암호학 개론

컴퓨터공학부 김상원

유튜브 주소 : https://youtu.be/HrfjFYwbScw

암호기술과 용어

평문의 암·복호화 과정

암호화의 분류

대칭키와 공개키

암호기술이란

암호기술은 중요한 정보를 읽기 어려운 값으로 변환하여 **제 3자가 볼 수 없도록 하는 기술**이다.
암호기술의 안전성은 수학적인 원리에 기반하며, 보안에 있어서 중요한 정보를 직접적으로 보호하는 **원천기술**이다.
암호기술을 통해 보호하고자 하는 원본 데이터를 **평문(plaintext)**라고 하며, 평문에 암호기술을 적용한 것을 **암호문(ciphertext)**라고 한다. 이렇게, 평문에 암호기술을 적용하여 암호문으로 변환하는 과정을 **암호화**라고 하며, 다시 평문으로 복원하는 과정을 **복호화**라고 한다. 암호화하기 위해서는 **암호 키(key)**가 필요하며, 키가 있어야만 암호문을 복호화할 수 있습니다. 그렇게 때문에 암호 키는 비밀(secret)로 유지되어야 하며 제3자가 알 수 없어야 한다.

암호기술을 이용하여 데이터 기밀성, 데이터 무결성, 인증 및 부인 방지 등의 기능을 제공할 수 있다.

암호학 용어

평문(planetext)

- 비밀 유지를 요구하는 통신문

암호문(ciphertext)

- 평문을 일정한 기호 또는 수로 변경한 문서

복호화(decryption)

- 암호문을 평문으로 복원하는 행위

열쇠(key)

- 평문을 암호문으로 또는 암호문을 평문으로 전환시키는 도구로 전자(평문->암호문)를 암호화 열쇠(encryption key), 후자(암호문->평문)를 복호화 열쇠(decryption key)라고 한다.

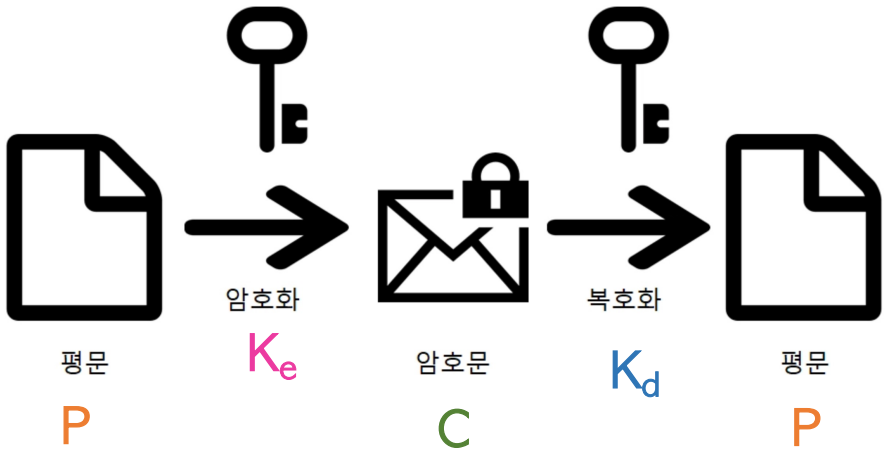
암호기법(cryptography)

-평문을 암호화해서 공격자가 암호문을 해독하기 어렵게 하는 방법

암호해독(cryptanalysis)

- 한정된 자료를 가지고 암호문으로부터 평문과 열쇠를 탐지하는 것

평문의 암·복호화 과정



다음 그림에서 **P**는 **평문**, **C**는 **암호문**을, K_e는 **암호화 열쇠**, K_d는 **복호화 열쇠**이다.

송신자는 먼저 전송할 **평문**을 적당한 유한수열 $a_1, a_2, \cdots, a_k$ 로 나타내고, **평문**을 **암호문**으로 전환시키는 암호화

알고리즘으로서 **암호화 열쇠** K_e에 의해 결정되는 암호화함수 $E_{Ke} : A \rightarrow A$를 이용한다. 즉 $\mathbf{C = E_{Ke}(P)}$.

암호문을 받은 수신자는 **암호문**을 **평문**으로 복원하기 위한 복호화 알고리즘으로서 **복호화 열쇠** K_d에 따라 결정되는

복호함수 $D_{Kd} : A \rightarrow A$를 사용해 **암호문**을 본래의 **평문**으로 복원한다. 즉 $\mathbf{P = D_{Kd}(C)}$.

이때 암호화 함수 E_{Ke}와 복호화 함수 D_{Kd}는 일대일 대응이고,

$$\mathbf{P = D_{Kd}(C) = D_{Kd}(E_{Ke}(P)) = D_{Kd} \cdot E_{Ke}(P)}$$

이므로 $\mathbf{D_{Kd} = E_{Ke}^{-1}}$, 즉 암호화 함수와 복호화 함수는 서로 **역함수 관계**에 있다.

암호화의 분류

암호화는 **평문**을 암호화하는 방법에 따라

비밀 키 암호체계(secret-key cryptosystem), **공개 키 암호체계(public-key cryptosystem)**로 나눈다.

비밀 키 암호체계에서는 **암호화 열쇠 K_e**와 **복호화 열쇠 K_d** 가 동일하고, 이 두 열쇠는 송신자와 수신자에게만 알려진 비밀 열쇠이므로 **대칭 암호체계(symmetric cipher system)**라고 한다.

공개 키 암호체계에서는 **암호화 열쇠 K_e**와 **복호화 열쇠 K_d** 는 서로 다르고, **암호화 열쇠**는 공개하나 **복호화 열쇠**는 비밀로 하므로 **비대칭 암호체계(asymmetric cipher system)**라고 한다.

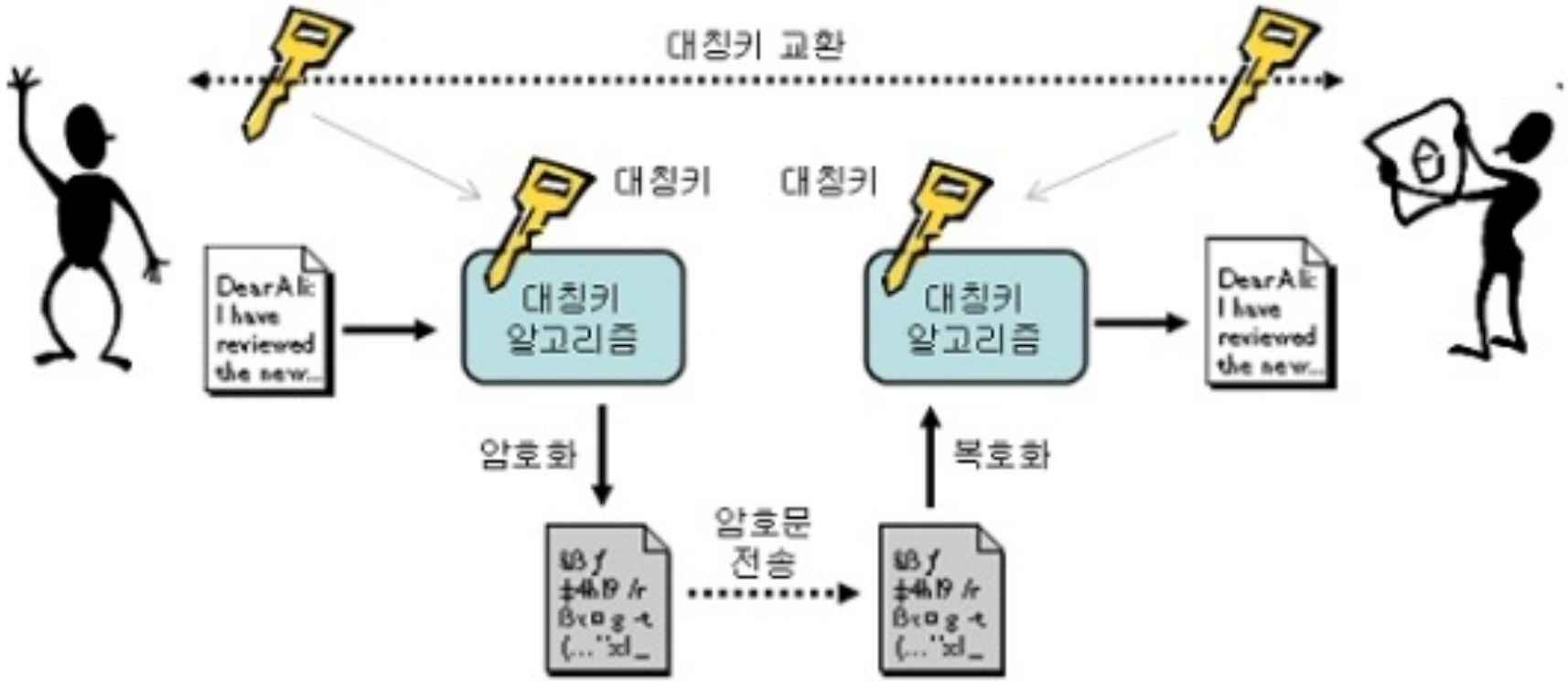
대칭 키 암호(symmetric-key algorithm)

정의

- 암호화 알고리즘의 한 종류로, 암호화와 복호화에 같은 암호 키를 쓰는 알고리즘을 의미한다.

종류

- 스트림 암호
- 블록 암호



대칭키 암호 방식

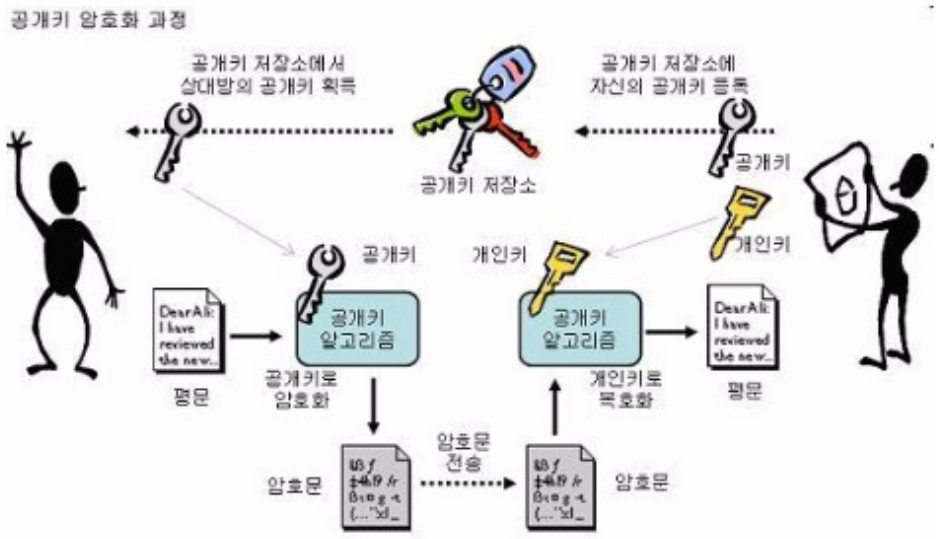
공개 키 암호(public-key cryptography)

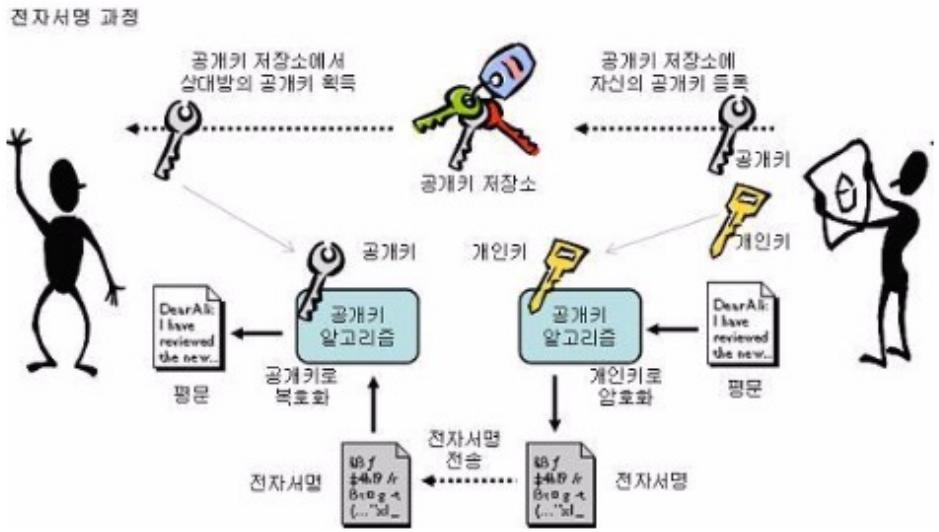
정의

- 암호 방식의 한 종류로 비밀 키 암호 방식과 달리 암호화와 복호화에 이용하는 키가 다른 방식을 말한다.

종류

- RSA(Rivest, Shamir and Adleman)
- ElGamal
- ECC
- 전자서명





Q & A