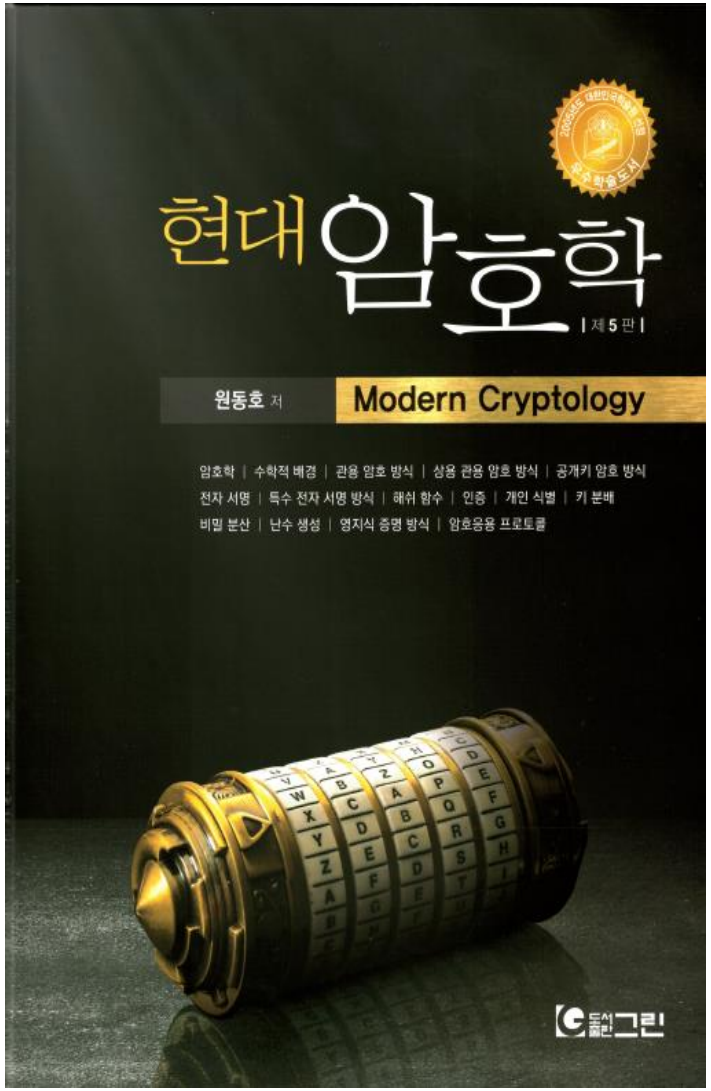
현대 암호학

한국IT 정보보안학부

교재소개



❖ 현대 암호학 (제6판)

- 도서출판 그린
- 저자 : 원동호

- 암호학
- 수학적배경
- 관용암호방식
- 상용관용암호방식
- 공개키암호방식
- 전자서명
- 해쉬함수
- 인증
- 개인식별
- 키분배
- ..

수업소개

❖ 도덕향 (dukhyang73@hanmail.net)

- 현대 암호학(제 6판)
- 도서출판 그린　　원동호저.

❖ 학점관련

- 전공필수
- 상대평가
  - 필기시험 - 중간고사 : 30, 기말고사 : 30
  - 과제 20 , 출석 20 (80%이상 출석 시 학점부여)

  - 과제
    - 1. 관용 암호 방식과 공개키 암호 방식의 암호 알고리즘을 하나 선택하여 조사하기
    - 2. 현재 우리가 사용하고 있는 시스템이나 응용 프로그램에 적용된 암호 알고리즘을 찾아보고 그 중 하나를 선택하여 분석 조사하기

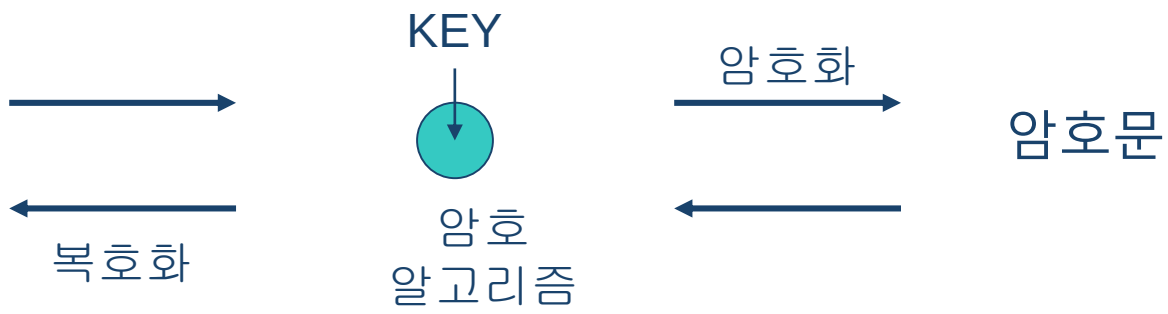
암호

❖ 암호가 갖춰야 할 특징

- 기밀성
- 무결성
- 인증

❖ 암호 과정

- 성격과 목적에 따라 과정의 차이는 있음.



암호

❖ 암호화 방식

- 양방향 암호화방식 (암호화,복호화 모두 가능)
  - 대칭키 (하나의 키 -> 암호,복호에 같은 키)
    - 예) AES
  - 비대칭키 (두개의 키 -> 다른 키)
    - 예) RSA

- 단방향 암호화방식 (암호화는 되지만, 복호화는 되지 않는 것)
  - 예) md5, sha

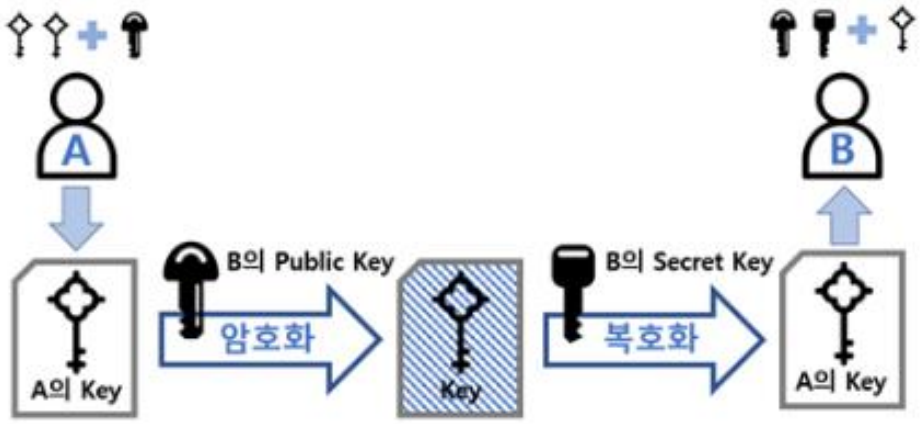
❖ 대칭키 암호

- 암호화 복호화에 같은 KEY 사용
- 필요로 하는 연산량이 매우 적고 빠름
- 대용량 데이터를 저장소에 보간할때, 중요한 데이터를 암호화해서 전송할 때 사용

- 송.수신자간의 사전 키 공유가 필요함.

❖ 비대칭키 암호

- 암호화, 복호화에 다른 KEY 사용
- 암호화키는 Public key 로써 암호화에만 사용.
  - 공유되어도 상관없음
- 복호화키는 Secret Key 로 복호화에 사용됨.
  - 절대 유출되어서는 안됨.
  - Secret Key를 가진 사람만 암호해독이 가능.

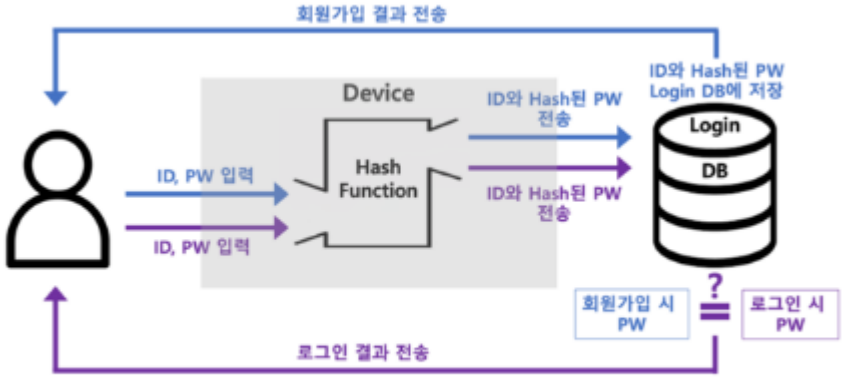


비대칭키암호의 사용 예시

❖ 해시암호

- 일방향 해시함수
- 암호화는 가능하지만 역방향 복호화는 불가능한 알고리즘

해시암호의 예시



해시암호의 사용 예시

- 어떤 서비스를 받기위해 로그인시, 패스워드 체크
- 전송중 데이터가 변경되었는지 여부를 판단하기 위한 무결성 체크
- 블럭체인

❖ 빅데이터와 4차산업혁명시대

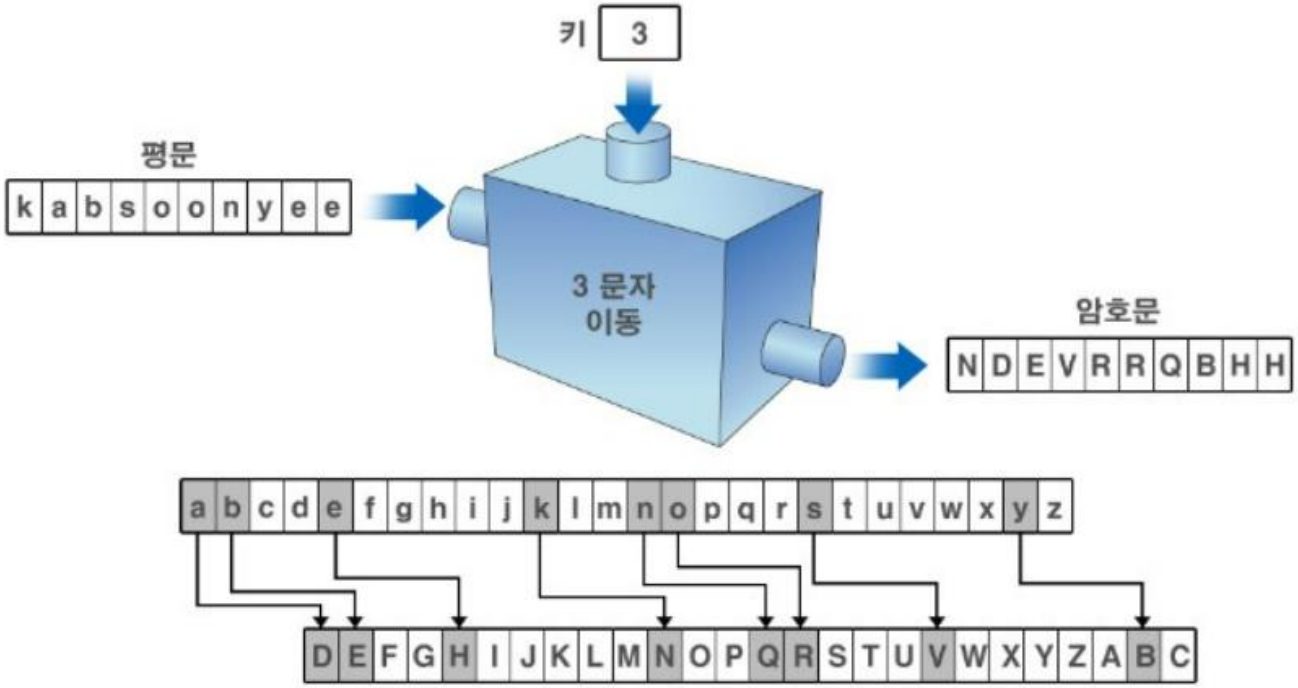
- 방대한 양의 빅데이터와 AI를 학습하고 활용하기 위해서 컴퓨터는 계속 발전.
- 발 맞추어 물리학계에서는 양자컴퓨터 상용화에 박차 가함.
  - 실용화 된다면 양자컴퓨터는 정말매우큰컴퓨팅파워에 가까운 컴퓨터 -> 비대칭암호 해독 가능.
- 암호학계는 차세대 비대칭키암호의 필요성이 대두되었고, 연구도 활발히 진행 중.

암호기술 분류

고대암호

❖ 로마 황제 줄리어스 시저 -> 시저암호

- 원본 메시지인 평문(plaintext)의 알파벳들을 몇 글자씩 밀려 써서 암호화 하는 방법



고대암호

❖ 앨런튜링

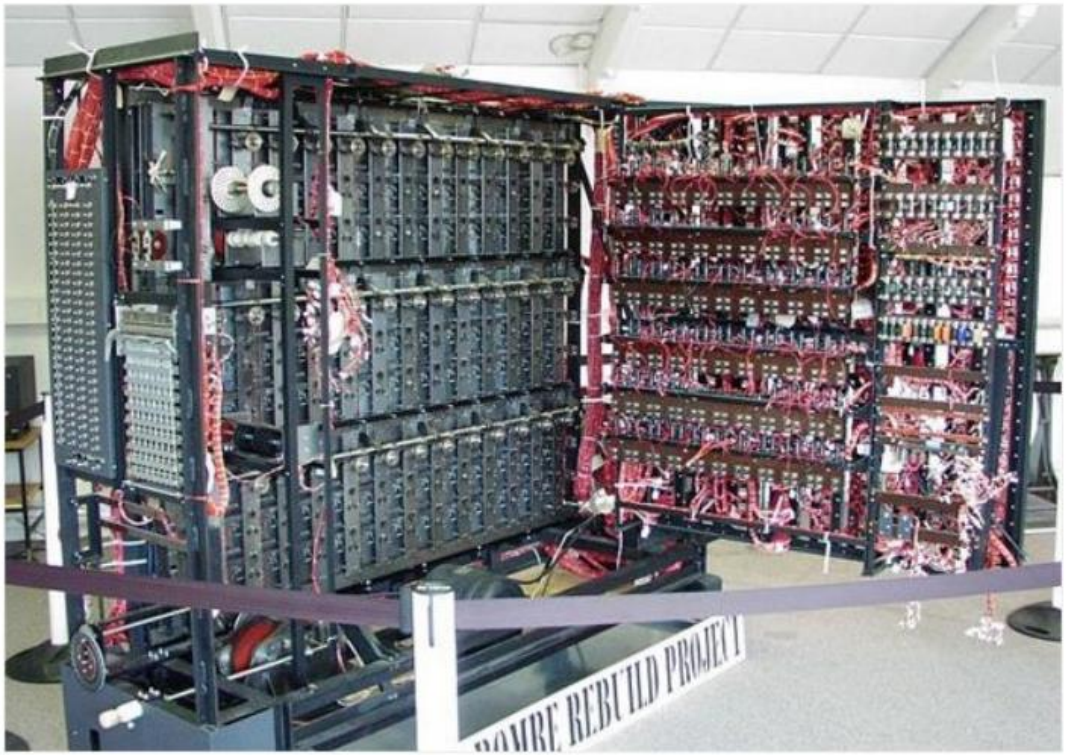
- 튜링 기계
- 프로그래밍이 가능한 가설적 기계 장치인 **튜링** 머신을 구상하여 제시함으로써 컴퓨터과학의 토대를 마련
- 세계2차대전 당시 암호해독반에서 근무하며 독일군의 에니그마 체계를 무너뜨려 연합군의 승리에 결정적 역할을 했던 인물

- 뛰어난 수학자였던 그가 청산가리가 든 사과를 먹고 자살하기까지.. 어떤 일이 있었던 것일까?

- -> 2015년 영화 <이미테이션 게임>

에니그마

2차 세계대전 당시 독일군이 사용했던 암호 기계 에니그마



튜링 봄베. 영국군이 독일 잠수함의 위치와 공격 계획을 꿰뚫어볼 수 있었던 것에는 튜링의 암호해독반의 공이 컸다.

암호학

❖ 암호학

- 암호법이나 암호해독법을 연구하는 학문
- 암호법 : 암호를 사용하여 비밀통신을 하는 절차를 의미한다.
- 암호해독법 : 비밀통신을 크랙하거나 해독하는 절차를 의미한다.

❖ 정보이론

- 클라우드셰넌 (Claude Shannon)이 고안.
  - 확산(Diffusion) : 평문을 구성하는 각각의 비트들의 정보가 여러개의 암호문 비트에 영향을 주어야한다.
  - 혼동(Confusion) : 평문과 암호문 사이의 관계를 알기 어려워야한다.