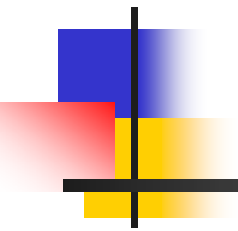
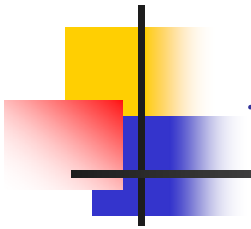


암호시스템



목차

1.대칭키 암호시스템

- DES
- Triple-DES
- SEED

2.공개키 암호시스템

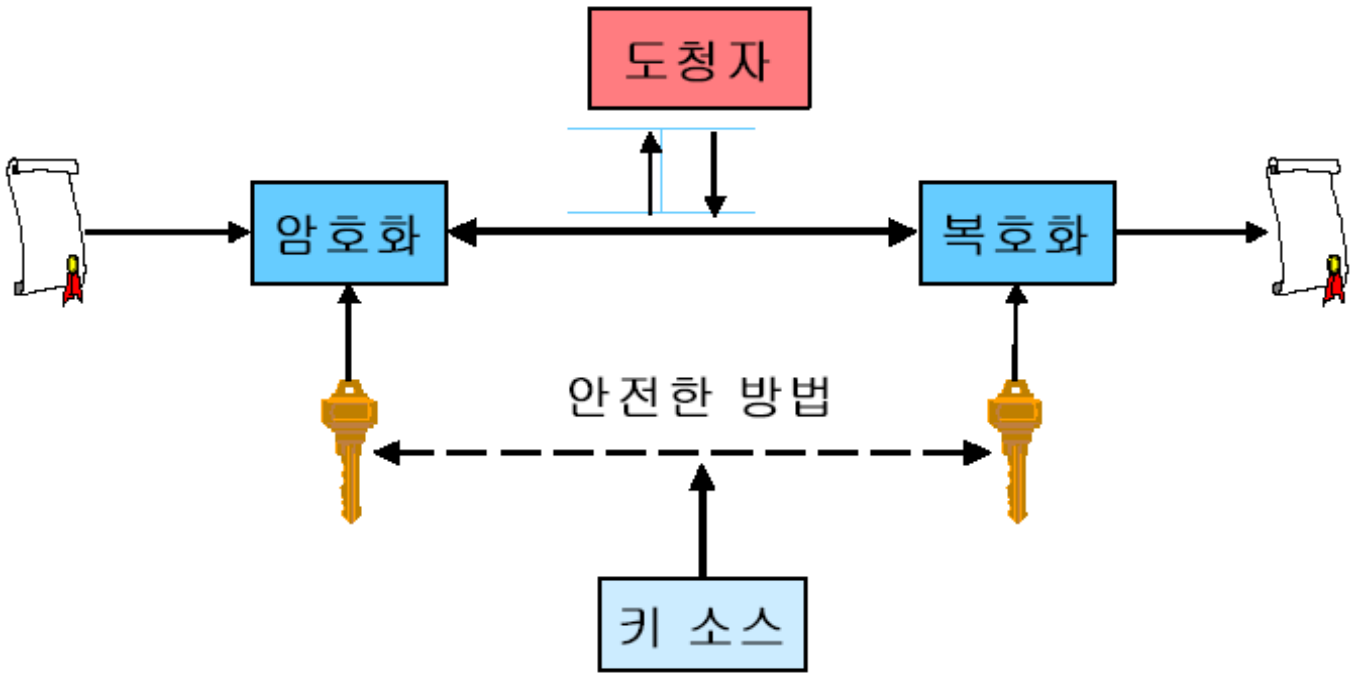
- RSA

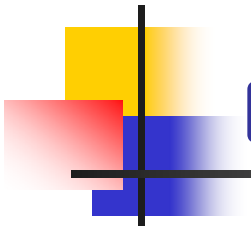
3. 해쉬 알고리즘

- SHA

대칭키 암호시스템

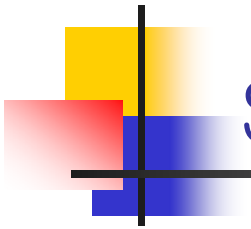
개요: 암호화와 복호화에 사용되는 키가 동일.





DES(Data Encryption Standard)

- 75년 IBM에서 만든 후 77년 NIST(National Institute of Standards and Technology)에서 표준으로 채택.
- 56비트 키를 사용하며 64비트 단위로 메시지를 암호화.
- 전체 16라운드의 Feistel 구조.
- 99년 전수 조사에 의해 깨어짐.



SEED

- 한국정보보호진흥원(KISA)에서 주관하여 개발.

- 전체 16라운드의 Feistel 구조

- 128비트 키를 사용하며 128비트 단위로 메시지를 암호화.

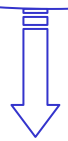
공개키 암호시스템

-공개키 암호의 개념은 1976년 Diffie와 Hellman의해 처음 제시.

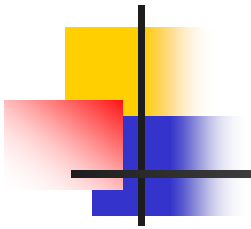
-송신자는 메시지를 공개키로 암호화하여 수신자에게 보내면

수신자는 자기만이 알고 있는 개인키로 복호화 함.

-일방향성 함수 사용.



x가 주어지면 y=f(x)의 계산이 용이한 반면, y가 주어졌을 때 x를 구하기 위한 f(x)의 역함수를 구하는 것이 불가능한 함수



RSA

- 1978년에 Rivest, Shamir, Adleman이 제안한 대표적 공개키 암호시스템.
- 큰 합성수의 소인수 분해가 어렵다는데 근거.

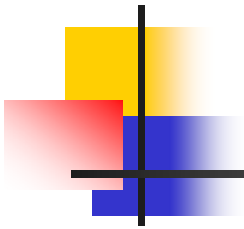
해쉬 알고리즘

- 정의

  -임의의 길이의 비트 열을 고정된 길이의 출력값인 해쉬코드로 압축시키는 알고리즘

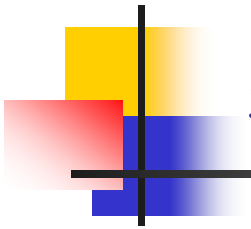
  -데이타의 무결성 검증, 인증 에 사용.

  종류: SHA ,HAS-160, MD5, RMD160, TIGER ....등.



SHA(Secure Hash Algorithm)

- 디지탈 서명 표준인 DSA를 위해 개발된 해쉬함수.
- 1995년 4월에 정식 표준으로 승인(FIPS PUB 180-1).
- 출력: 160비트



참고문헌

- DES, TDES,SHA : http://csrc.nist.gov/publications/fips/index.html
- SEED :http://www.kisa.or.kr
- RSA: http://www.rsasecurity.com