암호프로그래밍
CRYPTOGRAPHY PROGRAMMING

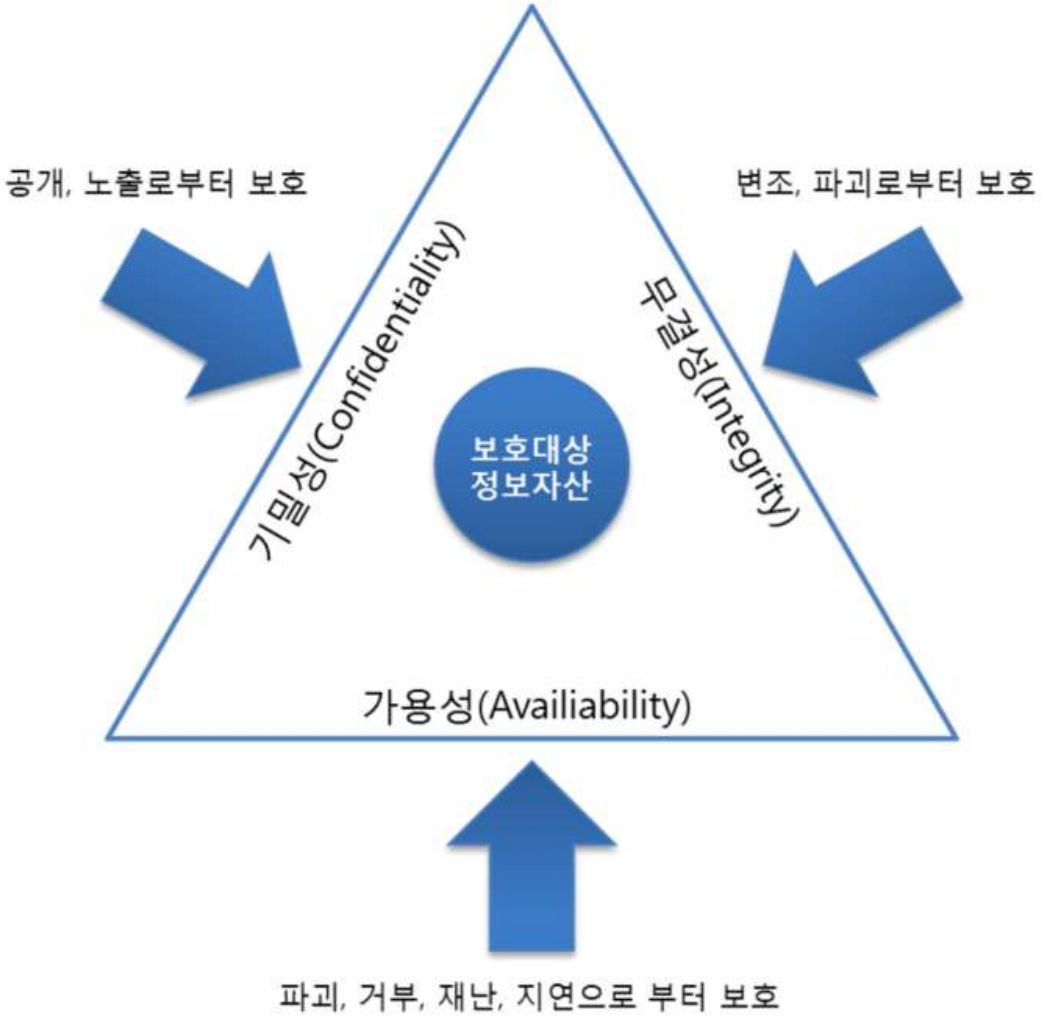
2. 암호와 정보보호

정보보호학과
이병천 교수

차례

2. 암호와 정보보호

보안의 3요소

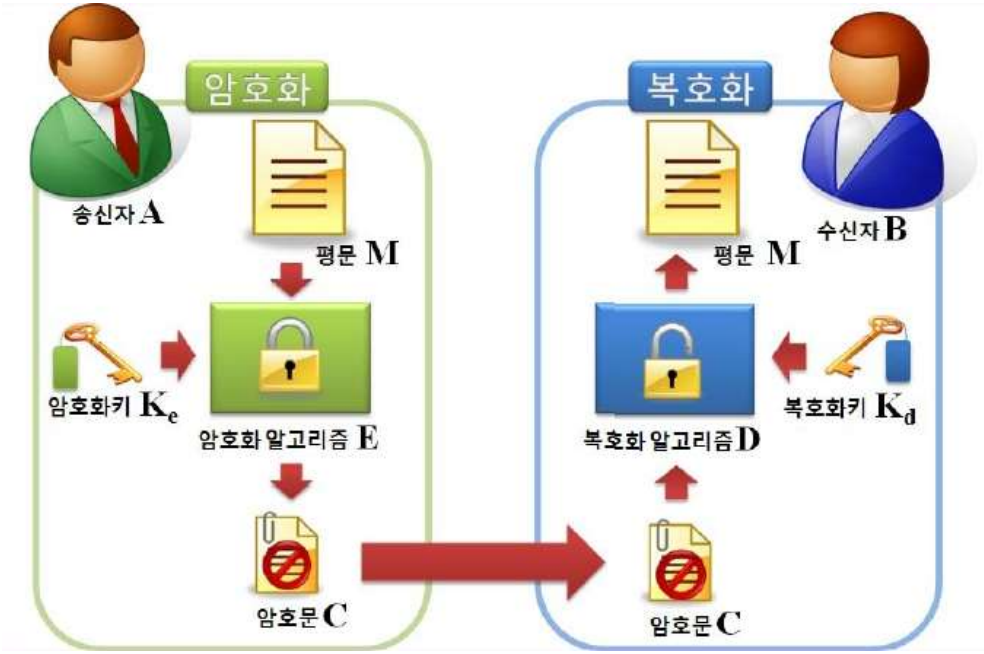

공개, 노출로부터 보호
변조, 파괴로부터 보호
기밀성(Confidentiality)
무결성(Integrity)
보호대상
정보자산
가용성(Availiability)
파괴, 거부, 재난, 지연으로 부터 보호

보안의 3요소 +

- 기밀성:
  - 공개, 노출로부터의 보호
  - 오직 허가된 사용자만이 정보, 시스템에 접근 가능해야 함
- 무결성:
  - 변조, 파괴로부터의 보호
  - 허가되지 않은 사용자에 의한 정보의 불법 변조, 손상을 방지
- 가용성:
  - 파괴, 거부, 재난, 지연으로부터의 보호
  - 허가된 사용자는 필요한 시간에 자산에 접근 가능해야 함
- 부인방지: 사용자가 행위를 부인하지 못함
- 인증, 접근통제:
  - 사용자의 신분을 확인하고 정보에 대한 적법한 권한을 부여
  - 인증되지 않은 공격자에게는 접근을 통제함

암호의 개념

- 암호(cryptography)
  - 암호의 어원: 그리스어 Cryptos에서 유래
  - 평문을 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 원래의 해독 가능한 상태로 복구하는 것



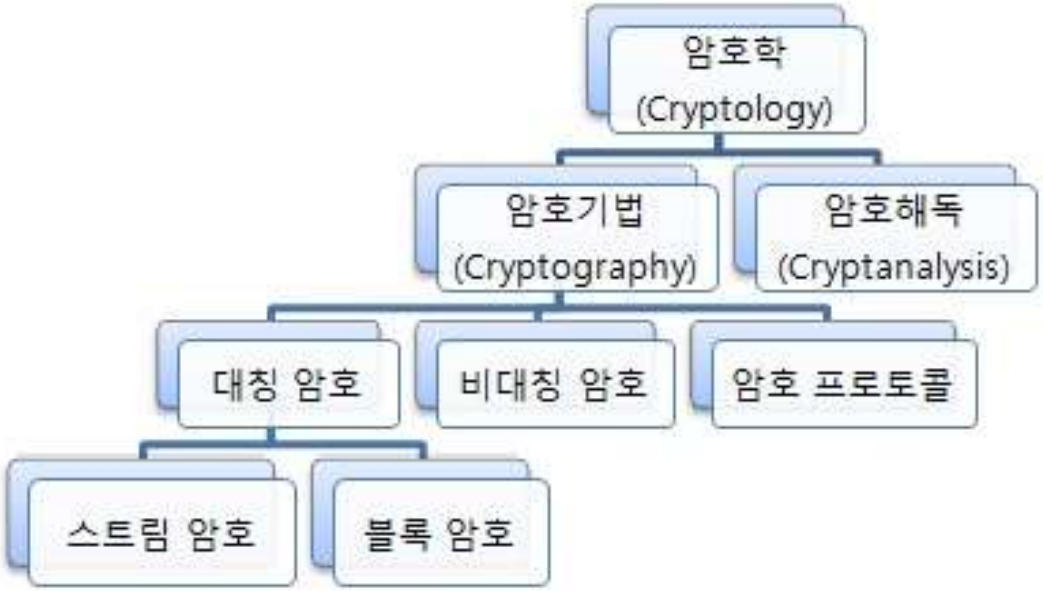
송신자 (sender)

도청자(eavesdropper) 공격자(attacker)

수신자 (receiver)

암호학

- 암호학(cryptology)
  - 암호학이란 정보를 보호하기 위해 사용할 수 있는 모든 수학적인 원리, 수단, 방법 등의 기반기술을 말함
  - 암호기술을 사용하지 않고 궁극적인 정보보호를 성취하는 것은 불가능

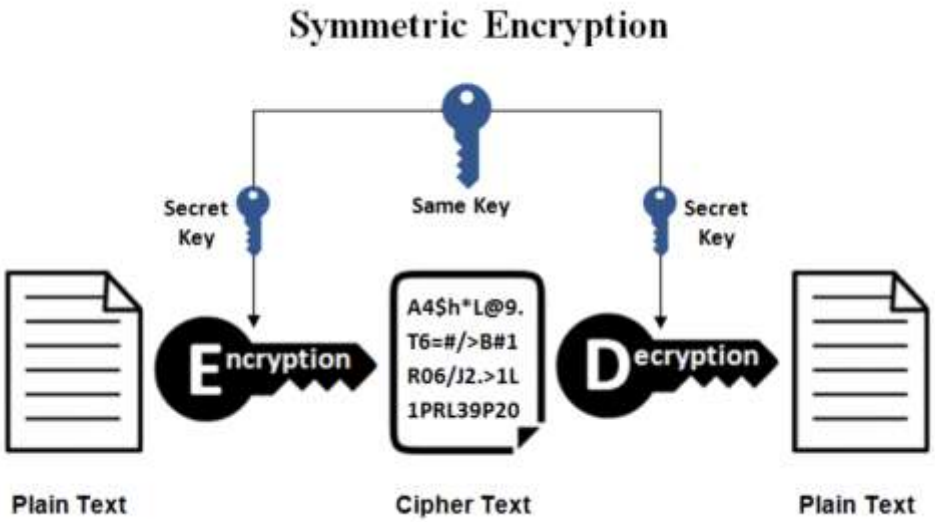


암호 관련 용어 설명

- 도청자(eavesdropper)
- 공격자(attacker)
- 암호설계(cryptography)
- 암호해독(cryptanalysis)
- 수동공격(passive attack)
- 능동공격(active attack)

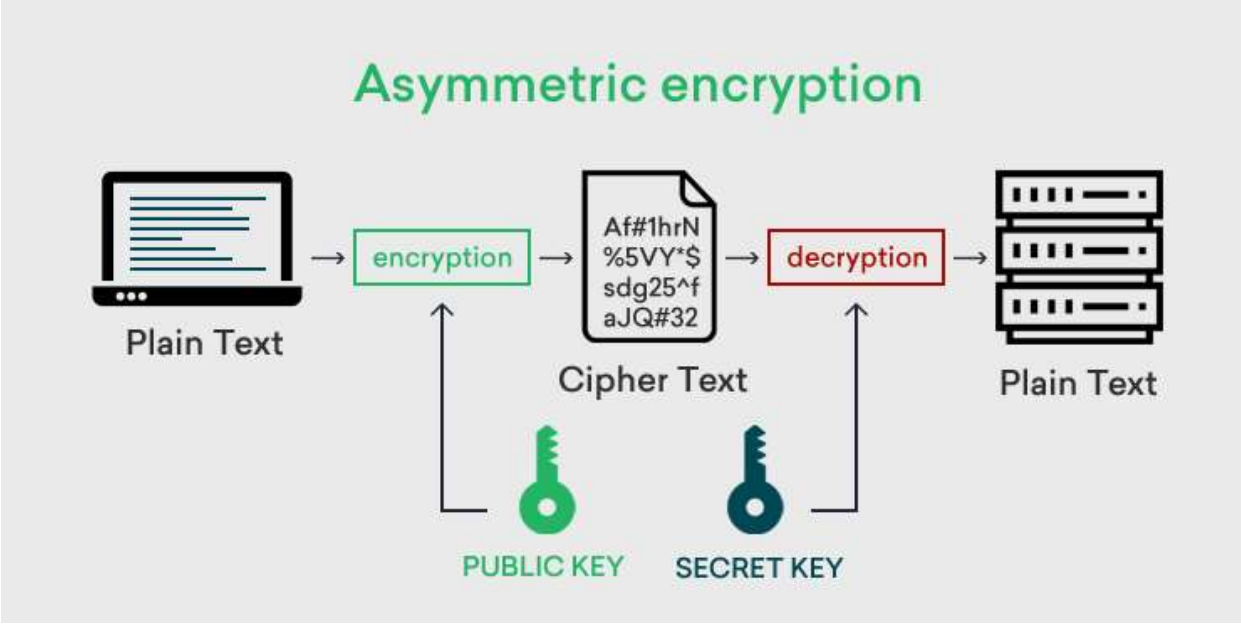
암호의 여러가지 방식

- 대칭키 암호 (비밀키 암호)
  - 암호화와 복호화 알고리즘에 동일한 키가 사용되는 방식의 암호
  - 비밀키는 제3자에게 알려지면 안되므로 송신자와 수신자는 사용되는 키를 비밀리에 공유하고 안전하게 보관해야 한다.
  - 블록 암호와 스트림암호



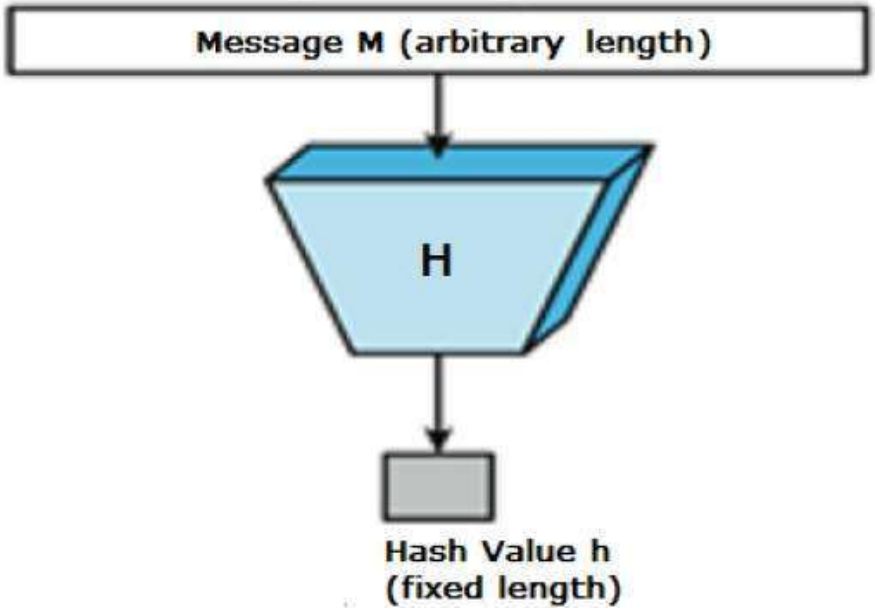
암호의 여러가지 방식

- 비대칭키 암호(공개키 암호)
  - 하나의 쌍이 되는 두 개의 키를 생성하여 하나는 암호화에 사용하고 다른 하나는 복호화에 사용한다.
  - 암호화에 사용하는 키는 공개할 수 있어서 공개키라고 부르고 복호화에 사용하는 키는 사용자만이 안전하게 보관해야 하는 키로 개인키(비밀키)라고 부른다.



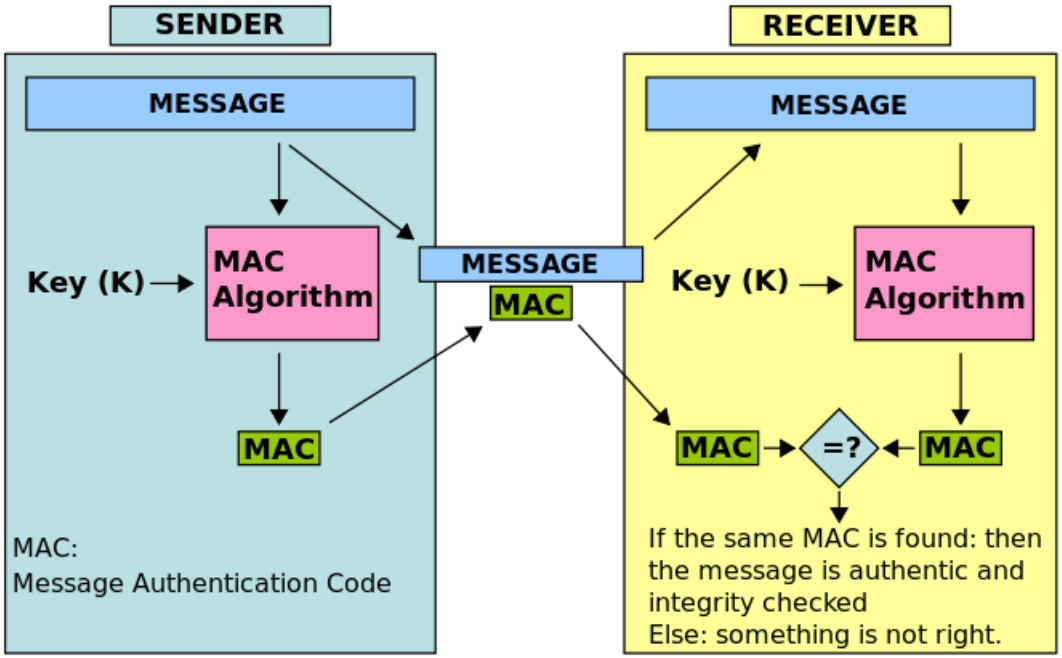
암호의 여러가지 방식

- 해시함수
  - 임의의 길이의 정보(비트스트링)를 입력으로 하여 고정된 길이의 출력값인 해시값을 생성해내는 함수
  - 해시값은 입력정보에 대한 변조할 수 없는 특징값을 나타내며 통신 중에 정보의 변조가 있었는지 여부를 확인하는 용도에 사용된다.



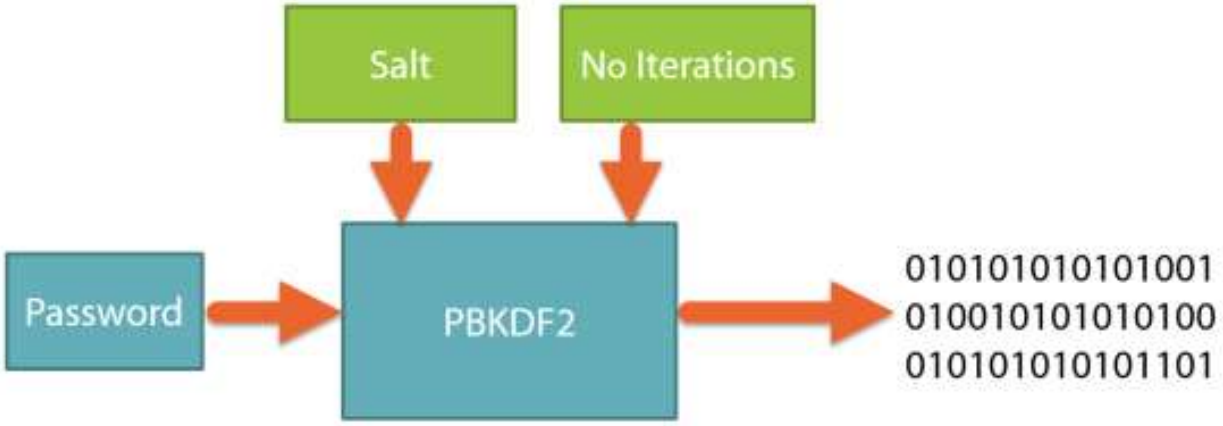
암호의 여러가지 방식

- 메시지인증코드 (MAC: Message Authentication Code)
  - 데이터가 변조(수정, 삭제, 삽입 등)되었는지를 여부를 검증할 수 있도록 데이터에 덧붙이는 코드
  - 송신자와 수신자는 비밀키를 공유하고 있으며 MAC 계산에 비밀키를 사용한다. 그러므로 송신자와 수신자만이 MAC을 계산하고 검증할 수 있다.



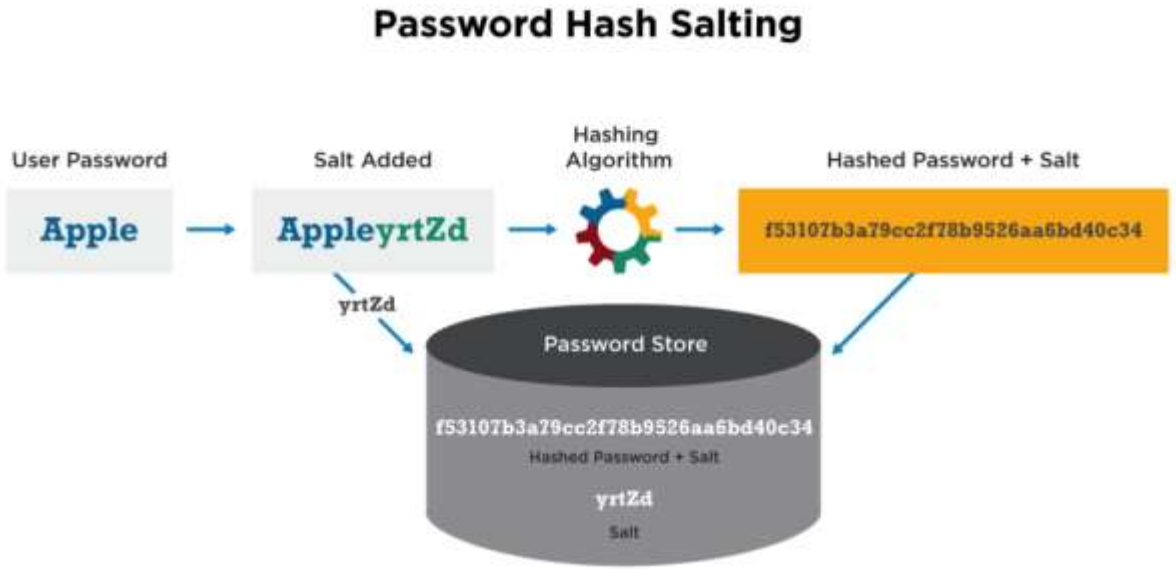
암호의 여러가지 방식

- 패스워드 기반 키생성함수 (PBKDF2)
  - Password-Based Key Derivation Function v2
  - 사용자가 입력하는 패스워드를 직접 암호알고리즘의 비밀키로 사용하는 것은 추측 가능한 키를 사용하게 되므로 위험
  - (1)사용자 입력 패스워드, (2)랜덤한 salt값, (3)반복횟수(iteration) 값을 이용하여 난수처럼 보이는 비밀키를 생성하여 사용



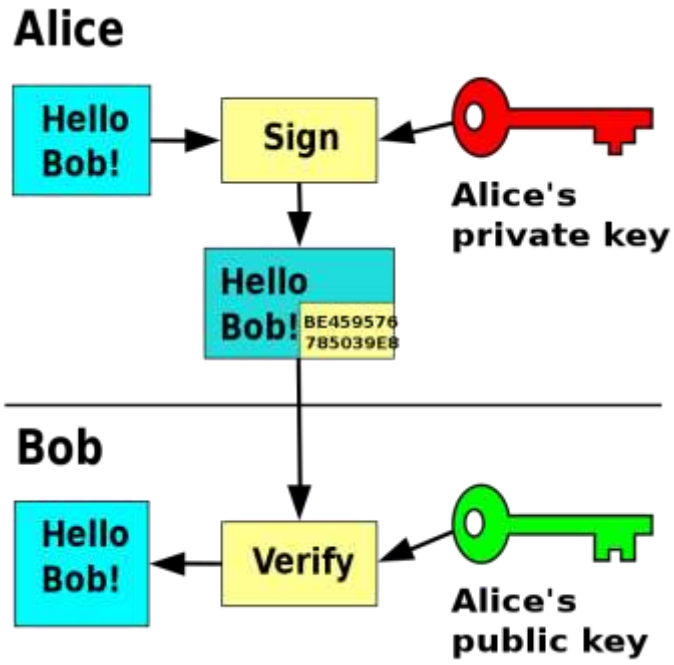
암호의 여러가지 방식

- 패스워드 해시 - 로그인 패스워드의 안전한 저장
  - 사용자 인증을 위해 서버는 사용자 패스워드를 저장해야 함
  - 패스워드를 그대로 저장하는 것은 관리자에게 노출
  - Hashed password + salt 로 저장
  - bcrypt 패키지 활용



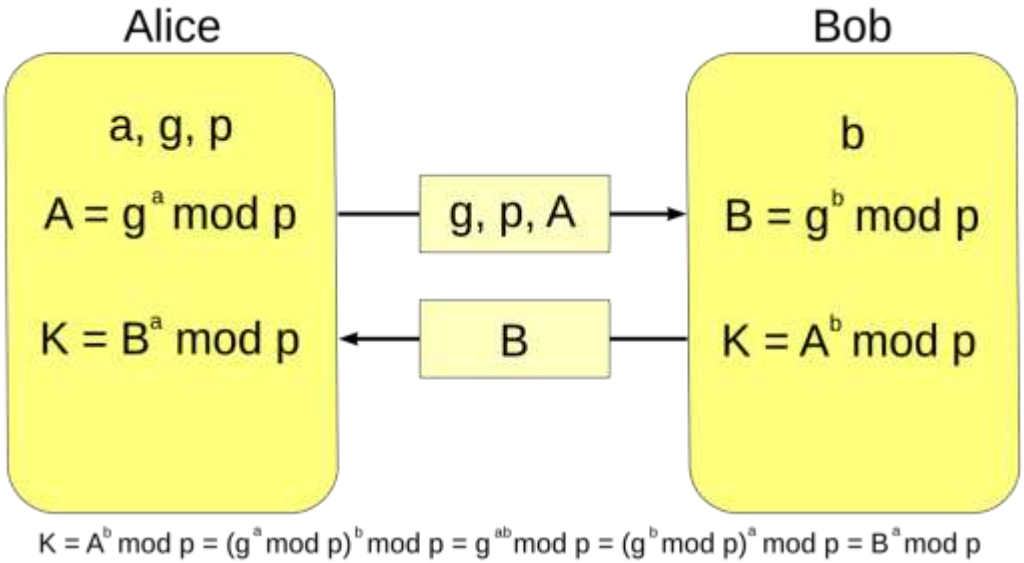
암호의 여러가지 방식

- 전자서명
  - 전자문서에 대한 전자적인 방식의 서명으로 서명자의 개인키로 서명을 생성하고 서명자의 공개키로 서명을 검증한다.
  - 개인키는 해당 서명자만이 가지고 있으므로 다른 사람이 서명을 위조할 수 없으며 서명자는 자신이 서명했다는 사실을 부인할 수 없다(부인방지 기능).



암호의 여러가지 방식

- 키합의 (key agreement)
  - 송신자와 수신자가 비밀키 암호를 사용하기 위해서는 미리 비밀키를 공유하거나 안전한 통신 채널을 사용하여 세션키를 전송하는 것이 필요하다.
  - 송신자와 수신자가 직접 만나지 않고도 공개된 통신채널을 통해서 특정한 방법으로 세션키를 안전하게 공유하는 방식을 키합의라고 한다.



암호의 여러가지 방식

- 인증기술 (Authentication)
  - 사용자 인증: 클라이언트(사용자)의 신분을 서버에 증명하고 로그인하는 기술
  - 메시지 인증: 전송하는 메시지가 변조되지 않고 송신자가 보낸 것임을 확인하는 기술

- 토큰인증 기술 (Token Authentication)
  - 1차 사용자 인증을 바탕으로 더 편리하게 사용할 수 있는 토큰을 발행하고 이를 사용하여 2차 인증하는 기술

정보보호를 위한 암호의 역할

- 정보화 사회란?
  - 정보의 축적, 처리, 전송 능력이 획기적으로 증대되면서 정보의 가치가 물질이나 에너지 이상으로 중요해지는 사회
  - 정보시스템, 정보서비스에 크게 의존하는 사회
  - 정보가 상품으로서의 가치를 인정받아 시장에서 유통되는 사회

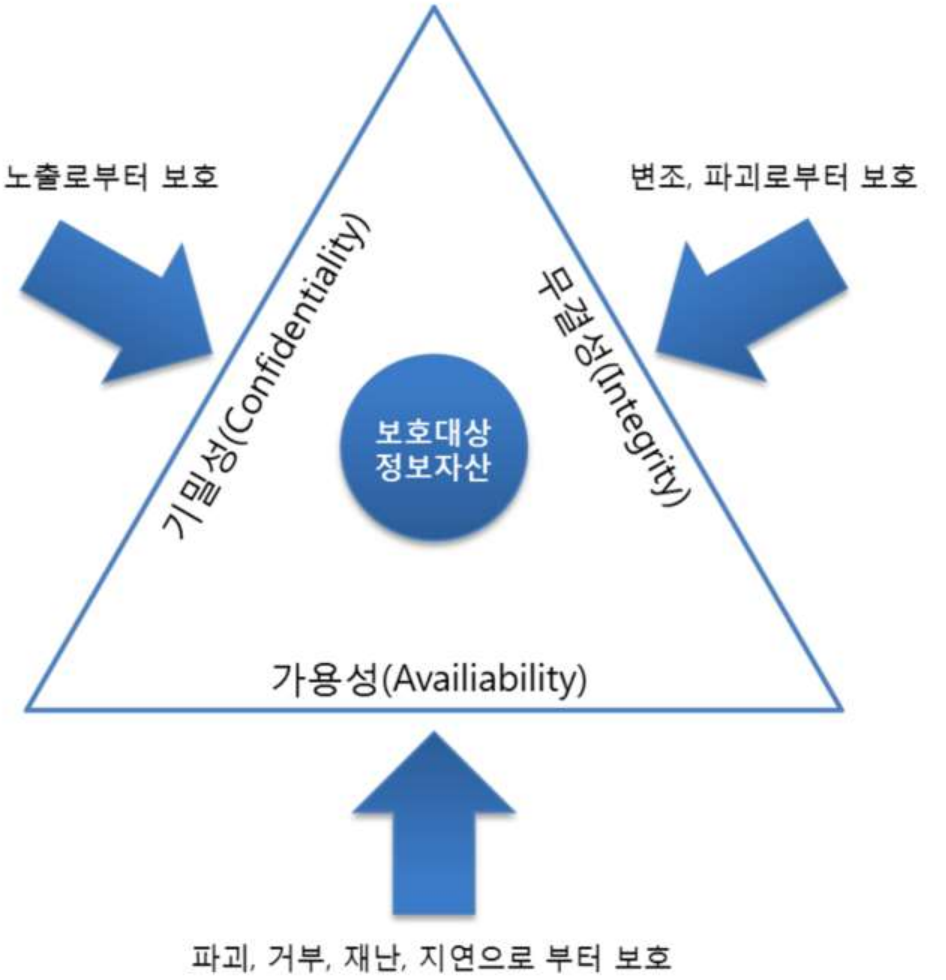
- 정보보호의 중요성
  - 정보시스템의 오류, 마비로 인한 피해
  - 정보의 불법적 노출시 피해, 개인정보를 이용한 사기
  - 해킹공격에 의한 피해
  - 산업스파이
  - 정보전

현대 암호가 제공해야 하는 정보보호 기능

- 기밀성:
  - 오직 허가된 사용자만이 정보, 시스템에 접근 가능해야 함
  - 암호기법: 암호화 (대칭키 암호화, 공개키 암호화)
- 무결성:
  - 허가되지 않은 사용자에 의한 정보의 불법 변조, 손상을 방지
  - 암호기법: 해쉬함수, 전자서명, 메시지인증코드
- 가용성:
  - 허가된 사용자는 필요한 시간에 자산에 접근 가능해야 함
  - 인증 및 접근제어, DOS/DDOS 방지
- 부인방지: 사용자가 행위를 부인하지 못함 (전자서명)
- 인증, 접근통제: 사용자의 신분을 확인하고 정보에 대한 적법한 권한을 부여

보안의 3요소를 제공하기 위한 암호기술

암호화
대칭키암호화
공개키암호화



해시함수
전자서명
메시지인증코드

인증 및 접근통제