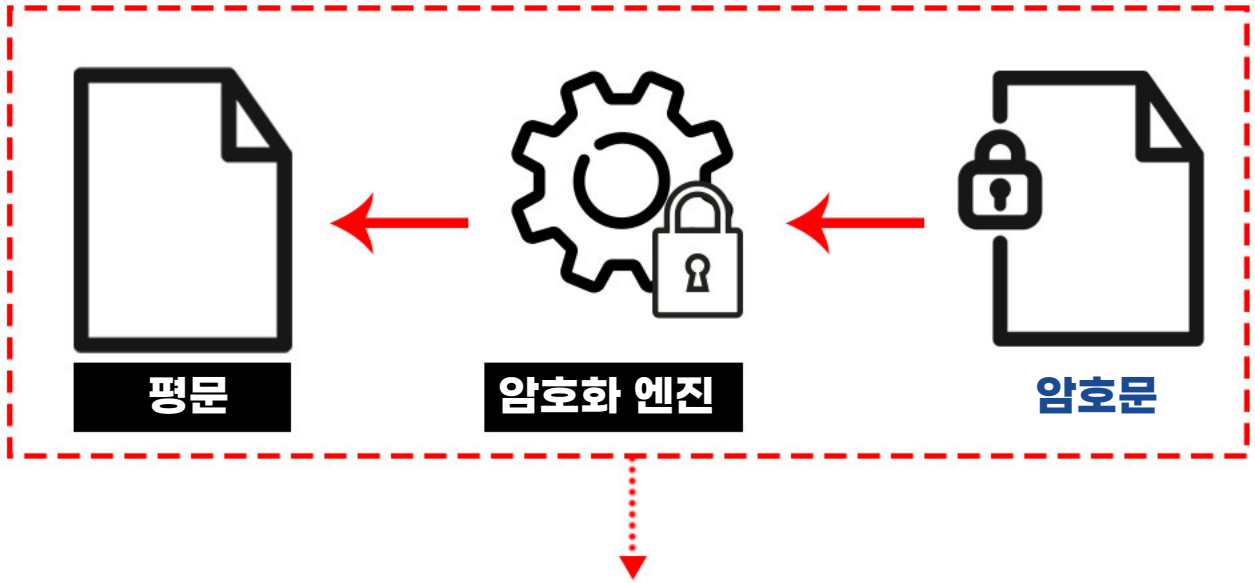
중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 기술



평문에 암호기술을 적용하여 암호문으로 변환하는 과정

KISA 암호기술의 정의

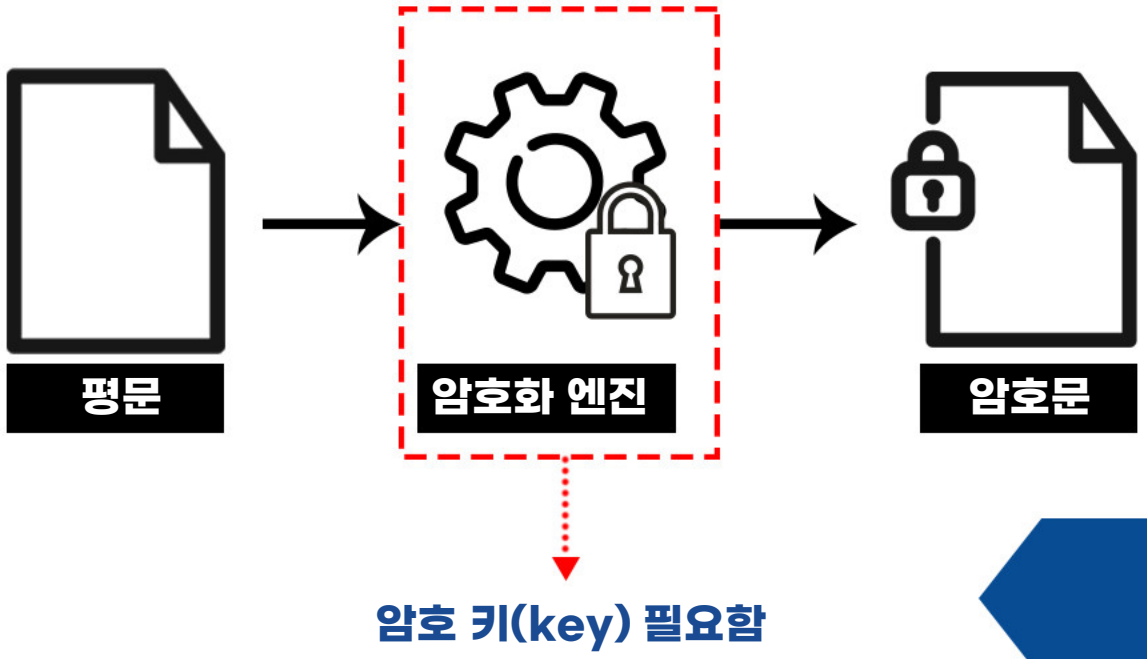
중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 기술



복호화 : 다시 평문으로 복원하는 과정

KISA 암호기술의 정의

중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 기술



암호 키는 비밀로 유지되어야 함

KISA 암호기술의 기능

기밀성 (Confidentiality)
무결성 (Integrity)
인증 (Authentication)
부인방지 (Non-repudiation)

허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 성질

KISA 암호기술의 기능

기밀성 (Confidentiality)
무결성 (Integrity)
인증 (Authentication)
부인방지 (Non-repudiation)

허락되지 않은 사용자 또는 객체가
정보를 함부로 수정할 수 없도록 하는 성질
(제3자에 의하여 변형되지 않았는지 확인하는 기능)

KISA 암호기술의 기능

기밀성 (Confidentiality)	
무결성 (Integrity)	
인증 (Authentication)	사용자 또는 객체의 디지털 정체성을 식별
부인방지 (Non-repudiation)	

KISA 암호기술의 기능

기밀성 (Confidentiality)	
무결성 (Integrity)	
인증 (Authentication)	
부인방지 (Non-repudiation)	정보를 보낸 사람이 나중에 정보를 보냈다는 것을 부인하지 못하도록 함

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- 암 · 복호화에 같은 암호 키를 사용하는 알고리즘
- 송신자와 수신자는 암호 키가 노출되지 않도록 비밀로 관리
- 치환 + 전치의 조합 = 연산 속도가 빠름
- 송 · 수신자 간 동일 키를 공유해야 하므로 많은 사람들과의 정보 교환 시 많은 키 관리해야 함

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- **블록 암호(Block Cipher) :**
  - 평문을 고정된 크기의 블록단위로 암 · 복호화 수행
  - 각 블록마다 동일한 키 사용
- 패딩(padding) : 원하는 크기로 평문을 나누는 기법
- 운용 방식(mode of operation) : 하나의 키로 여러 블록을 안전하게 처리

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- Shannon의 암호 이론 :
  - 전치/환자의 반복으로 평문의 통계적 성질이나 암호 키와의 관계가 나타나지 않아
  - 안전한 암호 구성 가능
- 블록 암호 알고리즘 :
  - 국산 : SEED, HIGHT, ARIA, LEA
  - 외산 : DES, AES

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- **스트림 암호(Stream Cipher) :**
  - 평문과 동일한 길이의 키스트림(key stream) 수열을 생성
  - 평문과의 XOR연산을 통하여 암・복호화 수행
- 동기식 스트림 암호 : 평문과 독립적으로 생성하는 경우
- 비동기식(혹은 자기동기) 스트림 암호 : 평문이 키스트림 수열에 영향을 미치는 경우
- 구현 여건이 제약된 환경에서 구현 용이, 무선 통신 등의 환경에 주로 사용
- 대표 알고리즘 : RC4, A5/1, A5/2

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- **공개키 암호(Public-key Encryption)**
- 대칭키 암호와 달리 암·복호화에 서로 다른 키를 사용하는 알고리즘
- 송신자 : 수신자의 공개키를 이용하여 암호화
- 수신자 : 자신의 공개키로 암호화된 암호문을 자신의 개인키로 복호화
- 수학적인 난제를 기반으로 설계 : 대칭키 암호에 비해 효율성 저하
- 여러 송신자가 하나의 공개키로 암호화 수행 : 키 관리에 유리
- 대표 알고리즘 : RSA, ElGamal, ECC

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- **전자 서명(Digital Signature) :**
  - 인터넷 상에서 본인임을 증명하기 위해 서명을 하는 수단
  - 공개키 암호를 거꾸로 활용하는 방식
- 개인키 소유한 사람만이 전자 서명 알고리즘을 통해 평문에 대한 서명 값 생성 가능
- 생성된 서명 값에 공개키 이용 시 평문 검증 가능 : 누구나 서명 검증 가능
- 대표 알고리즘 : DSA, RSA SIgnature, ECDSA

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

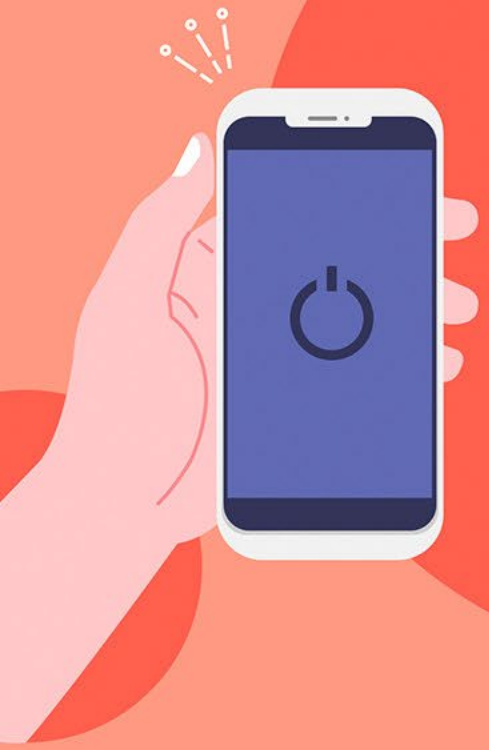
- 임의의 길이의 메시지를 입력으로 받아 고정된 길이의 해시 값을 출력하는 함수
- 암호 키 사용 안함 : 같은 입력에 항상 같은 해시 값
- 목적 : 무결성 제공

KISA 암호기술의 종류

대칭키 암호 (Symmetric-key Cryptography)	비대칭키 암호 (Public-key Encryption)	해시 함수 (Hash Function)

- **역상 저항성 :**
  - 어떤 해시 값에 대하여, 원래 입력 값을 찾는 것이 어려워야 함
  - 일방향성(One-wayness)
- **제2역상 저항성 :**
  - 어떤 입력 값에 대하여, 그 입력값의 해시 값과 같은 해시 값을 같은 또다른 입력값을 찾는 것이 어려워야 함
- **충돌 저항성 :** 같은 해시 값을 갖는 두 입력 값을 찾는 것이 어려워야 함

FIPS 140-2 표준
(Over-the-Air programming)



암호화 모듈을 IoT 환경에 접목하려면?

KISA

비대칭키 암호
(Public-key Encryption)

미국정부 암호화 모듈 표준 NIST 용어 차용

FIPS 140-2 암호화 모듈 인증 수행

FIPS 140-2 표준

(연방정부 정보처리 표준)

**승인되고 강력한 암호화 알고리즘 및 방식과 같은
안전한 보안 수단이 제품에 사용되고 있음을 보증**

개별 또는 다른 프로세스들이 제품을 활용하기 위해
어떻게 승인되어야 하는지 규정

모듈이나 구성품이 다른 시스템과 안전하게 상호작용하기 위해
어떻게 설계되어야 하는지 규정

FIPS 140-2 표준
(연방정부 정보처리 표준)

FIPS 140-2 인증의 제품에 따른 보안 레벨

1 레벨 1: 소프트웨어만 암호화하는 제품,매우 한정적인 보안 요건 적용

2 레벨 2 : 역할 기반 인증 필요

3 레벨 3 : 물리적 부당 변경 방지 기술을 추가, 인터페이스간 물리적/논리적 분리 요구

4 레벨 4 : 물리적으로 보호되지 않는 환경에서 작동되는 제품에 적용

FIPS 140-2 표준

(연방정부 정보처리 표준)

FIPS 140-2 인증 마크

FIPS 140-2 표준

(연방정부 정보처리 표준)

요구사항 범위

- 암호화 모듈 사양
- 암호화 모듈 포트 및 인터페이스
- 역할, 서비스 및 인증
- 유한 상태 모델
- 물리적 보안
- 운영 환경

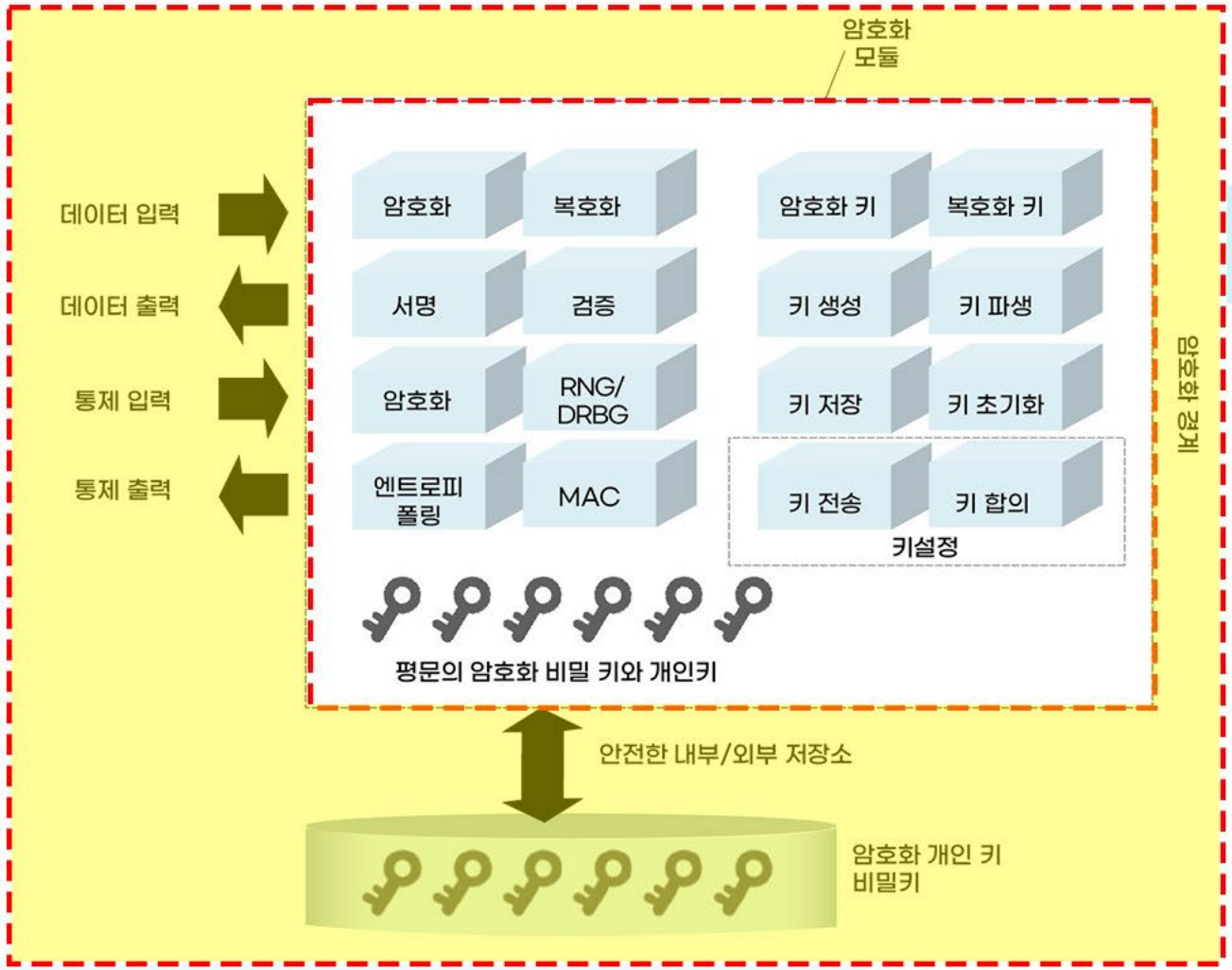
FIPS 140-2 표준
(연방정부 정보처리 표준)

요구사항 범위

- 암호화 키 관리
- 디자인 보증
- EMI/EMC
- 기타 공격 완화
- 자가 테스트

IoT 암호화모듈

암호모듈
(IoT 관점)



IoT 환경의 암호와 모듈

내장된 암호화 모듈을 사용하는
IoT구매자와 통합수행자는
암호화 모듈의 경계 밖에서
실행되고 있는 암호화 확인이 필요함

암호모듈
(IoT 관점)

장점

- 암호화 경계의 정의
- 모듈의 포트, 다른 인터페이스 보호
- 물리적 보안 및 시스템 통합 가능
- 암호화키 관리, 암호화 자체 테스트 및 장애 대응

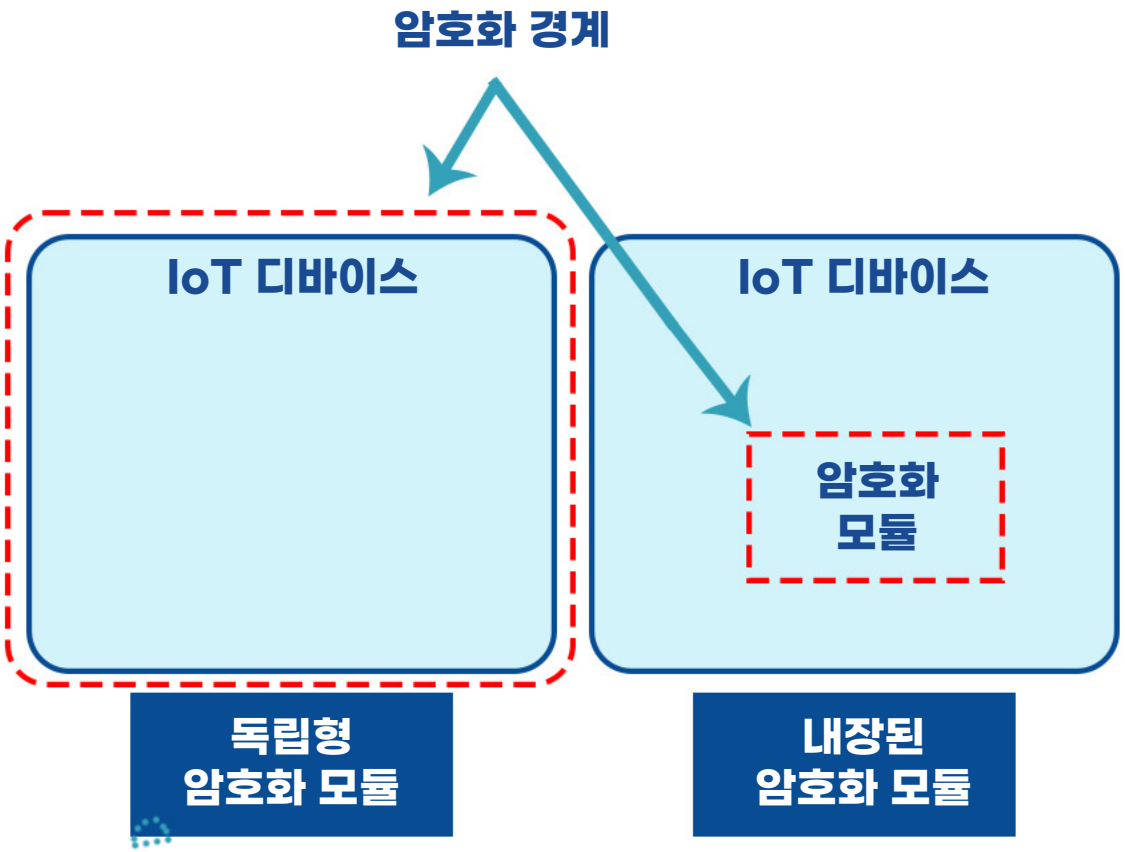
IoT 환경에서 암호모듈 사용 이유

침해로부터 암호화 키를 보호하는 것

키가 침해된 경우

암호화 데이터의 무결성 보호 불가

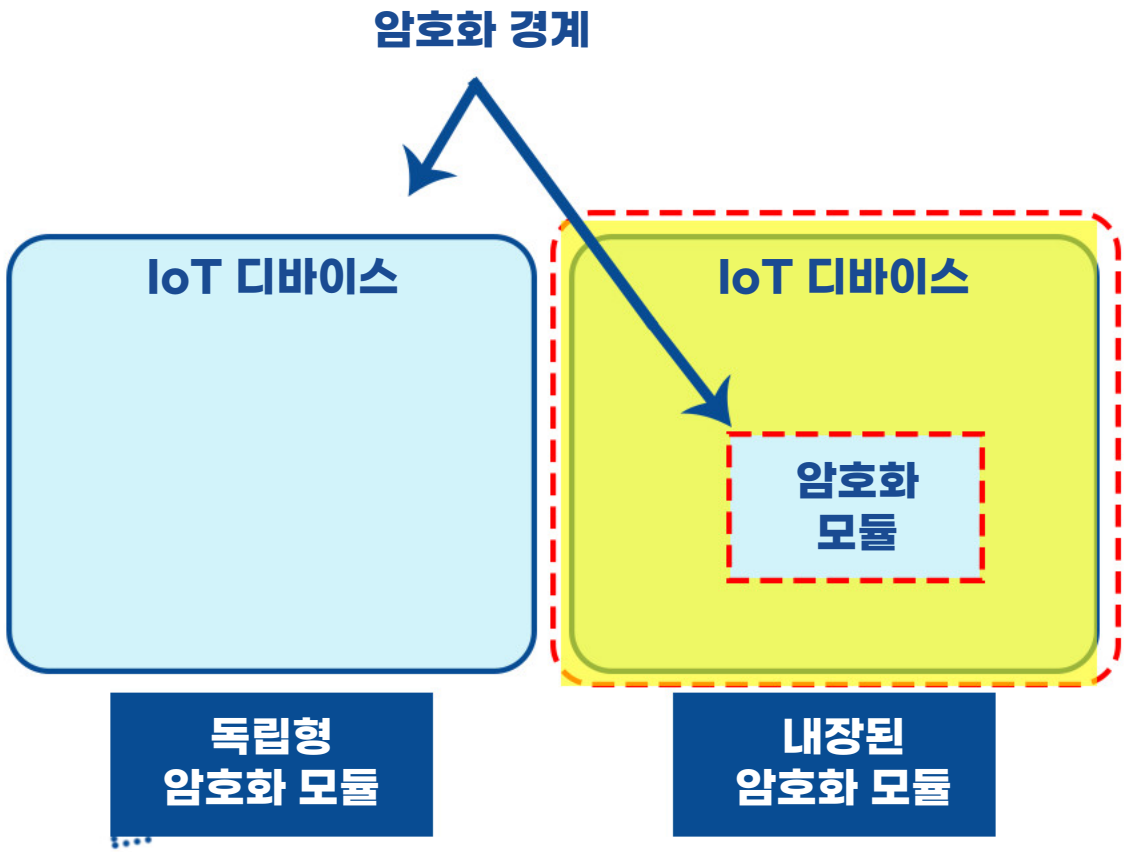
IoT 환경에서 암호모듈 사용 이유



IoT 관점에서 암호화 경계

모든 암호화 기능이 주어진 디바이스 내에서
실행되어야 하는 암호화 고립화

IoT 환경에서 암호모듈 사용 이유



내장된 암호화 모듈을 사용하는
IoT 구매자, 통합 수행자

암호화 모듈의 경계밖에서
실행되고 있는 암호화가 무엇인지
IoT 디바이스 공급 업자에게 반드시 확인

비검증암호모듈 사용 이유

작고 견고한 암호모듈	독립형 암호모듈
· 공격접점이 상대적으로 적음 · 상대적으로 적은 소프트웨어나 펌웨어에 그리고 하드웨어 로직을 유지	· 비암호화 로직 변경에 유연성이 줄어듬 · 중요도가 높은 구성요소 추가됨

보안 설계자, 시스템 보안 통합수행자는 암호화 구현 방법의 의의를 충분히 인식해야 함

IoT 환경에서 내부 암호화 모듈 통합

증명되지 않은 알고리즘의 사용은 원치 않음

신뢰할 수 있는 알고리즘 선택하여 안정성 확보

AES, ECDSA, ECDH 등 권장

IoT 환경에서 내부 암호화 모듈 통합

알고리즘 검증

모듈에서 작동하도록
암호화 알고리즘 구현의 정확성 검증

암호화 모듈 검증

- FIPS 140-2 보안 요구사항만족 여부 확인
- 적합성 테스트를 통해 실시됨

IoT 구현에서 FIPS 140-2 암호화 모듈 활용 및 배포

1. 임의 장치는 부모 암호모듈이 제공하는 암호 알고리즘 이외의 암호알고리즘 사용은 지양
2. 임의 디바이스는 암호화 모듈의 경계 외부에 평문 암호화 키를 저장해서는 안됨
3. 시스템 통합수행 시 암호화 모듈 정의에 앞서 데이터베이스 확인 및 컨설팅

IoT 구현에서 FIPS 140-2 암호화 모듈 활용 및 배포

4 배포 시 위협 환경을 고려한 암호화 모듈 선택

5 암호화 모듈 통합 시 실제 사용자 및 디바이스에 매핑되는지 확인 필요

6 복잡한 통합 구현 시, 조직은 암호화 적용, 암호화 모듈, 디바이스 구현, 통합을 상담

핵심정리

모듈이란?

독립된 기능을 하는 함수나 변수들의 집합이라 할 수 있고, 모듈 자체가 하나의 프로그램이면서 다른 프로그램의 부품으로 사용하여 재사용에 용이합니다.

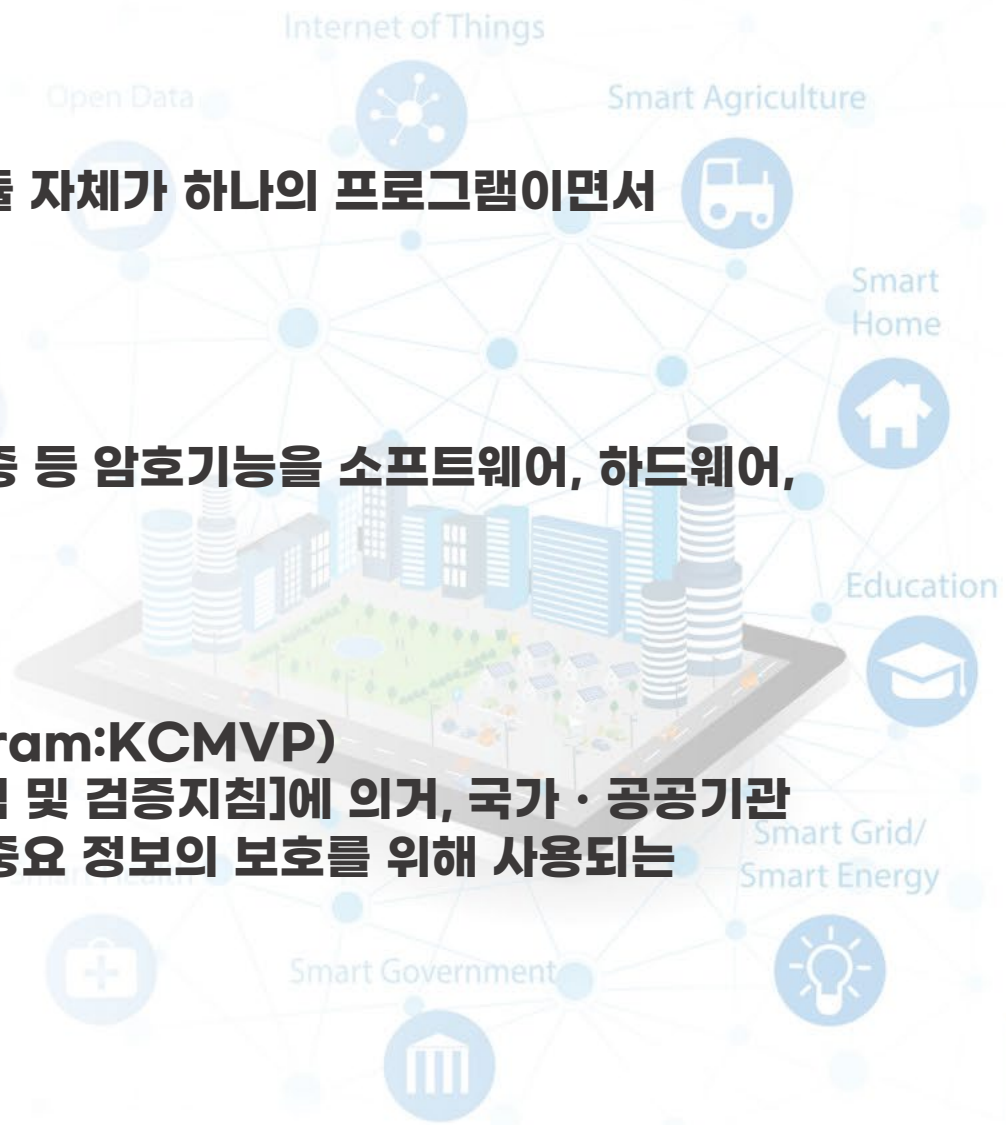
암호화 모듈이란?

암호(대칭/비대칭), 난수 생성, 소수 판정, 해시, 전자서명, 인증 등 암호기능을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합하는 형태로 구현한 것입니다.

암호모듈 검증

(Korea Cryptographic Module. Validation Program:KCMVP)

암호모듈 검증은 전자정부법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가 · 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도입니다.



FIPS(연방정부 정보처리 표준) 140-2 표준

IT 제품이 기밀은 아니지만 민감한 용도로 사용될 때 충족해야 할 암호화 및 관련 보안 요건을 규정한 미정부 표준

FIPS 140-2 인증의 제품에 따른 보안 레벨

- 레벨 1: 소프트웨어만 암호화하는 제품,매우 한정적인 보안 요건이 적용
- 레벨 2: 역할 기반 인증이 필요
- 레벨 3: 물리적 부당 변경 방지 기술을 추가, 인터페이스 간의 물리적/논리적 분리를 요구
- 레벨 4: 물리적으로 보호되지 않는 환경에서 작동되는 제품에 적용

IoT 환경에서 암호모듈 통합

- 알고리즘 선택
- 알고리즘 검증
- 암호화 모듈 검증

IoT 구현에서 FIPS 140-2 암호화 모듈 활용 및 배포

- 임의 장치는 부모 암호모듈이 제공하는 암호 알고리즘 이외의 암호알고리즘 사용은 지양
- 임의 디바이스는 암호화 모듈의 경계 외부에 평문 암호화 키를 저장해서는 안됨
- 시스템 통합 수행 시 암호화 모듈 정의에 앞서 데이터베이스 확인 및 컨설팅
- 배포시 위협 환경을 고려한 암호화 모듈 선택
- 암호화 모듈 통합 시 실제 사용자 및 디바이스에 매핑되는지 확인이 필요

QUIZ

QUIZ

1. 다음 중 암호화 모듈에 대한 설명으로 올바른 것은?

① 독립된 기능을 하는 함수나 변수들의 집합이라 할 수 있고, 모듈 자체가 하나의 프로그램이면서 다른 프로그램의 부품으로 사용하여 재사용 가능하다.

② IT 제품이 기밀은 아니지만 민감한 용도로 사용될 때 충족해야 할 암호화 및 관련 보안 요건을 규정한 미정부 표준이다.

③ 암호(대칭/비대칭), 난수 생성, 소수 판정, 해시, 전자서명, 인증 등 암호 기능을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합하는 형태로 구현한 것이다.

④ 국가 · 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증한다.

정답) ③

해설) 1번은 모듈에 대한 정의, 2번은 FIPS 즉 연방정보정보처리표준에 대한 정의, 4번은 우리나라 kisa에서 정의한 암호모듈검증에 대한 정의이다.

QUIZ

2. 다음 중 IoT 환경에서 암호모듈 통합 이유에 해당하지 않는 것은?

① 알고리즘 선택

② 알고리즘 검증

③ 암호화 모듈 검증

④ 연방정부정보처리 표준

정답) ④

해설) IoT 환경에서 암호모듈 통합은 국가에서 검증된 알고리즘 선택, 알고리즘 검증, 암호화 모듈 검증의 단계를 통해 보안성을 강화하기 위한 것이다.

QUIZ

3. 다음 중 IoT 구현에서 FIPS 140-2 암호화 모듈 활용 및 배포에 주의사항에 해당하지 않는 것은?

① 임의 장치는 부모 암호모듈이 제공하는 암호 알고리즘 이외의 암호알고리즘 사용은 지양한다.

② 임의 디바이스는 암호화 모듈의 경계 외부에 평문 암호화 키를 저장해서는 안된다.

③ 시스템 통합 수행 시 암호화 모듈 정의에 앞서 데이터베이스 확인 및 컨설팅이 필요하다.

④ AES 암호화/복호화에 AES-RSA 알고리즘을 사용한다.

정답) ④

해설) AES 암호화/복호화에 AES-GCM 알고리즘을 사용한다.